CYBER SECURITY: CHALLENGES AHEAD

Muhammad Adeel Javaid
Member Vendor Advisory Council, CompTIA

Abstract:

Cyber threats are fundamentally different from any other because they usually do not involve any kinetic, or in other words physical, effects or actions. Yet they nonetheless have a huge potential for damage because digital and networked enabled elements permeate our governments, infrastructure, businesses and even private lives.

Such threats are fundamentally borderless and global in nature. They can originate from absolutely any place in the world and target virtually any other place. In addition some attacks may originate in one country, use a botnet (a group of voluntarily or involuntarily remotely controlled computers, used to increase the effect of some types of cyber attacks) of computers in another (or even several other) country and target a server or website in a third. Thus effective solutions for such global threats have to in turn also be truly global.

Threats:

There has been confusion on the criteria used to determine the definition of the term Cyber Threats or computer crimes. Some argued that, it is any crime that involves the use of computer; some argued that, it is a crime in the presence of a computer.

However, some have criticized the categorization of cyber crime. Don Gotternbarn argued that, there is nothing special on the crimes that happen to involve computers. Is it possible for a crime being categorized in accordance to a tool, equipment, mechanism or means through which it was committed? If that's so, how many categories of crime would be there? How about the crime committed through using a television, automobiles, scalpel, scissors, and other tools, can we categorize each of them as individual crimes? Gotternbarn concludes that crimes involving computers are not necessarily issues in computer ethics.

For a start it might be helpful to split cyber threats into two very broad categories, namely cyber warfare and cybercrime. Cyber warfare is malicious cyber activity directly threatening the security, defense capabilities, vital infrastructure or societies of a particular state or region. An act of cyber warfare can include espionage (acquisition of sensitive information), disruption or destruction of critical infrastructure (such as communications), manipulation of defense or other vital systems. These attacks are generally taken to be perpetrated by states, terrorist or other militant organizations or by proxies acting on behalf of the aforementioned. Cybercrime (often referred to as computer crime in legal matters) on the other hand refers to criminal act perpetrated using computers and their networks. Cybercrimes often can include personal information theft by various means in order to use it to gain access to bank accounts. Other examples might include corporate espionage through cyber means. Yet not all cybercrimes are committed for financial gain. Hacktivism and so called recreation hacking are great examples of this. The former is done for political values, ideals (such as freedom, self determination, etc.) or on the behalf of particular causes and latter is done for the “lulz” (basically for fun or for recognition amongst peers, namely others in the hacker community).

Secondly it might be useful to identify some of the most prominent methods used to commit various cyber attacks. One of the most pervasive ones and probably one of the easiest to commit is called a denial of service attack (DoS) or more commonly a distributed denial of service attack (DDoS). These attacks are very common because of their relative ease of execution and significant impact upon the target. To put it simply perpetrators of these attacks often use computer programs called network stress tools, such as the Low Orbit Ion Cannon (LOIC) to target a particular website or network. These stress tools work by bombarding the target with very large numbers of requests, therefore overloading servers, consuming all the bandwidth and at least temporarily making the network or webpage inaccessible (DoS Attacks - CERT). DDoS attacks use the exact same principle but on a larger scale by enlisting multiple computers in a botnet (voluntarily or not) to amplify the effect of the attack. Network stress tools like LOIC can be easily downloaded on the internet and used by anyone with even minimal computer knowledge because they do not require any programming or coding skill. For these reasons DDoS attacks are very popular with hacktivists such as Anonymous, though they are also frequently used by other actors.

However the most popular method of committing cyber attacks is by way of malware which is catch all term that describes all malicious software or pieces of code. In fact malware attacks account for as much as 67.1 per cent of all committed cybercrimes according to recent surveys (CSI Comp Crime Survey 2010/2011). Malware probably most notably includes attacks with computer viruses or worms. These are types of malicious self replicating programs that infect computers and spread through networks and the internet. Worms specifically are a subset of computer viruses that spread by making copies of themselves in every infected computer or system. Viruses in general can be programmed to perform many different actions, from just spreading and replicating oneself, to deleting or altering programs in target computers, granting remote access to third parties to an infected computers, stealing or spreading data from computers or servers and performing other pre programmed actions. Thus their effects can range from the relatively benign to the very dire (Moir 2003).

While there are other means of committing various cyber attacks, they are all based on the same principles of exploiting vulnerabilities and finding system loopholes to achieve desired effects. Those effects can be anything from, disruption or destruction of information, to control or access of a system. Moreover in recent years there have been many different well publicized cyber attacks committed using various different methods, targeting a lot of different entities and ranging in scale and severity.

Many well publicized denial of service attacks were perpetrated during the Arab Spring uprisings by the hacktivist collective and internet grouping called ‘Anonymous’. One of the first of these was the so dubbed *“Operation Tunisia”* by the Anonymous collective, targeting several websites of the Tunisian government during the mass protests that took place in the country in the beginning of January 2011. The websites taken down by the DoS attacks included those of the ministry of foreign affairs, the stock exchange, the ministry of industry, the president and the prime minister (Hill 2011). While these attacks were considered by many to be commendable and positive, they nonetheless were at least formally criminal acts. Yet cyber attacks can be a lot more severe than just the disruption of websites which is usually simply a basic tactic employed by hacktivists.

This brings us to an example of probably the most famous cyber worm attack in recent times, namely that of the worm known as ‘Stuxnet’ that primarily affected the Natanz nuclear facility in Iran in June 2010. The worm had been called the most sophisticated cyber weapon to date and is credited by some with temporarily paralyzing the Iranian nuclear program; though the Iranian government has repeatedly denied that it caused any severe damage or disruption. Therefore it is hard to know the true scale of the impact of the attack. What is known is that the worm works by infiltrating and gaining remote control of the target system in turn reprogramming it. Stuxnet in particular target centrifuges used in uranium enrichment by changing the frequency of the electric current to them, thus disrupting their normal operation and potentially sabotaging the enrichment process. While the source of the Stuxnet worm is unknown, it was referred to by some as a military grade cyber weapon, which has lead to speculation that it has been created by some state trying to interfere with Iran’s nuclear program (Farwell 2011). Yet whatever its origin the Stuxnet attacked proved that cyber weapons can potentially cause not only damage in cyberspace, but can be used to manipulate processes that transfer in to kinetic effects, possibly inflicting physical, real world damage.

There have also been many prominent attacks that targeted corporations and other private entities. A good example of this is an intrusion in June 2011 by unidentified hackers into Citigroup (one of the largest financial services companies in the world) servers saw the mass theft of the credit card as well as other personal information of more than 200,000 of their customers (Kravets 2011). Another good example are the attacks that occurred in May 2011 on the US defense and aerospace company Lockheed Martin, which produces several fighter jets such as F-16 and F-22 for the US armed forces. While official reports suggested that the damage from the attacks was minimal and quickly responded to, it is reported that restoration of normal employee access to its systems took at least several days following the incident (BBC News 2011).

Besides the above stated specific examples of various cyber incidents it is also important in understanding the effect of global cyber threats on all types of global actors to take a look at broader trends and statistics to do with cyber threats to really get a clearer picture of the gargantuan scope of the problem.

For example a recent report on cyber threats in the United States provided a shocking insight into the exponential growth of these incidents every year. The report stated that cyber security incidents in US federal agencies have increased by a staggering 680 per cent over a period of six years. This huge rise in attacks is said to be especially due to the increased activity of hacktivists and state sponsored actors (Freedberg 2012). Furthermore a report done by Symantec has valued global losses due to cybercrime in 2011 at 388 billion USD with 441 million people worldwide being affected by them. As the report points out, cybercrime globally costs the world a much greater amount than the global illicit trade in marijuana, cocaine and heroin combined, which is valued annually at 288 billion USD (Norton Cybercrime Report 2011).

Additionally in 2010 the *"Second Annual Cost of Cyber Crime Study"* done by the Ponemon Institute based on a representative sample of 50 sizable companies from different industry sectors in the United States revealed that the costs incurred from cybercrime for them ranged from 1.5 million up to 36 million USD per annum, with the median cost being incurred standing at 5.9 million USD. These loses represented a staggering 56 per cent increase from the results of the same study conducted the year before. The study noted that the 50 organizations in the sample sustained about 72 successful cyber attacks per week, averaging out at more than one per week per company. This also showed an increase from the 2010 study by 44 per cent. Moreover it was also found that some of the most costly attacks for these companies were actually basic denial of service attacks that severely disrupted business (Ponemon Institute 2011).

Thus it is not difficult to see that cyber threats have severe security and financial implications to the public and private spheres. Due to the global nature and prevalence of information systems with network enabled capabilities cyber threats do not leave any state, business or private individual safe from their adverse effects. In addition cyber attacks are no longer rare occurrences, but very common, pervasive and at times extraordinarily damaging events. Furthermore, precisely the global nature of these threats once again leads to the inevitable conclusion that any significant solution to them has to be global as well. Yet despite the nearly universally harmful nature of cyber threats there has not been a comprehensive global response.

Threat Identification

This threat identification resource has been developed to assist system owners and developers. This resource presents a broad view of the risk environment. The threats presented below were selected based on their occurrence and significance.

Categories: The threat resource is categorized into four main groups: environmental/physical threats, human threats, natural threats, and technical threats. The categories list is not exhaustive. It was developed as a guide to spur identification of threats and vulnerabilities. As conditions and technology change, other categories not included here could apply to the system under review.

Threats: Within each section the threats are identified and described. The threat list is not exhaustive. Other threats not included here could apply to the system under review. For this reason, an entry for other threats has been included in each section. The effects of threats vary considerably from confidentiality and integrity of data to the availability of a system. Therefore, System Impact is identified within the threat column for each described threat.

Examples: To further assist those consulting this resource, examples of each type of threat have been provided. The examples are not all inclusive. They provide guidance. Other conditions requiring consideration may be present for the system under consideration. If they exist, these conditions should be addressed by system owners and developers.

Human Threats

	Threats	Descriptions	Examples
	1. Arson *Primarily affects system availability.*	Arson is the willful and generally malicious burning or starting of fires.	• Malicious fires caused by bombs and incendiary devices could result in damage or destruction of system hardware and loss of data. • The malicious intent could be the cause of a fire resulting from a contact of steel wool cleaning material and metal or wiring.
	2. Data Entry Errors or Omissions *Could significantly impact data integrity, and to a lesser extent data availability.*	Data entry errors and omissions are mistakes in keying or oversight to key data, which could affect system resources and the safeguards that are protecting other system resources.	• Failure to disable or delete unnecessary accounts, such as guest accounts and employees that no longer need access to system resources could result in unauthorized access to sensitive data. • Entering incorrect values for sensitive information such as SSN, financial data or personally identifiable data could result in data inconsistency. • Innocent data entry errors could result in inconsistency in spellings, which could make accurate reporting, or standard searches impossible.
	3. Espionage *Significantly impacts data confidentiality, but combined with other threats could impact data integrity and availability.*	Espionage is the covert act of spying through copying, reproducing, recording, photographing, interception, etc., to obtain information.	• Espionage could be conducted by foreign governments through technical means, such as electronic bugs and wire taps. • Foreign government could recruit an agent inside the target agency by either bribing or blackmailing an employee. • Companies could encourage employees to take positions in CMS to provide those companies with a constant supply of information. • Legitimate business agreements, such as licensing and on-site liaison officers or contractors could be used to provide unauthorized

			opportunities to gather information.
	4. Impersonation *Could significantly impact data confidentiality, and to a lesser extent data integrity and availability.*	Impersonations are threats that often become enablers for other threats. Impersonation for physical access could include misuse of badges, key cards, personal Identification numbers (PIN), etc. Impersonation for electronic or system access could include use of others' identification and authentication information in an attempt to gain system privileges and access to system resources.	• Sharing of badges, key cards, and PINs could provide an employee or cardholder with unauthorized access to sensitive information. • Forged documents could form the basis for data entry, modification, or deletion. • Social engineering such as tricking employees into revealing passwords or other information can compromise a target system's security.
	5. Improper Disposal of Sensitive Media *Primarily affects confidentiality, but in combination with other threats could impact integrity and availability.*	Improper Disposal of Sensitive Media is the discarding of information improperly which could result in compromise of sensitive information.	• Searching for residual data left in a computer, computer tapes, and disks after job execution could compromise that data. • Disposing of previously owned client PCs that contain sensitive and unclassified information could reveal sensitive data. • Readable data can be retrieved from hard copies, wastepaper baskets, magnetic tapes, or discarded files resulting in compromise of that data.
	6. Inadvertent Acts or Carelessness *Could significantly impact data confidentiality, integrity, and availability.*	Inadvertent acts or carelessness are unintentional acts that could cause system performance degradation or system loss.	• Programming and development errors result in software vulnerabilities. Successful compromise could lead to loss of data confidentiality, integrity, and availability. • Incorrect operations of database synchronization procedures could result in data errors, including entry, deletion, and corruption errors. • Improper upgrades to database management software could result in vulnerabilities that could impact data confidentiality, integrity, and availability. • Programming and development errors could cause a buffer overflow. This leaves the system exposed to security vulnerabilities.

			• Installation, upgrade and maintenance errors could leave data unprotected or overly exposed to security vulnerabilities. • Failure to disable or delete unnecessary accounts (network, Internet, and voice), such as guest accounts, and terminated employees could result in unauthorized access to sensitive data. • Failure to recover terminated employees' card keys and door keys could provide unauthorized access to system and data.
	7. Labor Unrest *Primarily affects the availability of the system. Could also affect confidentiality and integrity.*	Labor unrest is activities organized by employees designed to halt or disrupt normal operations such as strike, walkout, and protest job action.	• The unavailability of key personnel resources could disrupt normal operations. • Employee refusals to carry out work-related instructions or tasks could pose a threat to information security if they refuse to close vulnerability.
	8. Omissions *Primarily affects the confidentiality, integrity and availability of the system.*	Omissions are nonmalicious threats that could affect system resources and the safeguards that are protecting other system resources.	• Failure to disable or delete unnecessary accounts (network, Internet, and voice), such as guest accounts and employees that no longer need access could provide unauthorized access to system resources. • Failure to recover terminated employees' card keys and door keys could provide unauthorized access. • If the system administrator fails to perform some function essential to security, it could place a system and its data at risk of compromise.
	9. Procedural Violation *Primarily affects availability of the system.*	Procedural violation is the act of not following standard instructions or procedures, which could be either intentional or unintentional.	• Refusal to carry out work related instructions or tasks, such as the refusal to remove a User ID and logon access of an employee terminated for cause could place a system and data at risk of compromise. • Unintentional failure to carry out work-elated instructions or tasks, such as the failure to test a backup tape to determine whether or not the

			backup was successful could place data at risk of loss.
	10. Riot/Civil Disorder *Primarily affects the availability of the system.*	Riot/civil is a violent disturbance created by and involving a large number of people, often for a common purpose or over a significant event.	• The unavailability of key personnel resources could affect system availability. • The refusal to carry out work-related instructions or tasks could affect data availability. • Employees might not be able to reach the workplace to ensure data protection.
	11. Scavenging *Primarily affects confidentiality.*	Scavenging is the searching through object residue to acquire sensitive data.	• Searching for residual data left in a computer, computer tapes, and disks after job execution could compromise that data. • Examining discarded or stolen media could reveal sensitive data.
	12. Shoulder Surfing *Primarily impacts data confidentiality, but in combination with other threats could impact integrity and availability.*	Shoulder Surfing is the deliberate attempt to gain knowledge of protected information from observation. The unauthorized disclosure of protected information leads to information misuse (identity theft), or such information could be used to gain additional access or information.	• Housekeeping staff could observe the entry of sensitive information. • Failure to protect a UserID and Password from observation by others during logon could allow unauthorized users to capture sensitive information. • Visitors could capture employee's passwords and other sensitive information left unprotected on desktops. • Allowing remote dial-up access to networks or systems from off-site locations could disclose an agency's dial-up access phone number, user account, password, or log-on procedures. • Personal standalone workstations could be unprotected.
	13. Terrorism *Primarily affects confidentiality, integrity and availability.*	Terrorism is a deliberate and violent act taken by an individual or group whose motives go beyond the act of sabotage, generally toward some extreme political or social sentiment.	Terrorism is a constant danger as illustrated by the following attacks: • September 11, 2001 attacks. • Bomb threats/attempts e.g. 1998 Embassy bombings, 1993 World Trade Center Bombing. • Biological attack e.g. post September 11, 2001 anthrax attack. • Cyber terrorism or information warfare. For example, Hackers broke into the U.S. Justice

			Department's web site and replaced the department's seal with a swastika, redubbed the agency the "United States Department of Injustice" and filled the page with obscene pictures. Also, in December 2001, computer hackers tapped into WebCom, one of the nation's largest worldwide web service providers on the Internet, and removed more than 3,000 sites for 40 hours, many of them retailers trying to capitalize on the Christmas rush.
	14. Theft, Sabotage, Vandalism, or Physical Intrusions *Could significantly impact data integrity and availability, and to a lesser extent data confidentiality.*	Theft, sabotage, vandalism, or physical intrusions are deliberate malicious acts that could cause damage, destruction, or loss of system assets. Such an act could also enable other threats, such as compromise of interconnected systems.	• Disgruntled employees could create both mischief and sabotage of system data. • Deletion or corruption of data could occur through acts of vandalism. • Logic bombs could destroy system data at a given time or under certain circumstances. • Sensitive data could be captured through application vulnerabilities, and held hostage. • Cleaning staffs/vendors could have access to sensitive information. • Disgruntled employees could sabotage a computer system by installation of software that could damage the system or the data. • Destruction of hardware or facilities could destroy data that might not be recovered. • Computer abuse such as intentional and improper use, alteration and disruption could result in loss of system assets. • Cleaning staffs/vendors or contractors could steal unsecured sensitive information.
	15. User Abuse or Fraud *Could significantly impact data confidentiality,*	User abuse or Fraud addresses authorized users who abuse their assigned access privileges or rights to gain additional information or privileges.	• Users could browse systems and applications in search of specific data or characteristics. • Use of information (password) as an indirect aid for subsequent

	integrity, and availability.		misuse, including unauthorized access could compromise data security. • Information (Social Security numbers) could be used as a direct aid for illegal purposes, including identity theft. • A user could engage in excessive use of an Information System asset for personal means (e.g., games, resumes, personal matters). • The opening of an unprotected port on a firewall could provide unauthorized access to information.
	16. Other Threats… (To be specified by system owner or developer.)		

Technical Threats			
	Threats	Descriptions	Examples
	1. Compromising Emanations *Primarily affects confidentiality.*	Compromising emanations are the unintentional data-related or intelligence-bearing signals, which, if intercepted and analyzed, could disclose sensitive information being transmitted and/or processed.	• Radiation or signals that emanate from a communications circuit could disclose to unauthorized persons or equipment the sensitive or proprietary information that is being transmitted via the circuit. • Use of an inductive amplifier on unprotected cable could reveal unencrypted data and passwords.
	2. Corruption by System, System Errors, or Failures *Could impact confidentiality, integrity, and availability of the system.*	Corruption by System, System Errors, or Failures addresses corruption of a system by another system, system errors that corrupt data, or system failures that affect system operation.	• Failure of system software/hardware could result in database failures leading to financial loss. • Failure of application software could prevent users of these applications from performing some or all of the tasks assigned to them unless these tasks could be carried out manually. • Flawed designs, such as newly discovered vulnerabilities not addressed by requirements could place system at risk of compromise. • Faulty implementation, such as inconsistency with design or new bugs not covered by specifications could allow compromise of data and application.
	3. Data/System Contamination *Could significantly impact data confidentiality, and to a lesser extent data integrity and availability.*	Data/system contamination is the intermixing of data of different sensitivity levels, which could lead to an accidental or intentional violation of data integrity.	• Data values that stray from their field descriptions and business rules could be revealed to unauthorized person. • Anomalies and multiple account numbers for the same entity could allow unauthorized access to data. • Corrupted system files could contain strings of sensitive information. • File fragments containing sensitive information could be scattered

			throughout a drive instead of in an encrypted sector to protect them from compromise. • Cross-site scripting attacks (CSS) could be launched by inserting malicious tagging as an input into dynamically generated web pages. Malicious tagging could enable an attacker to accomplish compromise of data integrity, set and read cookies, intercept user input and execute malicious scripts by the client in the context of the trusted source. For example, Citibank closed a CSS vulnerability identified by De Vitry at the bank's C2IT.com Internet payment site that enabled attackers to grab users' credit card and bank account information.
	4. Eavesdropping *Could significantly impact data confidentiality, but combined with other threats could impact data integrity and availability as well.*	Eavesdropping is the deliberate attempt to gain knowledge of protected information. The unauthorized disclosure of protected information leads to information misuse (identity theft), or such information could be used to gain additional access or information.	• Eavesdropping devices, such as Electronic Bugs, could be used to intercept sensitive, unencrypted data. For example, keystroke monitoring could transmit every keystroke so that all user input could be reproduced. • Trojan Horse applications could surreptitiously capture user or system activities. • Use of an inductive amplifier on unprotected cable could permit unauthorized intercept of transmission. These transmissions could include sensitive information, such as passwords, in the clear. • Use of a Packet Sniffers could permit unauthorized intercept of transmission. These transmissions could include sensitive information, such as passwords over networks (e.g., in telnet or ftp). • Electromagnetic radiation from standard computers could be used to reconstruct the contents of the computer screen. These signals could carry a distance of several hundred feet, and even further when

			exposed cables or telephone lines function as unintended antennas. • Attackers could use offshore hackers to break into Federal computer systems and steal protected information. The fact that the attack could come from outside the United States increases the difficulty of protection.
	5. Hardware / Equipment Failure *Primarily affects the integrity and availability of the system.*	Hardware / Equipment Failure is the unexpected loss of operational functionality of any system hardware asset.	• Malfunction or failure of Central Processing Unit (CPU) or other hardware could result in the loss of system data. • Faulty network components such as hosts, routers and firewalls could result in interruption of communications between the connected stations. • Improper hardware maintenance could allow a system crash to occur. • Internal power disturbances could result in loss of system data. • Self-generated or other internal interference could damage data or interrupt system function.
	6. Impersonation *Could impact confidentiality, integrity and availability.*	Impersonations are threats that often become enablers for other threats. Impersonation for physical access could include misuse of badges, key cards, personal Identification numbers (PIN), etc. Impersonation for electronic or system access could include use of others' identification and authentication information in an attempt to gain system privileges and access to system resources.	• Sharing of badges, key cards, and passwords could provide unauthorized access to sensitive information. • Masquerading, such as impersonation: false identity external to computer systems or playback and spoofing attacks could result in unauthorized access to sensitive data. • Social engineering, such as tricking employees into revealing passwords or other information could compromise a target system's security. • Forged email messages could reveal sensitive information.
	7. Insertion of Malicious Code or Software; or Unauthorized Modification of a	Insertion of Malicious Code or Software; or Unauthorized Modification of a Database is the malicious intent to change a system's configuration	• Modification, insertion, or deletion of data or lines of code could compromise data and/or system. • Unauthorized modification of database records could compromise

	Database. *Could significantly impact data confidentiality, integrity, and availability.*	without authorization by the addition or modification of code, software, database records, or information. The intent and impact could range from subtle annoyances and inconveniences to catastrophic failures and outages.	data integrity and availability. • Trojan Horse applications could be installed through code and software modifications. Some examples are SubSeven Trojan, NetBus, BackOrifice, NetCat and Deep Throat • Logic bombs could be placed within authorized software and perform malicious system actions on a given trigger event. • Trap door functions could be inserted into authorized code and software. • Improper database entries and updates could be executed.
	8. Installation Errors *Could impact confidentiality, integrity and availability of the system.*	Installation errors are the errors, which could occur as a of result poor installation procedures. Installation errors, whether hardware or software, could undermine security controls.	• Poor installation procedures could leave data unprotected, e.g. built-in security features of software packages are not implemented. • Failure to educate and prepare for installation and uninstallation methods could leave data unprotected. • Incorrect installation or a conflict with another device that is competing for the same resources within the computer system could impact system data and resource availability. • Installation of programs designed by users for personal computers could modify the system initialization scripts and change the configuration of a system allowing unauthorized access to sensitive data. • Installation of patches and hot fixes could modify the system initialization scripts and change the configuration of a system. This could reset security settings and place data at risk of compromise.
	9. Intrusion or Unauthorized Access to System Resources *Depending on the level*	Intrusion or Unauthorized Access to System Resources is gaining unauthorized access to system resources. The intent	• Trojan Horses perform malicious system actions in a hidden manner, including file modification, deletion, copying, or the installation of system

	of intrusion and the safeguards, the intrusion or unauthorized access to system resources could impact confidentiality, integrity, and availability.	could be malicious or nonmalicious (e.g., curiosity seeker) in nature.	backdoors. Some examples are SubSeven Trojan, NetBus, BackOrifice, and Deep Throat. • Trap Door (back door) attacks could result in improper identification and authentication, improper initialization or allocation, improper runtime validation or improper encapsulation. • Network worms, e.g. Code Red worm, W32/Leaves worm, and power worm could damage the system and associated data. • Authorization attacks, such as Password cracking or Token hacking could result in unauthorized access and system/data compromise. • Hotmail vulnerability– Microsoft was informed on August 29, 1999, of a weakness that allowed anyone to read the inbox of any Hotmail user, provided the username was known. • In February 1998, hackers launched an attack against the Pentagon and MIT. In the attack against MIT, hackers were able to collect user names and passwords to computers outside the network through the use of a packet sniffer. Details on the attack against the Pentagon were not made available.
	10. Jamming (Telecommunications) *Primarily affects the availability of the system.*	Jamming is the deliberate radiation, reradiation, or reflection of electromagnetic energy, which could cause communications degradation, or total loss of the system.	• Jamming the radio frequency could produce electrical interference that prevents system operation.
	11. Misrepresentation of Identity *Could significantly impact data confidentiality, and to a lesser extent data integrity and availability.*	Misrepresentations of identity are threats that often become enablers for other threats. Misrepresentation for electronic or system access could include use of others' identification and authentication information in an attempt to gain privileges	• Abuse of privileges such as misuse of USERIDs and passwords could be used to gain unauthorized access to sensitive data. • Personal profile extraction could allow an unauthorized person to assume an otherwise authorized role. • Forged documents and messages could form the basis for costly

		into system resources.	business decisions. • Social engineering, such as tricking employees into revealing passwords or other information that provides access to an application could compromise data security.
	12. Misuse of Known Software Weaknesses *Could impact confidentiality, integrity and availability.*	Misuse of Known Software Weaknesses is the deliberate act of bypassing security controls for the purpose of gaining additional information or privileges. This weakness could be at the operating system, application or access control levels of a system.	• User IDs, especially root/administrator with no passwords or weak passwords for all systems could allow unauthorized access to the application and its data. • Remote Procedure Call (RPC) weaknesses in rpc.ttdbserverd (ToolTalk), rpc.cmsd (Calendar Manager), and rpc.statd could allow root compromise. This affects multiple Unix and Linux systems. • IMAP and POP buffer overflow vulnerabilities or incorrect configuration could allow compromise of data and application. • Sendmail buffer overflow weakness, pipe attacks and MIMEbo could allow compromise at the root level. • Global file sharing and inappropriate information sharing via NFS and Windows NT ports 135-139 (445 in windows 2000) or UNIX NFS exports on port 2049 as well as Appletalk over IP with Macintosh file sharing enabled, could result in data compromise. • The RDS security hole in the Microsoft Internet Information Server (IIS) could allow an attack to damage or destroy the application and its data.
	13. Saturation of Communications or Resources *Could impact integrity and availability***.**	Saturation of communications or system resources is the condition in which a component of a system has reached its maximum traffic handling capacity. Saturation of communications or system resources is a threat that creates an unstable	• Denial of Service (DOS) and Distributed Denial of Service (DDOS) attacks, such as network saturation attacks and bandwidth consumption attacks could result in system/data unavailability. • Sendmail buffer overflow weakness, pipe attacks and MIMEbo could allow compromise at the root

		environment, which could degrade communications capabilities and/or consume processor time (e.g., flooding the buffer).	level.
	14. System and Application Errors, Failures, and Intrusions not Properly Audited and Logged *Could significantly impact data integrity and availability.*	Auditing and logging of system and application errors enable administrators to troubleshoot and safeguard performance issues, and reconstruct events of unauthorized access. The lack of sufficient auditing and logging of System and Application Errors, Failures, and Intrusions reduces these capabilities.	• Auditing and logging settings not properly configured at the system and application level could prevent tracking of malicious acts. • Intruders could gain unauthorized system access and abort auditing processes. • If Audit logs reach their maximum threshold they could remove logged data, or stop logging new data.
	15. Takeover of Authorized Session *Could significantly impact data confidentiality, and to a lesser extent data integrity and availability.*	Takeover of Authorized Session is gaining control of an authorized session, and assuming the access rights of the authorized party. This session could be used for further unauthorized access.	• Network sessions could be compromised through session hijacking techniques. • When a user leaves the immediate work area and a session remains open, unauthorized use could occur. • Database communications could be captured, modified, and sent to the original destination.
	16. Tampering *Primarily affects the integrity and availability of the system.*	Tampering is an unauthorized modification that alters the proper functioning of equipment in a manner that degrades the security functionality the asset provides.	• Web hacks could deface a web site, or disable the web server functionality. • Domain Name Service hacks could prevent authorized users from properly accessing network or Internet resources.
	17. Other Threats… (To be specified by system owner or developer)		

Environmental / Physical Threats

	Threats	Descriptions	Examples
	1. Electromagnetic Interference (EMI) *Primarily affects the integrity and availability of the system.*	Electromagnetic Interference (EMI) is the impact of signal transmitters and receivers operating in proximity to a CMS system, which could cause an interruption in the electronic operation of the system.	• Malfunctioning equipment: Electromagnetic impulses and radio frequency interference (RFI) are common causes of line noise. Line noise could cause corrupted data transfers from a CPU to disk, printing errors, power supply damage, and static on computer monitor screens. • EMI could cause an extended power surge, over-stress power supplies and lead to computer equipment damage. • EMI could cause a power failure, disrupting network operation, computer screens to go blank, and servers to crash. • Electromagnetic radiation from standard computers could be used to reconstruct the contents of the computer screen. These signals could carry a distance of several hundred feet, and even further if exposed cables or telephone lines act as unintended antennas.
	2. Environmental Conditions *Primarily affects the integrity and availability of the system.*	Environmental conditions are controlled and noncontrolled climate conditions, which have the potential to cause system damage or degradation. This threat could be a result of the natural environment (extreme heat, cold, humidity, etc.) or faulty/poorly designed heating, ventilation, and air conditioning systems.	• Water leaks in server rooms could cause equipment damage. • Both excess and insufficient humidity in the computer room could threaten system reliability. • Overheating in computer rooms could result in computer failure and downtime. • Poor ventilation and air conditioning failure in server rooms could cause mechanical parts, such as disk drives containing data, to fail. • Air conditioning system failure could impair utilization of the

			building due to excessive heating, cooling, or insufficient air exchange.
	3. Hazardous Material Accident *Could impact system availability.*	Hazardous material accident is the unexpected spill of toxic material. Hazardous materials are substances that are either flammable, oxidizable or combustible, explosive, toxic, noxious, corrosive, an irritant or radioactive.	• Office cleaning materials with flammable contents could cause a fire or explosion if spilled or not kept at a specific temperature. • Spilled chemicals could cause a fire, releasing toxic smoke. • Chemical drain cleaners (also called drain openers) are extremely corrosive. Common ingredients in drain cleaners include lye or sulfuric acid. These chemicals work by eating away materials including skin if they should come in contact. • Household ammonia is considered to be an irritant rather than a corrosive hazard. Vapors, even in low concentrations, can cause severe eye, lung, and skin irritation. Chronic irritation may occur if ammonia is used over long periods of time. • Solvents such as alcohols are considered combustible because they evaporate easily at room temperature and can readily ignite given heat, spark, or flame. • Bleach, when mixed with phosphoric acid cleaner, produces a noxious gas with a strong odor.
	4. Physical Cable Cuts *Could affect system availability.*	A physical cable cut could be an intentional or unintentional event that affects the system's ability to perform its intended function. Depending upon the power and communications backups built into the system, the effects could range from minimal to catastrophic.	• A disgruntled employee could sabotage transmission media • Animals could cause damages to cables resulting in broken cables. • Lightening strikes could cause a structural fire, which could, in turn, burn out circuits resulting in a power failure. • Lightening strikes could cause a structural fire, which could, in turn, burn out circuits resulting in a power failure. • Lightening strikes could cause severe damage resulting in broken cables.

	5. Power Fluctuation *Could impact system availability.*	Power Fluctuation is a disruption in the primary power source (power spike, surge, brownout, and blackout) that results in either insufficient or excessive power.	• A power outage could affect the timeliness and quality of the delivered service. • Malfunction or failure of Central Processing Unit (CPU) or hardware could impact the timeliness and quality of the delivered services.
	6. Secondary Disasters *Could affect system availability.*	Secondary disasters are successive disasters that are likely to result from natural disasters or environmental conditions. Secondary disasters could strike communities at any time, with or without warning. The probability of secondary disasters should be anticipated.	• Spilled chemicals could cause a fire, releasing toxic smoke. • Broken water pipes could cause internal flooding. • An earthquake could cause a structural fire, which could, in turn, burn out circuits resulting in a power failure.
	7. Other Threats (To be specified by system owner or developer)		

Natural **Threats**			
	Threats	Descriptions	Examples
	1. Natural Disaster *Could impact system availability.*	Natural disasters, such as hurricanes, wind damage/tornadoes, earthquakes, and floods could result in damage or destruction of system hardware or software assets. Any of these potential threats could lead to a partial or total outage.	• An internal/external fire could result in damage to system hardware and facility. • Internal/external flooding could result in damage or destruction of system hardware. • Earthquakes are among the most deadly and destructive of natural hazards. They could be the direct cause of injury or death to a person responsible for security. They often destroy power and telephone lines. They could cause severe damage to facilities.
	2. Secondary Disaster *Primarily affects the availability of the system.*	Secondary disasters are successive disasters that are likely to result from natural disasters or environmental conditions. Secondary disasters could strike communities at any time, with or without warning. The probability of secondary disasters should be anticipated.	• An earthquake could cause a structural fire, which, in turn, could burn out circuits resulting in a power failure. • Intense rains could cause flooding. • Spilled chemicals could cause a fire. • Broken water pipe could result in internal flooding.
	3. Other Threats (To be specified by system owner or developer)		

Threat / Category Matrix

Confidentiality

Human	Espionage
	Impersonation
	Improper Disposal of Sensitive Media
	Inadvertent Acts or Carelessness
	Omissions
	Scavenging
	Shoulder Surfing
	Theft, Sabotage, Vandalism, or Physical Intrusion
	User Abuse or Fraud
Technical	
	Compromising Emanations
	Corruption by System, System Errors, or Failures
	Data/System Contamination
	Eavesdropping
	Insertion of Malicious Code, Software, or Database Modification
	Installation Errors
	Intrusion or Unauthorized Access to System Resources
	Misrepresentation of Identity / Impersonation
	Misuse of Known Software Weaknesses
	Takeover of Authorized Session
Environmental	None
Natural	None

Integrity

Human	Data Entry Errors or Omissions
	Inadvertent Acts or Carelessness
	Omissions
	Terrorism
	Theft, Sabotage, Vandalism, or Physical Intrusions
	User Abuse or Fraud
Technical	Corruption by System, System Errors, or Failures
	Data / System Contamination
	Insertion of Malicious Code, Software, or Database Modification
	Installation Errors
	Intrusion or Unauthorized Access to System Resources
	Hardware / Equipment Failure
	Misuse of Known Software Weaknesses
	Misrepresentation of Identity / Impersonation
	Saturation of Communications or Resources
	System and Application Errors, Failures, and Intrusions not Properly Audited and Logged
	Tampering
Environmental	Electromagnetic Interference
	Environmental Conditions
Natural	None

Availability

Human	Arson
	Espionage
	Inadvertent Acts or Carelessness
	Labor Unrest
	Omissions
	Procedural Violation
	Riot / Civil Disorder
	Terrorism
	Theft, Sabotage, Vandalism, or Physical Intrusions
	User Abuse or Fraud
Technical	Corruption by System, System Errors, or Failures
	Data / System Contamination
	Hardware / Equipment Failure
	Insertion of Malicious Code, Software, or Database Modification
	Installation Errors
	Intrusion or Unauthorized Access to System Resources
	Jamming (telecom)
	Misrepresentation of Identity / Impersonation
	Misuse of Known Software Weaknesses
	Saturation of Communications or Resources
	System and Application Errors, Failures, and Intrusions not Properly Audited and Logged
	Tampering
Environmental	Electromagnetic Interference
	Environmental Conditions
	Hazardous Material Accident
	Physical Cable Cuts
	Power Fluctuation
Natural	Natural Disaster
	Secondary Disaster

Correlation of Threats to Categories

C = confidentiality I = integrity A = availability

Threat Area	Environmental / Physical	Human	Natural	Technical
Arson		A		
Compromising Emanations				C
Corruption by System, System Errors, or Failures				C I A
Data / System Contamination				C I A
Data Entry Errors or Omissions		I		
Eavesdropping				C
Electromagnetic Interference	I A			
Environmental Conditions	I A			
Espionage		C A		
Hardware / Equipment Failure				I A
Hazardous Material Accident	A			
Impersonation		C		
Improper Disposal of Sensitive Media		C		
Inadvertent Acts or Carelessness		C I A		
Insertion of Malicious Code, Software, or Database Modification				C I A
Installation Errors				C I A
Intrusion or Unauthorized Access to System Resources				C I A
Jamming (telecomm)				A
Labor Unrest		A		
Misrepresentation of Identity				C I A
Misuse of Known Software Weaknesses				C I A
Natural Disaster			A	
Omissions		C I A		
Physical Cable Cuts	A			
Power Fluctuation	A			
Procedural Violation		A		
Riot / Civil Disorder		A		
Saturation of Communications or Resources				I A

Scavenging		C		
Secondary Disasters			A	
Shoulder Surfing		C		
System and Application Errors, Failures, and Intrusions not Properly Audited and Logged				I A
Takeover of Authorized Session				C
Tampering				I A
Terrorism		I A		
Theft, Sabotage, Vandalism, or Physical Intrusions		C I A		
User Abuse or Fraud		C I A		

Threat Analysis and Assessment

It has been identified that analysing and examining vulnerabilities constitutes a challenging problem facing today’s organizations. However, in the modern electronic era that we are living in, there is an obvious need for a formal technique to be developed in order to help with the process of identifying and analysing vulnerabilities in a complex organizational environment. Today’s methodologies and systems are static in nature, or at best reactive, designed only to respond to certain events after those occur. These systems are not efficient enough for today’s rapidly changing environments because they cannot cope with constant transformation, since the latter is not supported naturally by their models, but is rather being retrofitted into them. Therefore, in order for these systems to be able to incorporate change a hard, time-consuming process is often required.

Furthermore, the fact that significant effort is required in order to expand those systems, or in order to reflect and reconsolidate upon previously identified vulnerabilities through the use of some methodology is in itself significant and stems from the fact that those methodologies and\or systems have been based upon equally inadequate definitions regarding vulnerabilities. As an example let us ponder over some of the different definitions of the term vulnerability that have been developed over time:

The concise oxford dictionary (Sykes '81), defines the term Vulnerability to mean: “is susceptible to damage”. Vulnerability has been defined as follows:

- A point where a system is susceptible to attack (Kabay '96).
- A weakness in the security system that might be exploited to cause harm or loss (Pfleeger '97).
- Some weakness of a system that could allow security to be violated (Blyth '01).

However, for the purpose of a threat assessment we require a definition that is more general to information security and encompasses, information technology, communication systems, and business processes. Therefore, for the purposes of this paper we will define vulnerability as: "*A measure of the exploitability of a weakness*".

After applying some kind of threat assessment methodology, the user should be able to compile a list with the vulnerabilities that the system is suffering from. Nevertheless, just creating flat lists where there is no mentioning as to how the various identified vulnerabilities relate to each other, is simply not adequate. Usually, there is an identified requirement for the user of the methodology to be able to answer a series of questions after the assessment such as:

- How easy or difficult it would be for a vulnerability to be exploited by a threat agent (Stalling '00), (Carroll '96), (Ammann '02).

- Whether or not a threat agent needs to exploit another vulnerability in order to achieve his/her goal.

- What are the possible attack paths (Moore '01) that the agent might follow? How long will it take for an agent with a given set of capabilities (Vidalis '01), (Blyth '01), (Barber '01), (Hoath '98), (Rees '96), to exploit a vulnerability, and will he/she be able to manifest a threat in that time window?

- How complex is for the different types of threat agents to exploit system vulnerabilities and how concerned should the information security officers be?

In this paper we will discuss a methodology that will allow the user to measure vulnerabilities by identifying and analysing their relationships using a hierarchical organization and representation approach To this end, we believe that this approach can provide the answers to the above questions by helping the users of a threat assessment methodology to identify key vulnerabilities that are common to more than one assets of the system and help them to counter them in a cost effective manner (Summers '77).

State of The Art of Vulnerability Assessment

There are quite a few tools that can be used for analyzing systems and identifying vulnerabilities. Some of the tools are: COPS (COPS '02), NESSUS , SystemScanner (SystemScanner '02), Retina, NetRecon, Whisker, and CyberCop. It is recognized in (Ammann '02) that just identifying individual vulnerabilities is not sufficient and adequate in today's electronic era of cyber-crime (Bequai '01).There are quite a few approaches when it comes to modelling vulnerabilities in order to perform some sort of analysis in a computing system. The safety critical systems field examines the hazard analysis process. Vulnerabilities can be perceived as being hazards for a computer system. The different techniques that analyse hazards include: checklists, fault tree analysis, event tree analysis, and cause-consequence analysis.

Checklists are static and cannot demonstrate the relationships between the vulnerabilities. Furthermore, they do not examine the how and the why two vulnerabilities are related to each other. Fault trees are just chronological orderings of events over time and are not adequate to visualize and model the different types of vulnerability relationships. Each level of the fault tree merely shows the same thing in more detail. Event tree analysis is a Boolean approach to examine vulnerabilities and failures. Most of the vulnerability types of a computing system though cannot be expressed with Boolean values. The technique work very well for hardware vulnerabilities, but according to (Nuemann '95) there are six other vulnerability types, that cannot be addressed effectively. Cause-Consequence Analysis (CCA) is a top-down or backward technique that can determine the causes of an event. It can model both time dependencies and casual relationships among the events. The negative side of CCAs is the size of the diagrams, their complexity and the fact that they cannot accept data from other diagrams.

Another commonly employed technique is the use of history attack data for producing patterns and attack trees. This technique is trying to predict the path that the threat agent will follow by analyzing the exploits that might be used. Each path through an attack tree represents a unique attack on the enterprise. The problem with attack trees is that they cannot analyse big systems or large—size networks (Ammann '02) mainly due to their complexity. A different number of exploits might be used for attacking more than one vulnerabilities, and the same exploits can be used for attacking different vulnerabilities. Producing attack trees using exploits as nodes is not efficient for a system that changes constantly.

The Mathematical nature of Hierarchy Trees and OO

Classification hierarchies are built in close association to each member making up the structure. That is, not only do they impose ordering of the member nodes making it up, but they also depict clearly the relationships between each member node. Both of these qualities of classification hierarchies find a natural way of implementation in the theory of directed graphs (also known as di-graphs). By letting a non-empty set V expressed as $V=\{[X_t] :1 \leq t \leq i\}$ represent the vertices of the graph, consisting of all the equivalence classes defined, and also a set E representing all the edges of the graph defined to be: $E=\{([X_1], [X_2]) \in V \text{ x } V : [X_1] \text{ R } [X_2]\}$, then the resulting di-graph is $G= (V, E)$.

In relation to the above, an equivalence class $[X_i]=\{k \in S: k\sim X_i\}$ can be viewed as a collection of elements (things, events, objects, etc) that share a common trait, or are “similar” in some logical perspective. In fact, it would not be wrong to say that equivalence classes are cognitive functions, used to organise and cluster together information and knowledge regarding a certain domain, given a set of criteria. If G has n vertices and n-1 edges then it can be considered to be a “tree” (i.e. a di-graph with out loops) (Merris `01), (Godsil `01), which by definition imposes a hierarchical arrangement of the data that it represents. a structure that resembles the one shown in figure1 below can be constructed.

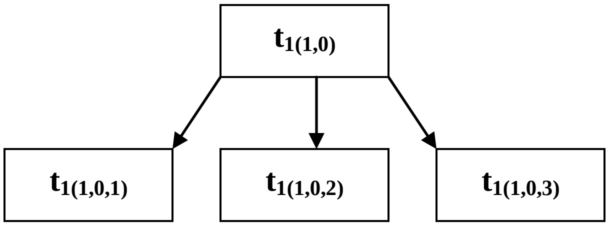


Figure 1: A graphical representation of a Theoretical Tree Structure.

Due to the mathematical nature of those structures, it is easy to imagine that a number of mathematical functions, each performing a specific task is easy to define (Morakis `03). So for example one could define functions that return the parent of any given node, functions that return the children of a node and in general any type of function that on would wish to define.

A natural way of implementation of the previously mentioned mathematical semantics of the proposed method is by applying the features and aspects of the Object Oriented model (OO). By introducing (OO) concepts in vulnerability assessment one can greatly enhance the analyst's ability to analyse, and classify vulnerabilities. These concepts, include developing highly cohesive but independent object classes for the various events reported by vulnerability scanners, or threat assessment methodologies, allowing the analyst to view incoming events not only as containing static information, but as objects being able to act and being acted upon, and exploiting powerful concepts that provide forms of abstraction not found in other models such as natural language, or process oriented analysis.

Another reason, as to which an OO approach was chosen, stems from the straightforward mapping between the mathematical constructs described previously and the Object Oriented components. In other words, the OO model possesses all the necessary functionality to built and describe the hierarchical tree structures in question. The first and foremost important construct provided by the model is the object. The latter as it is seen in the OO context is the lowest construct provided by the model (Bennett `99), (Embley `92). Thus, we can use the notion of an object to describe the output reported by various vulnerability scanners, or threat assessment methodologies, chosen to perform cyber vulnerability assessment in a system.

Additionally, in close relation to the notion of an object is another construct that builds upon it, that of an Object class. This type of construct is the direct analogy of a mathematical equivalence class and is used to organise and cluster together all knowledge available about a system object into a singe logical location. Thus, we can now organise the existing vulnerabilities of a system into locations that hold similar in some logical perspective items, therefore making easier for the analyst to locate, examine, and understand system critical vulnerabilities. Object classes, also can possess attributes that better describe and personalise the events (objects) that are hosting. In relation to vulnerabilities some proposed (but not exhaustive) attributes could be: Vulnerability name, Vulnerability type (one of the six basic types present in all type of systems, i.e. physical, h/w, s/w, etc.), and especially when it comes to studying cyber vulnerabilities, one could include source/destination IP, source/destination port, and also CVE number that stands for Common Vulnerability and Exposures giving the analyst the ability to index and cross-reference information about publicly known vulnerabilities and exposures with databases and scanners. It is also possible to include vulnerability attributes that deal and describe other aspects such as educational complexity, and time to exploit (Vidalis `03).

Also, another significant benefit of an OO approach is that it offers the concept of relationships. Although, it is very useful to be able to represent various events as objects and further organise and abstract them using object classes, often enough diagrams used to depict objects and classes are meaningless unless we understand some relationships to hold amongst them. The role of a relationship is to establish a logical association between objects, or object classes which although an important aspect, it is often overlooked, especially when it comes to analysis and assessment of cyber vulnerabilities where the load of incoming information from vulnerability scanners, online databases, etc. is very high and complex.

In relation to the relationships possessed by the OO model the following can be mentioned:

- The generalisation also known as *"is-a"* relationship (Bennett `99),(Embley `92), used to signify that the set of objects in object class A is really a subset of object class B. That is: $A \subseteq B$ (if $\forall x \in A \Rightarrow x \in B$), which therefore implies that the superset object class B, is a generalisation of the subset class A.

- The aggregation, also known as *"is-part-of"* relationship (Bennett `99),(Embley `92).

- Also, the OO model possesses a number of special constraints on specialisations such as the union constraint, the mutual exclusion, and the partition constraint (Embley `92) in an attempt to be more convenient and more expressive.

As an example of how the construction of hierarchical classifications could be applied to vulnerability assessment of a critical system component let us consider the hypothetical scenario where the main broker server of a micro-payment system (MPS) (Vidalis '01), (Manasse '95), (W3C '99), (O'Mahony '97) is in jeopardy. According to (Pfleeger '97), (A.J.C.Blyth '01), (Summers '77), (Scambray '01), (Smith '93), (Forte '00), there are six types of vulnerabilities that can exist in any system, and these are: Physical, Natural, Hardware/Software, Media, Communication, and Human and for the purposes of a complete vulnerability assessment all of them should be considered and analysed. However, to keep things straightforward we will only consider the situation where someone is performing a series of port scans, in an attempt to locate open ports and identify the surroundings of the system.

Hence, from what we have seen up to know, the constructed tree should look like the one presented in figure 2. The root node of the tree is an abstraction used, to glue together all the subsequent levels of the tree build around the complementary concept of generalisation-specialisation. That is, the parent node named in this case "*Broker ServerVulnerability*" is a generalisation of the vulnerabilities examined. Conversely, the leaf nodes of the tree are specialisations of the parent class, offering more specific information regarding the various vulnerability types with increasing levels of specification as one is traversing the tree, from the root to the leaf nodes. In addition, the union and plus symbols embedded in the triangle are used to signify a partitioning constraint which implies that the specialisation sets are pairwise disjoint and at the same time that their union constitutes the partitioned set itself, i.e. the root node.

Figure 3: Port Scan Hierarchy Tree Example.

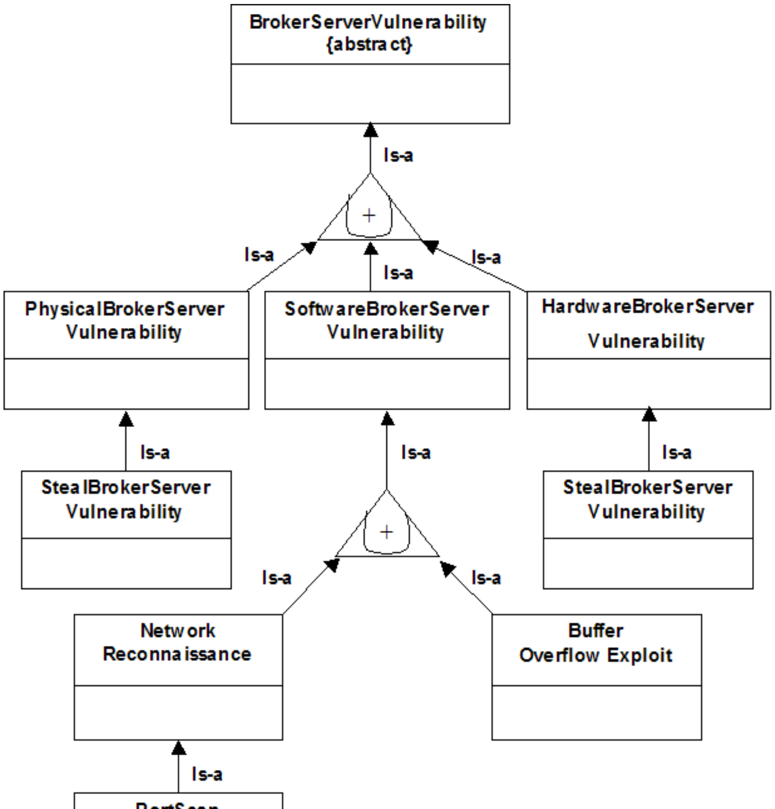
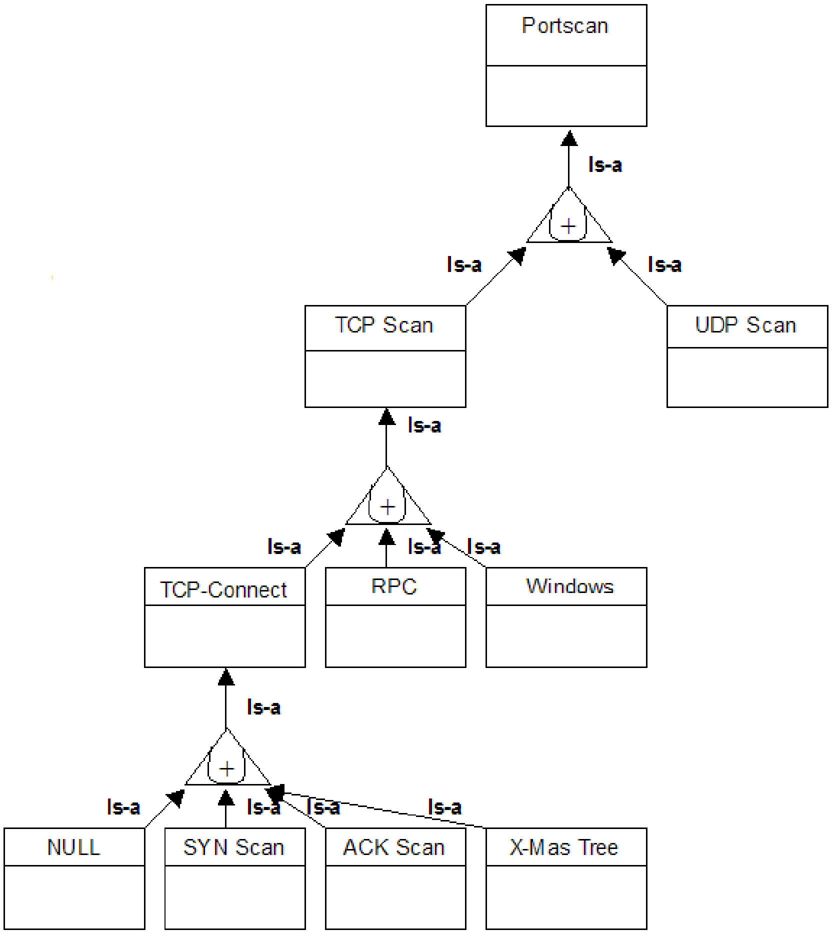

BrokerServerVulnerability
{abstract}
Is-a
+
Is-a
Is-a
Is-a
PhysicalBrokerServer Vulnerability
SoftwareBrokerServer Vulnerability
HardwareBrokerServer Vulnerability
Is-a
Is-a
Is-a
StealBrokerServer Vulnerability
+
StealBrokerServer Vulnerability
Is-a
Is-a
Network Reconnaissance
Buffer Overflow Exploit
Is-a
PortScan

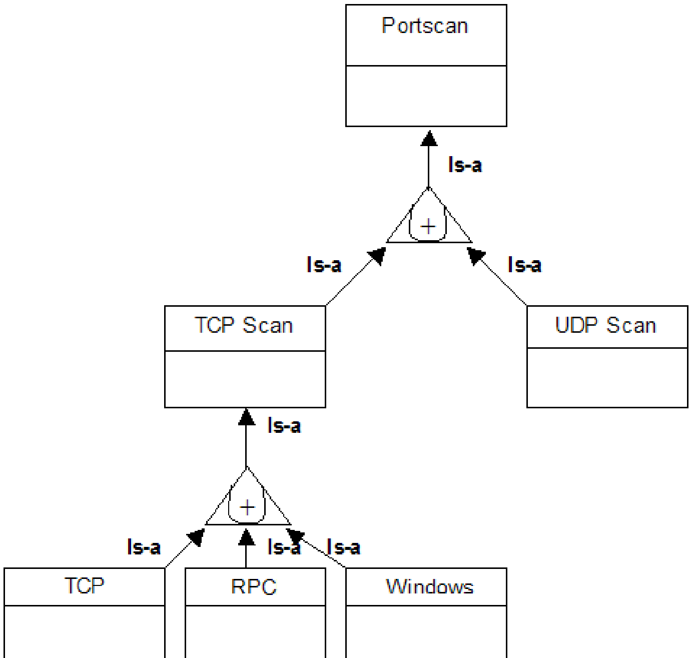
Figure 2: Broker Server Vulnerability Tree Example.



Scenaı

After coı fy the vulnerabilities
associate ıntly, how these are
related tc nent by constructing
what we individual steps that
have to b ıis/her target. As the
name im rint left behind by a
common ry similar that is, to
identify e oing to be discussed
later on, :

Moreove tive regarding which
events pı ıently guard against.
Footprint iguration of symbols
for repre ırticular object class.



We consider footprints represented this way as being behavioural templates, specifying possible expected behaviour to be demonstrated by an attacker. Alternatively, footprints can be viewed as "directional" vectors (to avoid confusion, the term is not employed with the strict mathematical meaning, but rather as a linguistic concept), pointing to nodes of the previously constructed classification hierarchies with the purpose of connecting them to each other, in order to create chains of events. As it might have been expected, the attractive force that holds together the various links of the chain, are logical operators such as the logical *AND* (^), and logical *OR* (|). The case of having footprints comprised of a single link chain is also possible.

Furthermore, we consider footprints to be classified into groups based on two criteria: 1) whether they are *simple* or *compound* and 2) whether they are *abstract*, or *specific*. *Simple* footprints are those that cannot be decomposed any further, i.e. they are chains containing a simple link only and can be formally described as: $F_x := Y$ where Y is some kind of event existing as a node in a tree hierarchy. On the other hand, *compound* footprints, are the ones that can be decomposed into more than one *simple* footprint held together by logical operators. The latter form of footprints, can be formally expressed as: $F_x := X\ (*)Y$ where X and Y are some kind of events as before, and * signifies any logical operator. Also, *abstract* footprints represent chains of events, made up off the abstract classes, usually located closer to the root of the hierarchy, or the root point of each new level of the hierarchy. Finally, *specific* footprints are usually formed by those classes of events closer to the leaf nodes of a tree, since those are the ones representing more specific types of events.

To apply these concepts to the previously described scenario of someone trying to identify the network topology of a critical system such as a micro-payment system, an analyst using the trees depicted in figures 2-3 could construct a series of footprints resembling the ones shown below:

- F_1*: =Broker Server Vulnerability*
- F_2*:= Network Reconnaissance*
- F_3*:= Buffer Overflow Vulnerability*
- F_4 *:= Software Vulnerability*
- F_5*:= Network Reconnaissance| Buffer Overflow Vulnerability*
- F_6*:= Tcp Connect Scan | X-mas tree Scan*

Let us now examine each of them individually and see what their significance is. The footprint F_1 is an example of a *simple, abstract* footprint. The analyst is just expressing his/her concern regarding any type of vulnerability deployed against the server, without going into any details. The next three footprints (F_2-F_3), represent yet another example of *simple*, *abstract* footprints. The analyst has started to become more explicit regarding his/her concerns. For example, the analyst has expressed concern regarding network reconnaissance attempts (footprint F_2) against the system, has also shown explicit interest on buffer overflow attacks (through footprint F_3), and also expressed interest on any type of software vulnerability in general, that could be deployed against the target system (by specifying footprint F_4). Albeit these footprints are more informative and more specific than footprint F_1 is, are still considered to be *simple, abstract* ones because they are made up of abstract classes.

In addition, F_5 is an example of an *abstract*, *compound* footprint. Specifically, it is comprised of the *simple*, *abstract* footprints F_2 and F_3 connected via the logical operator OR. Thus, in this case the analyst has specified an interest regarding the occurrence of either a network reconnaissance attempt, or a buffer overflow attack deployed against the target system. Finally, the last footprint shown, (F_6) is an example of a *specific*, *compound* footprint, made up of two specific classes i.e. Tcp connect scan and X-mas tree scan and again connected to each other via the logical OR operator.

Hence, the next thing that should be considered is what the benefits of expressing footprints and representing them as petri-nets are. The answer to this question is that by doing so one is able to clearly depict and understand the distinct stages/actions that an attacker might engage in. Having done so, the same person is now able to employ countermeasures effectively and proactively. Up until now, the usual scenario meant that a system would only respond to events after they occurred and thus the danger existed that even if some type of countermeasure was deployed it might have been too late. In contrast by employing the aforementioned concepts the analyst, who now has a more holistic view of the vulnerabilities that the system is suffering from, and most importantly how these are related to each other, can predict and describe the actions of a threat agent building possible scenarios of how a threat might be exploited against the system.

As an example, let us consider the situation of figure 4 shown over the next page, depicting a petri-net representation of the given set of footprints i.e. F_1 to F_6 defined previously. In specific, if the system enters the state represented by place P_1 (i.e. the state where a Tcp scan against the target system has been deployed), then transition T_1 fires and the system changes to the next logical state P_3, by moving the token from P_1 to P_3. This very distribution of a token from place P_1 to P_3 is causing transition T_3 to fire, which in turn moves the distribution of tokens from P_3 to place P_5. This new state represents a situation where a network reconnaissance has been attempted against the target system. Following the same way of reasoning, it must be clearer that the distribution of tokens would continue until the token would reach the bottom part of the petri-net and would repeat in a similar fashion next time that a similar event would occur or appear.

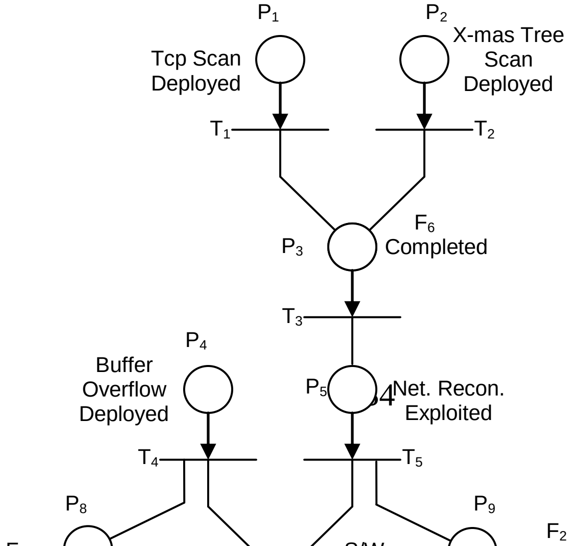


Figure 4: Petri-net Representation of Footprints F_1 to F_6.

In fact, it is this very chain reaction of tokens that makes it possible to produce a scenario of possible attacks perpetrated against the system. More precisely, the cascade of all the footprints that the analyst has defined, model out the causality principle where each observed event (for example a Tcp scan) causes in turn the system to change to the appropriate state and so on and it is therefore the collection of all footprints that enable the analyst to envision the different avenues of attack followed by a threat agent based on a representational form of causality. It is also possible to effectively deploy countermeasures in such a way so as to tunnel an attacker towards a desired direction.

For example, a simplistic countermeasure that could be deployed in relation to a certain type of port scan would be to reconfigure on the fly the rule set of a firewall so as to drop incoming packets that have set the desired attributes/flags. By doing so, the analyst has effectively blocked this avenue of attack that was concerning him/her (reflected on the footprints expressed) thus leaving only one other avenue exposed to a possible attacker. In the case of figure 4 the only other way that could result in the exploitation of a software vulnerability (given the specified set of footprints) would be through a buffer overflow attempt. However, the analyst is feeling confident that by keeping the system regularly patched and updated this factor does not possess a major threat. This way, the analyst by carefully deploying countermeasures in strategic locations has managed to tunnel the threat agent.

Classification hierarchies form the basis of the proposed technique. They deal with the semantics of the terms they describe. Their main purpose is to provide an in-depth classification of vulnerabilities, what they really are and how they relate to various other vulnerabilities. Additionally, classification hierarchies provide the main mechanism and the starting point for an analyst to build footprints, i.e. chains of events of interest that can identify different scenarios reflecting how a threat agent might exploit a vulnerability.

Furthermore, the proposed concept is not considered a stand-alone threat assessment methodology since it does not deal directly with asset identification, stakeholders, or vulnerability identification, but it rather assumes that all the required information is known from a previous stage. What the proposed method does is scenario construction. Having defined the classification trees the analyst can proceed in identifying critical paths and differentiate between vulnerabilities that must be countered immediately and those that could be countered some time in the future, thus securing the system in a cost effective manner. Finally, the motto of the proposed methodology is pro-action. That is, our main belief is that processes (and for that matter vulnerabilities) should be handled at an early stage. In today's complex environments that simply means that countermeasures should be employed in strategic locations, and that timing is a serious issue in cyber vulnerability assessment.

Threat Assessment Using TAME

The wide development of the mobile Internet has destabilized the already fragile balance between the defenders and the attackers of computing infrastructures. That balance is very sensitive, being dependent on vulnerable computers controlling priceless information. The current risk assessment methodologies are obsolete weapons in the hands of techno phobic "grey haired" men. We should not repeat the mistakes of the 80s and go through a new "software crisis". In today's' computing environment, organizations have been forced to allocate considerable resources for protecting their information assets. Unfortunately, worldwide statistics are indicating that things do go wrong, with catastrophic results most of the times. Computers are around for more than three decades. During that time we have learned that most risks cannot be avoided. What we should do instead is try to control them, to some extent, in a practical and cost effective manner. We argue that risk is not controlled by the assessors but by the threat agents. Having that in mind we developed a methodology called Threat Assessment Methodology for Electronic Payment Systems (TAME). TAME is a methodology for the assessment and analysis of threats and vulnerabilities within the context of security risk management and it consists of four stages. This methodology actively involves stakeholders and focuses upon a technical, socio-technical and business aspect of the system, and can form part of the wider risk assessment process.

TAME was developed during an EU framework-5 research project in order to perform the security assessment of a Micro-Payment System (MPS). After the application of the methodology to the prototype of the system, a number of issues came to surface. It was found that the methodology was too cumbersome, despite the development efforts to maintain a light and simplistic approach. This was addressed, and the outcome is the version of TAME that is presented in this paper. It was found that the "bones" of the methodology were light and accurate, but once all the activities were executed, the large number of the I/O operations was a hindrance towards the successful completion of the threat assessment. The ultimate goal of the developers of the methodology was to make the security auditor obsolete, and the specialized knowledge about threat assessment a luxury. TAME was developed with one purpose: to become a tool in the hands of any computer literate employee of any type of company.

The initial approach of TAME was to gather as much information as possible, put it on the table, and in cooperation with the stakeholders of the enterprise, filter everything and keep only data that were relevant to the scope of the assessment. The scope though was identified only after the cumbersome process of gathering the data. It was found that the above approach was time consuming and required the constant attention of the members of the enterprise. In other words, it was bringing the enterprise in a standstill until the end of the first assessment. The new approach of TAME tackles the above issues. The scope of the assessment is defined first in cooperation with the stakeholders of the enterprise, the relevant data are gathered from various sources, threat scenarios are constructed, which are then evaluated and approved by the stakeholders in order to calculate their impact towards the survivability of the enterprise.

TAME Overview

In agreement with Schneier (Schneier '01) the existing risk assessment methodologies, cannot address the needs of a modern computing system. There is still no clear distinction between a threat and a risk assessment although there have been a lot of discussions around the current methodologies. After the examination of the existing methodologies, a suitable one tailored to Electronic Payment Systems (EPS) was developed. All the examined methodologies were following the waterfall development model, which was not suitable for EPSs. These systems are generally sensitive and prone to changes. Because of their nature, their life span and their "internationality" a waterfall assessment model would be too monolithic and too slow. It would require a great amount of effort and time for producing results only half of which would be useful for the business conducting the assessment. Furthermore, most of the examined methodologies were missing a very important factor, the factor of the business analysis for understanding the environment into which the business is operating.

Another development option was to follow the spiral development method. Yet again, even that is limiting the assessor to a specific sequence for conducting the different model stages. What we really want is the assessor to be able to change his way of thinking and working "on-the-spot", be as much flexible as possible, and be able to change the parameters of the experiment on the fly, from any point of the experiment, without having to restart it. This can be seen in figure 1. The formal entry point of the methodology is Phase 1: Scope of Assessment. Depending on the information that is available to the auditor using the methodology, he can perform some system modelling (Phase 3: Scenario Construction and System Modelling) or he can perform some threat agent & vulnerability analysis (Phase 2). Of course, Phase 3 cannot really be executed without some inputs from Phase 2 (see later sections). Should the inputs are available though, then the auditor can move straight to Phase 3. Once information on threat agents and vulnerabilities are analysed, and relationships between them are identified, then the auditor might want to go back to Phase 1 and change the scope of the assessment. Eventually the auditor will run Phase 3, and construct the threat scenario that will be presented to the Stakeholders in Phase 4, for their evaluation. Once the stakeholders are consulted then there might be a need to change the scope of the assessment again or perform corrections to the threat agent and/or vulnerability data. After a number of cycles, the auditor will eventually execute process 14, which is part of Phase 4: Evaluation, which is the formal exit point of the methodology.

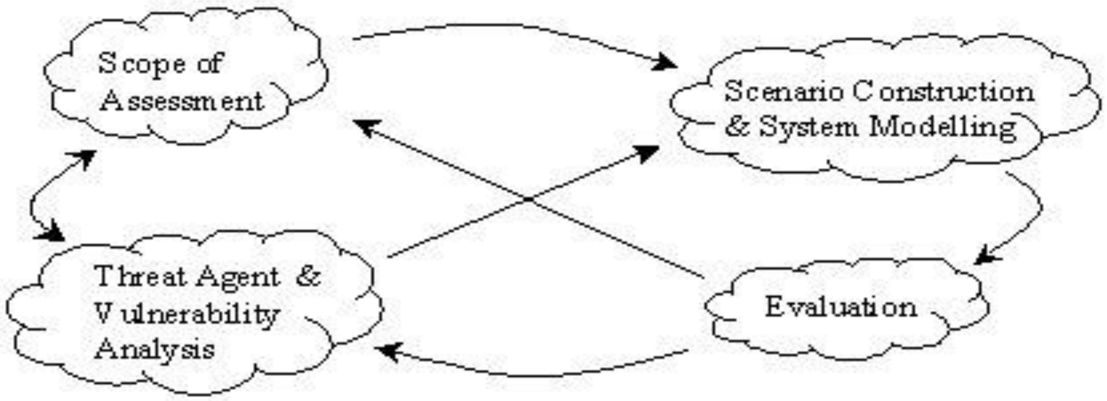

Scope of Assessment
Scenario Construction & System Modelling
Threat Agent & Vulnerability Analysis
Evaluation

Figure 1 - TAME Diagram

According to Finne (Finne '98), a method is a set of steps used to perform a task, and a methodology is a set of tools, or research methods, translating management theory to management practice. TAME is a "third generation threat assessment methodology" that is based on the organisational analysis of the customer's business, using business-modelling techniques. Internal and external stakeholders are actively involved through out the assessment.

Each phase contains a number of processes. Most processes are happening simultaneously (depending on the resources of the enterprise) and the output of one can be the input of another, or the output of one might change the input of another and vice versa. The methodology, once applied to a system should never come to an end, as constant attention is needed to ensure that countermeasures remain appropriate and effective. The ultimate goal of TAME is to help the security manager to decide how much security is necessary and where it should be applied. According to Hancock (Hancock '98) the above should be the only goal of a modern and effective threat assessment methodology.

The methodology examines organisational and technology issues to assemble a comprehensive picture of the threats facing a company. The four phases of the methodology contain the following processes and activities:

- Phase 1:Scope of Assessment

  - Process 1: Business Analysis,
    - Activity 1.1: Business Goals Analysis,
    - Activity 1.2: Business Processes Analysis,
    - Activity 1.3: Environmental Analysis,
  - Process 2: Stakeholder Identification,
    - Activity 2.1: Stakeholder Identification,
    - Activity 2.2: Stakeholder Responsibility Identification,
  - Process 3: System Boundaries Identification,
    - Activity 3.1: System & Boundary Identification,
    - Activity 3.2: Ascertain Boundary Control,
  - Process 4: Threat Agent Identification & Selection
    - Activity 4.1: Threat Agent Identification,
    - Activity 4.3: Intention Identification

    - Activity 4.3: Threat Agent Selection
  - Process 5: Asset Identification & Selection
    - Activity 5.1: Asset Identification Using Staff Knowledge
    - Activity 5.2: Asset Identification Using Other Inputs
    - Activity 5.3: Asset Value Calculation
    - Activity 5.4: Asset Selection

- Phase 2: Threat Agent & Vulnerability Analysis

  - Process 6: Threat Agent Preference Structuring,
    - Activity 6.1: Likelihood Analysis,
    - Activity 6.2: Importance Analysis
  - Process 7: Vulnerability Identification & Selection,
    - Activity 7.1: Vulnerability Type Identification,
    - Activity 7.2: Vulnerability Type Selection,
    - Activity 7.3: Automated Vulnerability Identification,
    - Activity 7.4: Manual Vulnerability Identification,
    - Activity 7.5: Vulnerability Selection.
  - Process 8: Threat Agent Attribute Calculation,
    - Activity 8.1: Threat Agent Capability Calculation,
    - Activity 8.2: Threat Agent Opportunity Calculation,
    - Activity 8.3: Threat Agent Motivation Calculation,
  - Process 9: Vulnerability Complexity Calculation
    - Activity 9.1: Pre-analysis,
    - Activity 9.2: Structural Analysis,
    - Activity 9.3: Node Analysis,
    - Activity 9.4: Value Analysis,
    - Activity 9.5: Optimization Analysis,

- Phase 3: Scenario Construction & System Modeling

  - Process 10: Scenario Generation,
    - Activity 10.1: Threat Identification,
    - Activity 10.2: Scenario Construction,
    - Activity 10.3: Scenario Unification,
  - Process 11: System Modeling,
    - Activity 11.1: Pre-Analysis,
    - Activity 11.2: Structural Analysis,

- Phase 4: Evaluation

  - Process 12: Stakeholder Evaluation,
    - Activity 12.1: Output Identification,
    - Activity 12.2: Output Allocation,
  - Process 13: Impact Analysis,
    - Activity 13.1: Impact Field Identification,

    - Activity 13.2: Tangible Impact Analysis,
    - Activity 13.3: Intangible Impact Analysis,
  - Process 14: Threat Statement Generation

A discussion and a high-level overview of the above phases can be seen in the following pages. The numbering of the phases and of the processes is only for presentation purposes and for getting a better understanding of the data flows inside the methodology. The numbering does not declares some sort of priority in executing the phases or the processes inside those phases. Depending on the assessor, and the data available to him during the assessment, different paths might be followed in every cycle of the execution of the methodology.

In phase 1, the business area of the organization is identified and interrogated. This allow for the different stakeholders participating in the business to be identified. The information that has been gathered by this point can be used to identify the boundaries of the system. These boundaries will have to be protected from the threat agents. This need leads to another process. Threat agents that are active or inactive are being identified. These threat agents will be targeting assets. From the other processes of the methodology, the assessor has now the required information to perform the asset identification. All the information gathered from the above processes can be used as a first set of security requirements. The high level overview of phase 1, presenting its inputs and outputs, can be seen in Figure 2. Phase 1 is using information about the organization under analysis, staff knowledge and threat agent data for identifying boundaries, threat agents assets and stakeholders as well as understanding the environment that the organization is conducting business in.

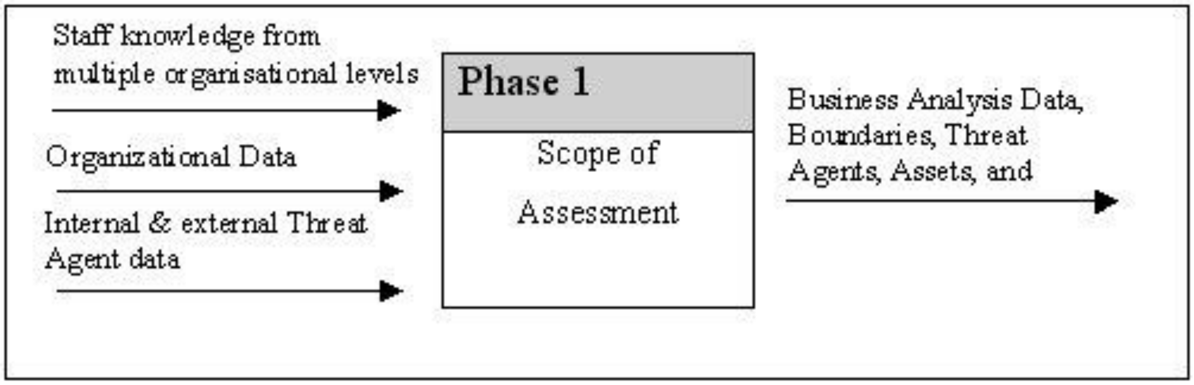

Staff knowledge from multiple organisational levels
Organizational Data
Internal & external Threat Agent data
Phase 1
Scope of Assessment
Business Analysis Data, Boundaries, Threat Agents, Assets, and

Figure 2 - Phase 1 Scope of Assessment

In phase 2, the threat agents identified in phase 1 are being examined and their attributes are analyzed. This will allow for a preference structuring according to their importance towards the organization. From all the previous phases, we have acquired enough information to perform a vulnerability identification, which will lead to the analysis of their exploitation complexity. This is taking under consideration the capabilities of the agents. The high level overview of phase 2, presenting its inputs and outputs, can be seen in figure 3.

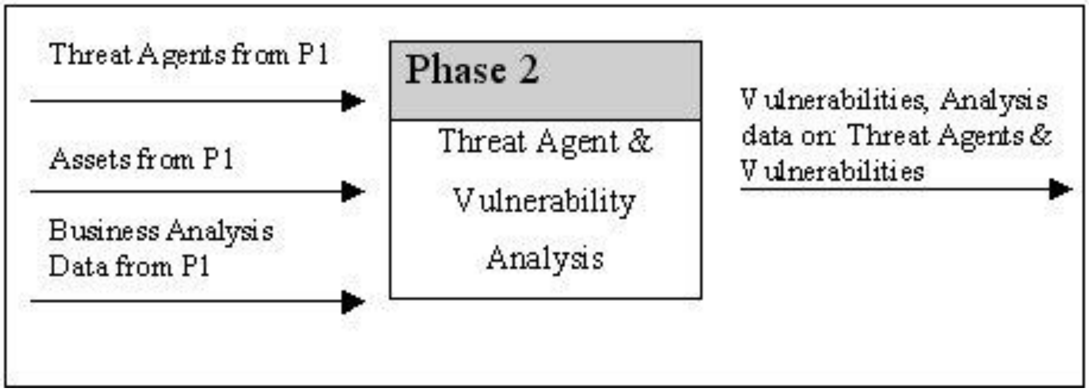

Threat Agents from P1
Assets from P1
Business Analysis Data from P1
Phase 2
Threat Agent & Vulnerability Analysis
Vulnerabilities, Analysis data on: Threat Agents & Vulnerabilities

Figure 3 - Phase 2 Threat Agent & Vulnerability Analysis

In phase 3, information gathered from phase 1 & phase 2 can be used to create scenarios about threat agents (identified in phase 1, analyzed in phase 2), attacking individual assets (identified in phase 1), or processes, by exploiting one or more of their vulnerabilities (identified in phase 1, analyzed in phase 2). In this phase, for the first time in the methodology, all the three variables of a threat (threat agent, asset and vulnerability) are combined and examined as a whole. The outcome of the phase is the system models and the attack scenarios that will be used in the fourth phase. The output of this phase can be considered as a second set of security requirements that will have to be met. The high level overview of phase 3, presenting its inputs and outputs, can be seen in figure 4.

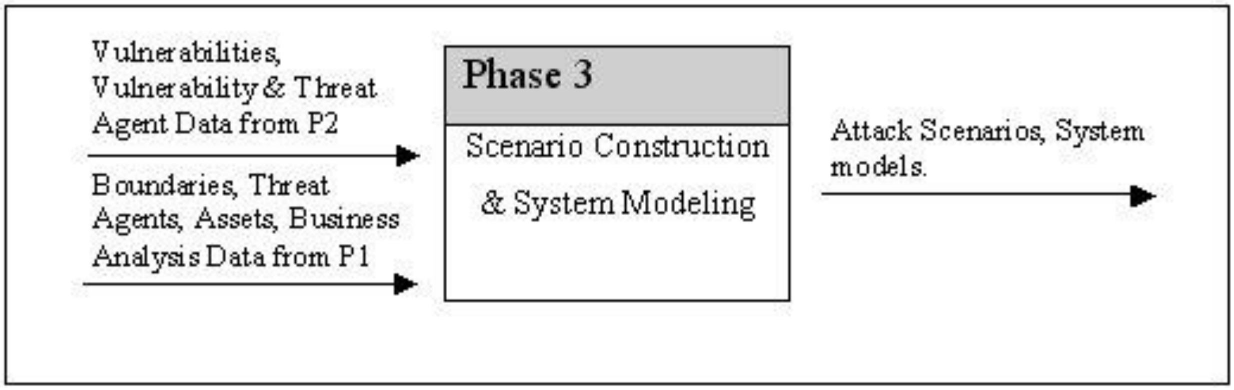

Vulnerabilities, Vulnerability & Threat Agent Data from P2
Boundaries, Threat Agents, Assets, Business Analysis Data from P1
Phase 3
Scenario Construction & System Modeling
Attack Scenarios, System models.

Figure 4 - Phase 3 Scenario Construction & System Modeling

In phase 4, the stakeholders are evaluating the results of each process, the impact of each threat identified in phase 3 is being calculated towards all the different levels of the business, and finally the threat statement is being generated and transferred over to the stakeholders of the business for their consideration. The high level overview of phase 4, presenting its inputs and outputs, can be seen in figure 5.

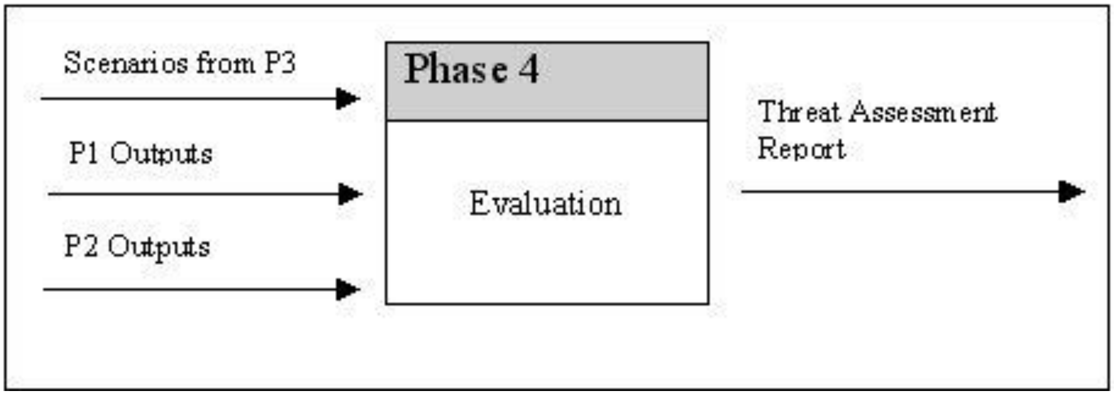


Figure 5 - Phase 4 Evaluation

The uniqueness of TAME lies in the interactions between the different steps and in the data flows. There is not one unique path to execute the methodology. The auditor can follow whatever path he chooses so, depending on the restrictions of the security audit and the restrictions of his knowledge. It is not necessary for the auditor to perform all the steps of the methodology for getting meaningful results. Everything is dependent on the system under analysis. The simpler the system the fewer steps will have to be executed. The golden rule though is that the more steps the better the results. A high level overview of the data flows can be seen in figure 6. In the figure we can see the interactions between the different processes of TAME.

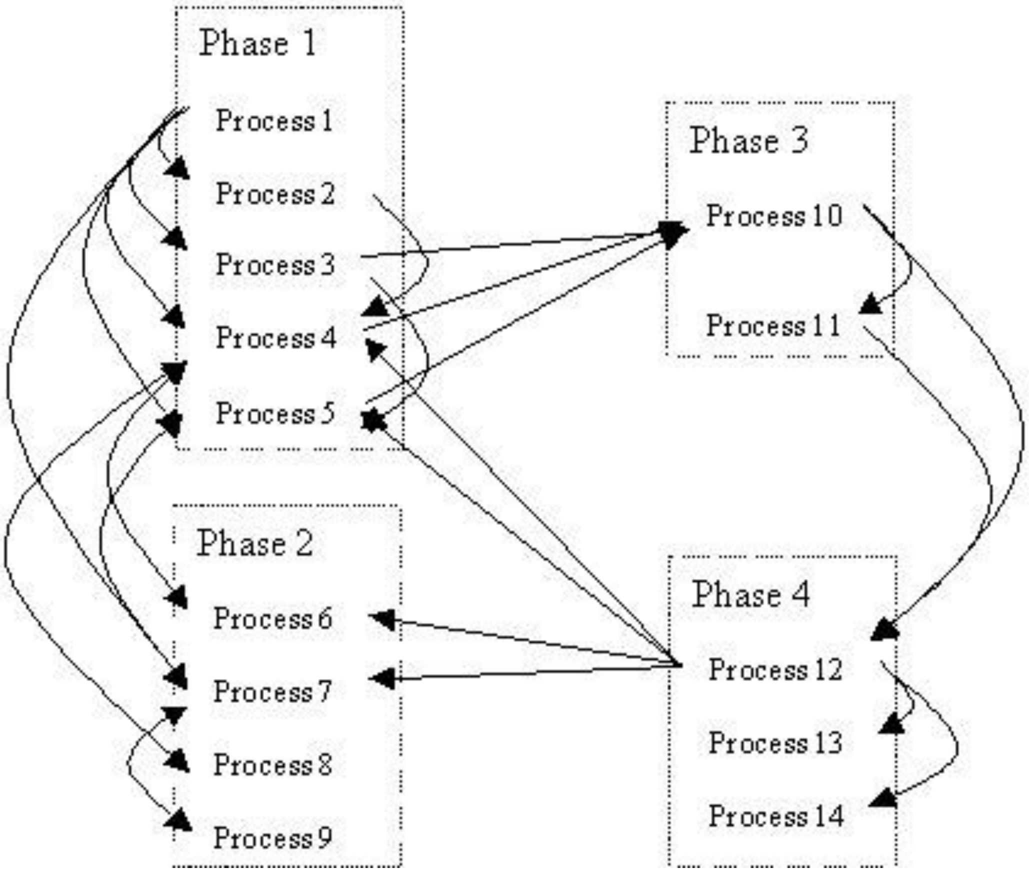


Figure 6 - TAME Data Flows

The formal entry point of the model is the Scope stage. As with all the experiments in the applied sciences field, it is essential to clearly define the scope and the boundaries of the experiment. The formal exit point of the model is the Evaluation stage. At the exit point, the management will be provided with the impact of each threat that the enterprise is facing, and with a shortlist of all those threats. The criteria for the short listing are: the importance of the threat, its impact to the business after its realization, and its complexity for occurring towards the system. As an extension to the methodology, a module can be developed to associate each threat with one or more countermeasures based on two standards: the Common Criteria and the ISO17799. The need for been accredited is partially discussed by Eloff (Eloff '00). The need for having an assessment standard has been discussed and accepted by the EU and is one of its main goals under the *e*Europe 2005 initiative.

A proposed "path" for "running" TAME is the following. First determine the Scope of the Assessment where the system will be described in detail. The business environment and the business processes will get analyzed and the stakeholders will get identified. The business analysis that is conducted in phase 1 will allow the identification of the business assets. In agreement with Nosworthy (Nosworthy '00) and Carroll (Carroll '96) the threat agent identification should be continuous. Hence, the Threat Agent Identification & Selection step is introduced in the scoping. The auditors should then conduct an analysis of the vulnerabilities and of the threat agents that the system is facing. Phase 2 is the Threat Agent & Vulnerability Analysis. After that we proceed to Phase 3, Scenario Construction & Modeling. In this phase, all the variables come together and the threats against the system are identified and evaluated. Here we construct one or more scenarios (depending on the threats that were identified and filtered) with the system under discussion, and the auditors model the system components that need further examination, using the information gathered in the Phase 1 Following that, we proceed to Phase 4. The stakeholders must evaluate the findings of the experiments and select the scenarios that will be further investigated. These scenarios will be unified and fused in one scenario. After the completion of the above steps, Process 13 will be able to estimate the impact of the identified threats to the various impact fields, and produce a statement based on the threat preference order. The methodology might be executed more than once. As the stakeholders are interacting with the experiment findings and the auditors, more information will surface and more variables will be introduced and/or excluded. The number of loops is left to the auditor. Presumably, each loop will provide the auditor with more detailed findings.

Example Scenario

KOMITIS is a unified Internet/mobile payment solution for contents and services, to be used in the so-called "Mobility Portals". A mobility portal is defined as Web/WAP information based system, which provides information or services related to mobility:

- Information related to a geographical position (which can be the position of the consumer or the one specified by him) or movement (how to go from a point to another one)
- Services like ticketing (entertainment, reservation, parking, etc.)
- Emergency services: reception of SMS signaling events (strikes or delays for travels, stock exchange conditions, etc.)
- Advertisement and advantages related to position or interest profile of the end-user.

A mobility portal has the major characteristics to address multiple terminals: fixed terminals like PC's or mobile terminals like mobile phones or PDA's. It also addresses multiple payment modes: aggregated and single payment.

The client can access the sites of on-line sellers to buy coupons, which are stored in the Core Payment System (CPS). The clients can then buy electronic/mobile contents using these coupons, which the CPS authenticates with an intermediary bank. Alternatively the client can pre-pay the bank and create an account with the system. The client can then use the CPS to buy e/m contents from online sellers, without dealing with the bank at all. The core system architecture combines an authentication layer at the CPS that connects to an aggregation engine and a single payment gateway that interfaces to an external payment system in charge of authorization and money transfers. Other important functional blocks are:

- Web back-offices: merchant back-office, consumer front-office, system/application back-office, that are all implemented as https portals,
- The system interconnection block.

The Core Payment System offers both aggregated and single payment mode, the authentication depending from the terminal capability. The KOMITIS model does not specify how the back-offices and front-offices work but only state their existence. Each implementation will use its specific interfaces. There are two specific and innovative solutions for on-line payments that will be used in the KOMITIS prototype. They represent state of the art solutions to the problem of open access aggregate payments with on-line central wallet and open access single payments. P-Wallet is a payment access solution that interfaces to multiple banking systems and to be more precise, SSL bank intermediaries. It can be used as a unique access point either for direct connections to central authorization/payment systems or to secondary access system like SSL intermediaries. P-Wallet is used for the single payments. Micro-CM is a typical third party aggregation system built for contents. It uses strong authentication through a security agent that wraps communication on http. Micro-CM is used for the aggregated payments.

Process 1: Business Analysis

Business Goal Analysis

Description: **Business goals will lead bring to the surface important variables for our assessment such as key assets and key vulnerabilities. Business goals will also give an indication about threat agents, as other enterprises with common goals will have to be included in the threat agent list.**

Inputs: Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Information Security Policy Document (I1.3)

Outputs: Business Goal List (O1.1), (Successful deployment of KOMITIS system to Hellas, Achieve a threshold of 1000 users during the first six months of operation, Maintain the above threshold as a minimum number of users during the first year of operation).

Business Process Analysis

Description: By identifying critical business processes we identify more assets, and we bring to the surface more vulnerabilities.

Inputs: Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Information Security Policy Document (I1.3), Knowledge of staff (I1.4), Organizational data (I1.5),

Outputs: Business Process List (O1.2), (Customer registration, Merchant registration, Contents management, Plafond authorization, Aggregated payment, Instant payment, Infrastructure, Human resource management, Money transfer).

Environmental Analysis

Description: Environmental analysis is based on the five forces approach that Porter proposes as a means of examining the competitive environment at the level of the strategic business unit. The environmental analysis will bring to surface more assets and help populating the threat agent table.

Inputs: Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Current knowledge of staff (I1.4), Organizational data (I1.5)
Outputs: Omitted due to size limitations.

Process 2: Stakeholder Identification

Identify Stakeholders

Description: Each computer system will have a set of stakeholders who can be used to define its function and form.
Inputs: Information Security Policy Document (I1.3), Current knowledge of staff (I1.4), Organizational data (I1.5), Service Level Agreements (I2.1)

Outputs: Stakeholder List (O2.1) (Bank, University, TelcomA, Soft-house A, TelcomB, Soft-house B)

Identify Stakeholder Responsibilities

Inputs: Business Process List (O1.2), Information Security Policy Document (I1.3), Current knowledge of staff (I1.4), Organizational data (I1.5), Service Level Agreements (I2.1), Stakeholder List (O2.1)

Output: Responsibility List (O2.2). The following figure illustrates the roles of the different stakeholders of the system.

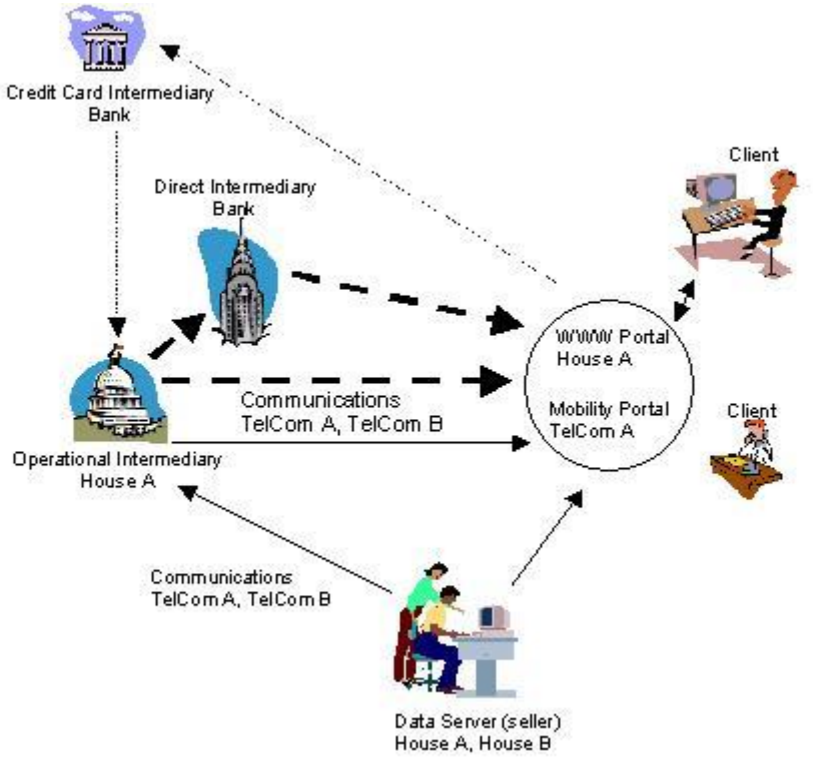

Credit Card Intermediary Bank
Direct Intermediary Bank
Client
WWW Portal House A
Mobility Portal TelCom A
Client
Communications TelCom A, TelCom B
Operational Intermediary House A
Communications TelCom A, TelCom B
Data Server (seller) House A, House B

Figure 7 – Stakeholder Roles

Process 3: System Boundaries Identification

System Identification

Description: In this activity the interfaces of the system under analysis will be identified. Furthermore the type of interaction that the system has with its surrounding environment through the above interfaces is also important. These interactions will help identify more assets and vulnerabilities.

Inputs: Stakeholder List (O2.1), Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Current knowledge of staff (I1.4), Service Level Agreements (I2.1)

Outputs: Boundary List (O3.1) (Firewall computers of the CPS, The KOMITIS gateway, the administrators/users of the system, the customers of the system).

Ascertain Control

Description: In this activity we ascertain who has control over each boundary, and what type of control it is.

Inputs: Boundary List (O3.1), Responsibility List (O2.2), Current knowledge of stakeholders (I1.2), Current knowledge of senior managers (I1.1), Current knowledge of staff (I1.4), Service Level Agreements (I2.1)

Outputs: Control List (O3.2). For presentation purposes the control list and the responsibility list have been integrated in Figure 7.

Process 4: Threat Agent Identification & Selection

Threat Agent Identification

Inputs: Threat agent catalogue (I4.1), History threat agent data (I4.2), Technical environment report (O1.3), Business environment report (O1.4), Physical environment report (O1.5), Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Current knowledge of staff (I1.4), Stakeholder List (O2.1).

Outputs: Threat Agent List (O4.1)

Threat Agent Type	Threat Agent Description
Industrial Espionage	
TA 1	
TA 2	
TA 3	
Organised Crime	
Mafia	International – Italian and Russian based. Historically dealing with money laundering, construction, protection, debt collection, gambling, prostitution, smuggling, and small businesses. This type is not considered to be of any consequence for the trial.
Hackers and Crackers	Individuals and hacker groups will have to be identified during the lifetime of the complete system. It is pointless to analyse all the active agents in Europe. History data can be gathered from the authorities. This type is not considered to be of any consequence for the trial.
Pressure Groups	
Anti-Capitalist	Support for action in a large number of countries (Kyoto, Seattle, Geneva). Documented violent actions. The level of founding that they have is unknown. The types of targets they have been after included: city centres, world bank meetings, and the financial sector. All their actions are centred on a high level of publicity.

Table 1 – Threat Agent List

The companies included in the above table are involved with one or more electronic payment systems, which are competitive to the KOMITIS system. We do not suggest that the companies will actively get involved in some sort of industrial espionage. The threat is always there though and it would be catastrophic to exclude them from the table of the possible threat agents. A complete assessment for the final system would include an in depth analysis of the above companies, of their capabilities and their actions since they were founded.

Threat Agent Selection

Description: This activity gives to the assessor the opportunity to select certain individuals or a certain threat agent category for further analysis, based on data received from the stakeholders of the enterprise, and from external threat agent sources.

Inputs: Threat Agent List (O4.1), Service Level Agreements (I2.1), Information Security Policy Document (I1.5), Current knowledge of stakeholders (I1.2)

Outputs: Threat Agent Preference List (O4.2), [TA 1, TA 2, TA 3]

Process 5: Asset Identification

Asset Identification Using Staff Knowledge

Description: This activity uses staff knowledge from all the levels of the enterprise, (staff-level, senior management, and stakeholders), to identify assets that are important for the operation of the system.

Inputs: Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Current knowledge of staff (I1.4), Asset register (I5.1)

Output: Asset List (O5.1)

Asset Classification	Main Categories	ID Number
Hardware	I/O devices	
	Smartcard reader	0038
	Central machine	
Software	Appli.KOMITIS.net	0012
	Lillo.telcom.it	0013
	Fire.telcom.it	0014
	Routers	0045
	Application	
	SNORT	0001
	ACID	0002
	RSBAC	0003
	PostgreSQL	0004
	Rsync	0005
	SSH	0006
	BIND	0007
	APACHE	0008
	Operating System	
	DEBIAN “Woody”	0009

	SunOS 5.7	0010
	Programs	
	Xalan-Java 2	0011
Data	Sensitive	
	Customer transactions	0039
	Customer orders	0040
	www.KOMITIS.net	0046
	DNS Data	0047
	Software Banners	0048
	Operations	
	Customer registration	0015
	Merchant registration	0016
	Contents management	0017
	Plafond authorisation	0018
	Aggregated payment	0019
	Instant payment	0020
	Money transfer	0021
	Key Management	0041
	Generating Keys	0042
	Transferring Keys	0043
	Verifying Keys	0044
	Financial	
	Customer Details	0022
	Personal	
	Customer Details	0023
	Personnel	
	User Accounts	0024
Administrative	Documentation	
	KOMITIS Deliverables	0025
	Security Policy Document	0026
	Operations	
	Procedures	
	Inventory records	
	Operational procedures	
Communication		
	SSL	0049
	XML	0050
Human Resources	Computer personnel	
	House 1	0027
	System programmers	0027a
	Administrators	0027b
	House 2	0028
	Web developers	0028a
	Context administrators	0028b

	telcom A personnel	0029
	telcom B personnel	0030
	security analysts	0031
	web developers	0032
	bank clerks	0033
Physical	Environmental Systems	
	Environmental controls in secure server room in NTSys premises	0034
	Building	
	Software house A	0035
	Telcom A	0036
	Bank	0037

Table 2 – Asset List

Asset Selection

Description: This activity gives to the assessor the opportunity to select certain assets or a certain asset category for further analysis, based on data received from the stakeholders of the enterprise, and from the other activities of phase 1.

Inputs: Asset List (O5.1), Technical environment report (O1.3), Business environment report (O1.4), Physical environment report (O1.5), Current knowledge of stakeholders (I1.2), Boundary List (O3.1), Business Process List (I1.2), Business Goal List (I1.1).

Output: Asset Preference List (O5.2), [Data Operations (Customer Registration, Money Transfer), Hardware (Central Machine (Appli.KOMITIS.net, Lilo.telcom.it, Fire.telcom.it))].

Process 6: Threat Agent Preference Structuring

Likelihood Analysis

Inputs: Threat Agent Preference List (O4.2), History Threat Agent Data (I4.2), Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Current knowledge of staff (I1.4).

Output: The activity does not produce a distinct output, but amends and updates O4.2

Threat Agent	**Likelihood**	**Importance**
Hackers and Crackers	0.5	3
TA 1	0	1
TA 2	0	1
TA 3	0	1

Table 3 – Threat Agent Preference List

Importance Analysis

Inputs: Threat Agent Preference List (O4.2), Technical Environment Report (I1.3), Business Environment Report (I1.4), Physical Environment Report (I1.5).

Output: Please refer to **t**able 3 as for presentation purposes the two tables were integrated to one.

Process 7: Vulnerability Identification & Selection

Vulnerability Type Structuring

Description: This activity examines the scope of the assessment, the reports describing the environment into which the enterprise is functioning, to identify the different types of vulnerability categories that exist in the enterprise. These categories will then be populated by the other activities of this process.

Inputs: Default Vulnerability Type Catalogues (I7.1), Technical Environment Report (I1.3), Business Environment Report (I1.4), Physical Environment Report (I1.5).

Output: Vulnerability Type List (O7.1) was omitted due to size limitations.

Vulnerability Type Selection

Description: This activity gives the assessor the opportunity to select certain vulnerability types and the vulnerabilities included in the relevant lists for further analysis, based on data received from the stakeholders of the enterprise, and from the other activities of phase 1.

Inputs: Vulnerability Type List (O7.1), Current knowledge of stakeholders (I1.2), Technical Environment Report (I1.3), Business Environment Report (I1.4), Physical Environment Report (I1.5)

Output: Vulnerability Type Preference List (O7.2) [Masquerading, Bypasses, Active Misuse, Pest programs]

Process 8: Threat Agent Attribute Calculation

Threat Agent Capability Calculation

Description: This activity calculates the capability of each selected threat agent to exploit the selected vulnerabilities of the assets that were included in the assessment from Phase 1.

Inputs: Threat Agent Metrics (I8.1), History threat agent data (I4.2), Threat Agent Preference List (O4.2), Vulnerability List (O7.3), Vulnerability Preference List (O7.4)

Output: The activity does not produce a distinct output. It processes and amends the Threat List (O10.1).

Threat Agent Opportunity Calculation

Description: This activity calculates the opportunities that are presented to each selected threat agent for exploiting the selected vulnerabilities of the assets that were included in the assessment.

Inputs: Threat Agent Preference List (O4.2), Current knowledge of stakeholders (I1.2), Technical Environment Report (I1.3), Business Environment Report (I1.4), Physical Environment Report (I1.5), Vulnerability List (O7.3), Vulnerability Preference List (O7.4).

Output: The activity does not produce a distinct output; rather it processes and amends the Threat List (O10.1).

Threat Agent Motivation Calculation

Description: This activity calculates the motivation of each selected threat agent for exploiting the selected vulnerabilities of the assets that were included in the assessment from Phase 1.

Inputs: Current knowledge of senior managers (I1.1), Current knowledge of stakeholders (I1.2), Threat Agent Preference List (O4.2), Threat Agent List (O4.1), History threat agent data (I4.2), Threat Agent Metrics (I8.1), Vulnerability List (O7.3), Vulnerability Preference List (O7.4)

Output: The activity does not produce a distinct output; rather it processes and amends the Threat List (O10.1).

Process 10: Scenario Generation

Threat Identification

Description: This activity uses the information gathered from most of the processes we have analyzed up to this point, for producing a list containing all the interactions between the identified threat agents and the identified vulnerabilities.

Inputs: Threat Agent List (O4.1), Threat Agent Preference list (O4.2), Vulnerability List (O7.3), Vulnerability Preference List (O7.4), Asset List (O5.1), Asset Preference List (O5.2)
Output: Threat List (O10.1), (Omitted due to presentation and size limitations, results can be seen in later processes.)

Scenario Construction

Description: In this activity all the threats that were identified in the previous activity are used by the assessors in order to construct attack scenarios.

Inputs: Threat List (O10.1)

Output: Attack Scenarios List (O10.2). The attack scenarios are summarized in the following table.

Scenario	Threat Agent	Asset
Scenario A: Intelligence	All	Disclosed

Gathering,		
Scenario B: System Penetration	Hacker, Cracker, Script Kiddies	Disclosed
Scenario C: Denial of Service	Hacker	Disclosed
Scenario D: SSL Attack	Cracker	Disclosed
Scenario E: XML Attack	Cracker	Disclosed
Scenario F: Man in the Middle	Hacker, Cracker, Organized Crime	Disclosed
Scenario G: Bad Customer	Corporate Agent, Organized Crime, Industrial Espionage	Disclosed

Table 5 – Summary of Attack Scenarios

The following table summarizes the tools used throughout the execution of the attack scenarios.

Tool	Use
Whisker	CGI vulnerability check
Retina	Vulnerability identification
Netrecon	Vulnerability identification
Nmap	Port scanning
telnet	Remote access
ftp	Remote access
Traceroute	Network reconnaissance
Dig / nslookup	DNS interrogation
Whois	Network enumeration (registrar query, organizational query, domain query)
Ping (gping)	Ping sweeps
PacketX	SYN flooding
Friendly Pinger	Network reconnaissance & enumeration

<Insert Table 6 – Security Tools used in Scenarios>

All the attack scenarios were conducted using a test-bed consisting of the assets that were involved in the assessment.

Scenario Unification

Description: In this activity the scenarios constructed in the previous activity are being unified in one report that combines all the different perspectives from each scenario.

Inputs: Attack scenarios List (O10.2)

Output: Unified Scenario (O10.3)

Process 13: Impact Analysis

Impact Field Identification

Description: This activity uses the environmental reports from Phase 1 to identify the different business fields that a threat might affect. Taking under consideration the unified scenario, we now know the business fields that are likely to be affected by the examined threats.

Inputs: Current knowledge of stakeholders (I1.2), Technical environment report (O1.3), Business environment report (O1.4), Physical environment report (O1.5),

Output: Impact Field List (O13.1)

Tangible Impact Analysis

Description: This activity uses the threat information gathered in Phase 3, and the asset information gathered in Phase 2 to calculate the impact of the threat to the enterprise.

Inputs: Threat List (O10.1), Impact Field List (O13.1), Asset List (O5.1), Threat Agent Preference List (O4.2)

Output: The activity does not produce a distinct output; rather it processes and amends the Threat List (O10.1), by updating the impact attribute of each identified threat.

Intangible Impact Analysis

Description: This activity uses the threat information gathered in Phase 2, and the asset information gathered in Phase 1, to calculate the impact of the threats that are associated with intangible assets.

Input: Threat List (O10.1), Impact Field List (O13.1)

Output: The activity does not produce a distinct output; rather it processes and amends the Threat List (O10.1), by updating the impact attribute of each identified threat.

Process 14: Threat Statement Generation

Each attack scenario discussed in process 10 represents a threat. Briefly the threats are: intelligence gathering, system penetration, denial of service, ssl attack, xml attack, man-in-the-middle (unauthorized transactions), bad customer (sabotage). The same threat can have a variety of impacts depending on its realization. For example if there is a system penetration followed by a denial of service during the early hours of a day, but the customers do not realize it, then the impact will be a lot less severe than what it could have been. As it was discussed is process 13 the severity of the impact can be: minor, moderate, major, catastrophic, and the different fields that can be affected are: the human resources, the supply chain, the market share, the business capital, and the user trust.

The intelligence gathering is a threat that will be manifesting in a daily basis. Although it cannot be avoided it will have to be controlled, as it can be the first step towards an active more catastrophic attack. Should all the proposed countermeasures are in place, and should the details that are available to the public are not considered to be sensitive or classified, then the threat will have no impact what so ever. On the other hand, if the publicly available details contain data that can lead to personnel and to suppliers it might have a minor impact towards the human resources and towards the supply chain. For example, the information included in the web site of the system could lead to an employee and identify him as the connection between the system and the bank. A hacker can use that information to start gathering personal information that will help him identify usernames and passwords. Even worse, if the threat agent involved, falls under the organized crime category, he can start harassing the individual to part with sensitive information about the system. Back to the hacker, the suppliers of the system can also be identified from the web site. As it was mentioned before, the weakest link destroys the game. The hacker can now exploit the systems of the suppliers in order to identify holes that will allow him to attack the KOMITIS system. Here is where the system boundaries come into play. If in the future, the enterprise start conducting business with external suppliers, then the new system boundaries must be identified and properly fortified.

The threat of the system penetration is a multi-layered one, depending on the asset that will be involved in the manifestation of the threat. If the system penetration is against any of the main hardware components of the system, and the attack is realized from the public, then even if it will have no other side-effects, the impact against the market share and the business capital will be major, and against the user trust it will be catastrophic. Furthermore if the threat agent penetrate the CPS, and get access in the financial and personal data of the customers, the impact against the market share and the user trust will be catastrophic. That is why the need for a multi-layered security is important. Just by securing the CPS with a firewall machine does not mean that the system is “hacker-proof”. As it was identified in phase 1, there is a need to have very strict user permissions and in such a way that no one (not even the root) will be able to perform any modifications without authorization.

The denial of service is a threat that is directly linked with the user trust and the market share of the system. As it was discovered when analyzing other electronic payment systems, the user trust is the most important aspect of such a system. If the customer does not feel secure and confident in using the system, then it will definitely not use it. This will affect the market share of the system and in an extent the business capital. The realization of a series of manifestation of the above threat will have a catastrophic impact towards the examined fields. We do not believe that a single isolated incident will have any effect what so ever as it will be perceived as a glints of the Internet. Of course the reaction time of the system administrators is of the essence. If the system is down for anything more than a couple of minutes, that the incident will not be perceived as a glints but as a serious problem. That is why the concept of robustness is very important. If the administrators have backup equipment that they can bring on-line, that will provide the appropriate contingency.

The administration of the CPS was a real concern. According to the information gathered in phase 1, each server is hosting an SSL secured Web site dedicated to the administrators. To access these administration sites, the client must provide a valid X509 certificate. In this analysis we demonstrated how the SSL protocol can be broken and how the X509 certificates be acquired from the servers. It is essential that administrative connections are not accepted from the outside world. The only machines that should be able to remotely administer the CPS should be dedicated machines, not connected to the Internet, based on the premises of the stakeholder hosting the CPS. The discussion on the administration of the CPS and the vulnerabilities that it introduces can be seen in process 7 and 10.

As we are dealing with an on-line payment system, host integrity is the only issue between success and failure. If there is a breach in the integrity of one of the servers, and that breach is realized by the public, then we have demonstrated how catastrophic the impact will be. It is essential that certain countermeasures be deployed, no matter the costs, for ensuring that the data stored in the CPS and in the MGW are only accessible by authorized parties and in authorized ways.

It is well accepted that a system is never 100% secure. A threat agent with the proper motivation and the technical and financial capabilities can bring the KOMITIS system to a standstill. As it was proven, for causing a catastrophic impact to the system one hasn't got to break the 128bit keys that the system is using, nor to decode an XML pipe and start performing man-in-the-middle attacks. These are attacks that require a very good technical understanding of the involved principles, as well as the way in which the system is behaving and functioning. It is very unlikely that an individual will be ever able to deploy such an attack. The problem though is that the system can be brought to its knees simply by causing a DoS, which will dissatisfy the customers and make them loose their trust towards the new on-line financial system.

Sun Tsu (Tsu '81) would be considered an IW expert should he was alive today. He had effectively described the principles of the science before even humans created the term. All modern nations have the capabilities and the motivation to proceed in such tactics, but do they have the opportunity? All companies involved in at least one level of E-Commerce must ensure that their systems are secure and do not provide threat agents with any kind of opportunities. It is the duty of every single organisation to ensure the security of the country in which it is established, in the same way as it is the duty of every soldier to ensure the security of his platoon. In IW the weakest link is not thrown out of the game, it destroys the game altogether. By using a third generation methodology such as TAME we bring all the sciences needed for a complete and meaningful threat assessment together.

TAME uses the assessor as an asset for better understanding the system that he/she is analyzing. One could say that it is a chaotic theory, which is trying to model the chaotic nature of the threat. Furthermore, because time is considered to be a constraint, most of the steps have no pre-requisites. Although it is not easy to use a UML activity diagram to model TAME, this is not a drawback. Traditional techniques cannot be used for modeling threats. People and professionals, who insist in doing that, should reconsider unless they want more catastrophic incidents with world wide impact to take place.

Threat Mitigation:

In the digital age, intellectual property, personal and financial information, and other sensitive data types are at an increasing risk. Targeted attacks by Advanced Persistent Threats (APT) are becoming more and more widespread. APTs are the modern electronic versions of covert intelligence operations. *Advanced* here is defined as "sophisticated combination of multiple targeting methods, tools and techniques in order to reach and compromise target and maintain access to it." On the other hand, persistent is defined as "conducted through continuous monitoring and interaction in order to achieve the defined objectives". Threats comprise of both capability, intent and a level of coordinated human involvement.

A good case study for APT is the Stuxnet attack which occurred in 2010. Stuxnet is a sophisticated computer worm that infected Siemens' SCADA systems. This is a classic example of cyber attack targeting critical sectors. The attacks were primarily directed towards Iranian nuclear facilities, but there were also reports claiming that other countries such as India, Indonesia and Russia were also affected. Stuxnet is said to be the first known worm designed to target real-world critical sectors such as nuclear plant, power station and industrial unit. Some experts even believe that that Stuxnet is a government produced worm.

APT EXPLOITATION LIFE CYCLE

The APT exploitation life cycle involves reconnaissance, initial intrusion into the network, establishing a backdoor into the network, obtaining user credentials, installing various utilities, privilege escalation/lateral movement/data exfiltration and maintaining persistence. The explanation of each life cycle is explained below:

- Reconnaissance - Identify individuals of interest and develop methods of access.
- The targets range from executives to researchers to assistants.
- Initial intrusion into the network - Utilize several techniques to gain initial access.
- The most common form is social engineering combined with e-mail; e.g. spear phishing.
- Establishing backdoor into the network - Establish footing in the system using malware and move laterally to install multiple backdoors.
- Obtaining user credentials - Obtain domain controller credentials to allow operation within the network.
- Installing various utilities - Utility programs install backdoors, dump passwords, obtain e-mail from servers and list running processes to steal targeted information.
- Privilege escalation/Lateral movement/Data exfiltration - Exfiltrate data by compressing into smaller files and moving to a server in the APT's command and control infrastructure.
- Maintaining persistence - When backdoors are discovered, it will continuously evolve to gain additional footing and maintain position.

CHALLENGES

There are numerous challenges in achieving the high level of vision and knowledge required in order to address the threat of a targeted attack. Some of these challenges include:

- Organization usually has an extremely large database and information management environment. Trying to find certain information is like *looking for a needle in a haystack*. It is very difficult, if not impossible to find among everything else around it.
- Attackers are skilled at hiding in plain sight
- Anti-forensic techniques are being used more frequently
- Complexity, diversity, and lack of standardization are often a factor

Possible questions that should be thought about regarding specific information security practices are as follows:

- How do we track what digital information is leaving our organisation and where that information is going?
- How do we know who's really logging into our network, and from where?
- How do we control what software is running on our devices?
- How do we limit the information we voluntarily make available to a cyber adversary?

INCIDENT RESPONSE AND HANDLING

As attacks on information systems become more sophisticated and severe, it is important to develop a well-defined incident response capability. A dependable incident response program helps to quickly detect security incidents, minimize losses and destruction, identify weaknesses, and restore information technology operations rapidly.

There are four possible stages in incident response and handling as follows:

- Preparation - Ready to respond before an incident actually occurs. This stage is extremely important because many of today's incidents are so complex and time consuming that preparation is a necessity, not a luxury. Some basic notions behind preparation are setting up a reasonable set of defences/controls based on the threat that presents itself, creating a set of procedures to deal with incidents as efficiently as possible, obtaining the resources and personnel necessary to deal with the problem and establishing an infrastructure to support incident response activities.

- Detection and Analysis - Detection determines whether malicious code is present, files or directories have been altered, or other symptoms of an incident are present and, if they are, what the problem as well as its magnitude is. Detection is very important. Without detection, there is no meaningful incident response and detection triggers incident response. Sometimes, very small symptoms may indicate that an incident is in progress and therefore, analysing every anomaly that can be found is a very good measure.

- Containment, Eradication and Recovery - Containment is to limit the extent of an attack and thus the potential damage or loss. Containment-related activity should occur only if the indications observed during the second stage conclusively show that an incident is occurring. Eradication is to eliminate the cause of the incident, while recovery involves system and data recovery as well as providing back-up files.

- Post-Incident Activity - To review and integrate information related to an incident that has occurred. This stage is extremely critical, in that it is hard to envision a successful incident response effort if it is omitted.

Cyber space is borderless and difficult to control, and it is seemingly vulnerable to criminal and terrorist attacks. It provides the room for individuals with the necessary skill and capability to cause damage; even to a nation. Cyber attacks are relatively so much easier to launch compared to conventional military attacks. The constantly increasing number of security incidents in Malaysia is indeed worrying, given the high and rapidly growing rate of Internet usage in the country. Technological threats such as cyber crime and cyber terrorism require immediate attention and critical analysis by nations worldwide. For example, there is still a need for improvement of cyber laws and regulations in the country. At the same time, the competency level of the enforcement agencies must also be further improved to deal with the growing sophistication involved in cyber threats. Malaysia is committed in countering cyber crime and cyber terrorism by implementing and enhancing critical information infrastructure protection to ensure a trusted, secure and sustainable online environment. Cyber security requires both national and transnational mechanism to deal with threats.

References

(Ammann '02). Ammann, P., D. Wijesekera, et al. (2002). "Scalable, Graph-Based Network Vulnerability Analysis." Computer & Communication Security 18(22): 217-224.

(Barber '01). Barber, R. (2001). "Hacking Techniques." Computer Fraud & Security 2001(3): 9-12.

(Bennett `99). Bennett, S., McRobb, S and Farmer, R. (1999). Object-oriented Systems Analysis and Design Using UML. McGraw-Hill , England, pp61-72.

(Bequai '01). Bequai, A. (2001). "Organised Crime Goes Cyber." Computers & Security 20(6): 475-478.

(Blyth '01). Blyth, A. J. C. and L. Kovacich (2001). Information Assurance: Computer Communications & Networks, Springer-Verley.

(Carroll '96). Carroll, J. M. (1996). Computer Security, Butterworth-Heinemann.

(Coad '91). Coad, P. and E. Yourdon (1991). Object-Oriented Analysis, Prentice Hall Inc

(COPS '02). COPS (2002). Computer Oracle & Password System. 2002.ftp.cert.org/pub/tools/cops

(Embley `92). Embley, W. D., Kurtz B. D., Woodfield, S. N. (1992). Object –Oriented Systems Analysis: A Model-Driven Approach. Prentice-Hall, inc., New Jersey, US, pp1-52.

(Forte '00). Forte, D. (2000). "Information Security Assessment: Procedures & Methodology." Computer Fraud & Security 2000(8): 9-12.

(Godsil `01). Godsil, C. and Royle, G. (2001). Algebraic Graph Theory. Springer-Verlag New York, Inc., United States of America.

(Hinde '01). Hinde, S. (2001). "Cyberthreats: Perceptions, Reality and Protection." Computers & Security 20(5): 364-371.

(Hoath '98). Hoath, P. and T. Mulhall (1998). "Hacking: motivation & deterence, part 1." Computer Fraud & Security 1998(4): 16-19.

(Icove '95). Icove, D., K. Seger, et al. (1995). Computer Crime: a crime fighters handbook, O'Reilly & Associates.

(Kabay '96). Kabay, M. E. (1996). Enterprise Security: Protecting Information Assets, McGraw-Hill.

(Keeney '93). Keeney, R. L. and H. Raiffa (1993). Decisions with Multiple Objectives, Press Syndicate of the University of Cambridge.

(Storey '96). Storey, N. (1996). Safety Critical Computer Systems, Addison Wesley.

(Leveson '95). Leveson, N. G. (1995). Safeware: system safety & computers, Addison Wesley.

(Manasse '95). Manasse, M. (1995). The Millicent Protocols for Electronic Commerce. 1st USENIX workshop on Electronic Commerce.

(Merris `01). Merris, R.(2001). Graph Theory.John Wiley & Sons, inc., US, pp171-175, 31.

(Moore '01). Moore, A. P., R. J. Ellison, et al. (2001). Attack Modeling for Information Security and Survivability, Carnegie Mellon University: 1-21.

(Morakis `03). Morakis, E., Vidalis, S., Blyth, A.J.C. (2003). A framework for representing and analysing cyber attacks using object oriented hierarchy trees. In proceedings of the Second European Conference in Information Warfare, UK, pp235-246.

(Nuemann '95). Nuemann, P. G. (1995). Computer Related Risks, Addison-Wesley.

(O'Mahony '97). O'Mahony, D., M. Peirce, et al. (1997). Electronic Payment Systems, Artech House Inc.

(Pfleeger '97). Pfleeger, C. P. (1997). Security in Computing. Prentice Hall Int.

(Rees '96). Rees, F. (1996). "New perspective on computer hackers." Computer Fraud & Security 1996(6): 8.

(Scambray '01). Scambray, J., S. McClure, et al. (2001). Hacking Exposed: network security secrets & solutions. Osborn/McGraw Hill.

(Smith '93). Smith, M. (1993). Commonsence Computer Security: your practical guide_to information protection. McGraw-Hill.

(Stalling '00). Stalling, W. (2000). Network Security Essentials. Prentice Hall.

(Summers '77). Summers, R. C. (1977). Secure Computing: threats & safeguards, McGraw-Hill`.

(Sykes '81). Sykes, J. B. (1981). The Concise Oxford Dictionary, Clarendon Press.

(SystemScanner '02). SystemScanner (2002). Internet Security System: System Scanner. 2002.www.iss.net

(Vidalis '01). Vidalis, S. (2001). TAMMPS: a threat assessment model for micro-payment systems. School of Computing. Pontypridd, University of Glmaorgan: 1-152

(Vidalis `03). Vidalis, S., Jones, A. (2003). Using Vulnerability Trees for Decision Making in Threat Assessment. In proceedings of the Second European Conference in Information Warfare, UK, pp329-338.

Cyber Storm-Case Study

Recognising the increasing reliance of government, business and home users on information and communication technologies, the Australian Government established the E-Security National Agenda (ESNA) in 2001 to create a secure and trusted electronic operating environment for both the public and private sectors. As an outcome of a 2006 review, the Attorney-General's Department was tasked to develop a cyber exercise program to improve the ability of governments and critical infrastructure owners and operators to manage incidents affecting the National Information Infrastructure. As part of this role the Attorney-General's Department coordinated a national cyber exercise, Cyber Storm II, which formed part of a larger international exercise and was designed to align with national e-security objectives.

In February 2006 the US Department of Homeland Security (DHS) National Cyber Security Division conducted the first US National Cyber Exercise, Cyber Storm, as part of its own national cyber exercise program. The Australian Government participated in Cyber Storm, conducting a discussion exercise. The second US national exercise was scheduled for March 2008, and the US invited Australia, Canada, New Zealand and the United Kingdom to participate.

Cyber Storm II was structured and executed as a large-scale national exercise within an international framework. This structure allowed participants to exercise their internal incident response and communications in a national framework that allowed external communications to be more than notional and which encouraged a collaborative response. It provided a unique opportunity for stakeholders across the spectrum of e-security and critical infrastructure protection in Australia to participate in a global cyber exercise aimed at testing the decision-making which underpins any technical response. Cyber Storm II participants included Australian Government agencies, State and Territory governments, industry groups and private companies drawn from the IT industry and four critical infrastructure sectors - Water, Banking and Finance, Energy and Communications. Each participating organisation designed their exercise play to meet internal objectives while utilising the international framework and the extensive player set to realistically test their response and recovery to a large-scale cyber attack.

The exercise was conducted from 10-14 March 2008. The Australian component of Cyber Storm II was coordinated by an Australian Exercise Control Centre (AuExCon) established near Melbourne. Participants played the exercise from their usual work places using, where possible, normal communications channels.

This report is a consolidation of findings, observations, and lessons learned throughout the planning and execution of Cyber Storm II. It is a compilation of observations provided by participants in a ‘hotwash’ debrief held immediately after the exercise, and in more formal one-on-one debriefings conducted in the weeks following the exercise.

There are three points to bear in mind while reading this case study:

i. Cyber Storm II was conducted as a “no-fault” exercise. The purpose of Cyber Storm II was not to obtain a stock-take of participant’s internal crisis management arrangements;

ii. Cyber Storm II was not a test of the resilience of participant’s networks to cyber attack. The starting point for the exercise was that the adversary had sufficient time, money and motivation to penetrate any network; and

iii. the findings and supporting comments in this case study represent a wide range of opinions from a diverse player set. All are generalised to some extent – some are common observations, others the views of one or two players. This case study should be read from the perspective of “could this apply to my organisation” rather than “who said that”.

Background

Purpose

Australia’s first national e-security exercise was designed to support the goals of the Australian Government’s E-Security National Agenda, encourage information sharing across various boundaries, and importantly, to facilitate participating organisations to meet their own internal objectives.

The exercise enabled participants to test their response and recovery capabilities, test their information sharing arrangements and to promote awareness of e-security within their own organisation. The exercise scenarios were based on participants’ objectives and designed to stimulate technical, operational, communication and/or strategic responses to cyber incidents with a view to reviewing and refining current arrangements.

Concept

Planned in close coordination with, and driven by, its stakeholders and participants, the exercise focused on a series of cyber-specific events which were intended to escalate to a level requiring a coordinated national response. The adversary in Cyber Storm II utilised coordinated cyber attacks on the selected sectors to meet a specific political and economic agenda. A basic assumption within the exercise was that the adversary had sufficient resources and motivation to mount and successfully execute these attacks. The resulting impact on global cyber infrastructure, and associated physical infrastructure, was designed to prompt coordinated responses from the Australian Government and from within relevant industries, and to emphasise the interdependencies that exist in critical infrastructure and the national information infrastructure.

Scope

The scope of the exercise was defined to maximize the participants’ ability to assess, test or validate:

- the full range of incident response and recovery mechanisms (technical, operation and strategic),
- the spectrum of players involved from multiple sectors, across government and the private sector,
- internal and external communications of organisations and sectors and with government, and
- the need for continuing improvement to cyber security procedures and processes.

Objectives

As a stakeholder-driven exercise, the objectives of participating organisations are broadly summarised to include the following objectives:

- to examine internal capabilities to respond to, and recover from, a cyber attack,
- to validate, examine and exercise information sharing relationships and communications paths for the collection and dissemination of cyber incident situational awareness, response, and recovery information,
- to promote awareness and education of appropriate points of contact and correct procedures to use when responding to a cyber incident, and
- to exercise, examine and validate international communication, cooperation and collaboration between participating governments.

Scenarios

Australian participants played varying combinations of 12 scenarios, some of which were intended to provoke international play. Scenarios were designed largely by the participants to meet their internal exercise objectives. All elements of these activities were simulated and did not impact any live networks - there were no physical consequences as a result of any of the scenarios. Scenarios ranged from widespread internet degradation, to attacks on Supervisory Control and Data Acquisition (SCADA) systems, through to the compromise of a Certificate Authority.

Media Outreach

The communication ‘real world’ media strategy to promote Australian participation in Cyber Storm II was prepared by the Public Affairs Branch of the Attorney-General's Department. The communication strategy was developed to:

- increase awareness of e-security issues;
- promote Australian involvement in Cyber Storm II;
- publicise the event; and
- manage media issues as they arose.

Australia’s participation in Cyber Storm II was conducted in accordance with existing national security arrangements with the aim to build on the outcomes of the first Cyber Storm exercise. The Australian Government has a close working relationship with the business community and Cyber Storm II aimed to further develop that relationship**.**

Planning and Execution

Cyber Storm II planning took 18 months. The Attorney-General’s Department provided a framework in which participants could run an internal e-security exercise in conjunction with many of their suppliers and/or customers. The main benefit was that external relationships, so often notional in a purely internal exercise, could be tested.

This planning period was valuable not only to facilitate a world class exercise, but also as it enabled robust information sharing, and encouraged private-public sector relationships and coordination across industries and between competitors. Many participants also noted that the design process assisted them to engage various disparate sections of their organisation, creating convergence between business interests and technical expertise in crisis management communication.

Others noted that the mere fact of participating in the planning process caused them to review (and in many cases repair) existing plans and processes.

The Master Scenario Event List (MSEL)

The MSEL provided the unfolding exercise scenario inputs in a manageable and observable format. This list was comprised of individual events, referred to as MSEL injects, that were "injected" into play throughout the exercise in various forms. Scripts for phone calls, emails, faxes and news media articles were developed. The MSEL injects also contained the expected player actions to assist the planners and observer/controllers in measuring player response. While much of the information in the database was scripted, the members of exercise control sometimes had to execute dynamic play in direct response to actual player actions. Key exercise control planners from participating organisations were intimately familiar with their respective organisation's business, making them uniquely qualified to simulate the adversary, similar to the role of a "red team." Assuming this kind of role provided the flexibility to increase or decrease the intensity of attacks or alter attack vectors.

The MSEL management process utilised a software tool provided by the US Department of Homeland Security.

Milestones in the planning process were marked by planning conferences. The following is a breakdown of the 18-month planning and design period.

Concept Development Conference (CDC) to Initial Planning Conference (IPC)

In December 2006 the US held a concept development conference that gathered stakeholders, including Australia, to set out the exercise scope, goals, and objectives. The US exercise was planned using the concept of exercise 'threads' -working groups that consolidated planning for each critical infrastructure sector involved in the exercise. Planners in the US worked in eight threads representing the chemical sector, the transportation sector (specifically rail and pipelines), Federal, States, international, information technology/communications (IT/Comms), law enforcement/intelligence (LE/I), and public affairs. The dedicated participation of the Federal and public affairs threads were a result of needs identified in Cyber Storm I. Australia followed this model, creating planning threads for banking and finance, water, electricity, communications, information technology, government and public affairs.

In March 2007, the growing Cyber Storm II community met in Washington at an IPC to finalise objectives and develop primary scenario paths. The IT/Communications thread produced a scenario menu which catalogued potential scenarios, and the Law Enforcement/Intelligence (LE/I) thread began crafting the adversary for the exercise. Australia was represented at this meeting in the US IT/Communications, LE/I and international threads.

In May an Australian IPC was held in Sydney. The point of the conference was to introduce the planners from the various participating organisations and to finalise exercise objectives for each of the participant's internal exercises.

IPC to Midterm Planning Conference (MPC)

Planners focused on scenario concept design and development during this period, with threads beginning to craft scenarios that met their objectives and examined perceived vulnerabilities. A 'trusted agent' community, bound by signed agreements, enabled the sharing of sensitive information across industry and government via the US Computer Emergency Readiness Team (US-CERT) portal. By the MPC, scenario concepts were formed and in the US the adversary framework was established.

MPC to Final Planning Conference (FPC)

Planners continued to develop depth in scenarios by confirming attack vectors, adversary requirements, business impacts and expected player actions. In the US, LE/I planners worked with other threads to assist shape malicious activity and coordinate adversary relationships. At the FPC, planners were required to report their progress on scenario injects to reconcile timing and other conflicts. In most cases, this was not actually achieved until the Final MSEL Conference (FMC). At the FPC, exercise planners were also familiarised with exercise mechanics issues such as establishing player sets and exercise contact lists, and the role of Observer/Controllers. Planners at the MPC were also trained in the use of the MSEL management tool.

FPC to Final MSEL Conference (FMC)

Following the FPC, planners began inputting scenario content into the MSEL tool. Thread meetings were held for various sectors in order to foster coordinated and coherent scenario development. In February 2008 planners met at the FMC to complete an inject-by-inject review of the exercise scenarios. Planners also learned about exercise control mechanics and protocols and Observer/Controller training requirements.

Pre-Exercise build-up (Pre-Ex) and Execution

The pre-ex period, which began in February 2008, was designed to prompt the identification and discussion of information sharing requirements between participating law enforcement, intelligence and private sector communities in preparation for the exercise.

The exercise was conducted in March 2008. AuExCon, located in the Yarra Valley, served as the national coordinating body for the Australian exercise. USExCon was located in Washington DC. AuExCon was in frequent contact with the US ExCon regarding the exercise mechanics and in order to facilitate international exercise play. The concept of a centralised coordinated exercise with decentralised execution was designed to be both practical and realistic for the players involved in the exercise across Australia and internationally.

At AuExCon, 45 individuals representing public and private sector organisations, sectors and industry groups monitored exercise play at the external locations through regular contact with observer/controllers via phone and email. Exercise control staff also responded to requests for information from players, coordinated real-time injects to facilitate play and supported all stakeholders to ensure objectives were met. Some Exercise control staff also simulated those entities not represented in the player set and notional companies.

The Cyber Storm II MSEL was the driver for the entire exercise. It was the MSEL injects that set the pace of the exercise and elicited player responses

Each thread leader was responsible for making coordinated and informed thread decisions. Thread leaders monitored MSEL injects and overall thread play. They also worked closely with the Exercise Managers, who also monitored upcoming injects, coordinated injects with each thread, verified the timing and validity of injects, and ultimately sent injects to players. As Cyber Storm II unfolded, the exercise design provided thread leaders and planners the flexibility to create new MSEL injects or alter existing injects to facilitate a logical game flow. These new or altered injects went through the same coordination process with subject matter experts in the relevant threads prior to dissemination, albeit on an expedited timeline. Planners and observer/controllers tracked inject edits and status changes throughout the exercise through the MSEL management tool and discussions with exercise control personnel.

Given the time zone differences, play ranged from 0700hrs to 2300hrs during the course of the 3-day exercise, though the majority of play occurred between 0800 hrs and 1800hrs, Australian Eastern Summer time. At the conclusion of each day’s play, thread leaders and the exercise management team met to assess key issues, exercise conditions and to provide a summary of the day’s play in preparation for the following day. On the last day, exercise control staff, the exercise management team and most observer/controllers attended a ‘hotwash’ debrief session at AuExCon to gather initial observations of the exercise play and key lessons learned.

Security Policy

The goal of Cyber Storm II information security policy was to ensure that any sensitive information shared during the exercise was only used for the stated objectives. The willingness of participants to disclose potentially sensitive information was one of the key factors in the success of the exercise, since it allowed:

- the development of plausible, realistic and meaningful scenarios to maximise the value of the exercise,
- planners to understand the implications of specific attacks on their infrastructure, and
- planners to understand the responses expected from other planners and players from an organisational perspective.

The Cyber Storm II information security policy involved a multi-layered approach that included creating a trusted community and a secure network environment for exercise planning and execution.

A Trusted Agent Agreement (TAA) was signed by all planners in Australia and essentially required individuals to comply with the US Department of Homeland Security Management Directive 11042.1: “Safeguarding Sensitive but Unclassified (For Official Use Only) Information.” Australian planners signed a version of the agreement consistent with applicable Australian law and all planners world wide signed a version of a similar agreement. Australian Government employees signed an acknowledgement of their responsibilities under both the *Public Service Act 1999* (Cth) and the *Crimes Act 1914* (Cth).

The obligations imposed upon exercise planners included a duty not to disclose any content containing any patent, trademark, trade secret or any other proprietary rights of any party. These obligations did not alter the obligations or release signatories from their responsibility to comply with contractual or fiduciary arrangements, obligations, or applicable international or Australian laws relating to the disclosure of sensitive information.

Participants also agreed to adopt practices designed to reduce the possibility of security breaches and the introduction of malware into exercise systems and databases. All participants in the Australian national exercise have complied with these agreements for the duration of the planning, execution and “after action” processes.

Significant Findings

Observations recorded during the exercise and in the post-exercise debriefs revealed several significant findings. Comment on these arrangements focused on communication and escalation paths, organisational roles and responsibilities, and information sharing and coordination among organisations. The findings were determined with reference to the overarching objectives of the exercise and the findings included in this case study reflect those that are applicable to both the private and public sector. Observations by individual organisations or sectors are grouped below to support these significant findings.

Many participants noted that merely planning the exercise prompted internal reviews and modifications to their existing crisis arrangements.

Finding 1: Effective response is enhanced by routinely reviewing and testing Standard Operating Procedures (SOPs), Incident Response Plans and /or crisis management arrangements.

Effective response to a cyber crisis is significantly enhanced by having tested procedures or arrangements, in which crisis-management relationships in the cyber response community are regularly reviewed to solidify communications paths and clarify organisational roles.

Observations:

a. Coordinated responses to an e-security crisis are required across the critical infrastructure protection community. Processes were often found to be oriented toward the mitigation of, and response to, physical threats. More tailored and coordinated security response measures are needed to address cyber incidents, particularly when cyber threats have impacts across sectors.

b. Participants noted that their own internal response mechanisms could be improved. Clarification of escalation procedures internally and externally, in addition to the identification of a communication plan to facilitate closer working relationships between business areas within organisations, were two common themes.

c. Participants noted that in some circumstances formal processes tended to be circumvented under pressure or were not activated in a timely manner.

d. Organisations that acted as information clearing houses or coordination bodies were under intense pressure during the exercise due to the number of scenarios. Where formal protocols existed, under stress these tended to give way to informal processes. During a crisis the balance between formal and informal information sharing is likely to favour informal communication in order to facilitate rapid responses. It was also noted that informal processes outside of standard procedures could allow information to be lost.

e. Many participants stated that a key value of Cyber Storm II was the opportunity it provided to test their internal procedures in a realistic scenario that included external stakeholders. This external element enabled organisations to assess their procedures more accurately and many participants cited this as a major benefit of Cyber Storm that cannot be replicated by exercising internally.

Finding 2: Non-crisis interaction among key stakeholders enhances effective crisis response during an incident.

More frequent, non-crisis interaction between various stakeholders involved in protecting the national information infrastructure will enhance real world response capabilities. Established relationships facilitate rapid information sharing among community members and must include relationships across sectors, with suppliers, with vendors and with incident response organisations.

Observations:

a. The coordinated attacks simulated during Cyber Storm II highlighted the importance of pre-existing relationships between organisations prior to a crisis. This was particularly important in developing accurate situational awareness. Participating organisations commented that maintaining situational awareness across related critical infrastructure sectors during a cyber attack was critical to ensuring effective response and recovery.

b. Many participants reported that the exercise assisted in developing stronger relationships across and within sectors. A common theme was that the 18 month planning process allowed relationships to be built up that would help in a genuine crisis. Most participants found Cyber Storm II to be a trust-building exercise which will lead to greater information sharing and closer cooperation between participants in the real world.

c. Participants noted that the internal communication between business areas in their organisation improved during Cyber Storm II. Participants also commented that the exercise, both in the planning and the execution, forced the organisation to engage across the whole business to address issues. This drove home the need to routinely engage with different business groups on cyber issues and as a result some organisations have already begun to identify an internal communication plan to facilitate closer working operations between different business areas. One participant found that the exercise identified many working groups that are dealing with substantially the same issues but were not aware of the commonality (due to the scale of the business).

d. Many participants relied on sector-specific relationships (developed through Infrastructure Assurance Advisory Groups, for example) as focal points for sharing information during the exercise. In a coordinated attack, the underlying questions are how to contact another organisation similarly affected and who to contact within that organisation. This is especially true where there is no pre-existing relationship. Existing relationships are crucial as organisations are not able to create trusted relationships in the centre of a crisis.

e. Interaction between participating private organisations and Australian Government agencies differed greatly between sectors. Some players noted that internal education on engagement with Government and law enforcement agencies would be undertaken following the exercise. Interaction outside established lines of communication between industry and law enforcement was a beneficial outcome of the exercise.

Finding 3: Crisis communication procedures, predicated on accurate and appropriate points of contact, must be formalised within contingency planning.

Communication during a crisis significantly impacts the timeliness and effectiveness of responses. A unity of effort can be more effectively maintained when there is a clear understanding of roles and responsibilities and the interfaces between them.

Observations:

a. Greater clarity of roles and responsibilities at every level of response will greatly increase the ability of organisations to harness their own resources to address incidents. Coordination and cooperation internally within organisations was most efficient when roles and responsibilities were clearly defined. Likewise, communication between organisations was most effective when organisations had already identified who was responsible for what areas within external organisations.

b. The exercise enabled players across sectors and government bodies to test and, in some cases, develop crisis communication procedures to respond to a cyber security incident. It was a common finding that crisis management procedures were oriented towards mitigating physical threats and that cyber incidents will require additional contacts within an organisation. Raising awareness around cyber incident response and how it differs from other emergency management responses was a valuable exercise outcome for many players and participants have indicated that they will further promote e-security education internally.

c. A tangible result from the exercise for one participant was identification of the appropriate person to attend crisis management meetings during an e-security incident. This organisation found that during the exercise those attending the crisis meeting did not have the appropriate expertise. They identified a need for a high-level decision maker supported by a technical expert. This person has since been appointed

d. Another participant discovered that their contractual arrangements outlining crisis communications did not reflect reality. The organisation has already reviewed these disparate arrangements and refined the protocols (including updating contact lists), to ensure consistency of real practice with SOPs.

Finding 4: Cyber crises require a tailored response that takes into account multiple interdependencies.

The borderless nature of cyber attacks, and the speed with which they can escalate across infrastructure sectors, was demonstrated in Cyber Storm II. Contingency planning must include potential flow-on effects.

Observations:

a. Organisations noted that participation in the exercise was critical in exploring unforeseen interdependencies and escalation paths within and across sectors. An important learning was the need to formalise lines of communication between Government and industry to ensure that the scope of any problem is properly understood to enable a coordinated and effective response.

b. Interdependencies within organisations were also explored during the exercise. Some industry players noted that a key value of the exercise was the opportunity it provided to stimulate the convergence of business and technical expertise in responding to incidents. Cyber Storm II was the impetus for ensuring more effective communication within separate functional areas for many organisations. A major benefit for one player was demonstrating the need to routinely engage with different functional areas on cyber issues.

c. Several participants observed that more interaction across borders and sectors will improve the response capabilities of all concerned. One participant commented that Cyber Storm II amply demonstrated the benefit in “more people from more areas talking more often” about cyber security.

d. One participant found that interdependencies existed within their own disparate functional business units, in addition to those discovered across sectors. For example, communication interdependencies were illustrated in relation to SCADA systems where visibility and ability to manage SCADA systems are compromised once communications are affected. When power supplies are affected by SCADA problems, the communications systems fail to function. One organisation has identified the need to test interdependencies in internal systems and between sectors in more depth in future exercises as a priority.

e. Another participant noted that a unique benefit of the exercise was the opportunity to detect new areas of possible risk by observing the play of others. They gathered invaluable information from watching the finance sector exercise.

Finding 5: Developing internal reporting and external notification thresholds assists in effective incident response by creating better situational awareness.

Identifying the problem, rather than simply addressing the symptoms, is critical to effective cyber incident response. In order to ensure situational awareness within and between organisations, clear notification thresholds should be developed and promulgated so that technical incident responders know when escalation internally or externally is necessary.

Observations:

a. It was a common finding amongst participants that IT incident responders tend to focus on managing incidents rather than addressing the wider problem and its ramifications. A common observation was the tendency among IT incident responders to instinctively minimise the scale of the problem and to focus on what they knew or could manage when reporting to management. Many participants noted a need to educate incident responders to brief management on the limits of their understanding of problems, and the possible broader exposure faced by the organisation.

b. The natural tendency to minimise the scale of the problem was also found to be true in many crisis committee meetings that were convened during the course of the exercise. Incident management meetings need to ask what the exposure ‘might’ be at worst case and develop strategies to minimise impact. They need also to be able to accept that the responders may not have all of the answers.

c. A common problem, particularly in coordination centres, was that while responding to multiple incidents the responders failed to realise that there was a crisis. The focus tended to be on what was broken or performance metrics.

d. One player stated that an exercise outcome was the clarification of guidelines to support escalation of IT security incidents with narrow spectrum impact to high priority status. This same company will also modify their crisis response plans to ensure that regular status updates are provided from crisis management teams to incident responders and vice versa.

Finding 6: Attempts to facilitate an interactive international game were hampered by time zone differences, isolated scenario building and unexpected player actions.

International play was not extensive in the Australian national exercise. A longer pre-exercise build up, a longer exercise duration (to account for the 18 hour difference between Wellington and Washington) and more international communication during the exercise planning phase will need to be incorporated into Cyber Storm III.

Observations:

a. Attempts to facilitate international cooperation and communication through the Certificate Authority compromise were not successful. Despite high-level efforts made by planners, the scenario did not escalate as planned and resulted in limited communication and coordination within the international community during the exercise.

b. International play was severely hampered by the time difference. In essence the US exercise started a day later than the Australian exercise which meant that Australian play was winding down while the US play was winding up.

c. Through the planning process, participants gained insight on how each nation or international organisation would respond to a cyber incident. Many participants commented that, with the benefit of hindsight, they would have planned and executed their scenarios differently to engage their own international partners. They did not fully capitalise on the framework and opportunities that Cyber Storm II provided to exercise as broadly as they could have.

d. Players noted that the interactive international elements of Cyber Storm II were very appealing and an impetus for their involvement. For many organisations, participation in Cyber Storm III will depend on their ability and readiness to capitalise on the opportunity afforded by the international framework of the exercise. Many players noted that, in hindsight, they didn’t have the perspective to involve their international partners in Cyber Storm II as it was a completely new concept and they were unfamiliar with the likely execution of the exercise. They agreed that Cyber Storm III will allow them to build on these lessons and incorporate their international partners in the planning and design of Cyber Storm III.

e. Some players noted that greater involvement with and interaction between Australia and New Zealand in particular should be pursued as part of any Cyber Storm III given the commonality of the issues and players.

Annexe A: Participating Organisations

This list does not include six organisations that wish to remain anonymous.

Non-government Participants
AusCERT
AusRegistry Pty Ltd
Australia and New Zealand Banking Group Limited
The Australian Domain Name Administrator
Australian Securities Exchange
CISCO Systems Australia
The Commonwealth Bank of Australia
Country Energy
Ergon Energy Corporation Ltd
Energex Ltd
Energy Networks Association
Insurance Australia Group
Internode Systems Pty Ltd
Melbourne IT Ltd
Microsoft Australia
National Australia Bank
Powerlink Queensland
Singtel Optus Pty Ltd
Suncorp Metway Ltd
Telstra Corporation Limited
Westpac Banking Corporation
Woodside Energy Ltd

Observers
Attorney-General's Department – Emergency Management Australia
Bank of Queensland
Bendigo Bank
Citigroup
Foxtel
IT Security Experts Advisory Group
National Electricity Market Management Company
QANTAS Airways Ltd.

Commonwealth Agencies/Departments
Attorney-General's Department
Attorney-General's Department – GovCERT.au
Attorney-General's Department – Protective Security Coordination Centre
Australian Communications and Media Authority
Australian Federal Police
Australian Security Intelligence Organisation
Centrelink
Customs
Defence Signals Directorate
Department of Broadband, Communications and the Digital Economy
Department of Defence

Department of Finance and Deregulation
Department of Foreign Affairs and Trade
Department of Immigration and Citizenship
Department of Infrastructure, Transport, Regional Development & Local Government
Department of Prime Minister& Cabinet
Department of Resources, Energy and Tourism
Office of National Assessments

State Government
SA Department for Transport, Energy & Infrastructure
SA State Emergency Management
WA Department of Premier and Cabinet
WA Department of Treasury and Finance – ServiceNet

Using RFID for Cyber Threats Mitigation

Case Study

Cyber warfare, especially Computer Network Operations (CNO) has a deep technical aspect. Even minute technical shortcomings in the security of protected systems may lead to a complete compromise of the system. Conventionally, high levels of assurance have been achieved only with "six feet of air", or physical (and electromagnetic) network separation. Lately, though, even this has not proven sufficient, as the case with `Agent.btz` – computer worm has demonstrated [6]. `Agent.btz`, sometimes even considered to be a real case of *military* computer network exploitation (CNE), used USB-flash memories to transfer malware into closed networks and leak data out of them.

Radio Frequency Identification (RFID) is rather a broad concept. In this case study, we refer to the architecture in fig. 1, where each of the components and communication protocols use widely known or standardized techniques to implement their functionality.

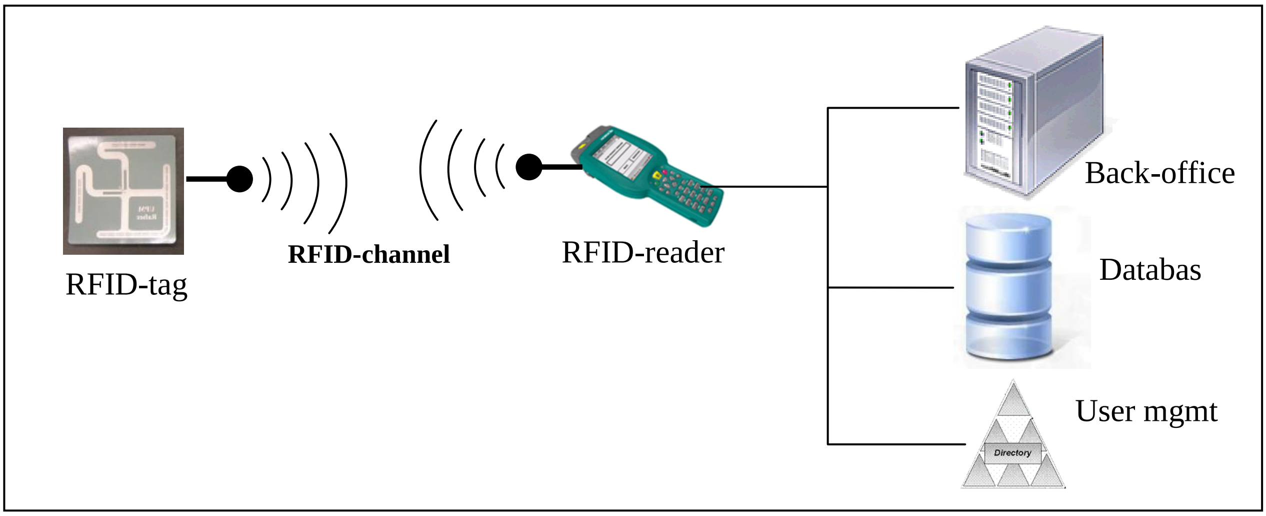


Figure 1: RFID system as a subsystem

RFID technologies in general use the spectrum very broadly: systems vary from LF to UHF and microwave. Due to regulatory issues, the UHF-range solutions tend to have further read ranges than LF, reflecting in the applications area. The LF and HF systems are used for close-range applications, such as physical access control and payment systems. UHF, on the other hand, is typically used in logistics.

The RFID subsystem can be thought to be consisting of a tag, channel and a (possibly mobile) reader. RFID tags are categorized in three groups, based on their role in the communication protocol and energy use:

- Passive tags that don't have a battery on their own, but operate on the energy of the reader transmitted by the electromagnetic field
- Active tags that contain a power source, and can initiate communication based on that energy
- Semi-passive tags, which employ a power source for extending their read range and holding internal state, but do not initiate communication unsolicited

In our view, RFID technology represents a similar threat in CNO as USB sticks, only more insidious due to the following characteristics:

- RFID systems are often readily connected from the edge of the closed network right to the core

- RFID technology, when present, is an integral part of the setup, going unnoticed
- Processes involving RFID are optimized to require as little user interaction as possible
- Traditionally, RFID-subsystems are considered as trusted, requiring little or no security (relying mostly on the vendor's IPR protection, a.k.a. "security through obscurity")

Due to the low cost, small size and weather-resistant packaging of some RFID tags, it is possible, for example, to construct a cyber minefield, with different types of virus-infested tags, such that when enemy battle systems move over the minefield, their RFID readers will pick up the contamination and disable or corrupt some of the mission-critical systems. This is one way the short-range wireless sensor types could be used to penetrate the seemingly thick wall of physical network separation of operational systems, and deliver information warfare type operations into closed networks.

The purpose of this case study is to present the results of our work for identifying and tackling the RFID threat in the CNO framework.

SCENARIOS

In the course of our research, we have identified two of the most typical scenarios using RFID in the military: logistics and physical access control. The requirements of the scenarios for INFOSEC and COMSEC are elaborated below.

Logistics

In logistics, there is need to monitor items and vehicles (fleet management) automatically, when they are stored and transported between locations. Typical tracked properties are, for example, environmental conditions and location. Tags could be placed on several types of items, from large containers down to individual rifles.

For logistics, the availability and integrity of the information in a larger scope has more weight than e.g. the confidentiality of single tags. These properties contribute to the situational awareness in logistics as well as the functionality of the whole logistics chain. (If the container destination addresses are mixed in a specific holding area, it could severely delay or even destroy the logistics of an entire mission.)

It is characteristic in logistic systems to have deep-reaching connections from the RFID subsystem to the internal database servers. This presents an extra attack vector not often present in access control systems.

Access Control

RFID is replacing or augmenting physical locks in many places. The sometimes rapid changes in personnel and facilities force the physical access control systems to be very flexible. Mapping from the user set to a lock set needs to be many-to-many, easily maintained and quickly configured. Administration needs to be able to centrally assign and revoke rights per lock and per user or group of users. Restrictions can also be based on the time of day, person of facilities classification or special circumstances.

Physical access control has two concerns:

- Preventing unauthorized access into facilities
- Ensuring access for authorized users

Thus the systems need to guard the confidentiality of single user's private access information as well as ensure the availability of the service as a whole.

The central access control management systems are usually separated from other systems and networks, so the attack paths from the access control to other mission critical systems are lengthy and unlikely. Additionally, the access control tags need not contain much memory or processing logic, making the threat of malware in the tag less prominent.

THREAT MODEL

RFID systems have long been isolated and proprietary systems, mainly due to their size and processing restrictions. This position has been very tempting for the vendors to overlook costly information security issues: the related risk has not so far presented a substantial threat to critical systems. However, due to the increased connectivity of RFID subsystems, their threat potential has increased nearly exponentially.

In our scenarios, the approach taken by some of the vendors has resulted in two main threat vectors. The first one is introduced by the increased connectivity is considering the RFID subsystem as a weapon instead of a target. From an abstract point of view, the RFID subsystem may represent an unguarded route to critical core systems, even in cases where the critical system has been physically separated from other networks.

The second threat vector is the low entropy of the tags in the access control system tags, allowing a fast enumeration of all the possible key alternatives, much like having a master key to the locks of a whole facility.

In the following, we detail the threat model and its application to our scenarios. This includes the attacker presumed abilities and restrictions as well as different attack types with examples and effects.

Attacker Abilities

The attacker abilities are modelled based on two typical models: Dolev-Yao for the general computer network security [1], and Chosen Ciphertext Attack (CCA) for the cryptographic components [7]. We applied these models to the RFID subsystem.

Dolev-Yao: the attacker

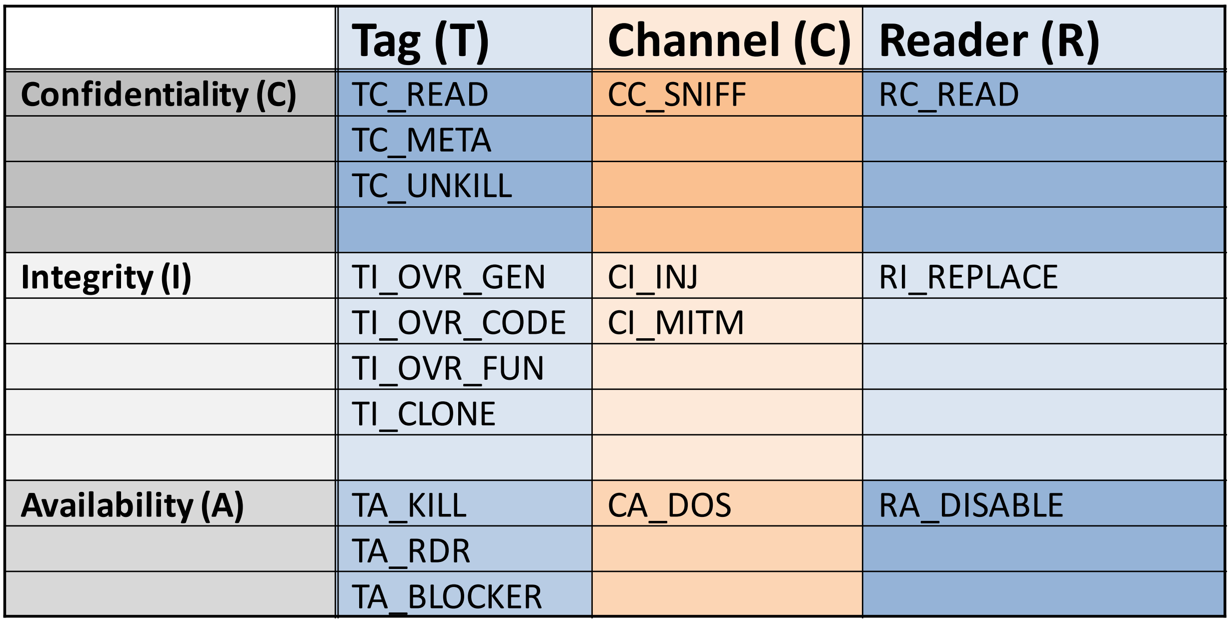
- can read the RFID channel at sufficient rates; specifically the attacker can demodulate the code, decode the line coding and discover possible hopping sequences
- can write to the RFID-channel at sufficient rates
- can inject compromised or even customized tags and readers to the system
- can corrupt a limited set of legitimate readers and tags, but not
  - corrupt their private data (i.e. smart card crypto keys)
  - readers without the interaction of the reader with the RFID-channel
- can *not*, in the general case:
  - delete RFID-traffic from the RFID-channel, implying that removal or rerouting of messages in the RFID channel is deemed infeasible, and modifying messages requires moderate to large resources and expertise
  - decrypt logical level ciphers or predict random number generators’ output

CCA: the attacker:

- can recover the encryption algorithm used, in detail

- can deceive the hardware and processes working under operative crypto keys to encrypt and decrypt arbitrary messages subject to the following constraint:
  - messages sent according to the pre-specified functionality of the system by legitimate and uncorrupted components can be encrypted and decrypted only case by case

Table 1: RFID threat categories



	Tag (T)	Channel (C)	Reader (R)
Confidentiality (C)	TC_READ	CC_SNIFF	RC_READ
	TC_META		
	TC_UNKILL		
Integrity (I)	TI_OVR_GEN	CI_INJ	RI_REPLACE
	TI_OVR_CODE	CI_MITM	
	TI_OVR_FUN		
	TI_CLONE		
Availability (A)	TA_KILL	CA_DOS	RA_DISABLE
	TA_RDR		
	TA_BLOCKER		

The threat model differs for access control and logistics cases for practical reasons: the logistics case is far more general, and requires a meta-level approach. It is possible to translate each model to the same type as the other, but in such a case the application will be more laborious. As the logistics case has a more general model, we recommend using that one for cases outside their domain.

Logistics

The logistics threat model considers all three types of attacks in the CIA-model (confidentiality, integrity and availability) targeted against each of the RFID-subsystem components: tag, channel and reader. These are then translated into examples and effects in the logistic and access control environment, displayed in table 1 and explained in tables 2-4.

It should be noted that the focus is on attacks to the tag and channel, as these are easiest for the attacker to get access to; in addition, the compromise of components further up the chain towards the backend systems nearly always implies the compromise of the components "below". Thus attacks targeting the reader from the back office are not considered, and attacks channelling from tag or the channel are grouped under respective categories.

Table 2: RFID tag-based threats and their effect in logistics

	Code	Explanation / example	Effect (in logistics)
Conf.	**TC_READ**	Unauthorized reading of tags; the possibly sensitive information in a tag or a their combination in a group of tags is leaked	Force tracking; deduction of operations by e.g. rifle IDs
	TC_META	Unauthorized deduction of metadata from the tag information (e.g. batallion ID, destination, PIN-code)	Intelligence on the blue force movements and hierarchy are leaked
	TC_UNKILL	Restoring information in a ”destroyed” tag	”Dumpster diving”, i.e. accessing sensitive information thought to be safely discarded (encryption keys, etc.)
Integr.	**TI_OVR_GEN**	Unauthorized overwriting of tags: tags contain inaccurate or false information	Items are transported to incorrect destinations, the logistic situational awareness is distorted
	TI_OVR_CODE	Tags contain malware affecting the backend systems, such as viruses or backdoors.	Takeover of the back office or user management systems, injecting viruses into the main systems
	TI_OVR_FUN	Changing the operational logic of the tags (injecting unauthorized commands to tags)	The tag will send continuously, ending the battery; tags will refuse to answer to authorized requests, but answer to unauthorized ones (i.e. track their location and send it to the attacker whenever possible)
	TI_CLONE	Breaking the connection between the tag information and the physical, authorized token represented by the tag (cloning or destroying the tag)	The basis for the identification is broken; distortion of the situational awareness of logistics (“ammunition left: 100 boxes”, when in fact very few are left)
Avail.	**TA_KILL**	Disabling the tags nearly permanently (e.g. a ”kill”-command)	Items are misplaced and their transport slowed down; situational awareness in logistics updates slowly or is distorted
	TA_RDR	Using a contaminated tag to crash the reader applications or operating system	Slight distortion in the situational awareness in logistics
	TA_BLOCKER	Disabling the tags by actively blocking their radio channel or communication protocol	cf. TA_KILL; more easily remedied

Table 3: RFID channel-based threats and their effect in logistics

	Code	Explanation / example	Effect (in logistics)
Conf.	CC_SNIFF	Eavesdropping	cf. TC_READ and TC_META
Integr.	CI_INJ	Injecting unauthorized messages in the channel; breaking the authentication of the channel	cf. TI_OVR_* and TC_*
	CI_MITM	Man-in-the-Middle attack (rerouting a message, altering a message actively during a protocol run)	Slight distortion in the situational awareness in logistics
Avail.	CA_DOS	Blocking the communication channel with other than electronic warfare methods, i.e. RFID-DoS attacks (e.g. an unauthorized reader can query tag information too rapidly; a set of unauthorized tags can send hello-messages faster than standardized)	cf. TA_KILL

Table 4: RFID reader-based threats and their effect in logistics

	Code	Explanation / example	Effect (in logistics)
Conf.	RC_READ	Unauthorized reading of tag contents from the reader; the possibly sensitive information in a tag or a their combination in a group of tags is leaked	cf. TC_READ and TC_META
Integr.	RI_REPLACE	Replacing a trusted reader with an unauthorized reader	All the tag- and channel-based threats
Avail.	RA_DISABLE	Disabling or destroying an authorized reader by another means than via the RFID-channel (i.e. physically)	cf. TA_KILL, TA_RDR, TA_BLOCKER and CA_DOS

Not all of the threats are equally significant. The significance of the threats forms an application-specific RFID threat profile, which we have categorized as follows:

- *Critical*: system cannot be accredited / operation of existing systems should be discontinued
- *Major*: the threat should be handled according to the risk management policy as soon as possible
- *Prioritized*: the threat should be handled according to the risk management policy
- *Minor*: the threat should be acknowledged on a per-system basis

For logistics, the RFID tags are not usually placed very individually (per soldier) but attached to more collective units, such as containers. Thus, hostile force tracking is not as likely. In addition, the situational awareness picture is formed as a total from a large set of widely distributed tags, making a local breach less significant.

On the other hand, certain computer virus types have been demonstrated to fit into as low as 100 – 200 bytes [5]. This can easily be accommodated in the storage capacity of most modern RFID tags – even EPC Global Gen2 standard passive tags include a maximum of 88 bytes of memory [3], well within the reach of skilfully optimized virus codes. As the RFID subsystem is very often optimized in cost, the tag memory content is simply passed along the route – without validation - to the core systems, which finally consumes the unfiltered payload. As the logistic IT-systems are well networked into the core operational C2 systems, this poses a significant threat for the back-end systems *via* the RFID.

In the logistics application, RFID can be transformed from an enabler to a cyber warfare tool. Otherwise closed C2 systems may have unexpected unguarded routes past their security perimeter, leading to both information leakage and internal information corruption. The detailed RFID threat profile for logistics is, according to our studies, as follows:

- *Critical*: TI_OVR_CODE, CI_INJ, RI_REPLACE
- *Major*: TI_OVR_GEN, TA_KILL, RA_DISABLE, TA_RDR
- *Prioritized*: TI_OVR_FUN, TA_BLOCKER, TC_META, TC_READ, CC_SNIFF, RC_READ
- *Minor*: TI_CLONE, CI_MITM, CA_DOS

Access Control

The access control threat model stems from the more precisely defined subsystem, including personal tags and possible PIN-codes, reader functionality (opening a door and relaying / checking a PIN) and placement (at entrances and security perimeters), and back-end functionality (user- and group management, auditing). We were able to pinpoint the threats in a more practical level, and map the dependencies between each threat. The work was performed jointly with Oulu University Secure Programming Group (OUSPG) and the framework has been published separately in [8].

In current access control systems much of the security is often implemented with “security by obscurity”. Thus, for existing systems, even reverse engineering can be considered a security threat. Certain issues related to privacy in conventional systems can also be seen as a threat in access control systems: for example marking the tags (which act as security tokens) too clearly with their intended purpose may help the attacker to select its targets better.

We present here only a summary of the detailed threats identified in [8], but describe here instead the RFID threat profile for access control translated into the general threats specified in the logistics section.

Table 5: RFID threat-vectors in access control

Threat	C?	I?	A?	Arch. elements
BackendFloodingThreat			X	Backend
BadHashThreat	X	X		All
BadPrngThreat	X	X		Tag, Reader
BruteForceKeySpaceThreat	X	X		Tag
DeltaDebuggingPacketThreat	X			All
DeltaDebuggingThreat		X		Channel
DenialOfRfChannelThreat			X	Channel
DenialOfServiceThreat			X	General
DenialUsingAnticollisionThreat			X	Channel
DisconnectionThreat		X	X	Reader, Backend
ForgeryThreat		X		Tag, Backend
GetPinFromTagThreat	X	X		Tag
GetPinFromUserThreat	X			Reader
KeyCopyingThreat	X	X		Tag
KeyLeakingThreat	X	X		All
PoorlyUsedKeySpaceThreat	X	X		Tag
ReaderBreakingThreat			X	Reader
ReaderTracingThreat	X			Reader
RelayingThreat	X	X		Channel
ReplayThreat		X	-	Channel
RfidDataMalwareThreat	X	X	X	General
SpecLeakingThreat	X	X	-	General
TagbreakingThreat			X	Tag
TagCollisionIdTrackingThreat	X			Tag
TagHolderRecognitionThreat	X			Tag
TagReaderRecognitionThreat	X			Reader
TagSignalFingerprintTrackingThreat	X			Tag
TagTrackingThreat	X			Tag
UnauthorizedAccessThreat	X	X		General
WeakBackendHashThreat	X	X	X	Backend
WeakEncryptionThreat	X	X		General

In cyber warfare, a significant part of hacker attack preparation is intruding some of the premises containing network operations equipment, such as NOCs (Network Operation Centre). If these premises are physically protected with RFID access control technology, its threat profile poses an equally large risk for the mission critical systems as planting malware.

The RFID threat profile for access control was identified as follows:

- *Critical*: TI_OVR_CODE, TI_CLONE, TC_READ, RI_REPLACE, RC_READ
- *Major*: TA_KILL, CA_DOS, TA_RDR, CI_INJ, CC_SNIFF, CI_MITM, RA_DISABLE, TC_META
- *Prioritized*: TA_BLOCKER
- *Minor*: TI_OVR_GEN, TI_OVR_FUN

AUDITING

The acquisition of third-party commercial hardware and software for military purposes is becoming increasingly commonplace. Ideally, sufficient and authenticated information of the acquired system can be readily accessible for the system users, and the claimed functionality corresponds to the actual real-life functionality. However, too often the relevant security properties are too vaguely specified and / or inadequately implemented in the system. Auditing is required to validate that the claimed security properties of system are present.

Technical security audits for conventional ICT systems have well established procedures for varying degrees of depth (e.g. [2]. However, due to the nature of RFID systems, there is considerable significance on the reverse engineering process, or establishing the inner workings of the system. This nature stems from

- Wide variety of technologies and vendors within the RFID subsystem, from radio technology to logistics applications
- Extremely optimized manufacturing processes to produce cheap tags and readers, leaving little motivation for the vendor to disclose the more detailed functionality of the RFID-components, making the available documents rather vague about the security properties of the system
- Tendency to rely on “security by obscurity”, i.e. omission of security measures in the hope that if the details remain secret, the system cannot be fruitfully attacked

The RFID security auditing process follows the main principles in typical information system audits [2,9], that is:

- Planning and preparation
- Performing risk analysis based on a threat model and the goals
- Gathering necessary information about the audit target
- Analyzing the gathered information based on the threat model and the claimed functionality
- Disclosure of the results

The process for the audit is similar for both of our applications: access control and logistics. However, the required tools for analysis and information gathering vary somewhat, mostly depending on the RFID channel characteristics and reader platform.

Process

The general process is depicted in figure 2. The process is iterative in nature, as some later details may reveal new threats or vulnerabilities not anticipated beforehand, and requiring explicit permissions from management and vendors. (The exception to this is the results disclosure, which needs to be kept a separate process. If new important vulnerability information comes up during this phase, a new audit process may need to be started.) We anticipate at least two iterations, as the audit targets need to be refined at least once.

Planning and preparation includes the audit target identification, initially at a coarse level, but refining them during the process. Purpose statement includes a clear indication of the audit’s expected results, motivation, and scope, e.g.

- Examination of a product against vendors claims and domestic security policy
- Audit of an internal system against a new security policy

- Checking a product implementation against its specifications
- Checking compatibility of a certain department IT systems with respect to a new legislation or standard

An obvious, but not to be underestimated, part is the management buy-in: especially external audits may be sensitive topics, and not possible to conduct with low-level acceptance only. Generally, the RFID setup may require actions (such as reverse engineering) that need vendor permissions / support. This is, however, dependent on local legislation and audit depth.

Risk analysis does not require the auditor to identify the assets and their value, but rather obligates the audit target owner to provide sufficient information to the auditor. The general risk analysis is then viewed with the RFID-specific threat model (e.g. the one presented before), identifying, for example:

- Which of the critical assets are theoretically accessible from the RFID subsystem
- What kind of attackers might be likely to access the assets and what resources are they likely to spend on it (in terms of hardware, knowledge, skills and inside information)
- Which of the threats listed in the threat model can be afforded by the attacker in consideration (based on the resources needed for the attack)?

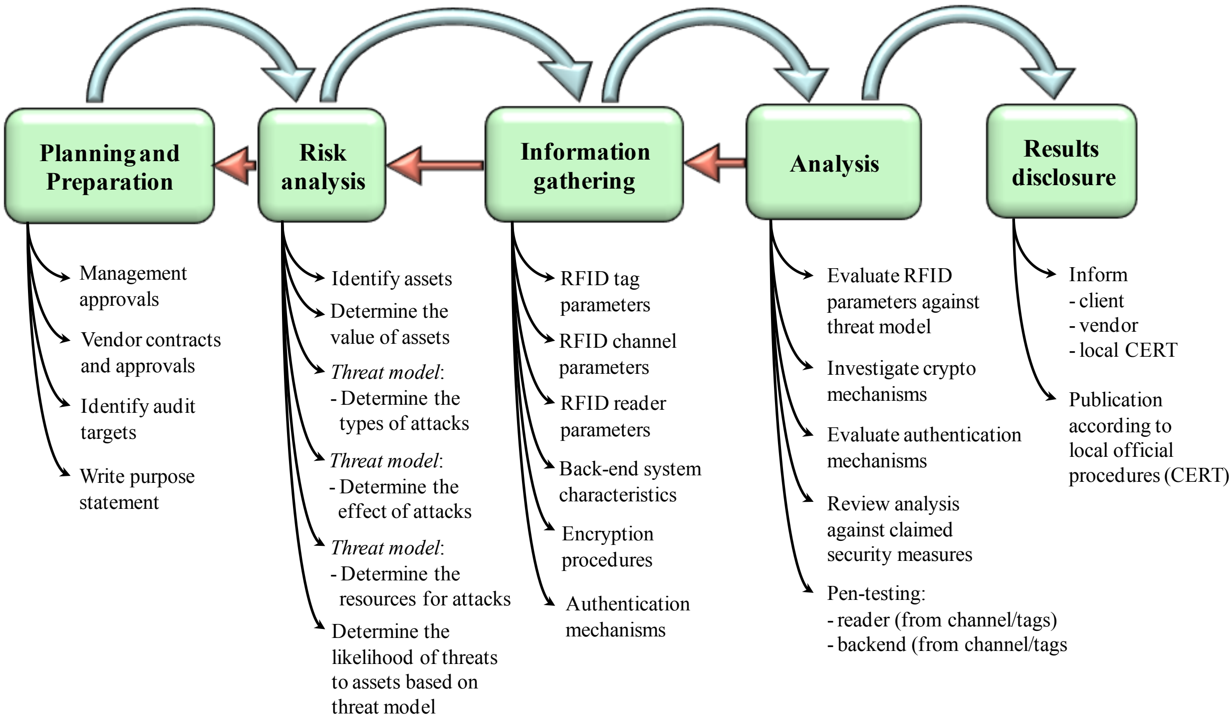

Planning and Preparation
Risk analysis
Information gathering
Analysis
Results disclosure
Management approvals
Vendor contracts and approvals
Identify audit targets
Write purpose statement
Identify assets
Determine the value of assets
Threat model: - Determine the types of attacks
Threat model: - Determine the effect of attacks
Threat model: - Determine the resources for attacks
Determine the likelihood of threats to assets based on threat model
RFID tag parameters
RFID channel parameters
RFID reader parameters
Back-end system characteristics
Encryption procedures
Authentication mechanisms
Evaluate RFID parameters against threat model
Investigate crypto mechanisms
Evaluate authentication mechanisms
Review analysis against claimed security measures
Pen-testing: - reader (from channel/tags) - backend (from channel/tags
Inform - client - vendor - local CERT
Publication according to local official procedures (CERT)

Figure 2: RFID security audit general process

Information gathering is, by our experience, the most laborious part of the audit. This is especially true with the access control case, as the systems are closed and small-scale, acquired from a large multi-national vendor via a chain of resellers and system integrators.

An audit, whose purpose is to harden systems against CNO, needs to investigate protocols, encryption schemes and other security controls on a logical level. However, for closed systems, this requires accessing the information on the physical level as well, not to mention knowledge on the data encoding, protocol type, data formats, etc.

If the system proclaims to follow a known standard, the information gathering phase is made easier by an order of magnitude. In most cases in logistics, this seems to be the case, but the access control systems often follow vendor-specific, and sometimes old conventions on defining the operation and formats of the RFID subsystem. We divided the information into six:

- RFID tag parameters, such as data encoding and format, memory size and usage (including security controls), accepted command language (if any), tag type and population control response
- RFID channel parameters, such as frequency, modulation, symbol speed and data encoding
- RFID reader parameters, such as data encoding and format, memory size and usage, accepted command languages, supported tag and population control types, external communication interfaces and their protocols, typical operation with the tags
- Back-end system characteristics: system type (database, ERP-software, user management, ...), security controls for the channel including data input from the RFID subsystem
- Authentication mechanisms and protocols, between the tag and the reader, and the reader and the back-end system
- Encryption methods: cryptographic algorithms, hash algorithms, pseudo random number generators (PRNG) and key management (including tokens and PIN-codes)

The analysis part here includes the actual review as well. Note that after information gathering it is likely needed to step back to refine the planning and preparation as well as the risk analysis. The review is meant to compare the results of the information gathering with the specifications and claims, which in turn are compared to the original contracts, security policies and / or standards and legislation.

Actual analysis is likely to be required on the different security controls in the RFID-subsystem, such as key management, PRNGs, use of cryptographic modes, protocols and authentication mechanisms, whether they actually fulfil their intended purpose.

Penetration testing is recommended in two cases:

- If the RFID reader blackout is sufficiently serious for the operation
- If the RFID reader transmits large enough packets (> 50B) of data to the back-end systems to give rise to malware injection attacks against the back-end systems

An alternative to pen-testing is to have sufficiently detailed documentation of the security controls in the RFID-reader (basically indicating a source-code audit).

Results disclosure finalizes the audit process. Note that due to the nature of a standard vulnerability disclosure process, it is generally very difficult to iterate backwards from this stage. The disclosure process may follow the standard conventions for RFID as well, noting again the possible discrepancy between the size of the vendors and the typical user organization.

Tools

We focus here on the tools required especially for the RFID auditing process. Tools for formal protocol analysis and pen-testing are available elsewhere, and can be used independently of the RFID subsystem. We did not consider the more advanced attacks, such as reprogramming a reader, but concentrated on attacks originating from the RFID-channel. This is due to the following reasons:

- It is possible to simulate any tag or reader operation to the other party by manipulating the channel only.
- If the tag is modifiable from the reader, new and customized tags can be generated (to a degree) from injecting suitable message in the channel only.

RFID-channel manipulation needs physical devices to send and receive data. Due to the multiple frequencies used in different RFID systems, different radios may be required. Based on our experience, LF and HF can be managed with the same radio and several antennas, but UHF and microwave bands require separate radios, even within UHF (e.g. ISO-18000-6c and 18000-7 systems are best analyzed with different radios).

UHF-radios are usually specialized systems due to the large symbol speeds compared to current state-of-the-art in general purpose computing platforms. For LF and HF systems, low-cost open hardware platforms exist (e.g. GNU-radio [4]).

The heart of the radios is naturally operating systems and signal generation software. Additionally, signal analysis tools are needed. We developed in conjunction with OUSPG a set of signal analysis and radio controller tools, available in [8]. These include:

- Different modulation generation and recording tools for the GNU-radio
- Demodulation tools
- Signal analysis tools
- Transmitting tools
- Data format manipulation tools
- Syntax analysis tools
- Automatic data generation tools
- Reference signals

The tools were tested only for the LF and HF signals. For UHF signals, a different set was developed.

CASE STUDIES

The audit process and tools were developed with the help of case studies, one from each of the application areas. The logistics case study involved a UHF active tag system used for item tracking, and the access control case a passive tag system for electronic door locks.

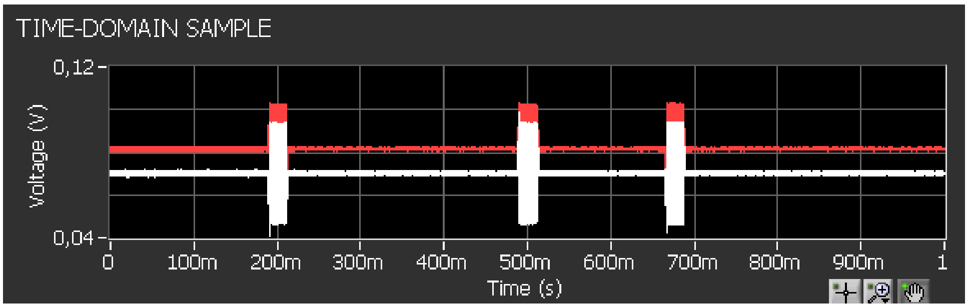


Figure 3: Data bursts and their spectrum of the active tags, indicating 2-FSK

Logistics

The active tag system investigated was built on a US-based company chip technology, repackaged and programmed by a Finnish company for fleet management. The tags were placed in containers, were they measured different environmental conditions as well as location. The system consisted of the tags, which transmitted about 30-100 meters regularly trying to contact a reader within range. When a reader appeared within range, the tags dumped their measurement information to the reader, which forwarded them over its WAN-connection to a centralized database.

The system was in an evaluation phase, and the purpose of the security audit was to find possible technical weaknesses in the RFID-subsystem. The audit was requested by the potential acquiring organization, and since the system was in evaluation phase, the Finnish reseller was co-operative in providing the sufficient information. However, some of the RFID channel characteristics were tied to the tag's chip itself, making it necessary to verify the Finnish reseller information separately.

We used the threat model described in chapter 3.2. For the information gathering phase we used a separate signal analyzer (different from the tools depicted in [8], due to the symbol speed, which the standard GNU-radio communication circuits could not handle adequately), dedicated for 800 – 1000 MHz band. The modulation recognition required yet more equipment (it turned out to be a form of FSK – RFID systems do not deploy complex modulation types, thus making them easy to identify; see fig. 3).

During information gathering and subsequent analysis, the main weaknesses found in the system were as listed below:

- No explicit authentication between the tag and the reader, beyond a shared secret key used in the communication encryption
- Communication in the RFID channel was encrypted, but the encryption keys were kept constant, and the encryption mode was that of a stream cipher. Thus XORing a known plaintext and the sniffed ciphertext, one could recover the keystream easily.
- Together these two weaknesses enabled a total control of the RFID channel by an attacker

- The reader was forwarding the measurement data without sanitation to a database management server, which inserted the data also without sanitation directly into the database.
- The packets forwarded by the reader could be between 100 and 200 bytes, making it large enough to contain viruses or SQL-injections
- The latter two weaknesses enable an attacker to inject malware from the tags right into the core systems, or to take full control of the database using an SQL injection.

Based on the analysis, the system could not be recommended for deployment, unless the weaknesses were resolved. (Later, however, the whole technology type was discarded due to compatibility issues).

Access Control

All of the access control RFID-subsystem's technology in our case is developed and marketed by a large multinational corporation. The integration into an access control and workforce tracking software was made by a Nordic integrator. The RFID subsystem in question has been broken multiple times in the past, but the vendor has prevented large scale publication through litigation, allowing the weaknesses to remain in place. Due to the closed nature of the product, as well as little or no available exact information on the weaknesses, the system was considered viable for a security audit by the organization employing it as their access control method.

The system consists of a passive LF tag, read normally from a distance of a few centimetres, and checked against access rights in a centralized server. It is possible to install a separate keypad beside the lock to require a PIN code as well as presentation of the token. The backend system is used to define the rights, as well as manage the key populations.

Since even the Nordic integrator would not provide or did not have the specifications of the system, it was reverse engineered from the physical layer upwards. As the system works in the LF band, it is possible to use generalized radio equipment and standard laptops for analysis and signal generation. (See [8] for a more detailed description of the auditing system.)

We used the threat model described in chapter 3.3. Modulation recognition was trivial, since the ASK modulation shows up in a basic oscillator screen. The system did not contain enough information capacity for malware to reside in the tags, but neither was it sufficient to enforce any rigorous access control. The main weaknesses were:

- The identification was based on the static contents of the tag only, making it possible to clone the tag
- The tag variable, personally identifying, information content was only 12 bits, after facility code was known. This 12-bit "ID-space" was not used equally, but in large clusters (a set of keys ordered in the same patch were sequentially numbered). This enabled brute-forcing the entire keyspace, even without knowledge of any key.
- The PIN-code was not independent of the key-ID, instead it was computed from the ID using a deterministic algorithm (thus could not be changed, if revealed).
- If the reader connection to the backend system was disconnected, they checked only the facility code, not the individual code nor its access rights.
- These properties lead to an attack, where even a PIN-protected door, where only one key in the whole facility had rights to, could be brute-forced open in less than an hour (in seconds, if it was not PIN-protected).

Based on the analysis, the access control system was completely inadequate. The audit recommended replacing the system, which the organization put immediately under process.

Because of the vendor’s history with vulnerability disclosures, the audit team left the disclosure process to be handled by the Finnish CERT-group. We are not aware of the process status, as of the time of writing this paper.

CONCLUSION

We have presented a threat model and an security auditing framework for an RFID-subsystem in military scenarios. Based on the threat models and our case-studies we have shown that RFID technology can be used in CNO both as a courier for malware over network separation and to breach physical access control systems.

Because of the multiple applications and ease of use, RFID technologies will continue to increase in popularity and appear in ever more unexpected places, even in military systems. Despite its current shortcomings in the information assurance arena we believe that RFID can be safely and securely integrated into other ICT systems. It *is* paramount to exercise care and perform similar validations for RFID systems as with any other new ICT system, but the security problems so far do not preclude the use of the whole RFID technology.

RFID should be included, with other ICT systems, early into company and organization risk analysis, and exercise similar caution and validation processes with RFID as with any other ICT system waiting for deployment. The bottom line is not to treat RFID subsystems as trusted, and not to assume physical separation will provide absolute protection from CNO.

REFERENCES

[1] D.Dolev, A. Yao. *On the security of public key protocols*, Proc. of the IEEE 22nd Annual Symposium on Foundations of Computer Science, pp. 350-357, 1981.

[2] ISACA. *IT Standards, Guidelines and Tools and Techniques for Audit and Assurance and Control Professionals*, Information Systems Audit and Control Association, available at: http://www.isaca.org/AMTemplate.cfm?Section=Standards2&Template=/ContentManagement/ContentDisplay.cfm&ContentID=55920 1.3.2010.

[3] ISO/IEC. *International standard ISO/IEC-18000-6, Information Technology, Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860 MHz to 960 MHz, Amendment 1: Extension with Type C and updates of Type A and B*, 15.6.2006.

[4] J.Lang. *GNU Radio*, in: http://gnuradio.org/redmine/projects/activity/gnuradio, 15.3.2010.

[5] M.Rieback,. B.Crispo, A.Tanenbaum. *Is Your Cat Infected with a Computer Virus?* Proc. of the 4th IEEE conference on Pervasive Computing and Communications, pp. 169 – 179, IEEE Computer Society, 2006.

[6] S.Shevchenko. *Agent.btz – A Threat That Hit Pentagon*, in: http://blog.threatexpert.com/2008/11/agentbtz-threat-that-hit-pentagon.html, (Threat Expert weblog) 30.11.2008.

[7] D.Stinson. *Cryptography, Theory and Practice*, §1.2., CRC Press, 1995.

[8] University of Oulu. *FRONTIER-RIDAC - An Open Source RFID Audit Framework*, in

https://www.ee.oulu.fi/research/ouspg/RIDAC, 1.3.2010.

[9] Wikimedia Foundation. *Information Security Audit*, in: http://en.wikipedia.org/wiki/Information_security_audit, 23.2.2010.

Using RSC for Cyber Threats Mitigation

Case Study

Remote Secure Controller (RSC) was developed in one of the projects funded by Polish Ministry of Science and Higher Education, titled “Federated Cyber Defence System” (FCDS). The aim of the project was to develop and implement FCDS prototype that provides:

- security improvement in federation of networks environment,
- support of network administrators in decision making and attack counteraction,
- automation of unauthorized actions detection and reaction to them, and
- analysis of events coming from different networks parts to enable distributed attack recognition.

FCDS’ architecture defines three main elements of the system: Detection Subsystem, Decision Module (DM) and Reaction Subsystem. Simply - on the basis of information from different sensors DM detects malicious activity and prepares so called Generic Decision Rule (GDR). This rule should be then translated into the language of a certain reaction element in order to take action against detected malicious activity. However for many architectural reasons the execution of the GDR is done through the Remote Secure Controller.

Therefore, Remote Secure Controller is used to control reaction elements on the basis to Generic Decision Rules prepared by the Decision Module. The proposed solution of RSC realization seems to be universal and can be used in other systems, which operate similarly to the FCDS and have similar needs of controlling the components. As the remote controller was designed for working in federation of systems, for sure it can be also successfully used in other, not so open systems.

DESCRIPTION OF THE FCDS SYSTEM

FCDS is a system prototype designed for cyber security improvement in federated networks. It supports cyber situational awareness in protected federation of systems. FCDS enables fusion of information from various sensors deployed in different layers of protected networks/domains. This capability enables detection of sophisticated attacks/ unauthorized actions, which is impossible for individual sensor. Moreover FCDS supports administrators in decision making process facilitating joint reaction to attack.

FCDS consists of autonomous subsystems which are deployed in protected networks (domains). Each protected domain is composed of typical network elements e.g. routers, switches, servers, user terminals, equipped with security software (e.g., firewalls, IDSs/IPSs, antiviruses). In such environment there are deployed FCDS elements such as: a number of sensors (S), decision module (DM) and a number of reaction elements (RE).

Sensors are responsible for:

- monitoring the protected network;
- supplying DM with alarms about events observed in the network.

Decision module enables:

- acquisition of sensor alarms;
- processing network events;
- correlating network events;
- attack detection;
- applying reaction to attack;
- sharing cyber information with other cooperating domains;
- Visualisation of security measures and statistics.

Reaction elements are responsible for attack mitigation/prevention. Possible reactions include:

- Administrator notification;
- Redirection to trap;
- Blocking (if possible).

Decision Module is responsible for collecting data retrieved from sensors and generation of Generic Decision Rule (GDR). GDR is produced based on sensor information. This process takes advantage of the ontology engine. The decision rule carry information about the identified threat, the source and target important for the reaction elements.

After being accepted by the administrator, rules are distributed from the Decision Module to the Translator Module that is implementation of the Remote Secure Controller. It converts the received data to be able to efficiently react. The main goal of TM is to correctly configure and control subordinate Reaction Elements. An exemplary reaction could be blockage of the required IP host address on the firewall.

The FCDS performs the following activities/processes:

1 Gathering information from sensors, which monitor network inside the domain (see Fig 1 – point 1). Information about identified anomaly/attack can be also sent from distant but cooperating domain.

1. Generating reaction decision (GDR) on basis the information collected from sensors. GDR defines the scope of reaction. Sending the GDR to the Translator Module. (see Fig 1 – point 2)

2. Application of elaborated security decisions in Reaction elements (see Fig 1 – point 3).

As depicted in Figure 1, apart from Sensors, Decision Module and Reaction Elements, the FCDS promotes application of so called – Translator Modules (TMs), that are used to apply developed by DMs reactions to the reaction elements. TM is responsible for translating so called General Decision Rule (GDR) developed by DM into language of the reaction element and configure it appropriately.

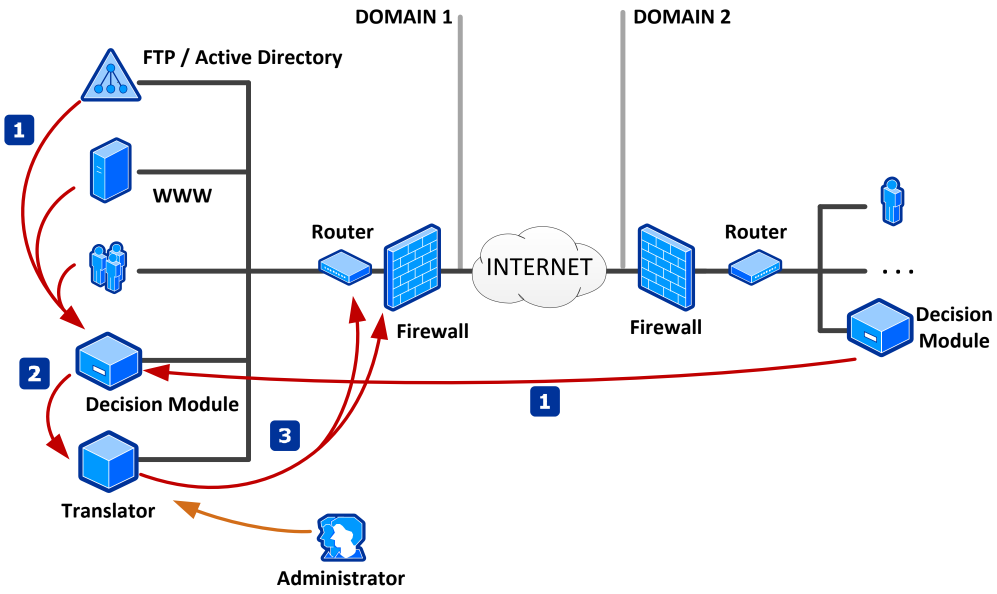


Figure 1: Architecture of the FDCS system

Figure 1 shows application of the Translator Module (TM) as a separate and autonomic element of FCDS system.

A strong advantage of this system is that the network administrator can quickly and efficiently react on identified threats. In this way the security configuration in every domain in any moment reflects identified threats. The domain administrator has constant insight into settings of reaction elements (security), and reaction is automatic.

Information about threats are collected form sensors, and exchanged between Decision Modules of federated domains. The administrator can manage cross-domain security policy, through setting importance of rules received from other federated domains. For example, he could drop rules from a specific, untrusted domain or set the rules to be automatically applied when the domain is 100% trusted and has more sophisticated and reliable sensor subnet.

FCDS USE CASE

An important feature of the TM is the possibility of automatic selection of Reaction Modules (devices) that are the most convenient in this special case of the identified incident and a given rule. In Figure 2 there is presented a situation of the protected system consisting of 2 domains. A rule is generated, with information about 2 users that performed unauthorized activities, and 1 infected FTP server.

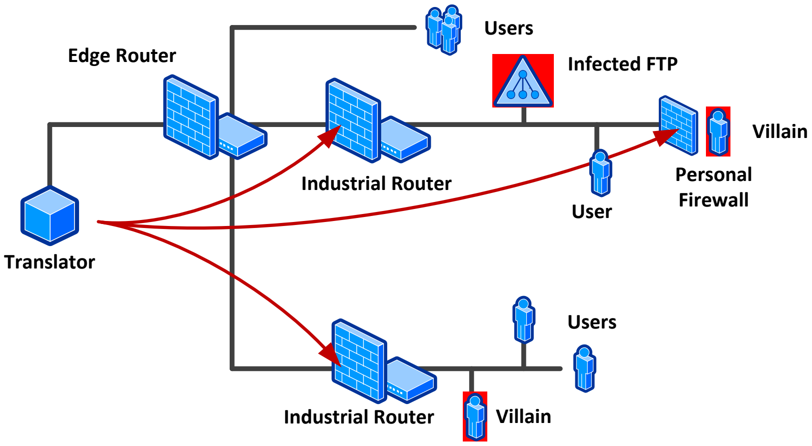


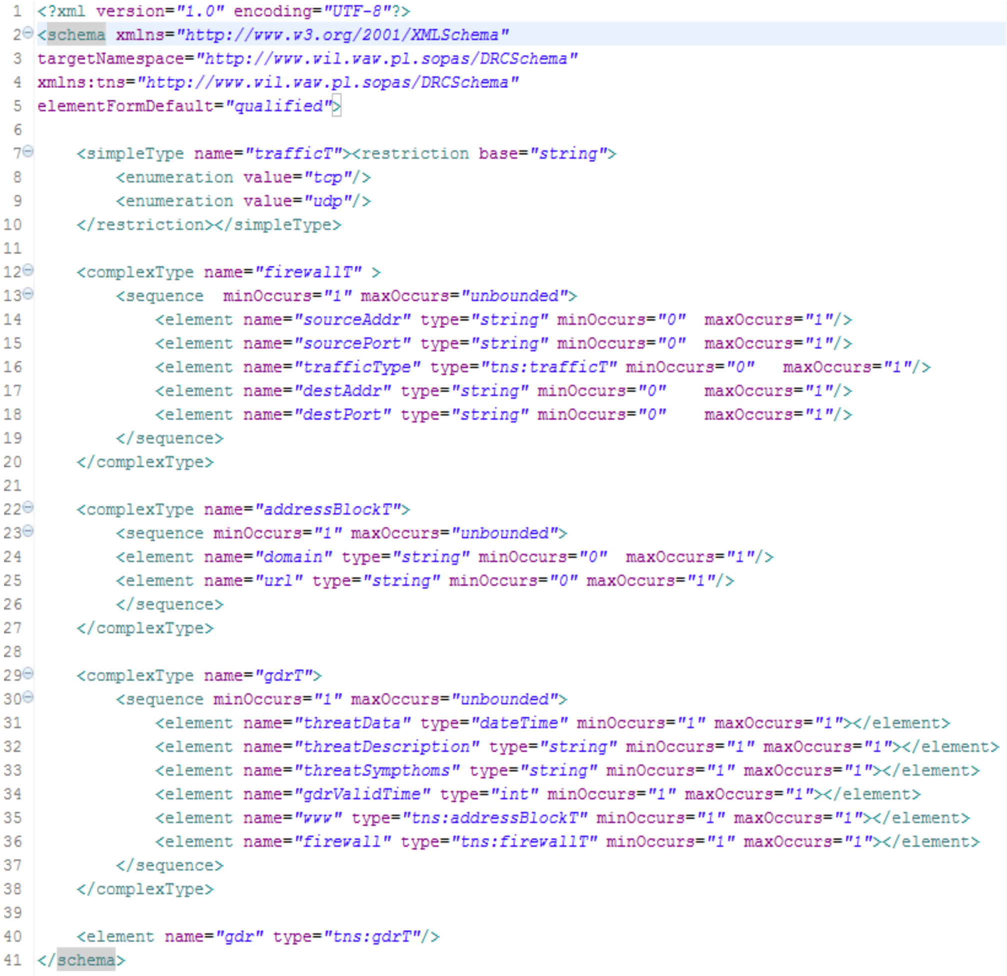
Figure 2: Scenario of reaction over infected resource and suspicious users

Retrieved decision rule in TM have 3 IP addresses, which must be blocked. TM also have information about the topology of the network, and can configure reaction elements localized close to the identified threats. In the use case presented in Figure 2 one of the dangerous users would be blocked on his own computer by the personal firewall (e.g.; IpTables). Infected FTP server and the second suspicious user would be blocked on the closest routers.

THE DETAILED DESCRIPTION OF THE TRANSLATOR MODULE

The TM can efficiently cooperate with other modules capable of generating rules related to identified threats, or work independently allowing administrator to manually create rules.

Keeping in mind interoperability issues, the Translator Module was designed to accept rules in standardized, uniform data format. This format is based on XML, and has its own template (XSD). According to this format the information about threats, and generated decision rules are transferred form Decision Module to the Translator Module. The format of data used in TM is presented in Figure 3.



```
<?xml version="1.0" encoding="UTF-8"?>
<schema xmlns="http://www.w3.org/2001/XMLSchema"
targetNamespace="http://www.wil.waw.pl.sopas/DRCSchema"
xmlns:tns="http://www.wil.waw.pl.sopas/DRCSchema"
elementFormDefault="qualified">

    <simpleType name="trafficT"><restriction base="string">
        <enumeration value="tcp"/>
        <enumeration value="udp"/>
    </restriction></simpleType>

    <complexType name="firewallT" >
        <sequence  minOccurs="1" maxOccurs="unbounded">
            <element name="sourceAddr" type="string" minOccurs="0"  maxOccurs="1"/>
            <element name="sourcePort" type="string" minOccurs="0"  maxOccurs="1"/>
            <element name="trafficType" type="tns:trafficT" minOccurs="0"   maxOccurs="1"/>
            <element name="destAddr" type="string" minOccurs="0"    maxOccurs="1"/>
            <element name="destPort" type="string" minOccurs="0"    maxOccurs="1"/>
        </sequence>
    </complexType>

    <complexType name="addressBlockT">
        <sequence minOccurs="1" maxOccurs="unbounded">
        <element name="domain" type="string" minOccurs="0"  maxOccurs="1"/>
        <element name="url" type="string" minOccurs="0" maxOccurs="1"/>
        </sequence>
    </complexType>

    <complexType name="gdrT">
        <sequence minOccurs="1" maxOccurs="unbounded">
            <element name="threatData" type="dateTime" minOccurs="1" maxOccurs="1"></element>
            <element name="threatDescription" type="string" minOccurs="1" maxOccurs="1"></element>
            <element name="threatSympthoms" type="string" minOccurs="1" maxOccurs="1"></element>
            <element name="gdrValidTime" type="int" minOccurs="1" maxOccurs="1"></element>
            <element name="www" type="tns:addressBlockT" minOccurs="1" maxOccurs="1"></element>
            <element name="firewall" type="tns:firewallT" minOccurs="1" maxOccurs="1"></element>
        </sequence>
    </complexType>

    <element name="gdr" type="tns:gdrT"/>
</schema>
```

Figure 3: Container used to carry GDR

The transmitted message should acquire information that is needed by the administrator to become aware of the identified threats, and evaluate importance of particular rule. After verification of symptom that were used to identify a threat or malicious activity, administrator could undertake additional steps, which better protect his domain. The information about symptoms are required by the administrator in any message sent. The rest of the information elements are optional. These are information describing the type and special characteristics of particular reaction, which should be undertaken in order to protect the domain. For example it might be the URLs of WWW infected sites, or IP addresses of users that behave suspiciously in the network.

The concept of TM cooperation with DM is presented in Figure 4.

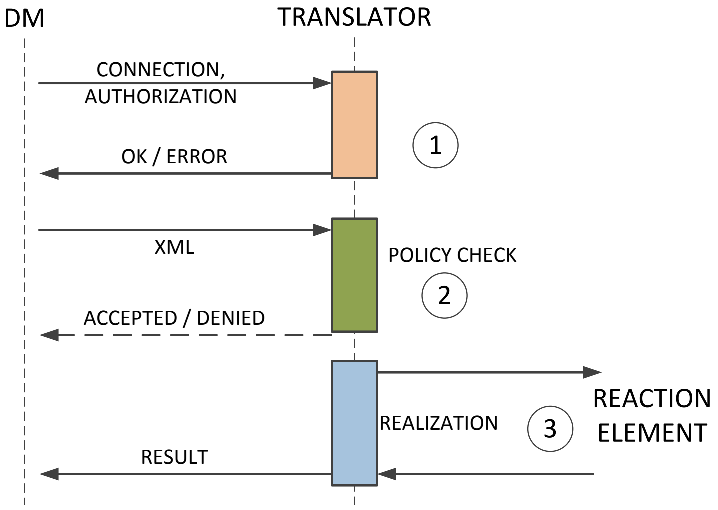


Figure 4: Activity diagram for Translator Module (TM)

Connection with the TM is possible after successful authorization to this element. Then the TM must connect with particular RE in order to implement decision rule. TM modules analyzes if the decision rules correspond to and fit into the domain security policy. After a positive analysis result the rule is implemented in the reaction element (by modification of RE's settings). All information related to authorization, rule rejection, configuration results, are available to administrator through the TM management interface.

One of the main assumption while developing the technical project of TM was the possibility to expand its functionality afterwards. The architecture of TM allows an easy extension of its capabilities by adding new components to handling RMs, and actualization of existing components in TM. To meet this criterion Translator Module has pluggable architecture that is presented in Figure 5.

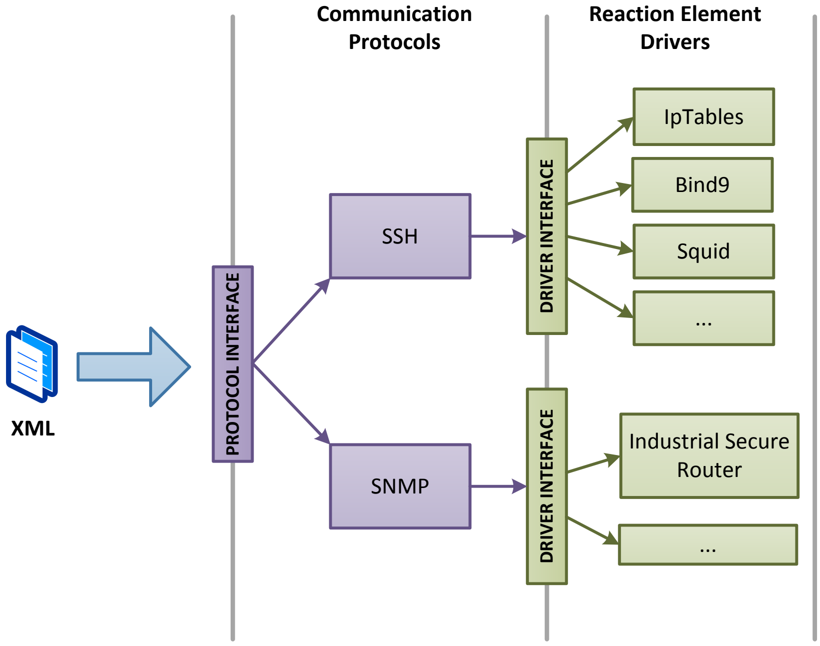


Figure 5: Pluggable architecture of TM

Application of the generated rule to RE is divided into two steps. Each component of TM is responsible for different step. The first step is to set up a connection with the reaction element by the means of handshake and authorization. This functionality is handled by communication manager component, which is used by different REs which are reached by that given protocol. Next step is to convert Generic Decision Rule to Concrete Applicable Command (CAC) in order to change configuration of RE. For each of that action a dedicated driver to adapt commands to appropriate RM is necessary. In Figure 6 the Translator Module sequence diagram that depicts full process of rule application in RM is shown.

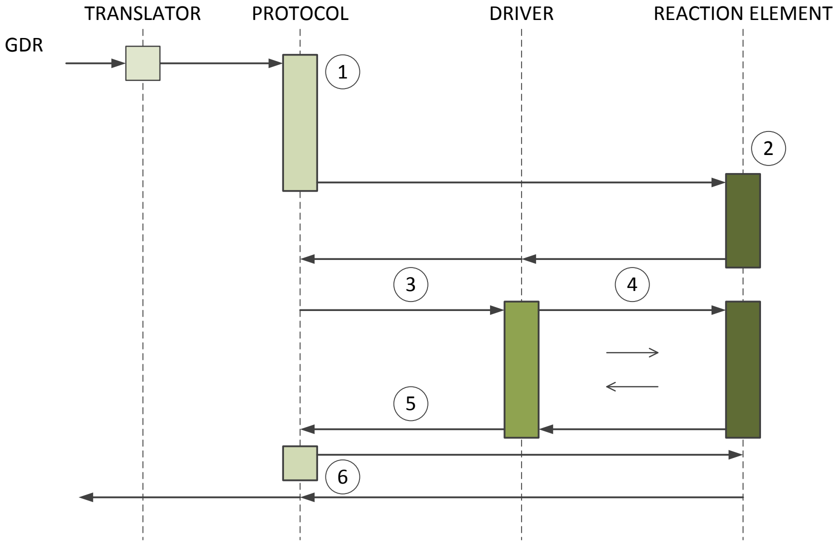


Figure 6: TM – Activity diagram

Figure 6 presents activity diagram for the Translator Module. The numbers indicated on it have the following meaning:

1. Performing validation of input message (Generic Decision Rule). Preparing to connection with Reaction Element;
2. Connecting with RE using authentication and authorization;
3. Data Exchange Streams (Input /Output) are passed to appropriate Driver, which is dedicated to appropriate RM;
4. The Driver element converts GDR to CAC and configures given RM;
5. End of RM configuration, recurrent delegation of the data exchange streams to the element handling communication protocol;
6. Finalizing configuration. Closing connection, and disconnecting with RM.

VERIFICATION AND DISCUSSION OF RESULTS

Implementation of the Translator was done in Java. The implementation class diagram for Translator Module is presented in Figure 7. This implementation was tested against its functionality and efficiency. Figure 8 presents the test-bed environment.

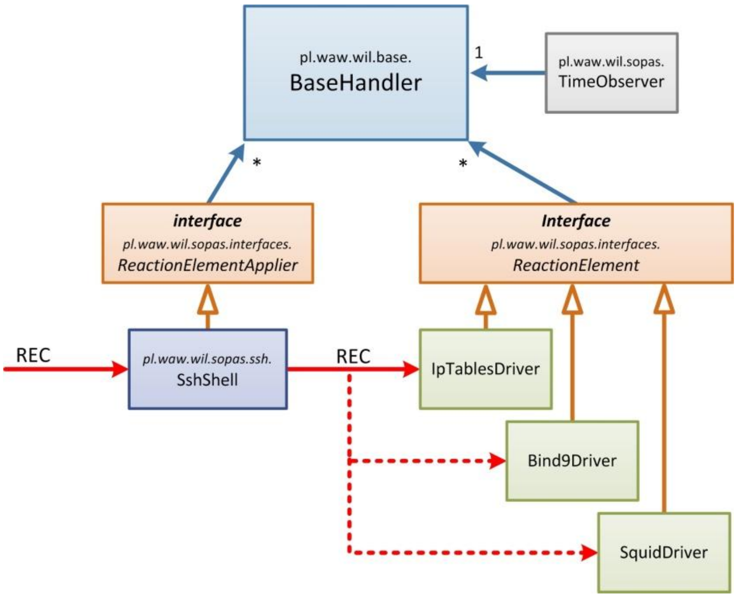


Figure 7: Class diagram of the TM

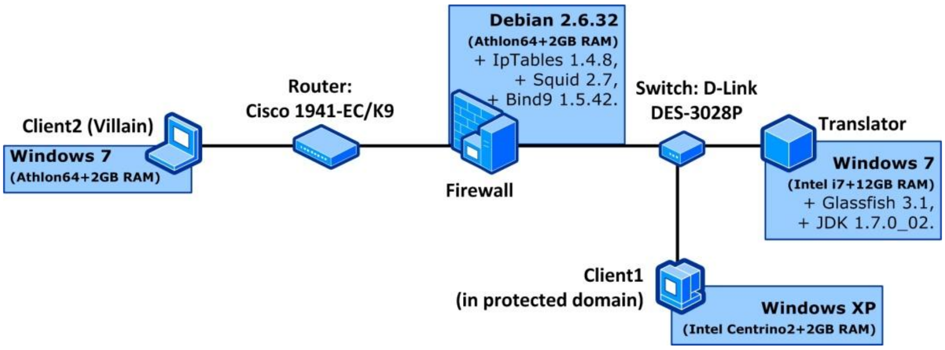


Figure 8: Measurement testbed diagram

The aim of the tests was to measure times of cooperation between RSC (TM) and REs. Tested REs were IPtables and Bind9. In Figure 9 is presented the chart with RCE - IPTables cooperation times. When RSC gets instruction, it processes it and executes on IPtables (see Fig 9). On X axis are times:

T1 – RSC gets instruction;

T2 – processing for audit purpose;

T3 – RSC is connected with RE (IPtables);

T4 – RSC is authorized in RE (IPtables);

T5 – Instruction has been executed at CE (IPTables).

Axis Y depicts time in miliseconds. The average total time of IPtables configuration by RSC was 0,9s (average for 20 discrete measurements). Test results with average times are shown in Table 1 below.

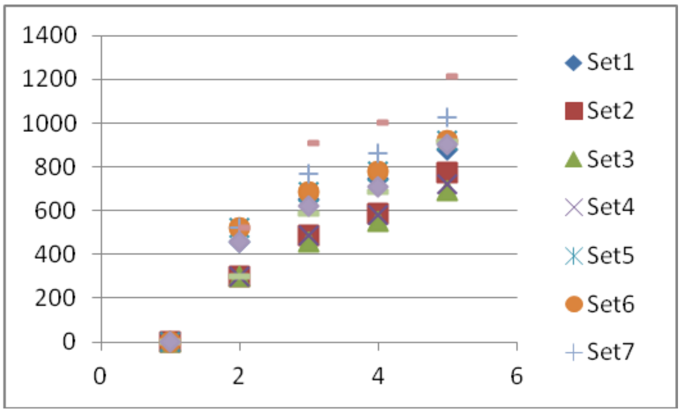


Figure 9: RSC – IPtables cooperation times (set 1 – set10 are values for particular measurements)

Table 1: RCS-IPtables average time of cooperation

	T2-T1 [ms]	T3-T2 [ms]	T4-T3 [ms]	T5-T4 [ms]
Average	430	230,5	94,8	173,05

The aim of the second test was to measure configuration time of the Bind9 DNS Server used as Reaction Element. Figure 10 shows similar time periods as in the previous test, measured when configuring Bind9. When RSC gets instruction, it processes it and executes on Bind. Axis X shows the following time periods:

T1 – RSC gets instruction;

T2 – processing for audit purpose;

T3 – RSC is connected with RE (Bind9);

T4 – RSC is authorized in RE (Bind9);

T5 – Instruction has been executed at RE (Bind);

T6 – Bind9 has been restarted;

T7 –Bind9 configuration has been checked after execution new instruction.

Axis Y presents time in milliseconds. The average total time of Bind configuration by RSC was 1,1s (average for 20 discrete measurements). The average times T1-T7 are shown in Table 2 below.

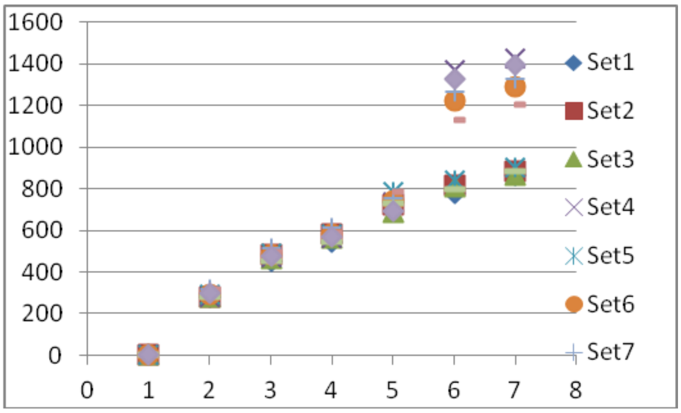


Figure 10: RSC – Bind9 cooperation times

Table 2: RSC – Bind9 average cooperation times

	T2-T1[ms]	**T3-T2 [ms]**	**T4-T3 [ms]**	**T5-T4 [ms]**	**T6-T5 [ms]**	**T7-T6 [ms]**
Average	296	189,6	96,2	169,8	304,25	71,4

SUMMARY AND FUTHER WORK

Presented in the paper RSC enables to work with many Reaction Element types. Its architecture is flexible and can be extended to support further types of REs. Speed tests have shown that time of executing an instruction depends on RE's type. The time is longer when RE needs to be restarted after performing an instruction (like Bind9). Nevertheless results obtained from tests are satisfactory and prove that RSC can be used to support automatic reaction on threats in FCDS and other cyber defence systems.

The crucial advantages of this solution are:

- Mobility of RSC – RSC may be run on the majority of software environments (PC, servers);
- Adaptability of RSC - it supports rules that indicate different REs with different configuration data (IP Addresses, network addressing);
- The complete production system may be built based on robust secured application server, static IP, and also monitored server units (IPS, IDS, antivirus software);
- Cooperation (configuration) is protected in local domain by using Secure Shell;
- The connection is secured by using TLS (VPN network could be used when needed);

The implementation is extendable through the application of the plugins to the new Reaction Elements, and/or Services:

- operating system processes (Scheduler),
- other business processes(User Services).

Some of the solutions in the presented realization of RSC can be seen as disadvantages:

- Necessity of installing additional software: JVM, and JEE 6 compliant application server needs to being installed.

- The server unit should be deployed in the DMZ

- RSC needs to be authenticated as a root in CE via SSH.

- Any CE units must have installed SSH server software.

The RSC plays an important role in the architecture of FCDS. The architecture of the whole system improves network security in FoS (based on the synergy effect), improves cyber situational awareness in protected FoS and integrates available IPS, IDS, FW systems (PnP). Application of the RSC enables fast and coordinated reaction against attacks.

REFERENCES

[1] “The Response to Cyber Threats in Federation of Systems Environment.”, MCC 2011: Military Communications and Information Systems Conference, Amsterdam,” R.Piotrowski, B. Jasiul, M. Śliwka, G. Kantyka, T. Podlasek, T. Dalecki, M. Choraś, R. Kozik, J. Brzostek;

[2] “Implementacja komponentu programowego do odbioru ORD od modułu decyzyjnego”, G. Kantyka

[3] “Opracowanie implementacji translatora”, T. Podlasek;

[4] “Integracja i weryfikacja komponentu programowego do odbioru I translacji ORD dla potrzeb elementów reakcji w środowisku testowym.” P. Skarżyński,

[5] “Opracowanie wersji docelowej komponentu programowego do sterowania WebProxy”, T. Szymczyk

[6] “Information exchange between domains in the Federated Networks Protection System” R. Kozik, M. Choraś

[7] Open SSH Server http://www.openssh.com/

[8] http://ibr94.multiply.com/journal/item/13/DNS_Blackhole_for_Spywaremalwareadware

[9] Black hole DNS for Spyware: http://www.malwaredomains.com/bhdns.html

[10] DNS Tutorial http://www.gnc-web-creations.com/dns-tutorial.htm

[11] http://www.hackcommunity.com/Thread-How-to-Make-Money-From-Your-Botnet-No-Surveys

[12] IPTables Guide, https://help.ubuntu.com/community/IptablesHowTo

[13] Glassfish Server Open Source Edition 3.1.1 http://glassfish.java.net/downloads/3.1.1-final.html

[14] PostgreSQL database server http://www.postgresql.org/

[15] The Secure Shell (SSH) Protocol Architecture http://www.ietf.org/rfc/rfc4251.txt

[16] SSH Tools, http://sourceforge.net/projects/sshtools/

[17] How to use Symantec Scan Engine 5.2 content scanning technologies for direct integration with your applications or devices, Symantec, http://www.symantec.com/connect/articles/how-use-symantec-scan-engine-52-content-scanning-technologies-direct-integration-your-appli

[18] Debian Home Page http://debian.org

[19] Java SE 6, Oracle, http://www.oracle.com/technetwork/java/javaee/tech/index.html

[20] Java EE 6, Oracle, http://www.oracle.com/technetwork/java/javaee/tech/index.html

[21] SSH Tools, http://sourceforge.net/projects/sshtools/

[22] How to use Symantec Scan Engine 5.2 content scanning technologies for direct integration with your applications or devices, Symantec, http://www.symantec.com/connect/articles/how-use-symantec-scan-engine-52-content-scanning-technologies-direct-integration-your-appli

[23] Debian Home Page http://debian.org

[24] Java SE 6, Oracle, http://www.oracle.com/technetwork/java/javaee/tech/index.html

[25] Java EE 6, Oracle, http://www.oracle.com/technetwork/java/javaee/tech/index.htmlhttp://www.securedsector.com/index.php?topic=93.0;wap2

Mitigating Denial of Service (DoS) Attacks
Case Study

The ultimate aim of a DoS attack is to prevent users from accessing a system or resource, and the potential cost to critical infrastructure can be considerable. The impact of downtime to critical infrastructure organisations may not be limited to lost revenue and goodwill, but can extend to social and human costs. Internet-dependent and networked infrastructure components are generally most at risk of a DoS attack.

A sufficiently motivated and skilled attacker may be able to commandeer adequate resources to overwhelm an organisation's infrastructure regardless of its level of preparedness. However, implementing an appropriate framework to manage the DoS threat can maximise the robustness of systems and minimise their downtime in the event of an attack.

Threat Assessment

A Threat Assessment is the most effective way to identify the DoS risks to your organisation. Following the AS 4360 Standard for Risk Management is considered best practice. Firstly, the context of DoS as relevant to your organisation is established, then attack vectors are identified, followed by an analysis of risk, and finally the evaluation of those risks, as illustrated in Figure 1, below.

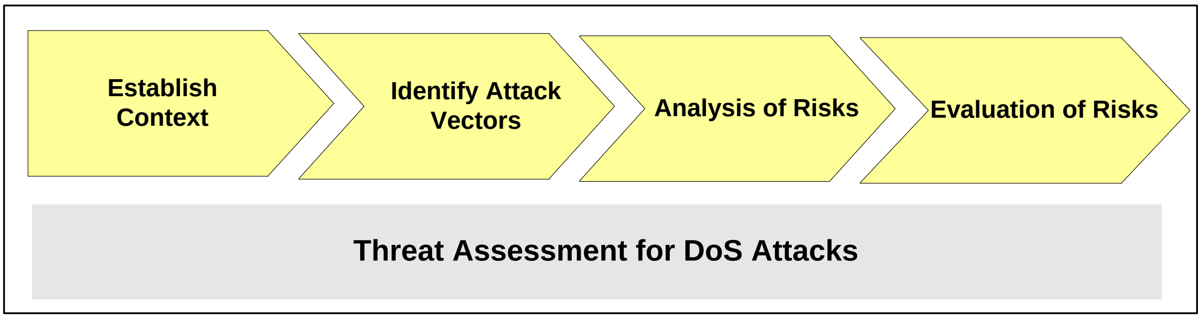


Figure 11 – High Level AS 4360 Risk Assessment Model

This section provides information to help organisations identify potential DoS targets in their business operations and IT environments, qualify the level of risk these targets are subject to, and consider the evolution of technology and threats and how this will change the risk assessment over time.

At first glance DoS attacks appear simple to define and distinguish; however, they can be categorised and sorted in numerous overlapping ways, and have a variety of very important factors to consider when assessing likelihood and impact. Important distinctions are:

- **Attack vectors** – Services subject to DoS attacks are not restricted to the electronic medium; people can be 'socially engineered' and procedural loopholes can be abused. In addition, pre-existing relationships between organisations can be exploited by attackers and leveraged in DoS attacks. For example, domain names can potentially be hijacked if an attacker is able to convince a domain name registrar to point a URL belonging to an organisation to an IP address controlled by the attacker. This prevents the web site of that organisation from being accessible to legitimate Internet users.
- **Attack mechanics** – For any DoS attack, it is important to ask "how was the attack executed?" and the most widely accepted categories are:

  - Consumption of scarce resources, such as network connectivity and bandwidth consumption.
  - Destruction or alteration of configuration information.
  - Physical destruction or alteration of network components.
  - Abuse of business logic.

- **Single point vs. distributed** – The aim of a DoS attack is to abuse specific weaknesses in business logic or system components. A Distributed DoS (DDoS) typically involves using a number of previously compromised computers to attack a target. A DDoS attack can be more difficult to defend against and detect. Reaction to a DDoS attack usually requires the help of the organisation's external service providers.

- **Client vs. server** – Compromising a networked service or functionality can be achieved either by impeding the ability of the server to provide the service or by impeding the client's ability to access the service. DoS attacks against the server are by far the most common, with the intention of affecting all clients of a resource rather than a particular subset.

- **External vs. internal –** DoS incidents can originate both from sources external to an organisation, or from within the organisation itself. Internal incidents can include the deliberate acts of disgruntled employees, inadvertent acts such as mis-configuration of systems or through internal security incidents that affect the availability of systems.

- **Internally managed vs outsourced** – Your business operations may rely on systems and networks over which you have little or no control, especially with the increasingly common use of cloud computing services and Software as a Service (SAAS). In such an environment, protective measures implemented by external service providers are also important for an organisation to consider.

- **Communication layers** – It is possible to target any of the seven OSI communications layers. Attacks directed at the higher layers (particularly the application layer) are generally more prevalent, sophisticated and harder to detect and prevent.

- **Weaknesses Exploited** – Most DoS attacks, especially distributed attacks, rely on fundamental weaknesses in computing infrastructure:
  - Unpatched systems
  - Lack of authentication
  - Poorly configured systems (including virtual systems)
  - Existence of reflectors/amplifiers
  - Difficulties in identifying an attack
  - Shared, vulnerable infrastructure

- **Motivation for Attack** – DoS attacks began to occur when a critical mass of organisations and individuals became Internet connected, giving attackers real incentive to strike. Their motivations include:
  - Credibility with other hackers for compromising a high-profile site
  - Retaliation for real or perceived slights or injustices
  - Monetary gain (criminal extortion or competitive tactics)
  - Political activism and cyber terrorism
  - Simple boredom, a desire for entertainment, or 'experimenting' with new attack techniques

  Some organisations may also be unintended targets for a DoS attack, either through a misdirected attack or sharing infrastructure with the intended target. Even in these cases, an appropriate strategy will still need to be in place to respond to such an attack.

- **Scope of attack** – While a DoS attack may be targeted against a specific component of an organisation's infrastructure (for example, its public website), the attack may also affect other systems as well (for example, the ability to send and receive email).

Attack Trends

The following summarises current and future trends in DoS attacks for use in identifying current DoS threats, and how these are likely to evolve over time:

Current:

- Reflection and amplification (including DNS recursion)
- Larger botnets & autonomous propagation
- Botnet markets which are increasingly sophisticated in nature
- Peer-to-peer botnets
- Botnets using encrypted communications
- Attacks against government infrastructure for political purposes
- Use of DoS by organised crime
- Attacks against virtual servers
- Increasing sophistication of malware and malware packaging

Future:

- Attacks on emerging technologies
- Application layer DoS
- Realistic behaviour of DoS traffic (further difficulty in detection)
- Attacks against anti-DoS infrastructure
- Attacks against SCADA systems
- Attacks against shared infrastructure and the 'cloud'
- Attacks against web services

Case Study: Major Australian ISPs subjected to DDoS Attacks

What happened?

In late 2009, two prominent Australian ISPs, aaNet and EFTel, were reportedly subjected to sustained DDoS attacks for a number of weeks. This severely inhibited their ability to provide quality service to customers due to a significant increase in packet loss and network latency.

The source of the attacks was initially unable to be pinpointed. Despite the longevity of the attacks, it is not clear whether the ISPs chose to contact law enforcement authorities for assistance. Nevertheless, the attacks confirmed that Australian organisations with a reliance on the Internet are a legitimate target for DoS attacks and need to take appropriate precautions to deal with the threat posed by such attacks.

What was the impact?

It was reported that for several weeks the customers of both ISPs experienced significant deterioration in the quality of their service. The attacks received significant publicity in the media and resulted in several complaints from customers.

How was the situation handled?

The ISPs embarked upon a series of core network upgrades, including installing additional equipment to alleviate the attacks and provide additional capacity to their customer base.

In addition, the ISPs contacted their upstream providers and worked with them to implement filtering mechanisms to block the hosts identified as playing a key role in the attacks.

The initial effectiveness of the attacks, however, highlights the importance of Australian organisations proactively implementing a management framework to address the threat of DoS attacks.

Sources & Further information:

http://www.infosecurity-magazine.com/view/3371/australian-isps-tackling-ongoing-ddos-attack/
http://www.itnews.com.au/News/153241,eftel-aanet-suffer-denial-of-service-attack.aspx
http://forums.whirlpool.net.au/forum-replies.cfm?t=1263410#r1

Threat Management

Developing an effective DoS threat-management strategy is a significant task. Therefore, focusing on key operational infrastructure rather than attempting to protect all systems from all DoS threats is the most productive approach.

Actions that can be taken by organisations in their policies and strategic approach to managing the DoS threat are:

- Incorporating DoS into organisational risk management
- Implementing a security management framework
- Undertaking staff training
- Negotiating Service Level Agreements with external service providers
- Participating in joint exercises
- Improving information sharing
- Obtaining insurance
- Encouraging industry / government collaboration (examples include the Cyberstorm and Cyberstorm II security exercises)

At operational and technical levels, a range of actions can be taken to protect against attacks, detect attacks, and provide a structured and effective response.

Protect

Protection from DoS attacks poses a challenge because no single technology or operational process will provide adequate protection.

The following **operational** processes may be used to help protect an organisation from DoS attacks:

- Conducting technology risk assessments considering the key variables discussed in this paper in the Risk Identification section
- Capacity planning
- Ensuring secure network design
- Ensuring physical security
- Utilising secure application design
- Including DoS in business continuity management
- Including DoS in security testing scope

The following **technical** measures can be used to provide a degree of protection against DoS attacks to network and system resources:

- Deploying anti-DoS devices and services
- Traffic filtering
- Utilising timely patch management
- Deploying anti-virus software
- Performing system hardening

Detect

Given the range of attacks covered by the broad titles DoS/DDoS, it is often not easy to know when an organisation is under attack. In the DoS case, the effects are likely to be immediate and result in a system or subsystem becoming unavailable. The symptoms of a DDoS attack may take longer to appear and are usually apparent in slow access times or service unavailability.

One **operational** measure is to develop relationships with key sources of current IT security intelligence. Groups such as CERT Australia are in a good position to predict, trace, and even work to shut down immediate threats to Australian critical infrastructure. Security vendors, including anti-virus firms and consulting firms, can also provide valuable advice on industry trends and response approaches. For this reason, it is recommended strong relationships are established with key security resources to keep abreast of the latest techniques and impending threats.

The following **technical** mechanisms do not always accurately detect and identify DoS/DDoS attacks. However, when used in combination a correlation of information can prove very effective. The following technical approaches can aid in attack detection:

- Deploying intrusion detection systems
- Developing and deploying monitoring and logging mechanisms
- Deploying honeypot systems to lure attackers away from the real systems

React

Reaction to attack is likely to be of greatest importance to many organisations but may be hampered by outsourcing and other technical hurdles. Organisations must be well prepared to act in the event of a significant and/or sustained DoS attack.
‘Reactive’ **operational** processes generally involve incident response and analysis. As such, items recommended for consideration to improve operational response capability are:

- Implementing incident response planning to define people’s roles and responsibilities, and the processes to be followed in an incident situation. Having clear incident escalation thresholds and clear internal communication paths between business areas in an organisation were identified in the Cyber Storm II exercise as key methods for improving incident response.
- Establishing relationships with telecommunications and internet service providers as these organisations can provide practical protection, detection, filtering and tracing in the event of a DoS attack. As identified in the Cyber Storm II exercise, established relationships with key organisations facilitates rapid information sharing during a DoS attack, helping to maintain situational awareness and ensuring more effective incident response and recovery. Establishing these relationships proactively is crucial because it is difficult to create trusted relationships during the middle of a DoS attack.
- Performing attack analysis to react to a current attack and to prevent future attacks.

Technical measures which can be deployed by organisations to respond to DoS or DDoS attacks include:

- Using upstream filtering to relieve pressure on subsequent infrastructure. This is the most common method used to mitigate active DoS attacks.
- Deploying Intrusion Prevention Systems (IPS) to automatically stop intrusion attempts when they are detected.
- Applying rate limiting to ensure that legitimate messages are not mistakenly discarded.
- Black holing malicious traffic to ignore network communications based on criteria that were identified in the attack analysis.
- Increasing capacity to maintain availability of systems in response to a resource consumption attack.
- Redirecting domain names as a short term mitigation approach to alleviating attack impacts by modifying or removing the IP address the domain name resolves to.

Conclusion

Denial of service attacks are a real threat to the operation of any networked computer system. While they can be difficult to detect and react to, prudent planning and preparation can mean the difference between a total shut down of the organisation and a slight inconvenience. The DoS management framework presented provides coverage of security before an incident, during an incident and after an incident. This is achieved by detailing a governing strategy and specific recommendations at both operational and technical levels for:

- Protecting against DoS attacks.
- Detecting attacks when they occur.
- Responding appropriately to counter current and future attacks.

Following the recommendations contained in this paper will provide your organisation with a solid base for minimising the impact of these potentially damaging attacks.

Available Resources

A considerable amount of work has been done in establishing strategies to cope with DoS and other malicious attacks. Following these established frameworks for DoS management will not only help to protect against DoS attacks but the flow-on effects to organisational security will be noticeable. These frameworks include:

- CERT/CC, *Managing the Threat of DoS Attacks* (2001) is the foremost best-practice framework for managing DoS risks. It is structured around the Protect, Detect and React triad, providing practical advice for all stages of the DoS lifecycles.
- *Consensus Roadmap for Defeating DDoS Attacks* (2000), developed by the Project of the Partnership for Critical Infrastructure Security in the United States, describes the problems and suggests remediation measures.
- ISO 27002 *Code of Practice for Information Security Management* (2005) outlines best practices for organisational protection of information resources. Aligning practices with these requirements will aid in the overall management of DoS threats.
- ISM *Australian Government Information Security Manual* (2009) provides policies and guidance to Australian Government agencies on how to protect their ICT systems.

- *ISP Voluntary Code of Practice for Industry Self-Regulation in the Area of e-Security* (2009) provides a code of conduct for Australian ISPs regarding the management of situations where subscribers have malware-infected computers that form part of botnets.

Summary of Recommended Actions

Strategic	• Incorporate DoS into risk-management program • Negotiate service-level agreements with suppliers for DoS protection and response levels • Consider running DoS scenarios to identify weaknesses (individually and also with business partners) • Participate in DoS information-sharing networks such as TISN, ITSEAG and CERT Australia

	Operational	**Technical**
Protect	• Include DoS security in testing scope (IT Security Manager) • Complete bottleneck analysis on finite network resources (Network Architect/System Administrator) • Include security in application and network design (Application/Network Architect) • Plan for capacity to endure DDoS attacks (Network Architect) • Implement appropriate physical security measures (IT Security Manager/Operation Manager) • Include DoS in business continuity management (Operations Manager)	• Utilise anti-DoS devices and services (Network Architect) • Apply ingress and egress filtering at network gateways (Network Architect) • Ensure rigorous patch management (System Administrator) • Ensure anti-virus controls are updated and effective (IT Security Manager/System Administrator) • Perform system hardening (System Administrator) • Configure routers and network edge devices according to best practice (Network engineer / System administrator)
Detect	• Create strong relationships with anti-virus vendors to keep abreast of the latest techniques and potential attacks (IT Security Manager)	• Deploy intrusion detection systems (IT Security Manager/Incident Response Team) • Develop monitoring & logging mechanisms (IT Security Manager/System Administrator)
React	• Form co-operative relationships with service providers (Operations Manager) • Establish DoS incident response plan (IT Security Manager) • Perform attack analysis (IT Security Manager/Operations Manager)	• Deploy intrusion prevention systems (IT Security Manager/Incident Response Team) • Implement rate limiting (System Administrator) • Apply black holing to drop malicious packets (Network Administrator) • Increase network/system capacity (System Administrator) • Redirect redundant domain names (System Administrator)

Cyber Crime Law Making
Case Study

Computer and Internet usage is on the rise due to lower costs of computer ownership and connectivity as well as faster and easier accessibility. As it is another mode of commercial and personal transaction and one that is heavily dependent on interaction through computers and automatic agents rather than face-to-face meetings, which increases distance and allows anonymity, it is another avenue for crimes to perpetuate.

“Computer Crime” encompasses crimes committed against the computer, the materials contained therein such as software and data, and its uses as a processing tool. These include hacking, denial of service attacks, unauthorized use of services and cyber vandalism. “Cyber Crime” describes criminal activities committed through the use of electronic communications media. One of the greatest concerns is with regard to cyber-fraud and identity theft through such methods as phishing, pharming, spoofing and through the abuse of online surveillance technology. There are also many other forms of criminal behaviour perpetrated through the use of information technology such as harassment, defamation, pornography, cyber terrorism, industrial espionage and some regulatory offences.

The existing criminal laws in most countries can and do cover computer-related crimes or electronically perpetrated crimes. Offences against the computer are relatively new as they arise from and in relation to the digital age, which threatens the functionality of the computer as an asset of a borderless information society. New laws are required in order to nurture and protect an orderly and vibrant digital environment. Offences through the use of computers merely constitute new ways to commit traditional offences using the electronic medium as a tool. In this case, existing legislation may not be suitable or adequate for several reasons; for example, the language in criminal statutes may not apply, jurisdictional issues may arise and punishments may not be appropriate.

In this case study, I will conduct an overview of the approach taken to criminal law making in three common law jurisdictions across three continents - the United States, the United Kingdom and Singapore. I will critically examine the adequacies or otherwise of the law making machineries of each country to meet the challenges posed by computer-related crimes. I will then assess the adequacies or otherwise of the global response to what is essentially a worldwide problem that requires a consolidated solution.

The selection of the three jurisdictions as the subject of study is meant to provide a taste of the challenges facing different sovereign entities with their unique blend of political, social, cultural and economic personalities. It allows a comparison of the treatment of laws by a federation of states on the one hand and unitary states on the other, and of the contrasting approaches between western and Asian as well as older and newer nations. This will be set against a common law backdrop, as these countries share similar legal systems and historical ties, and considered in the context of nations with developed information technology infrastructure. They will also provide a good springboard to assess the current trends in domestic crime prevention initiatives and in regional and global approaches to evaluate the current weaknesses in global response as well as to extract some suggestions to better the international criminal regime relating to electronically perpetrated crimes, which knows and respects no boundaries.

Because of the breadth of electronically perpetrated crimes and the depth to which an analysis of each type of crime can plume, the case study focus of this paper will be centered only on one of the most prominent form of crime that is relevant to both computer and cyber crime laws - Cyber-fraud and identity theft - through the act of what is commonly known as "phishing" and its progeny. The offence is also a useful case study as it is a 'universal offence' which is capable of uniform treatment,[1] and that makes it a worthy subject for a good comparative study.[2] "Phishing" is a term coined by the relatively new form of *modus operandi* by which scams are perpetrated through the Internet. It involves the theft of the identity of a target organization (the secondary target) for the purpose of stealing the identities of its users or customers (the primary target) without their knowledge or consent (i.e. a series of identity theft). This is done through the use of professional-looking, HTML-based e-mails that include company logos, font styles, colours, graphics, and other elements to successfully spoof the supposed sender (i.e. constituting fraudulent conduct). Most also contain a hyperlink to a web site, which is almost always an exact replica of the spoofed site, to lure users or consumers into a false sense of security and into relaying their personal information. The motive may be purely pecuniary but not always necessarily so. Also, the approach may be similar, but the *modus operandi* has since mutated and taken on many innovative forms. Hence, the type of offence that may be implicated can vary and can constitute a computer crime, a cyber crime, or both.

In Part 1 of this case study, I shall differentiate electronic criminal activities from its physical analogue and delve deeper into the distinctions between computer crime and

* Assistant Professor of Law, Singapore Management University. Executive Director, Society of International Law, Singapore. LLM in International Business Law, University College London, 2004. LLM in International & Comparative Law, Tulane University, 2001. LLB, National University of Singapore, 1996. Solicitor, England & Wales. Attorney & Counsellor at Law, New York. Advocate & Solicitor, Singapore.

[1] Moreover, cyber-fraud and identity theft is probably the biggest threat to electronic transactions (in particular, commercial transactions) today and it is the basis to many computer-related offences as well as other concerns relating to electronic transactions such as privacy and data protection, and the protection of intellectual property rights.

[2] In contrast, for example, 'content' related offences such as obscenity legislation and defamation laws are susceptible to a range and variety of treatment in different jurisdictions depending on the political and socio-cultural personality of the nation. Hence they are less useful as subject matters of a fair comparison of laws. See, e.g., Sofya Peysakhovich, *Virtual Child Pornography: Why American and British Laws Are At Odds With Each Other*, 14 Alb. L.J. Sci. & Tech. 799 (2004); Katherine S. Williams, *Child-Pornography and Regulation of the Internet in the United Kingdom: The Impact on Fundamental Rights and International Relations*, 41 Brandeis L.J. 463 (2003); and Dina I. Oddis, *Combating Child Pornography on the Internet: The Council of Europe's Convention on Cybercrime*, 16 Temp. Int'l & Comp. L.J. 477 (2002). Moreover, and this will be relevant later on in this paper, they are also less likely to be the subject of a universally harmonized legal response in the form of a widely subscribed treaty or of a consistently adopted model law. However, there are other approaches to dealing with such offences in as consistent a manner as possible.

cyber crime. The latest trends in the phishing case study will also be examined in some detail with particular emphasis on the latest developments in the United States, the United Kingdom and Singapore. In Part 2, I will analyze the current state of criminal legislation in the United States, the United Kingdom and Singapore with regards to computer and cyber crime and consider amongst other things the promptness of, and approaches to, law making as well as the extent that they have each successfully or otherwise managed to develop a response to new and novel types crime and forms of criminal activities. Some suggestions will be made to the current approaches to improve the system. The phishing case study will further illustrate the diversity in approaches and the problems relating thereto. Finally, in Part 3, I will examine and propose a multilateral *and* multifaceted approach to criminal law making in this field to adequately and promptly address the emergence of 'new' offences and the evolution of the ways in which 'old' offences are perpetrated. In the process, I will provide an overview of the current state of affairs and show that in fact international efforts have already been made; they only need to be done in a concerted, coordinated and consistent manner in order to be a more efficient and effective weapon against crime in the cyber realm.

Part 1 – Electronically Perpetrated Criminal Activities: Similarities and Distinctions

Crimes committed against the computer are relatively new offences that relate to the computer, the materials contained therein and its uses as a processing tool. This is to ensure that owners and users of the computer and electronic systems will continue to enjoy their usage with minimal incursion into their socio-economic well being or personal space as a result of the anti-social behaviour of others who seek or facilitate illegitimate access. It is the medium itself that is threatened in the case of computer crimes. On the other hand, there are traditional crimes committed *through* the electronic medium, which is used as a tool to commit offences that already exists. In such a case, the digital media is merely used as an alternative instrument to perpetrate criminal objectives. In order to distinguish between the two and their separate legislative regime, a different term will be used to describe them.

It is very common to deal with any computer-related offence under a singular term, whether as "computer crime" or as a form of "cyber crime".[3] However, it is important to differentiate offences that are more appropriately termed "computer crime" and those activities that fall under the description of "cyber crime" and to accurately categorize them.

A. Computer Crime and Cyber Crime Are *Different Offences*

Computer crimes are to be distinguished from computer-enabled crimes. They relate to crimes against computer hardware as well as the digital contents contained within it such as software and personal data. Computer crimes have an adverse effect on the integrity

[3] See, Marc D. Goodman and Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 2002 UCLA J. L. Tech. 3 (2002). The authors noted that cyber crimes are "complex and sometimes elusive phenomena" and that "there is no comprehensive, globally accepted definition that separates the sensational from the sensible and scientific".

and trust in information technology infrastructure such as computer or telecommunications networks and in the security of transactions conducted through them.

"Computer crimes" is often used to define any criminal activities that are committed against a computer or similar device, and data or program therein. In computer crimes, the computer is the *target* of criminal activities. The "computer" in this context refers to the hardware, but the crimes, as we shall see, more often than not relate to the software and the data or program contained within it. The criminal activities often relate to the functions of the computer; in particular, they are often facilitated by communications systems that are available and operated through the computer, thereby contributing to a less secure computing environment. Examples of interactive systems include Internet connectivity for access to the World Wide Web (WWW) through PCs, laptops, tablets and hand-held devices, and telephony or messaging connection through hand phones and other mobile devices. Crimes are also perpetrated not merely through the means of connectivity alone but also through other software programs and applications that are available for use in transaction and human interaction, such as electronic mail and instant messaging services, audio-visual conferencing programs and file transfer facilities.

Due to its very nature, computer crimes are generally new, technology-specific criminal behavior for which specialized legislation is required.[4] These offences are related to, for example, computer usage and access and crimes against other's interests and rights so related. Examples of such computer crimes include hacking, denial of service attacks and the sending of unsolicited electronic or "spam" mail. The array of crimes relating to cyber-trespassing has become more diverse due to advances in technological developments. This is illustrated, for example, by the amendments made to the Singapore Computer Misuse Act (Cap. 50A) (CMA) since its enactment in 1993, which expanded the list of such offences significantly.

On the other hand, it is often the case that cyber crimes are considered adequately dealt with under existing legislation albeit with some necessary modifications in their language and terms, particularly relating to their scope of application as determined by their definition and interpretation.

"Cyber crime" will be taken to mean offences committed *through* the use of the computer in contrast to "computer crime" which refers to offences *against* the computer. Under this distinction, cyber crimes are a sub-set of the general term "crime" and the only difference is the use of the computer as the facilitative device and the use of electronic media as another means to commit a 'traditional' offence. On the other hand, computer crimes, as we have seen, are non-traditional crimes that arose directly from the advent of the age of personal computing for managing information and communication, and that do not exist

[4] See, Douglas H. Hancock, *To What Extent Should Computer Related Crimes Be the Subject of Specific Legislative Attention?*, 12 Alb. L.J. Sci. & Tech. 97 (2001). See also, Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. Pa. L. Rev. 1003, 1013 (2001). The author described different types of computer crimes without real-world analogue. See further, Stephen P. Heymann, *Legislating Computer Crime*, 34 Harv. J. On Legis. 373, 373-91 (1997). The author analyzed technological advances that require new criminal legislation.

separately from its existence. One can characterize computer crimes as cyber-trespass – the crossing of both tangible as well as intangible, but no less real, cyberspace boundaries onto property that are owned and controlled by another without permission or authorization. It can also involve the infringement of another's rights including privacy, informational, proprietary and economic rights.

Cyber crimes are activities committed using the Internet or computer or other electronic devices as the medium, in violation of existing laws for which punishment is imposed upon successful conviction. What we call cyber crimes largely consists of common crime, the commission of which involves the use of computer technology, and for which penalties already exists under existing legislation. For example, in the Singapore context, the offences listed under its Penal Code (Cap. 224) and other criminal legislation and provisions. Substantively, there is no difference between generic individual crimes such as fraud, theft, extortion, harassment, forgery, impersonation, and their cyber-analogues. Only those that relate specifically to computer usage and materials are specialized offences for which the CMA has been specifically enacted to tackle. Of course, in certain cases, both computer crimes and cyber crimes may be committed by an act or a series of acts.[5] In such a case, more than one charge may be brought in the alternative against the offender.

Cyber crime also includes the *use of digital resources* to commit traditional crimes such as theft of identifiable information and other forms of proprietary information or property in both *digital and physical form*. The relevance of this to the phishing case study will become apparent in due course.

B. Cyber Crime and Traditional Crimes Can Get *Lost in Translation*

There are three main characteristics that differentiate traditionally terrestrial crimes from cyber crimes. First, the absence of physical barriers such as customs to enter or exit the WWW allow netizens to roam freely within it and to visit web pages wherever their origin. In turn, this means that the actions and potential victims for cyber-criminals are not geographically limited. Hence, for example, the randomness and volume of emails sent in the attempt to perpetrate scams online, most famously the "Nigerian scam" involving advanced fee fraud. Second, the cyber realm affords the cloak of anonymity, fakery and deception much more easily than the physical realm. This is even more so if the entire criminal transaction can be performed electronically without the need for physical manifestation. For example, electronic communications can lead to online money transfers for the sale and purchase of digital products and services that can be delivered electronically without the need for any physical contact or movement at all. Third, traditional evidence gathering techniques are not effective because cyber-criminals

[5] For example, see section 4 of the Singapore CMA which makes it an offence to cause a computer to "perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence…involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years." This section will overlap with the relevant provisions under other legislation, in particular the Penal Code that fits the criteria.

can execute their schemes without being physically present and they can do so through automatic agents. These pose unique challenges to law enforcement and criminal investigations and forensics. They all contribute to the electronic medium as an attractive tool for criminal activity, over and above the speed, ease of use, low costs (e.g. no need for the middleman) and efficiency of the digital realm.

Some people even go so far as to argue that cyber crime is a separate and distinct phenomenon from traditional crime with material differences that require a new approach in the imposition of criminal liability and in the administration of criminal justice. Underlying this belief is the perception that virtual crimes are actions in cyberspace, with its shared virtual community and virtual citizens, and consisting of a mixture of real identities, alter egos, clones and even virtual beings. Hence, it is fundamentally different from crimes committed in the physical world. As such, the application and standards of criminal laws for the virtual community should be markedly different from those commonly applied in the courts of the physical world. Though their views appear futuristic and far-fetched at this point in time, the potential for its full or partial adoption may be foreseeable. Already, there are serious talk of the creation of cyber-courts to administer and dispense cyber-justice, which may entail punishments that are unique to the medium and that may not have a real world equivalent (e.g. banishment from a cyber-community such as an e-commerce portal).

As we are now aware, cyber crimes are traditional crimes committed through electronic mediums such as PCs, laptops, tablets, blackberries, palmtops, mobile phones and pagers (i.e. various forms of electronic medium), and networks or programs such as the Internet, telecommunications systems and messaging services. Cyber crimes are perpetrated across the board against individuals, businesses, organizations and even governments, often through fraud, deception or stealth such as *via* system infiltration. Let us consider some of the more prominent categories of cyber crimes.

If the crime relate to political, religious or other such causes and to the administration, they can constitute niche offences like sedition or even “cyber-terrorism”. These are a separate type or breed of problems with their own unique legal solutions, although the *modus operandi* may remain the same. And then, of course, there are the content-based offences relating to obscene (e.g. pornographic, violent or otherwise offensive) materials or defamatory statements, which are susceptible to differential treatment in different jurisdictions. Last but not least, there are the infamous cases of cyber-fraud and identity theft conducted through emails and other forms of communications, which illustrate the potential randomness and worldwide effect of certain cyber-criminal activities.

Fraudsters are evolving with the times and always seem to be able to find new tricks to perpetrate old crimes. We can expect the actual permutations of cyber crimes to be larger if we consider other lesser-known methods; and to grow as we see more innovative and ingenuous technological ways to commit crimes.

Although cyber crimes are generally an extension of traditional crimes in that the electronic media is a relatively new instrument by which traditional offences are carried out, that does not mean that existing laws are adequate or even appropriate to deal with these new scenarios in terms of coverage or public policy. Moreover, as we have seen, there are more unique problems that relate to cyber crimes more than they do to real world crimes, in particular, jurisdictional and enforcement issues.[6]

There is a *lost in translation* phenomenon when it comes to country practices in updating traditional penal laws in a piecemeal, statute-by-statute manner to cyberspace transactions.[7] This happens whenever the process of augmentation is either slower than developments in cyber crime techniques or technology used to further such offences, or is fraught with mistakes or is immediately outdated due to the speed of developments in this area. These lead to a lacuna in the law, which cyber criminals can take advantage of. Even where there is coverage, it does not mean that the punishment suits the crime as some of the existing provisions may contain penalties that are outdated or that fail to achieve other social policy objectives such as in deterring or preventing further offences or in punishing or rehabilitating offenders. Examples in relation to the phishing case study in the context of United States, United Kingdom and Singapore law will be considered in Part 2 of this paper.

Returning to the question of the significance of the distinction between the two categories just enunciated; it is clear that there is good reason to categorize them separately. They are as follows:

1. Differences in Objective or Subject Matter

First, the elements forming both categories of offences are very different, particular the *mens rea*. For instance, the knowledge or intention element required to prove that a computer crime has been committed generally relates to its use and its contents and involves objectifying the computer and the contents therein as a form of property that is inherently in need of protection. Very often, motive is irrelevant either as an element of the offence or as a form of full or partial defence. On the other hand, the range of mental elements involved in the proof of a cyber crime is more complex and relate to the commission of the specific offence concerned that has little or nothing to do with the computer or its contents but more to its functions, and even then only to the extent that it is used as a conduit or instrument to perpetrate and realize the primary offence. The *actus reus* for computer crimes relate directly to the computer and its contents while the physical element for cyber crimes primarily relate to the offence concerned such as that relating to tangible property, a person's body or reputation, and public policy.

[6] Hence, many computer-related criminal legislation provides for extra-territorial application of the statute to acts perpetrated in another country even if the activity may be lawful where it is committed, which is likely not the case. However, the true effects and reach of such legislation is probably less effective than we would prefer. See, Michael Geist, *Cyberlaw*, 44 B.C. L. Rev 323, 345-346 (2003).

[7] See, Justin Hughes, *The Internet and the Persistence of Law*, 44 B.C. L. Rev. 359, 360 (2003). The author noted three possible treatment of the law and cyberspace relationship: The "no-law Internet", the "Internet as a separate jurisdiction", and Internet law as "translation". The latter is the most pragmatic approach, which involves finding legal tools to approximately reach the same balance of interests in the Internet that we have developed for the real world. This is the approach that is endorsed in this paper and that is the predominant approach in most jurisdictions.

2. Differences in Treatment Under Some Legal Systems

Second, the comparative analysis to follow will show that in fact the two categories of offences have been treated differently as two separate regimes in some countries such as Commonwealth countries, such as the United Kingdom, Singapore and Malaysia, which enacted a specific statute to deal with computer crimes, while leaving cyber crime to be dealt with under existing legislation; sometimes but not always with the necessary amendments to ensure adequate coverage and appropriate enforcement mechanisms.

3. Universal or Differential Treatment in Different Jurisdictions

Third, most computer crime offences are universal in treatment, whereas there are two sub-categories of cyber crimes. Cyber crimes consists of those that are generally universal in nature and hence are susceptible to equal and similar laws and punishments in most, if not all the countries in the world; and those that receive differential treatment in different jurisdictions due to the social and cultural make-up of the country and the political environment of the jurisdiction concerned.[8]

On a more holistic level, there are similar policy objectives between both categories of offences, which can together fall under the umbrella term of "computer-related offences" or "computer-related crimes". It is to protect individual users and consumers as well as legitimate organizations and companies in their use of computers and information technology to interact and to transact; and in so doing protecting and promoting the effective and efficient use of information technology such as the Internet for human interaction and transactions such as e-governance (i.e. G2B and G2C), e-commerce (i.e. B2B and B2C) and e-communications (e.g. C2C).

C. The Great Expansion of Cyber Crime Activities: The "Phishing" (Cyber-Fraud and Identity Theft) Case Study

1. Horizontal Expansion – The Rising Problem of Electronically Perpetrated Criminal Activities in Every Jurisdiction

a. Latest Updates on Phishing Scams in the United States and the United Kingdom

All the world is a pond for phishers. Scams including those perpetrated through the phishing technique continue to grow despite the ongoing efforts by private technological initiatives and public law enforcement to combat them. This is due in part to the extraterritorial nature of such schemes, the availability of crimeware and the ease of modification, use and abuse of new technologies. Reports of phishing scams, for

[8] However, it is foreseeable and it is indeed the case that for some offences there will be an overlap of coverage such that the relevant provisions of both types of crimes can be applicable. In such a situation, which is common in criminal law, it is for the prosecuting authority in its discretion to select the criminal law provisions for which the offender should be charged with, taking into account many factors such as the profile of the offender, the magnitude and severity of the offence, the available punishment and so on.

example, have been on the increase in the United States and the United Kingdom and other countries where users have already experienced such scams for years; and they show no signs of abating. In the United States, the threat is treated with such seriousness that the Department of Homeland Security (DHS) has created a new position, the Assistant Secretary of Cyber Security and Telecommunications, to oversee the department's effort to address ongoing cyber threats. [9] Not only are the effects of the threat felt in the United States, they also increasingly originate from these countries.

Statistics collated by the Anti-Phishing Working Group (APWG)[10] show that the number of targeted brands for phishing activities has increased within a one-year span.[11] The United States and to a lesser extent the United Kingdom and some other countries have already seen litigation on phishing scams, but these have invariably been based on non-specific legislation.[12]

These phishers of men believe in casting their nets far and wide. Even countries that have a smaller base of computer users or less developed Internet connectivity are starting to see the emergence of such activities, partly due to the randomness and expansion of the scammer's activities and the transnational nature of their activities. In these countries, the authorities are beginning to see the need to educate its public and enhance security measures, including the prescription and enforcement of relevant criminal provisions.

b. The Singapore Experience: New Phishes in the Pond

In Singapore, reported cases of phishing have only emerged more recently but it seems to have become more prevalent.[13] In July 2006, National news agencies reported that two banks in Singapore have been the targets of the latest phishing scam.[14] Emails purportedly from Citibank and OCBC Bank were sent to their customers asking the

[9] See, Leroy Baker, *IRS Sends Out Warning After New Wave Of "Phishing" Scams* (Tax-News.com, N.Y., 11 July 2006), available at: http://www.investorsoffshore.com/asp/story/storyinv.asp?storyname=24193; and Brooke Nelson, *I.R.S. Warns: E-mail Fraud on the Rise* (Standard-Examiner, 11 July 2006), available at: http://www.standard.net/standard/84203. This appointment follows in the shadow of a 2003 report entitled "National Strategy to Secure Cyberspace" that detailed the possible threats faced by United States, and how the private and public sectors might combat those threats. The new Assistant Secretary will be working closely with the United States Computer Emergency Readiness Team (US-CERT) a partnership created in 2003 between DHS and private businesses to protect the Internet infrastructure defending against and responding to cyber attacks.

[10] The Anti-Phishing Working Group (APWG) web site is at: http://www.antiphishing.org/. The APWG is "the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types." It has a data repository that contains updated information on phishing trends.

[11] See also, Bob Sullivan, *Consumers Still Falling for Phish: FTC, DOJ Announce Prosecution of Teenager* (MSNBC, 22 March 2004), available at: http://www.msnbc.msn.com/id/4580909.

[12] See, e.g., FTC, *FTC, Justice Department Halt Identity Theft Scam: Spammer Posed as AOL and Paypal to Con Consumers Into Providing Credit Card Numbers* (FTC News Release, 22 March 2004), available at: http://www.ftc.gov/opa/2004/03/phishinghilljoint.htm.

[13] One case was reported in 2004 and another in 2005. This year so far two cases have been reported to the police.

[14] Wong Mun Wai, *Two Banks the Targets of Latest Phishing Scam* (Channel NewsAsia, 11 July 2006), available at: http://www.channelnewsasia.com/stories/singaporelocalnews/view/218454/1/.html.

recipients for their personal data in order to verify their accounts, otherwise access to their accounts would be denied. OCBC Bank issued a media release to advise the recipients to ignore the email, stating that it was not the bank's practice to conduct such random security verification checks on customers in this manner. It also warned its customers not to respond to emails requesting them to provide their passwords, PIN or confidential information *via* hyperlinks, redirection links within an email or on a third party website. The fraudulent sites have since been closed and the matter was brought to the attention of the Monetary Authority of Singapore (MAS) and the Singapore Computer Emergency Response Team (SCERT) for further investigations and action.[15] The Singapore Police Force (SPF) and the Infocomm Development Authority (IDA) are also currently working with local banks to monitor phishing scams closely. Ironically, the MAS itself was a target of phishing within the same month.[16]

A new poll conducted on a regional news channel, channelnewsasia.com, indicated unsurprisingly that Singaporeans want more security from banks and companies while transacting online.[17] Visitors to channelnewsasia.com were asked for their views are on Internet banking and shopping transactions. The latest figures read that 44 percent of them want additional security when shopping and banking, but another quarter felt it was really up to the individual user to take personal precautions.[18] It was also reported that the sentiment on the street showed a similar wariness of the Internet.

2. Vertical Expansion – The Constantly Evolving Technological Landscape and Emerging Crimeware Technique

Practices, targets and objectives relating to phishing and other activities have expanded thereby greatly exacerbating the problem. For example, backdoor Trojans, which are malware programs that perform unexpected or unauthorised actions on the user's computer, are now also used to enable unauthorised access to a user's computer and the information contained therein by remote systems. Phishing has also now expanded its bait to include e-government web sites such as monetary, tax and social security agencies, where users often transact, sometimes in financial assets, using personal

[15] In the meantime, warnings have also been made to the public of fraudulent emails and web sites through the media. Warning even appear on Auto-Teller Machine (ATM) screens advising its users to be alert to devices attached to the card reader of money dispensing machines that have been installed by fraudsters to steal their financial passwords and identification numbers in order to access their bank accounts to withdraw or transfer their money. See also, Joyce Chen, *Two Banks Hit by a Spate of Phishing* (Today Paper, 1 August 2006), available at: http://www.todayonline.com/articles/130010.asp.

[16] Lorna Tan, *Singapore's Central Bank Targeted by Phishing Scam* (Straits Times, 29 July 2006) at H7. The Central Bank issued a statement that it had learnt of "isolated cases of fraudulent e-mails containing the MAS' name, logo and letterhead". The matter had been handed over to the Commercial Affairs Department for investigations. The matter was given coverage on the local newspapers to alert and educate te public. It is worth nothing that these cases of phishing were all notified by suspicious consumers and users, which shows the importance and power of public education and involvement in crime prevention.

[17] Wong Mun Wai, *Channel NewsAsia poll suggests online banking & shopping security important* (Channel NewsAsia, 13 July 2006), available at: http://www.channelnewsasia.com/stories/singaporelocalnews/view/218999/1/.html.

[18] That was the response of 960 people that had responded at the time of reporting.

information. Phishing may involve the theft of identity for purposes other than mere illegitimate pecuniary gain.

New technologies emerge that can be both used and abused, such as surveillance technology. The phenomenon of emerging innovative crimeware techniques and of "blended threats" are due to, first, the changing intent of software creators, in particular of malware writers, and second, the attempts by them to keep one step ahead of the increasingly sophisticated Internet users in order to perform acts on and in relation to their computers and its communications function.

The profile of malware creators is not one-dimensional. They can be motivated by a variety of purpose and even by more than one objective. There are those who create such programs for fame and respect, particular within the programming community; others do so for the purposes of financial gain[19] or for business advantage;[20] and there are also those motivated by genuine personal interest and intellectual stimuli. The profiles of malware users are more varied as they can be motivated by curiosity, greed, revenge or any other objective. The threat in itself is a problem for information integrity and financial security, which require the maintenance of privacy and confidentiality of personal data, transactions and communications.

Because of the abovementioned motivations of the malware creator and user and the fact that the ongoing effectiveness of a malware depends very much on its evolution to maintain its immunity against anti-malware programs and the increasingly sophisticated Internet user, crimeware evolves in several ways through the confluence of technology and techniques:

a. New Technologies

The APWG in their web site refers to "technical subterfuge" as "schemes [to] plant crimeware onto PCs to steal credentials directly, often using Trojan keylogger spyware. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning."[21] It is only the use of new technologies *per se* if there is no active engagement of the victim, such as subterfuge through the use of spoofed emails and counterfeit web sites in order to get the victim to actively download the crimeware albeit while under a false assumption. New technologies also include new

[19] Involving the intention to steal passwords, bank account information, credit card numbers, social security numbers, and other forms of sensitive information in order to use that information for the illegal purpose of transferring financial or other assets (e.g. intellectual assets such as trade secrets, client lists and other valuable confidential information) belonging to the victim to the malware creator/user who installed it on the user's computer, with or without any action from the latter but without his knowledge or consent.

[20] E.g. Corporate or industrial espionage. Anyone can be a victim, whether targeted or otherwise, of such technologies including individuals and corporations, public sector or private sector entities, employers and employees, etc.

[21] See, the APWG web site at: http://www.antiphishing.org/. The APWG refers to the current two main phishing methods as "social engineering" and "technical subterfuge". The former is used to describe the original method that is phishing.

forms of information technology such as Instant Messenging (IM) Systems, where we already see new variants of phishing emerging.[22]

b. Blended Techniques

An example of this is what is known as “spy-phishing” which is the progeny of spyware[23] and phishing or backdoor Trojans. “It uses phishing techniques to initially present itself to users, then typically engages a host of other techniques and exploits to surreptitiously download and install spyware applications in the background. These applications oftentimes download additional spyware applications to further extend their functionality.”[24]

c. New Techniques

One new method of stealing identifiable information and other forms of personal and corporate information, in particular through capturing password and login data, is through what is known as “pharming” which is a derivative term of phishing. It involves either the exploitation of vulnerability in the Domain Name System (DNS) software or by changing the hosts file on the victim’s computer in order to acquire the domain name for the pharmer’s web site so that the traffic that would normally be directed to the original and genuine web site will instead be redirected to his web site.

[22] See, *New Cyber Scams: Online Con Artists Are Getting Smarter* (Straits Times Digital Life, 25 July 2006); in particular Chua Hian Hou, *Phishing Methods Get More Inventive. Ibid.* at p.3. See also, Chua Hian Hou, *The Essential Cheat Sheet. Ibid.* at p.4 (introducing readers to new scamming methods like “escrow”, “vishing” and “reshipping”). Just as phishing derived its moniker from “phreaking” (telephone scams), it has in turned spawned the names of new electronic communications conduits for scams including “pharming” and “vishing” (i.e. VoiP scams). On the more recent phenomenon of vishing scams, see Andrew Lavallee, *Email Scammers Try New Bait in ‘Vishing’ For Fresh Victims* (The Wall Street Journal, 17 July 2006), available at: http://online.wsj.com/public/article/SB115309244673308174-dWwztRkdlWIvH6bL_mhk7RlSW7I_20070717.html?mod=blogs; and Justin Cole, *‘Vishing: Beware of E-mail Asking You To Phone Your Bank* (AFP, 23 July 2006), available at: http://news.yahoo.com/s/afp/20060723/lf_afp/usbankinginternet_060723223705.

[23] “Spyware” are software that secretly installs itself on a user’s computer and runs in the background in order to log the user’s personal information and perform surveillance on the user’s actions without his knowledge or real consent, although the user may have downloaded the software inadvertently or installed the spyware by his own actions.

[24] Internet security company Trend Micro has also issued a warning against spy-phishing, which uses the phishing technique as well as spyware programs to target online banks and other password-driven sites. It sees spy-phishing as the next step for phishers and spyware authors who want to steal money and personal information from users. Some do this by creating programs to steal credit card numbers, account log-ins or a variety of other types of personal information. See, Daniel Lim, *Trend Micro Warns Against Spy-Phishing* (HardwareZone.com News, 12 July 2006), available at: http://www.hardwarezone.com/news/view.php?id=4939&cid=8&src=rss. “According to data collected by Trend Micro, the amount of Trojan spyware such as that employed in spy-phishing attacks has been steadily increasing. According to the Trend Micro Trojan Spyware Index, the incidence of Trojan spyware has increased by over 250 per cent over the past 16 months. Similarly, according to a report published by the Anti-Phishing Working Group, an average of more than 188 new samples of Trojan spyware have been utilised in spy-phishing attacks each month in the first four months of 2006 – a 234 per cent increase over the same period in 2005.”

Part 2 – A Comparison of Computer and Cyber Crime Legislation in the United States, the United Kingdom and Singapore *featuring* Cyber-Fraud and Identity Theft Legislation

A. The United States

The United States is a Federal Republic and its Constitution allocates lawmaking authority between the federal and state levels in accordance with certain principles.[25] Federal legislative jurisdiction is limited and is exercised only where intervention at that level is required such as where problems are national in scope and the solution lies in a uniform and consistent law that is common to all states. In that sense, computer crimes and cyber crimes that are easily perpetrated across borders and that are considered illegal in all states is a good example of an area of law that is susceptible to federal treatment. In actual fact, computer crime and cyber crime legislation have been formulated and adopted at both federal and state levels.

Due to its political structure, computer-related crime legislation and enforcement remain largely under state jurisdiction of prescription, adjudication and enforcement.[26] Each state has its own unique set of criminal legislation and there is no formal mechanism compelling them to adopt uniform or consistent laws.[27]

The United States Department of Justice (DOJ) have defined “computer crime” as “any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution”,[28] which for our purposes would be the same as “computer-related crime”. However, the DOJ had also further divided computer-related crimes into three categories according to the computer’s role in the particular crime: The computer as the “object” of a crime, as the “subject” of a crime (i.e. computer crimes for which there is no analogous traditional crime and for which special legislation is needed), or as an “instrument” of traditional crimes.[29] This compartmentalization resembles the categorizations made under Part 1.

Since 1984, the United States Congress has pursued a dual approach to combating computer crime.[30] The Counterfeit Access Device and Computer Fraud and Abuse Law of 1984 and subsequent amending Acts address crimes in which the computer is the

[25] See, U.S. CONST. Art. I § 8, which lists the United States Congress’ power to legislate in various areas; and U.S. CONST. Amend. X, which states that: “The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people.”

[26] See, Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey,* 7 RICH. J.L. & TECH. 28 (Winter 2001), available at http://www.richmond.edu/jolt/v7i3/article2.html.

[27] Except, for example, insofar as federal legislation preempts state laws where they conflict. However, there are many non-mandatory instruments that seek to persuade states to adopt laws in as similar a fashion as possible, including Restatements of Law, Uniform Acts and the Model Laws (e.g. the Model Penal Code).

[28] NAT’L INST. OF JUSTICE, U.S. DEP’T OF JUST., COMPUTER CRIME: CRIMINAL JUST. RESOURCE MANUAL 2 (1989).

[29] *Ibid.* at Note 1.

[30] See, Dana L. Bazelon, Yun Jung Choi and Jason F. Conaty, *Computer Crimes,* 43 Am. Crim. L. Rev. 259, 264 (2006).

"subject". This line of statutes culminated in the National Information Infrastructure Protection Act of 1996 (NIIPA).[31]

The federal government's approach to regulating crimes involving the computer as an "instrument" has been to update traditional criminal statutes in order to reach similar crimes involving computers. The federal government has also used the United States Sentencing Guidelines (USSG) to enhance sentences for traditional crimes committed with the aid of computers. In fact, there have already been initiatives at the federal level to deal with cyber crimes and crime-specific legislation continues to surface at the national level that is worth serious consideration.[32]

There are several federal computer crime and cyber crime statutes including the omnibus federal computer crime/cyber crime statute which makes it an offence to, among other things, gain unauthorized entry to a computer and thereby gain access to information to which the perpetrator is not entitled to have access; and to gain unauthorized access to a computer and thereby further the perpetration of a fraud.[33] These are essentially computer crime offences that are *relevant to* but not specifically applicable to phishing scams and other fraud schemes involving identity theft and, in certain cases, to further the objective of financial cheating or stealing from the primary target.

More specifically in relation to phishing practices, a new federal law that is already in effect that is relevant to phishing, albeit *indirectly*, is the Identity Theft Penalty

[31] 18 U.S. Code § 1030. The latest amendments came from the infamous Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) as well as from the Cyber Security Enhancement Act of 2002 and the Computer Software Privacy and Control Act of 2004. *Ibid.* at 265-273.

[32] *Ibid.* at 273-290 (discussing the most prominent statutes that are used to prosecute traditional crimes committed with the aid of a computer). In relation to phishing and its relation to identity theft in particular, any number of federal legislation may be implicated depending on the method and objective of the perpetrator including statutes relating to wire fraud, credit card fraud, bank fraud, computer fraud, anti-spam and consumer protection. See, Matthew Bierlein and Gregory Smith, *Internet: Privacy Year in Review: Growing Problems with Spyware and Phishing, Judicial and Legislative Developments in Internet Governance, and the Impacts on Privacy*, 1 ISJLP 279, 308-309 (2005).

[33] 18 U.S. Code § 1030. The statute contains other computer-related offences as well. Other statutes include 18 U.S. Code § 1028 (making it a crime to produce, transfer or possess a device, including a computer, that is intended to be used to falsify identification documents); and 18 U.S. Code § 2319 (making it a federal offense to infringe a valid copyright.). Other existing criminal statutes and provisions may also apply to computer-related transactions as well. For example, sex-related statutes such as 18 U.S. Code § 1462-1463 (prohibiting the use of a computer to import obscene material into the United States or to transport such material in interstate or foreign commerce); 18 U.S. Code 2251-2252A (making it a crime to employ or to induce participation by a minor in the making of a visual depiction of a sexually explicit act if it was created using materials that had been transported, including by electronic means, in interstate or foreign commerce; prohibiting the use of a computer to sell or transfer custody of a minor knowing the minor will be used to create a visual depiction of sexually explicit conduct; and making it a crime to use a computer to transport child pornography in interstate or foreign commerce). For more on the Computer Fraud and Abuse Act, see Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 Berkeley Tech. L.J. 909 (2003); and Jo-Ann M. Adams, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 Santa Clara Computer & High Tech. L.J. 403, 409 (1996). See also Sara R. Paul, *Identity Theft: Outline of Federal Statutes and Bibliography of Select Resources* (LLRX.com, 18 September 2005), available at: http://www.llrx.com/features/idtheftguide.htm.

Enhancement Act of 2004 (ITPEA),[34] which establishes the federal criminal offense of aggravated identity theft and creates more stringent means and stronger penalties to punish phishers. Legislation aimed *directly* at phishing practices was first introduced to the United States Congress in 2004,[35] and again in 2005 in the form of the Anti-Phishing Act of 2005. [36] The Bill targets the entire scam process from the sending of the email to the creation of fraudulent sites.[37] It stipulates that the perpetrator must have the specific criminal purpose of committing a crime of fraud or identity theft before an offence is made out.[38]

A feature of the bill that is worth promoting as a model for other jurisdictions for any international treaty on such offences is that it criminalizes the bait. This 'poisoned bait' approach criminalizes the conduct engaged in before the actual commission of the fraud. For example, it makes it illegal to knowingly send out spoofed email that links to false web sites, with the intention of committing a crime. It also criminalizes the operation of such web sites that are the *locus* of the wrongdoing. This creates an opportunity to

[34] 18 U.S Code § 1028A. An individual commits aggravated identity theft if, while engaging in an enumerated identity theft related offense, the individual "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person." The commission of aggravated identity theft results in a mandatory minimum sentence of 2 years imprisonment in addition to the punishment imposed for the original offence. *Ibid*. at subsection (a)(1). *See also* DEPARTMENT OF JUSTICE, CRIMINAL DIVISION, SPECIAL REPORT ON "PHISHING", *available at* http://www.usdoj.gov/criminal/fraud/Phishing.pdf.

[35] It was introduced by Democratic Senator Patrick Leahy of Vermont as an Act to criminalize Internet scams "involving fraudulently obtaining personal information, commonly known as phishing". S. 2636, 108th Cong. (2004), available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:s2636is.txt.pdf. See U.S. Senator Patrick Leahy, *Senate Floor Speech: New Leahy Bill Targets Internet "PHISHING" And "PHARMING" That Steal Billions Of Dollars Annually From Consumers* (28 February 2005), available at: http://leahy.senate.gov/press/200503/030105.html. For an overview, see Robert Louis B. Stevenson, *Plugging the "Phishing" Hole: Legislation Versus Technology*, Duke L. & Tech. Rev. 6 (2005), available at: http://www.crime-research.org/analytics/phishing_duke/.

[36] The 2005 Bill was similarly introduced by Democratic Senator Patrick Leahy of Vermont for the same objective as the 2004 version. S. 472, 109th Cong. (2005), available at: http://thomas.loc.gov/cgi-bin/bdquery/z?d109:S.472: and http://www.theorator.com/bills109/s472.html. See also, Grant Gross, *Proposed Law Aims to Fight Phishing: Anti-Phishing Act of 2005 Allows for Prison Time and Hefty Fines* (IDG News Service, 5 March 2005), available at: http://www.pcworld.com/news/article/0,aid,119912,00.asp; Gearhead, *Will the Anti-Phishing Act Make a Difference* (NetworkWorld.com, 18 March 2005), available at: http://www.networkworld.com/weblogs/gearblog/2005/008234.html and http://www.internetnews.com/security/article.php/3487271.

[37] The 2005 Bill is similar to the 2004 version and covers both phishing and pharming scams. Parody web sites, both commercial and political, are exempted from the penalties in the bill, thereby avoiding free speech issues and Constitutional impediments.

[38] The statute seeks to amend the fraud and identity statute by including specific provisions on Internet fraud. The statute is directed at those with the intention of carrying on any activity that would be a federal or state crime of fraud or identity theft. If an individual knowingly engages in cybersquatting or spoofs a domain name to induce or solicit an individual to provide information, he may be subject to a fine, imprisonment, or both. If an individual sends an email or other Internet communication, which falsely represents itself as being sent by a legitimate business, refers or links users to a cybersquatted or spoofed location, and induces or solicits personal information, he may be subject to the same punishment. For other relevant legislation, see also, the Internet False Identification Prevention Act of 2000 and the Fraudulent Online Identity Sanctions Act of 2004 (proposed amendment to the Trademark Act of 1946).

prosecute before the actual fraud takes place, not just to successful phishing occurrences. It thus has a pre-emptive effect to such crimes and emphasizes the importance of deterrence and crime prevention.[39] The penalty of imprisonment and fine are also appropriately strong and will, hopefully, provide greater deterrent effect. But even then there continue to exist territorial limitations, both in law (i.e. the reach of the legislation) and in fact (i.e. in actual and effective implementation and enforcement).[40] The bill has also yet to be passed.[41]

The United States will continue to produce state-centric computer-related crime legislation as it does for other laws. However, two idiosyncrasies of cyberspace support greater federal involvement in computer-related criminal law making. First the 'borderless' nature of such criminal activities and the fact that jurisdictional rules that function effectively for physical activities do not translate well to the cyber realm.[42] Second, the diversity in procedural augmentation has led to a confusing cacophony of state laws that exacerbates the jurisdictional problems of adjudication and enforcement.[43] Seeking a consistent solution at the national level is preferable to sub-national efforts with varying degrees of effectiveness,[44] particularly if the objectives of eliminating or at

[39] The deterrent cum preventative aspect of legislation is very important, particularly to the primary policy objective of protecting and rebuilding trust and integrity in the Internet system of transaction. See Jennifer Lynch, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 Berkeley Tech. L.J. 259 298-299 (2005). See also Anita Ramasastry, *The Anti-Phishing Act of 2004: A Useful Tool Against Identity Theft* (Findlaw Comentary, 16 August 2004), available at: http://writ.news.findlaw.com/ramasastry/20040816.html. Criminalizing after the fact and low rates of reporting and enforcement action makes existing federal laws that indirectly criminalizes phishing acts inadequate.

[40] Another valid criticism is that currently many of the proposed solutions to phishing relates to the technique in general rather than the offence in particular. See Matthew Bierlein and Gregory Smith, *Internet: Privacy Year in Review: Growing Problems with Spyware and Phishing, Judicial and Legislative Developments in Internet Governance, and the Impacts on Privacy*, 1 ISJLP 279, 308-309 (2005). "[Many proposed solutions are still targeting spam in general and not the specific bad acts presented by phishing." *Ibid*. at 280. This can be limiting particularly when technology and techniques vary and change.

[41] Meanwhile, some states have already produced specific anti-phishing legislation. At the National Conference of State Legislatures web site at: http://www.ncsl.org/programs/lis/phishing06.htm, statistics show that as of 13 July 2006, ant-phishing bills have been introduced in at leas ten states and enacted in at least six states. See also, Hohn D. Saba, *The Texas Legislature Goes Phishing*, 68 Tex. B.J. 706 (2005); and HNS Staff, *Details From the Anti-Phishing Act of 2005,* (Net-Security.org, 5 October 2005) on California as the pioneering state to legislate against phishing.

[42] E.g. where is a "harm caused"? Where is a criminal offence "committed"?

[43] States have to varying extents amended or adopted legislation that target procedural and substantive issues relating to computer-related crime. Some have amended existing legislation in an attempt to update crime-specific statutes or general criminal statutes, while others have enacted entirely new laws. Jurisdiction, definitions and penalty provisions are just some of the changes made in an attempt to make their criminal law relevant to electronically perpetrated crimes. As one of the more technologically advanced countries in the world, the non-uniformity of treatment and lack of comprehensiveness of its substantive computer-related crime legislation is disappointing. The way the United States and many other jurisdictions have dealt with computer-related crime, that is, piecemeal and as it arises, can be analogized to how Microsoft continues to issue "patches" for its programs. It works to some extent, but not in a particularly satisfactory manner.

[44] Indeed, the United States has produced more than forty different federals statutes that contain criminal provisions for computer-related crimes. See, Heather Jacobson and Rebecca Green, *Computer Crimes*, 39 Am. Crim. L. Rev. 273, 287-304 (2002); Eric J. Bakewell, Michelle Koldaro and Jennifer M. Tjia,

least reducing computer-related crimes, through deterrence and punishment of offenders, are to be met.[45] Years after the United States signed the Cybercrime Convention, the United States Senate finally ratified the Convention in August 2006 becoming the sixteenth country to do so.[46] The significance of its ratification will only become apparent in time.[47]

B. The United Kingdom

The European community and its neighbouring countries influence the public policy and laws of the United Kingdom. The CoE has issued a number of documents, which have influenced the British criminal justice system. For example, through its acknowledgement of the standards set by the Council of Europe (CoE) in its Cybercrime Convention as a signatory state, the United Kingdom signified its intention to bring the provisions under the Convention into effect within the country.[48] The reason for the influence is the fact that European countries are a closely interconnected community of nations historically, geographically and economically.[49]

The United Kingdom computer crimes legislation is the Computer Misuse Act of 1990 (CMA).[50] The government is currently proposing amendments to the CMA to update it

Computer Crimes, 38 Am. Crim. L. Rev. 481, 287-304 (2001); Laura J. Nicholson, Tom F. Shebar and Meredith R. Weinberg, *Computer Crimes*, 37 Am. Crim. L. Rev. 207, 220-231 (2000); Michael Hatcher and Jay McDannell and Stacy Ostfeld, *Computer Crimes*, 36 Am. Crim. L. Rev. 397, 411-418 (1999); and Sheri A. Dillon, Douglas E. Groene and Todd Hayward, *Computer Crimes*, 35 Am. Crim. L. Rev. 503, 513-519 (1998).

[45] The objectives of harmonization and consistent laws that are enforceable anywhere in the world are equally applicable here at the national plane. See below Part 3 on the "Objectives of Multilateralism".

[46] See Nate Anderson, *"World's Worst Internet Law" ratified by Senate* (arstechnica.com , 4 August 2006), available at: http://arstechnica.com/news.ars/post/20060804-7421.html. As noted, civil libertarians have criticized the move, warning of the potential problems associated with the apparent dispensation of the dual criminality requirement in some cases for law enforcement. See also, Dan Kaplan, *Senate Ratification of Cybercrime Treaty Praised* (SC Magazine, 4 August 2006), available at: http://www.scmagazine.com/uk/news/article/576037/senate-ratification-cybercrime-treaty-praised/; and Anon., *Senate Ratifies Convention on Cybercrime* (Tech Law Journal, 3 August 2006), available at: http://www.techlawjournal.com/topstories/2006/20060803b.asp.

[47] Also, how this translates into its laws and how it will relate to existing federal and state laws will require closer examination.

[48] The U.K. Government was involved in the creation of two treaties on the prevention of cybercrime, under the CoE and the EU, both of which originated in Europe and both of which calls for international coordination to tackle abuses of computer systems. They are the Cybercrime Convention of 2001 and the E.U. Council Framework Decision on Attacks Against Information Systems (OJ L 069, 16 March 2005), which was proposed on 19 April 2002, adopted on 24 February 2005 and required to be transposed into national law by 16 March 2007 by member states.

[49] In contrast, the United States is not strongly influenced by the rule of law of Europe. Even if the United States government adopts some of the propositions set out by the European community, it is not bound to the same extent that other European countries are bound.

[50] The United Kingdom CMA is available at: http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm. For an overview, see generally, Martin Wasik, *The Computer Misuse Act*, 1990 Crim. L. Rev. 767. This CMA became the model and formed the template for many similar Acts in other Commonwealth jurisdictions including Singapore and Malaysia.

with more expansive provisions and stiffer penalties.[51] The amendments have been sent to the House of Lords for consideration as part of the Police and Justice Bill.[52] The only overlapping provision under the CMA with cyber crime offences is section 2 which makes it an offence to gain unauthorized access to any program or data held in any computer with the intention of committing or facilitating the commission of further offences that satisfy a set of criteria.[53]

Unlike the Cybercrime Convention that provides for both computer crime and cyber crime under one instrument, the United Kingdom itself has a distinctive dual track approach by enacting the CMA for computer crimes while leaving computer-enabled commission of more traditional offences to be dealt with under existing criminal legislation. Amendments to specific legislations and provisions have also been made to cover possible lacunas as a result of developments brought on by the advent of the electronic age. The application of traditional criminal concepts to non-traditional acts and actors, instruments, information and products arising from new technology require amendments, in particular relating to definition, interpretation and scope. The United Kingdom government has done this for some of its legislation such as those pertaining to fraud and theft, pornography and intellectual property offences.

With regards to amendments to fraud and theft legislation, which is relevant to our case study, section 2 of the CMA is a useful net to catch offences that are perpetrated through electronic means. Also, an offence of "obtaining a money transfer by deception"[54] was created under the Theft Act of 1968, which required that property "belonging to another"[55] must be obtained for fraud because it did not cover, for instance, an accounts-related fraud case where the data recorded in a set of accounts was altered, since it did not constitute the obtaining of *property* "belonging to another".[56] This appears to cover most

[51] Although the United Kingdom pioneered computer crime legislation, it has since been overtaken in terms of its relevance by other countries such as Singapore, which has seen many changes to it since it has been originally enacted, in particular, taking into account new problems relating to the uses of the computer for communications and as the gateway to the Internet. See, Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How To Kill Zombies*, 24 Cardozo Arts & Ent LJ 23, 36 (2006).

[52] See, Jeremy Kirk, *Analysts Wary of U.K. Cybercrime Law Revamp: Tougher Penalties, But Can the Law Stay Up to Date?* (IDG News Service, 7 June 2006), available at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Cybercrime_Hacking&articleId=9000999&taxonomyId=82 and http://www.networkworld.com/news/2006/060706-analysts-eye-revamp-uk-cybercrime.html?prl. An earlier proposal for revision, the Computer Misuse Act 1990 (Amendment) Bill, 2004-2005, H.C. Bill [102], sponsored by the chair of the All Party Parliamentary Internet Group (APIG), fell through when Parliament was prorogued in April 2005.

[53] Under subsection 2: "[O]ffences for which the sentence is fixed by law; or for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years…" Cf. section 4 of the Singapore CMA.

[54] Money can be transferred to a third party for the purchase of goods or it can be transferred to the offender's own account.

[55] Under the Act, "[a] person is guilty of theft, if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it". Section 4 defines "property" as "include[ing] all *personalty*, i.e. land itself cannot be stolen but anything severed from the land (with the exception of wild flowers) can be stolen, as can intangible property such as a chose in action."

[56] See section 1 of the Theft (Amendment) Act of 1996, available at: http://www.opsi.gov.uk/acts/acts1996/1996062.htm. There are now five offences, namely: Obtaining

phishing and related offences, since in all likelihood there will be some form of money transfer involved. However, the transfer of other financial or other assets such as something that is only of sentimental value, in particular those in digital form may not fall under either "money transfer" or "property".[57]

In the meantime, in a new development, a Fraud Bill has been tabled in Parliament for consideration, which is of direct relevance to the act of phishing and other such fraudulent acts.[58] It was introduced into the House of Lords on 25 May 2005 with the aim of modernizing the definitions of fraud, which have not been changed to take into consideration technological advances since 1968.[59] If enacted into law, it will ensure that criminals utilizing technology to commit offences will not escape prosecution due to a loophole in the law based on outdated and narrow definitions. For example, under the current narrowly defined offences of deception in the Theft Acts, criminals operating online often escape prosecution, as their crime does not technically fall within the definition of the offence.

The new Bill creates a general offence of fraud which can be committed in one of three ways: False representation,[60] failure to disclose information, and abuse of position. Other new offences relating to obtaining services dishonestly,[61] and possessing, making and supplying articles for use in fraud have also been created under the Bill.[62] The wording of

services by deception under section 1; evasion of liability by deception under section 2; obtaining property by deception under section 15; obtaining a money transfer by deception under sections 15A and 15B; and obtaining a pecuniary advantage by deception under section 16. It is also an offence to make off without paying. This does not require a deception.

[57] The Act also does not cover the use of improperly obtained passwords and identifiable information *per se* or its use to access data or information. It appears that that is left to other laws including the CMA and laws relating to trade secrets, confidential information, privacy and data protection.

[58] Bill 166 Sess. 2005-2006, available at the U.K. Parliament web site at: http://www.publications.parliament.uk/pa/cm200506/cmbills/166/06166.i-i.html or http://www.publications.parliament.uk/pa/cm200506/cmbills/166/2006166.pdf. For the latest updates, see: http://www.publications.parliament.uk/pa/pabills/200506/fraud.htm. See further, the House of Lords Explanatory Notes on the Fraud Bill, available at: http://www.publications.parliament.uk/pa/ld200506/ldbills/007/en/06007x--.htm; and the House of Commons Explanatory Notes on the Fraud Bill, available at: http://www.parliament.the-stationery-office.co.uk/pa/cm200506/cmbills/166/en/06166x--.htm.

[59] The Government's Response to the views expressed in earlier consultations was published on the U.K. Home Office web site on 24 November 2004, available at: http://www.homeoffice.gov.uk/documents/cons-fraud-law-reform).

[60] "This offence would also be committed by someone who engages in "phishing": i.e. where a person disseminates an email to large groups of people falsely representing that the email has been sent by a legitimate financial institution. The email prompts the reader to provide information such as credit card and bank account numbers so that the "phisher" can gain access to others' personal financial information." See the House of Lords Explanatory Notes on the Fraud Bill at para. 14; and the House of Commons Explanatory Notes on the Fraud Bill at para. 16.

[61] E.g. fraudulent credit card transactions on the Internet.

[62] See, Susan Barty and Phillip Carnell, *Fraud Bill Offers Protection from IT Fraud* (dCode.co.uk, 11 July 2005), available at: http://www.dcode.co.uk/site/home/20050711fraud.html; or Susan Barty and Phillip

the Bill has been specifically drafted to include online fraud and other offences involving the use of technology. It is to be noted that fraud by false representation is committed irrespective of whether the intended victim is deceived. Hence, it has a pre-emptive effect similar to that which is offered in the United States Anti-Phishing Bill, and punishes an offender without requiring a victim to materialize in the first place. If and when it is passed, it will overtake many of the offences under the Thefts Act.[63]

C. The Singapore Model

Unlike the United States and the approach taken by the CoE for the Cybercrime Convention, which combined computer crimes and cyber crimes in a single instrument, the Singapore legislature focused its efforts on producing a computer crime specific legislation, while attempting to leave cyber crime to be dealt with under its existing statutes through augmentation by amendment. Thus, it follows the United Kingdom model and approach to the problem. This stems from the perception that since the actual criminal acts relate to traditional offences, the inclusion of definitions and references to electronic modes of communication and commission of offences will be sufficient. However, as it will be shown in the case of phishing and similar offences of fraud involving identity theft, this approach is clearly inadequate as to its coverage under current legislation. It is also not able to satisfactorily meet public policy objectives such as crime deterrence, prevention and punishment.

Like the United Kingdom, only computer crime is dealt with under the Computer Misuse Act (Cap. 50A) (CMA).[64] Cyber crime remains to be dealt with under the provisions of

Carnell, *United Kingdom: New Protection Against Technology Abuse Under Government's Fraud Bill* (Mondaq, 5 July 2005), available at: http://www.mondaq.com/article.asp?articleid=33546&lastestnews=1.

[63] Meanwhile, the United Kingdom recently folded its national computer crime unit, the National Hi-Tech Crime Unit, into a new agency known as the Serious Organized Crime Agency (SOCA); while the Crown Prosecution Service (CPS) is sending its legal officers for special training on computer-related crimes in order to educate them on the technical aspects of such offences and to keep them abreast of developments so as to update their skills and knowledge in this area.

[64] In summary, the CMA adopts four approaches to fight computer crimes: First, creating of new computer crimes for new problems that arise which require regulation; second, providing appropriate penalties as punishment and for deterrent effect, often increasing penalties, particularly in relation to the seriousness of the offence, such as the increased penalties where "damage" occurs (sentencing guidelines and policy further complement this approach); third, giving enhanced and specific powers of investigation to law enforcement agencies and creating specialised agencies with trained professionals and experts to deal with what are specialty crimes; and fourth, acknowledging the trans-national nature of such offences and its effects by giving extra-territorial effect to the offences under the Act and making it also an offence to abet and even to attempt the commission of such offences. The CMA further enhances computer security, by broadening the powers of the police to investigate such misdeeds and by giving it extra-territorial effect. In relation to law enforcement, on top of broader police powers, the Singapore government has also established specialized technology units to handle computer crime investigations. These are the Computer Crimes Branch of the Criminal Investigation Department (CID), the Computer Forensics Branch of the Singapore Police Force (SPF), and the Singapore Computer Emergency Response Team (SingCERT) of the IDA. They were considered necessary to cope with the technological aspects of such cases and the increasing sophistication of computer programs and functions as well as of computer users. Finally, it is worth noting that section 4 of the CMA refers to offences involving "property", "fraud" and "dishonesty" (all of which appear mostly in the cheating provisions) or which causes bodily harm (offences against the person). However, the prerequisite of a punishable 2-year jail term appears arbitrary.

the Penal Code (Cap. 224) and the provisions of a host of other legislations,[65] which as stated are inadequate to deal with the problem in terms of both applicability and the effects of the punishment.[66]

The problem with relying on a legislation that was drafted before the electronic age, and that has not been amended, is that certain words and their interpretation do not apply to the electronic form of transacting or to such an environment. Under the current version of the Penal Code, the offence of cheating should apply to acts of phishing with the purpose of using stolen information for unlawful economic gain. A person cheats "by deceiving any person, [and] fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property."[67] The victim could be the person whose information is stolen, provided that such information can constitute "property" (which shall be an issue to be considered in relation to other property offences), or it could be the person or organization which is deceived or intentionally induced into transacting with the offender on the basis of that information (which can include banking and financial institutions, companies and business, and other forms of organization).

The definition of "property" here is a crucial one in order for there to be an actionable offence of cheating in relation to the theft of the users or customers' (the primary target) identity and other personal data and information such as passwords and identifiable codes *per se*.[68] In order for the scammer to face criminal prosecution in such a case, irrespective of any subsequent transaction on other forms of property occurring through the use of the identity or information, it must be accepted that personal data and information can constitute property. There is no general interpretation of "property" under the Interpretation Act (Cap 1). However, there is a definition of "immovable property" under section 2 of the Interpretation Act which "includes land, benefits to arise out of land and things attached to the earth or permanently fastened to anything attached to the earth", and of "movable property" which means "property of every description except immovable property". What "property of every description" means and whether it extends to personal data and information, and in particular, digital and electronic information, in the context of the Penal Code and other criminal provisions is still unclear. A purposive interpretation may still yield criminal recourse against perpetrators of phishing and similar offences.[69] Certainly, it would appear that it is easier to prove cheating if a subsequent transaction on financial or tangible assets takes place through the

[65] E.g. the Miscellaneous Offences (Public Order and Nuisance) Act (Cap.184).

[66] This statement relates to the general criminal offence provisions under the Penal Code (Cap. 224) alone. There may be other provisions in specific legislation providing against fraud and fraudulent transactions pursuant to the use of stolen information that can cover phishing and related activities.

[67] Section 415 of the Penal Code (Cap. 224).

[68] Additionally, the spoofing of the target organization's (the secondary target) web site can constitute copyright and trademark infringement under intellectual property laws.

[69] Clarity in the law such as in the language of the criminal provisions themselves as well as explanatory notes and modern illustrations will be most useful to remove any ambiguities.

use of such personal data or information, as can be seen in sections 421 to 424 which deals with fraudulent deeds and dispositions of property. However, they still relate to a different set of transactions.[70] The offence of cheating also does not have the effect of pre-empting further offences from occurring such as by allowing for the prosecution of theft of data or information *per se*.

Unlike the cheating provisions, which can still possibly to cover phishing and related scams, some other potential criminal offences are rendered inapplicable due to the limited scope of the "property" that forms the subject matter of the offence and one of its essential element. The preamble to section 2 of the Interpretation Act states that the definitions contained within it are only applicable to the extent that they are not inconsistent with the construction due to the subject or context in which they appear or unless it is otherwise expressly provided. Section 22 of the Penal Code provides that "movable property" is intended to include "corporeal property of every description, except land and things attached to the earth, or permanently fastened to anything which is attached to the earth." The ordinary meaning of "corporeal" is that which relates to, or has the characteristic of a material or tangible form. Personal information such as identity numbers and financial information do not appear to fall under this definition; neither will digital materials and property. Hence, it is unlikely that the offence of theft or criminal misappropriation of property, for example, will be useful in relation to cyberspace transactions as these offences refer to "movable property" only.

We have seen in the context of the United States and the United Kingdom there are two levels to the problems relating to phishing and its progeny: Fraud and identity theft. The solution to fraud, whether or not it leads to the theft of other forms of property comes in the form of general criminal legislation, such as provisions under a Criminal Code; specific legislation, such as a Theft and/or Fraud Act, or both. Identity theft can also constitute a criminal offence if it is provided as such under legislation as the United States have done.[71] Privacy and data protection laws as well as computer crime legislation also play a part if applicable to the fact situation. In Singapore's case, as we have seen, the basis for a fraud or theft action of intangible property such as digital assets and personal information is archaic and in need of reform, and there are no privacy or data protection laws against identity theft and personal data.[72]

[70] Forgery is another offence that can be applicable to cyber-fraud cases. It is a criminal offence to commit forgery for the purpose of Section 464 states that: "Whoever makes any false document or part of a document with intent to cause damage or injury to the public or to any person, or to support any claim or title, or to cause any person to part with property, or to enter into any express or implied contract, or with intent to commit fraud or that fraud may be committed, commits forgery."

[71] E.g. the United States' Internet False Identification Prevention Act of 2000 and the Fraudulent Online Identity Sanctions Act of 2004 (proposed amendment to the Trademark Act of 1946).

[72] It is also an offence to cheat by personation under section 416 of the Penal Code (Cap. 224), punishable under section 419. However, it has to involve the impersonation of a "person", whether real or imaginary, and does not extend to artificial entities or automatic agents. In Singapore, there is self-regulation in the private sector for some form of data protection but no general legal recourse, civil or criminal, for the taking of personal identifiable information *per se*.

There are also problems relating or extending other subject matters of penal provisions to their digital analogues such as “book, paper, writing, valuable security or account”[73] and “document”[74].

On the other hand, it is to be noted that despite its deficiencies in cyber crime law making, the Singapore CMA has been constantly amended and is more progressive than the United Kingdom’s CMA, upon which it was originally modeled after.[75]

D. General Observations, Comments and Criticisms

There are fresh legal challenges to cyber crimes that do not feature largely or at all in terrestrial crimes. Traditional crimes of theft and fraud often takes place within jurisdiction, unless it involves large scale or cross-border scams such as through syndicates and conspiracies respectively, whereas it is the norm for Internet scams to largely transcend borders and originate from countries with laxer law and enforcement mechanisms.

As we have seen, although existing laws can and do cover electronically perpetrated crimes, they may not be suitable, appropriate or relevant for several reasons, including the following main ones:

[73] See section 477A, which is a forgery offence that may be applicable, for example, to the case of the defrauding employee.

[74] Which is defined under section 29 of the Penal Code as: “[A]ny matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, as evidence of that matter.” Explanation 1 further states that: “It is immaterial by what means, or upon what substance, the letters, figures or marks are formed, or whether the evidence is intended for, or may be used in, a court of justice, or not.” Explanation 2 further states that: “Whatever is expressed by means of letters, figures or marks, as explained by mercantile or other usage, shall be deemed to be expressed by such letters, figures or marks within the meaning of this section, although the same may not be actually expressed.” However, this does not shed much light on whether electronic or digital forms of information or record are included in the definition. The Interpretation Act does not have a definition of “document”.

[75] However, the United Kingdom CMA is in the process of amendment. See, the Computer Misuse Act 1990 (Amendment) Bill. Bill 102 Sess. 2004-2005. See also, the U.K. Parliament web site at: http://www.publications.parliament.uk/pa/cm200405/cmbills/102/2005102.htm. In particular, it incorporates denial of services attacks as a computer crime. See, The Police and Justice Bill. Bill 119 Sess. 2005-06. See also, the U.K. Parliament web site at: http://www.publications.parliament.uk/pa/cm200506/cmbills/119/2006119.htm. It contains amendments to the CMA in Miscellaneous Part 5. It is likely to be accepted into law by the end of 2006. If it becomes law it will amend section 1(3) of the CMA by increasing the penalties for unauthorised access to computer material; section 3 of the CMA, by broadening the offence of unauthorised acts with intent to impair operation of computer to “any unauthorised act in relation to a computer”, which will widen the scope of the CMA to include denial of service attacks. The Bill is now at the House of Lords Committee (see: http://www.lga.gov.uk/Legislative.asp?lsection=59&ccat=1156). See also, Bill Thompson, *How to Legislate Against Hackers* (BBC News, 13 March 2006), available at: http://news.bbc.co.uk/1/hi/technology/4799338.stm.

1. The punishment is generic and is inadequate to meet public policy objectives such as crime prevention and control as well as the maintenance of the integrity and security of information technology networks.
2. Jurisdiction is still confined to acts perpetrated within the country and territorial jurisdiction is still the rule and only specified exceptions are triable within Singapore even if the acts are committed beyond it.[76]
3. Some provisions are rendered inapplicable due to antiquated definitions of key elements or words and statutory examples such as explanatory notes and illustrations are also outdated.

There are two possible legislative approaches in response to computer-related crime: Augmentation of existing criminal statutes or provisions through amendments; or the creation of new legislation, whether in the form of an omnibus statute which comprehensively deals with computer crime, cyber crime or both, or specific statutes addressing specific forms of electronically perpetrated crimes, particularly cyber crime. After looking at the general treatment of computer-related crimes, and also specifically on their responses to cyber-fraud and identity theft offences, we see that there are additional problems including disparity of treatment and slow, inadequate and the lack of comprehensive legislative response to new problems. In summary, the main differences are displayed in Table 1.

Table 1. Comparison of Legal Treatment of Computer-Related Crime in the U.S., the U.K. and Singapore

Country **Subject Matter**	**U.S.**	**U.K.**	**Singapore**
Legal Structure at the National Level	Federation (consists of 50 state which together form the federal state)	State (political union of 4 constituent countries)	State (single sovereign state)
Legal Involvement at the International Level (with the CoE Cybercrime Convention)	• Involved in the drafting • Member Party (recently ratified in August 2006)	• Involved in the drafting • Signatory Party • Member of the EU and part of its regional initiative	• Not involved in the drafting • Not a party
Legal Treatment of Computer-Related Crime Generally	Parallel system, overlapping Federal and State laws	Separate treatment of computer crime and cyber crime	Separate treatment of computer crime and cyber crime
Legal Treatment of Cyber-Fraud and Identity Theft	Protection against both fraud and identity theft but no	Protection against both fraud and identity theft in the	Limited protection against fraud and no protection against

[76] E.g., see sections 2 and 3 of the Singapore Penal Code respectively.

(the Phishing Case Study)	comprehensive or coherent structure; piecemeal and duplicitous in approach	form of both amendments existing legislation and the creation of new legislation	identity theft except indirectly through other legislative provisions

Just in relation to the case study on cyber-fraud and identity theft through such methods as phishing and similar activities, there are several levels to the problem for which a solution can and has be formulated in different countries.

Table 2. Levels to Phishing and Related Electronic Fraud/Theft Activities

Potential Victim	**'Property' Stolen through Deception**	**Possible Legal Recourse**	**Policy Objective of Criminalization**
Secondary Target (spoofed entity)	1. Corporate or public identity	• Copyright and Trademark infringement protection laws • Criminal law, if any	• The integrity of information technology for interaction and transactions • Pre-emptive effect (deters and prevents 2. & 3.) • Punitive effect
Primary Target (individual user or consumer)	2. Identity and Identifiable Information (e.g. passwords, ID, security codes, etc.)	• Privacy and data protection laws • Other laws (e.g. various forms of fraud) • Criminal law, if any	• Protecting human dignity and personal privacy • Pre-emptive effect (deters and prevents 3.) • Punitive effect
Primary Target (individual user or consumer)	3. Other assets, financial or otherwise, in physical or digital form (e.g. transfer of assets) owned by an individual that may be in the custody or control of another entity	• Criminal law, if applicable (e.g. existing criminal law such as theft and cheating)	• Pre-emptive and punitive effect if offence is made out without the offence necessarily carried out (criminalizing preparation and intention) • Punitive effect if offence is required to be made out (criminalizing realization and intention)
Secondary Target (other entities)		• Other laws (e.g. various forms of fraud)	

As we can see from Table 2, there are two types of property that are implicated in any electronic scams such as phishing, which should be kept in mind when legislating on the matter:

1. Identity and other personal information:[77] The protection of private information or data and identity through criminalization of identity and information theft *per se* such as those conducted through fraud or scams is necessary,[78] not just the use of such information and data for the further perpetration of other offences such as the transfer of money or other assets. Information in itself is valuable and requires protection, and they can include personal, corporate, organizational and governmental information. The question is, first, whether such laws already exists, and second, are they adequate, particularly in relation to the punishment and the objectives that they are meant to serve.[79]

2. Physical and digital assets: The act of information and data manipulation and collection through fraud and identity theft is for many criminals a means to an end. It is usually a preparatory act to facilitate the commission of other offenses such as theft and cheating to obtain various forms of property, both in physical and digital form,[80] such as products, financial assets and title to real property.

Part 3 – A Global Multifaceted and Multilateral Regime for a Borderless World of Criminal Activity

[77] See, Jacqueline Lipton, *Protecting Valuable Commercial Information in the Digital Age: Law, Policy and Practice*, 6 J. Tech. L. & Pol'y 2 (2001). The author notes that governments can and should do some work both at the domestic and international level to protect valuable commercial information. See also, Jacqueline Lipton, *Mixed Metaphors in Cyberspace: Property in Information and Information Systems*, 35 Loy. U. Chi. L.J. 235 (2003).

[78] 18 U.S. Code § 1028. See the United States' Identity Theft and Assumption Deterrence Act of 1998, available at: http://www.ftc.gov/os/statutes/itada/itadact.htm and http://www4.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html. For an overview, see the United States Federal Trade Commission web site at: http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm. For more information, follow the links provided at the crime-prevention.org web site at: http://www.crime-prevention.org/identity-theft-and-assumption-deterrence-act.html.

[79] E.g. as mentioned, if the Anti-Phishing Act is passed in the United States, the act or even the attempt to commit fraud or identity theft constitutes an offence. But if an additional element such as an intention to commit another offence is required for an offence to be made out, then a lacuna may exist. This problem may, however, be overstated as private information and data are more often than not invariably used for a purpose that constitutes a separate offence under other statutory provisions. In the United States, for instance, there is a variety of fraud under federal law alone, including identification fraud (18 U.S. Code § 1028), credit card fraud (18 U.S Code § 1029), computer fraud (18 U.S Code § 1030), mail fraud (18 U.S Code § 1341), wire fraud (18 U.S Code § 1343), or financial institution fraud (18 U.S Code § 1344). See the U.S. DOJ, *What's the Department of Justice Doing About Identity Theft and Fraud*, at: http://www.usdoj.gov/criminal/fraud/idtheft.html. However, recognizing information itself as an asset worth protecting is already a strong policy consideration for legal sanction. Hence, to fraudulently obtain information for *possession* should constitute an offence in itself.

[80] It can be an electronic form or representation of a physical asset or an entirely digital form of asset.

During the Euro-Southeast Asia Information Communication Technology (ICT) meeting held in June 2006, the problem of abuse of the Internet, which is an important medium of trade, commerce and communications, was raised. Member countries of both regional groupings were urged to improve their security measures to address the problem. The value and importance of multinational legal and cooperative measures were also brought up. In fact, the Singapore Minister for Community Development noted the importance of discussing issues within these *fora* in order to produce "future collaboration under the aegis of multilateral international security".[81]

There are two main objectives of multilateralism:

1. To remove or minimize legal obstacles to international cooperation that currently impedes investigations and prosecutions of computer-related crime.
2. To remove or minimize legal obstacles to comprehensive ratification, which will remove "safe havens" to cyber criminals.

There are three main jurisdictional hurdles to computer-related crimes such as phishing that have to be addressed by any effective prohibitory model of legislation:

1. Prescription and the harmonization and consistency of treatment, as far as possible, of categories of offences (challenge of optimization).[82]
2. Adjudication and the problem of jurisdiction and need for extra-territorial reach and effect (challenge of space).
3. Enforcement and the objectives of criminalization including deterrence (of offender), prevention (by victims, etc.) and punishment (social justice); which involve considerations of effective investigation (e.g. procedural assistance in apprehension and the gathering of evidence) and implementation (e.g. extradition and sufficiency or effectiveness of remedies) (challenge of cooperation).

A. Structure (Form)

What model the multilateral approach should take will in turn influence its transposition into domestic law both as to its form and substance. Hence the type of international law instrument is important in order to promote and produce a comprehensive and optimal legal response to computer-related crime. However, in the end, the approach will depend on the legal and political make-up of each country. But the virtues of clear, succinct and transparent laws for easy understanding and access, whether through umbrella legislation or a specific legislation, should be kept in mind by policy-makers.

1. Combined Approach

[81] See, Anon., *E.U., Asia Urged to Beef Up Internet Security* (newKerala.com, 19 June 2006), available at: http://www.newkerala.com/news3.php?action=fullnews&id=11164.

[82] E.g. by apply a similar sort of principle that appears in international law which is called the "peremptory norm or *jus cogens (*"compelling law") that applies to norms that are universally accepted and that cannot be violated by state entities (e.g. war, crimes against humanity, war crimes, genocide, slavery, torture and piracy) but applying it to the context of individuals and non-state entities. One author has suggested the use of the customary international law (which is an international law source of law) as an additional instrument to combat cybercrime. See, Jason A. Cody, *Derailing the Digitally Depraved: An International Law and Economics Approach to Combating Cybercrime and Cyberterrorism*, 11 MSU-DCL J. Int'l L. 231 (2002).

The benefit of an omnibus legislation is that it offers the most comprehensive treatment. It can serve as the impetus for convergence and compromise and as a collective statement of purpose reflecting international policy objectives and indicative of the mission to all stakeholders. A treaty that is widely ratified can create a consistent set of laws and enforcement processes in different countries.

However, the disadvantage of a broad-based treaty is that it must necessarily be broad-based and non-specific in order to achieve consensus. An example of this is the Cybercrime Convention, which provisions are painted in broad strokes, and even then it has not been ratified by many of the countries that were involved in its drafting and that have signed the Convention. There may also be tensions between segments of society.[83] Moreover, too many reservations (and even declarations) may dilute the effects and reciprocal undertaking between signatory countries.[84]

In any event, the Cybercrime Convention is still a good basis upon which to build some general consensus, promote discussion with a view to exchange of information, knowledge, experience and views, and to set the momentum going on more effective global legal solutions.

a. The European Convention on Cybercrime (Cybercrime Convention)[85]

The Cybercrime Convention is the first and only international treaty aimed at protecting society from computer-related crime, such as crimes committed *via* the Internet and other computer networks. The idea for the Cybercrime Convention grew from studies by the Council of Europe (CoE) from 1989 to 1995. The CoE established the Committee of Experts on Crime in Cyberspace to draft the Cybercrime Convention in 1997. It was completed in May 2001 and opened for signature and ratification on 23 November 2001 in Budapest, Hungary. To become effective, the Cybercrime Convention required ratification by five countries, at least three of which were in the Council of Europe. Those

[83] E.g. there are some human rights and privacy concerns with regard to the Cybercrime Convention in some countries such as the United States and Canada. See Ryan M.F. Baron, *A Critique of the International Cybercrime Treaty*, 10 CommLaw Conspectus 263 (2002); and see, Jason M. Young, *Surfing While Muslim: Privacy, Freedom of Expression & the Unintended Consequences of Cybercrime Legislation: A Critical Analysis of the Council of Europe Convention on Cyber-Crime and the Canadian Lawful Access Proposal*, 9 Int'l J. Comm. L. & Pol'y 9 (2005).

[84] Under Article 2(1)(d) of the Vienna Convention on the Law of Treaties, "reservations" constitute unilateral statements purporting to exclude or to modify the legal obligations and their effects on the reserving state. They are generally permitted so long as they are not inconsistent with the objectives and purposes of the treaty in question.

[85] The European Convention on Cybercrime (Budapest, 23.XI.2001) is available at: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm. The CoE Explanatory Report (ETS No. 185) is available at: http://conventions.coe.int/Treaty/en/Reports/Html/185.htm. For more background information, see The Council of Europe's (CoE) APC European Internet Rights Project web site (http://europe.rights.apc.org/coe.html#cybercrime); the U.S. Justice Department's web site with FAQs on the Convention (http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm). The Convention is open for signature to all countries. For an updated list of members, see: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

conditions were met and the Convention entered into force on 1 July 2004.[86] Many European Union (EU) member countries as well as some non-EU countries such as the United States have since signed and ratified it.[87]

The stated purpose of the Cybercrime Convention is to pursue a common policy aimed at combating computer-related crime through appropriate legislation and international cooperation. The Cybercrime Convention addresses three main topics, which also form its main mission:

1. The harmonization of national substantive laws regarding computer-related crime. First, the Convention aimed to create a level of consistency among signatory states on the nature and form of legislation criminalizing computer-related crime.[88] For example, it requires consistency in the legal definitions of "computer system", "computer data", "service provider" and "traffic data",[89] and sets out substantive computer and cyber crimes.[90] The Convention does not set out the offences in detail but merely lays out the required elements of each offence in broad strokes.[91]

2. The establishment of effective domestic investigative powers and procedures regarding computer-related crime and electronic evidence. The second goal of the Convention is to ensure that signatory states have consistent powers for investigating such crimes and in evidence gathering.[92] These powers include search and seizure,

[86] See, Peter Csonka, *The Council of Europe Convention on Cyber-Crime: A Response to the Challenge of the New Age, in Cyber-Crime: The Challenge in Asia 303* (Roderic Broadhurst & Peter Grabosky eds., 2005).

[87] In 2003, President George W. Bush recommended its ratification to the Senate (http://www.whitehouse.gov/news/releases/2003/11/20031117-11.html). In 2005, the Senate Foreign Relations Committee recommended ratification of the Convention. The bill has been opposed by the privacy community, endorsed by software companies and industry groups, and received broad support from the Senate Foreign Relations Committee. The Convention was finally ratified in 2006. It is to be noted that the United States already have laws that addresses many of the treaty's general provisions, particularly those relating to the enactment of substantive offences. However, the extent of its responsibilities relating to mutual cooperation and procedural processes vis-à-vis other countries have yet to be tested.

[88] The CoE created the Cybercrime Convention to resolve the unique legal issues raised by electronically perpetrated offences both as a *means* and as an *end* by promoting a common, cooperative approach to prosecuting people who commit computer-related crime. For example, the Cybercrime Convention requires signatory states to criminalize certain activities, such as hacking and child pornography, while stiffening criminal liability for other intellectual property-related violations.

[89] Chapter I of the Convention.

[90] Under Chapter II, Section 1, Titles 1 and 2 to 4 of the Convention respectively. Covering the basic and most common types of computer crimes, such as illegal access, illegal interception, data interference, system interference, misuse of devices; and cyber crimes including forgery, fraud, child pornography, copyright and neighboring rights crimes.

[91] The Cybercrime Convention provides a framework of measures for implementation by sovereign states. Like other multilateral conventions, the language is general and flexible to allow for adaptation by a variety of legal systems.

[92] Chapter II, Section 2 of the Convention.

preservation of data, disclosure of traffic data, production order and interception of content data.[93]

3. The establishment of a prompt and effective system of international cooperation regarding the investigation and prosecution of computer-related crime. The third main purpose of the Convention is to provide a mechanism for mutual legal assistance among signatory states. International mutual legal assistance is even more important given the borderless nature of the Internet, as crimes are often committed in one country with the effects felt in another.[94] However, as they say, the devil is in the detail as the Convention merely provides for general statements of principles.

It allows member states to ratify with reservations regarding various obligations.

b. Work in Other Regional or International Organizations and Groupings

Although the work of the CoE and the Cybercrime Convention is currently at the forefront of international efforts to handle the challenges of technological abuse, other regional multilateral political and non-political organizations have also been considering the issue for many years and have produced international policy and formulated some consensus on the problem of computer-related crime within their respective *fora*.[95] Some examples are as follows:

1. G8:[96] The G8 has been formulating policy and action plans to deal with high-tech and computer-related crimes for about a decade now. In December 1997, representatives from the eight major industrialized nations forming the G8 adopted ten principles and agreed on a ten-point action plan to fight international computer-related crime. The leaders of the G8 countries endorsed this template and G8 experts forming the Subgroup on High-Tech Crime continue to meet regularly to cooperate on the

[93] It also expands the powers of law enforcement to compel Internet service providers to monitor user content.

[94] Chapter III of the Convention provides for international cooperation. Traditional mutual legal assistance includes situations where no legal basis exists between parties such as by treaty or reciprocal legislation. When legal basis exists, existing arrangements apply to mutual legal assistance under this Convention.

[95] See generally, U.S. DEP'T OF JUST., COMPUTER CRIME AND INTELL. PROP. SECTION, INTERNATIONAL ASPECTS OF COMPUTER CRIME, available at: http://www.usdoj.gov/criminal/cybercrime/intl.html. It provides cases, recent law, press releases, speeches, testimony, reports, letters, manuals, and other documents relating to the efforts of G8, the European Union (EU) and the Organization for Economic Cooperation and Development (OECD) to combat cybercrime. See also, Michael A. Sussman, *The Critical Challenges From the International High-Tech and Computer-Related Crime at the Millennium,* 9 Duke J. Comp. & Int'l L. 451, 481 (1999); Shannon C. Sprinkel, *Global Internet Regulation: The R Computer Virus and the Draft Convention on Cyber-Crime*, 25 Suffolk Transnat'l L. Rev. 491 (2002); and Marc D. Goodman and Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, UCLA J. L. Tech. 3 (2002).

[96] See the Official web site of the G8 presidency of the Russian Federation in 2006 at: http://en.g8russia.ru/.

implementation of the action plan.[97] The Subgroup was charged with the task of enhancing the abilities of G8 countries to prevent, investigate and prosecute crimes involving computers, networked communications, and other new technologies. They have also expanded their work with non-G8 countries in this respect. The Subgroup meetings are attended by multi-disciplinary delegations that include cyber crime experts, investigators and prosecutors.[98] It is to be noted that as part of a holistic strategy, the Subgroup closely cooperates with private industries to achieve these ends.[99] The G8 has remained dedicated to the issue and to finding an international and concerted solution to the problem.[100]

2. OECD:[101] The Organization for Economic Cooperation and Development (OECD) conducted a study from 1983 to 1985 on the need for consistent national cyber crime laws, which culminated in a 1986 report listing a core group of cyber crimes that countries should outlaw. In 1992, the OECD adopted a recommendation concerning the security of information systems and the Guidelines for the Security of Information Systems were appended to the recommendation. Among other things, the Guidelines suggested that member states develop procedures to facilitate mutual legal assistance in dealing with cyber crimes. It was revised in 2002 to take into consideration the changes in the technology landscape since it was first drafted.[102] The Committee for Information, Computer and Communications Policy (ICCP) was set up to address

[97] In fact, expert group meetings began in 1995 and it was the recommendations of the 1996 Lyon Group of experts that triggered Recommendation Sixteen which first called for countries to "review their laws in order to ensure that abuses of modern technology that are deserving of criminal sanctions are criminalized and that problems with respect to jurisdiction, enforcement powers, investigation, training, crime prevention and international cooperation in respect of such abuses are effectively addressed." The Lyon Sub-Group on High-Tech Crime was created to implement the recommendations related to the subject, and they meet regularly to work on implementation. The G8 leaders also consider these matters at their annual meetings. See, Michael A. Sussman, *The Critical Challenges From International High-Tech and Computer-Related Crime at the Millennium*, 9 Duke J. Comp. & Int'l L. 451, 481-487 (1999).

[98] Significant achievements of the Subgroup include: (i) The creation of its Network for 24-Hour Points of Contact for High-Tech Crime and an international Critical Information Infrastructure Protection Directory; (ii) organizing international training conferences for national agencies and reviewing each country's legal systems and their adequacies relating to high-tech crimes; (iii) the negotiation of widely-accepted principles and action plan to combat high-tech crime to be adopted by the G8, which are recognized at other international *fora*; (iv) producing best practices documents, including guides for security of computer networks, international requests for assistance, legislative drafting, and tracing networked communications across borders; and (v) matters relating to the location and identification of computer criminals.

[99] See, John T. Soma et al., *Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?* 34 Harv. J. on Legis. 317, 359-360 (1997).

[100] They acknowledged that international efforts to develop a global information society must be accompanied by coordinated action to foster a crime-free and secure cyberspace. The G8 has also established a "Digital Opportunity Taskforce" to explore how to integrate the efforts of the G8 members into "a broader international approach". The approach was set out in paragraph eight of the Okinawa Charter on Global Information Society. See, Susan W. Brenner and Joseph J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. Marshall J. Computer & Info. L. 347, 364-365 (2002).

[101] See the OECD web site at: http://www.oecd.org.

[102] For publications and documents relating to its Information and Communications Policy, see the OECD web site at: http://www.oecd.org/department/0,2688,en_2649_34223_1_1_1_1_1,00.html.

issues arising from the "digital economy", the developing global information infrastructure and the evolution towards a global information society.

3. UN: The United Nations (UN) has also done some work in their attempt to provide some solution to the problem.[103] It has hosted eleven crime congresses so far and the issue of computer-related crimes often features on their agenda.[104] For example, in the Eighth United Nations Congress held in 1990 in Havana, Cuba, the Congress adopted a resolution on computer-related crime calling upon its member states to intensify their efforts to combat computer crime.[105] The UN also produced a Manual on the Prevention and Control of Computer-Related Crime in 1995, which examined the law governing such crime and the need for international cooperation in investigations. Workshops were likewise held in the tenth and eleventh congresses, with some focus on public-private sector cooperation and between countries. Even the UN General Assembly (UNGA) has addressed the issue. In December of 2000 the UNGA adopted Resolution 55/59, the Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-First Century, which committed member states to work towards enhancing their ability to prevent, investigate and prosecute computer-related crime.[106]

4. INTERPOL:[107] As the world's largest international police organization created to facilitate transnational police cooperation and other crime fighting organizations,

[103] Similarly, a regional example is the Council for Security Cooperation in the Asia Pacific (CSCAP), which had established a Working Group on Transnational Crime in 1997. See the CSCAP web site at: http://www.cscap.org. The Working Group focuses on cyber crime and on the need for law enforcement cooperation in the Asia Pacific region. For the links to CSCAP's six working groups, see: http://www.cscap.org/groups.htm#.

[104] See the latest on the U.S. Congress at the UN Office on Drugs and Crime web site at: http://www.unodc.org/unodc/en/crime_cicp_congresses.html.

[105] ***See, Susan W. Brenner and Joseph J. Schwerha IV,* Transnational Evidence Gathering and Local Prosecution of International Cybercrime, *20 J. Marshall J. Computer & Info. L. 347, 359 (2002). This was done at the thirteenth plenary meeting of the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders where a series of recommendations concerning the adoption of cyber crime legislation, investigative procedures, rules of evidence, forfeiture and mutual legal assistance in investigations were issued. Member states were called upon to consider the following measures: (i) Modernization of national criminal laws and procedures; (ii) improvement of computer security and crime prevention measures; (iii) adoption of measures to sensitize the public, the judiciary, and law enforcement agencies to the problem and importance of preventing computer-related crimes; (iv) adoption of adequate training measures for judges, officials, and agencies responsible for the prevention, investigation, prosecution, and adjudication of economic and computer-related crimes; (v) elaboration of rules of ethics in the use of computers and the teaching of these rules as part of the curriculum and training of informatics; and (vi) adoption of policies for the victims of computer-related crimes.* Ibid. *at 360.***

[106] The resolution also pointed out the need to eliminate safe havens for offenders, increase the effectiveness of cooperation among law enforcement agencies, and improve the training and equipping of law enforcement agencies. But balance has to be struck with the need to protect individual freedom and privacy.

[107] See the INTERPOL web site at: http://www.interpol.int. The INTERPOL is just one of many intelligence agencies worldwide that are forming alliances to fight the threat of technological crimes. Another more specific example is the U.K.'s National Hi-Tech Crime Unit's cooperation with the U.S.

> INTERPOL will naturally be concerned with the issue of cooperation in the field of computer-related crime (or according to INTERPOL, "Information Technology Crime" (ITC)).[108] Among its many efforts, INTERPOL uses a network of regional working party group of experts consisting of representatives from national computer crime units.[109] INTERPOL has also held conferences with its Sixth International Conference on Computer Crime held in April 2005 in Cairo, Egypt, and its First International Cyber Crime Investigation Training Conference in September 2005 at the General Secretariat. INTERPOL also promotes cross-disciplinary support between the academia, private industry and the authorities.[110]

These are just some of the more prominent efforts that are being taken at the regional and international level in an attempt to improve the global crime-fighting regime against the advent of technological abuse. Even though they remain largely political and informal cooperative vehicles,[111] they are no less instrumental and important as they reflect political commitment, international policy and consensus.[112]

2. Specific Approach

What are the alternatives, or additional recourses, to a broad-based multilateral instrument such as the Cybercrime Convention? There are two possible approaches: The use of crime-specific treaties and of uniform model laws.

Federal Investigation Bureau and Secret Service to investigate phishing attacks in the United Kingdom. See, Lauren L. Sullins, *"Phishing" for a Solution: Domestic and International Approaches to Decreasing Online Identity Theft*, 20 Emory Int'l L. Rev. 397 (2006).

[108] INTERPOL facilitates cooperation between national law enforcement agencies as they investigate multinational online crime. As part of its efforts, for instance, it produces a handbook that agencies use to train investigators in the best practices and techniques for dealing with information technology crime in order to improve technical knowledge among law enforcement officials. It also helps to increase the flow of communication between countries by developing web sites and contact directories for investigators.

[109] See the INTERPOL ITC web site at: http://www.interpol.int/Public/TechnologyCrime/default.asp. INTERPOL has also established a Steering Committee for Information Technology Crime, which coordinates and harmonizes the initiatives of the various working parties.

[110] These appear in the recommendations emerging from the First International Cyber Crime Investigation Training Conference, where the Conference recognized: "[T]he lack of globally harmonised training initiatives; the global need for training institutions; the need for the global exchange of training materials, trainers and free training sites; the difficulty in finding qualified trainers; [and] the willingness of academia and private industry to support law enforcement's development and delivery of training modules." See the Conference web site at: http://www.interpol.int/Public/TechnologyCrime/Conferences/1stCybConf/Conference.asp.

[111] ***The legal approach is still acknowledged as the most important approach due to its multifarious objectives (in particular, preventative and punitative) and its weapons of coercion. Hence, for example, the*** **Association Internationale de Droit Penal** ***(AIDP) passed a resolution in 1992 containing a number of recommendations on advancing current criminal laws. The AIDP recommendations stressed in particular the precision and clarity required in future refinements or enactments of criminal laws on the subject that are aimed at addressing computer-related crime. See the AIDP web site at: http://www.penal.org/new/index.php?langage=gb.***

[112] See, Susan W. Brenner and Joseph J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. Marshall J. Computer & Info. L. 347 (2002).

Specific treaties can separate the prescriptive regime for substantive offences depending on the commonality or differences in treatment in different countries. They can also contain the same or a different set of procedural, enforcement and cooperative arrangements tailored to the best possible compromise between countries. Model laws provide the impetus for consistent enactment as they serve as a template, obviating the need for each country to do most of its own research and study; and to encourage transposition into law, particularly for countries without the capacity or resources to produce such laws.

The advantages of the use of specific treaties are that it allows for more acceptability and greater membership (e.g. signatory states) with lesser exceptions and exclusions (i.e. reservations and declarations) and for the greatest harmonization and optimization of laws, particularly for 'universal offences'. It may be more useful to produce model laws rather than legally binding instruments for those crimes that are differentially treated in many countries, since the latter will either be too broad and ineffectual or too detailed but little subscribed.

Also, the problems from rapid technological advances and its abuses emerge much faster than the law can develop to counter its effects. For example, we have seen the string of amendments to fraud and identity theft in the United States, the United Kingdom and Singapore. In the United States, the proposed Anti-Phishing Act of 2005 may already be outdated due to new methods of perpetrating fraud such as "vishing" and other 'newer' offences. Similarly, the United Kingdom first amended the Theft Act, but is now considering a new Fraud Bill to further update its cyber crime laws as well as amendments to its CMA, the first since its inception. Meanwhile, Singapore's electronic fraud and identity theft laws are still lacking while its CMA has undergone several substantive amendments. Allowing for more focused and specific treatment will ensure that there will be faster reaction time to developments, shorter gaps between the problem and solution and assist states to enact amendments or new provisions more speedily.[113] The same argument applies to the use of model laws as well as in support of keeping laws as technologically neutral as far as possible without compromising too much on its clarity and focus.

The disadvantage is that there will be a proliferation of treaties with different substantive and procedural provisions as well as different standards of international cooperation.[114] This and varying approaches to the transposition of model laws can also cause differences in domestic law while purporting to solve the same problem and promoting the adoption such law in as many jurisdictions as possible.

There will also be some extent of overlap in coverage between specific cyber crime laws and traditional criminal provisions. However, duplicitous criminal provisions are not uncommon and they provide the prosecuting authorities the leeway to select the most

[113] In contrast, the 'package' approach will be fraught with delays because of developments in one area or another as well as differences in state-to-state treatment of certain offences.

[114] I.e. more disjoined, unless arrangements are kept as consistent as possible.

appropriate charges to make and allow for other procedures that are common under criminal procedure laws (e.g. plea bargains).

a. Using Multilateral Instruments[115]

Multilateral instruments such as treaties and conventions have the status of law under the international law regime.[116] They also have the advantage of being written in concrete form,[117] having undergone negotiations and hence reflecting greater consensus. At the same time, if in relation to a specific subject matter area, particular one that is susceptible to consistent worldwide treatment, it can be a once-and-for-all comprehensive solution. It can also include both substantive and procedural laws and procedures as state obligations to fulfill.

b. Using Uniform Model Laws

The benefit of model laws is that it provides a ready instrument for use, especially by countries that lack the capacity and capability for legislative drafting. The problem inherent in such instruments is that while it provides the impetus for enactment of laws relating to a subject matter, there is no control as to the nature and extent of its adoption which gives rise to adaptations that can diverge in substance and effect.[118] In contrast,

[115] In 2003, the American Bar Association's (ABA) International Cybercrime Project (by the ABA Privacy and Computer Crime Committee, Computer Law Division of the Science and Technology Law Section) published the International Guide to Combating Cybercrime. The project brought together representatives from the ABA, government, industry, non-governmental organizations, and academia to address the issue of cyber crime. The project recommended a multifaceted solution that attempts to improve the investigation and prosecution of cyber crime. First, the project urged uniformity of cyber crime laws, suggesting that developing countries model their domestic laws after those set forth by multinational organizations and developed countries; second, the project recommended the establishment of an international scheme to solve potential jurisdictional difficulties, for example, by harmonizing extradition laws regarding cyber crime offenses; third, the project urged governments to increase resources to train personnel in high-tech investigative and forensic techniques, establish internal organizations, and actively participate on the international plane; and fourth, the project pushed for information sharing between public and private sectors both within countries and internationally. See, INTERNATIONAL GUIDE TO COMBATING CYBERCRIME (Jody R. Westby ed., 2003). See also the ABA web site at: http://www.abanet.org and the project web site at: http://www.abanet.org/scitech/computercrime/cybercrimeproject.html. See further, *Editorial: We're Just Phish to Them* (Journal Sentinel, 12 March 2006), available at: http://www.jsonline.com/story/index.aspx?id=407391. There should be an international treaty that involves more countries, perhaps under the auspices of the UN.

[116] See Article 38 of the Statute of the International Court of Justice of 1945. International law has three primary sources of law: (i) International treaties and conventions ("international conventions, whether general or particular, establishing rules expressly recognized by the contesting states"); (ii) international custom ("as evidence of a general practice accepted as law"); and (iii) general principles of law ("recognized by civilized nations"). International treaty law is comprised of obligations states expressly and voluntarily accept between themselves.

[117] Cf. customary international law, which has to be deciphered from state practice and *opinio juris*.

[118] This ironically may have the inadvertent effect of propagating different approaches, which makes it even more difficult for harmonization in the future. However, this problem may be overstated as it is based on the presumption that countries will deliberately find their own approach when in fact it is more likely than

although reservations and declarations can and do exist in some treaties and conventions as well, the general rule under international law is that they cannot go to the extent of going against the objectives and purposes of the instrument. Also, unlike treaties and conventions that have stronger legal authority as a source of law, and hence that may have some coercive political or legal force for non-compliance, the adoption of model laws are entirely voluntary.[119]

Model laws are perhaps most useful for subject matter areas that do not have consistent international treatment and hence are impossible for international consensus in any credible form.

c. Suggestion: A Mixed Model

In the end, the best approach is not any single one but a mixture of both depending on which is the most appropriate for the category of offence, such as the 'universality' or otherwise of the category in question. For instance, fraud and identity theft is more susceptible to internationally consistent treatment (and hence specific treaty) rather than intellectual property offences and content-related offences such as pornography and defamation (which perhaps benefit more from model laws).

B. Content (Substance)

The substantive provisions of the computer-related criminal legislation will depend on the subject matter in question. In particular, there are some common features to electronically perpetrated offences that should be noted:

1. Offenders may rely on automatic agents. Primary victims may not be humans but can be organizations or systems.[120]

2. The subject matter of an offence may be in digital form. The changing notions of property to include digital information and other virtual products, and electronically carried out services require changes in definitions and paradigms.

3. Technology and techniques frequently change and may cause existing legislation to be inadequate or obsolete. Hence, as far as possible, computer-related offences should be drafted in as technologically (and technique) neutral a manner as possible.

not that they will try to be as consistent as possible to international and other domestic standards and not to overly amend the model law provisions unless necessary.

[119] Moreover, the constitutional and administrative law in a country may only be required to consider and to adopt an international law instrument into the domestic regime and not a 'non-legal instrument' like model laws, guidelines, etc.

[120] Hence, for example, the significance of clause 2 of the United Kingdom Fraud Bill, which would apply equally to representations made to machines as to representations made to people.

Otherwise the only alternative is to be alert to the requirement for constant amendments.[121]

4. The method of committing a 'traditional' offence itself should also be sanctioned in order to deter and prevent these offences from occurring. Hence, for example, the abuse of technology such as the use of surreptitious electronic means with the intention of obtaining information without the knowledge or consent of the originator should constitute an offence irrespective of the ultimate goal or motive such as financial gain.[122]

5. The problem of extra-territoriality.[123] As we have seen, computer crime and cyber crime do not respect national boundaries and often crosses multiple jurisdictions.[124] In fact, due to the nature of electronic transactions, they often transcend real space and involve the laws and people of different countries. The obvious difficulty in the enactment of any international treaty or domestic legislation to regulate conduct in cyberspace is the extent of jurisdictional reach. For computer-related criminal laws to be truly effectiveness, potential offenders must face the threat of legal sanction anywhere in the world for offences perpetrated by him in or through another jurisdiction or that has its effects in another country.[125]

C. Multifaceted and Multipronged Approach

Although the main focus of this paper is on the legal approach to the problem of computer-related crimes, on a more holistic level, a multifaceted approach is certainly

[121] As noted previously, for example, the United States' proposed Anti-Phishing Act of 2005 that would enter two new crimes into its criminal code (i.e. the prohibiting the creation or purchase of web sites for the purpose of scamming and emails that fraudulently purport to represent legitimate businesses) do not take into account other potentially new technologies or techniques used to perpetrate such scams such as vishing.

[122] This is the approach taken in computer crime legislation. See, e.g., the United Kingdom and Singapore CMAs.

[123] Note for instance the extra-territorial scope of the Singapore CMA under section 11. Section 11(1) provides that: "[T]he provisions of [the CMA] shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore." Where an offence under this Act is committed by any person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore." (subsection (2)). However, for the CMA to apply, either the accused must have be in Singapore at the material time; or the computer, program or data was in Singapore at the material time, for the offence in question (subsection (3)). See also Chapter II, Section 3 on jurisdiction under the Cybercrime Convention.

[124] Cyber crime is also challenging existing legal concepts, particular since it transcends sovereign borders. Cyber-criminals are often in places other than where their crime hits victims.

[125] E.g. it is due to such jurisdictional issues that section 11 of the Singapore CMA expressly provides that the accused person may be treated as if he had committed the offence in Singapore even if the offence under the CMA was committed outside Singapore. Furthermore, section 11(1) of the CMA applies to any person irrespective of his nationality or citizenship. In other words, the combined effect of these provisions is to extend the territorial reach of the courts to acts beyond the shores of Singapore. Extraterritorial laws are not easily enacted due to sovereignty considerations and to uphold comity of nations. However, in exceptional cases, the extraterritorial extension of legislation and judicial jurisdiction as well as extraterritorial enforcement arrangements is necessary. In this case, it is necessary in order for any country to effectively deal with the menace of computer-related crime.

required in order to comprehensively deal with the problem most effectively. For that to happen, not only is the approach relevant, that is, the legal and non-legal methods to deal with the problem, the different stakeholders in information technology should also be involved, including representatives from the public and private sectors, businesses, organizations and technology companies, and individuals.[126]

1. Education

Educating information technology users including individuals, corporate entities and organizations is a largely preventative measure. For example, consumer assistance through the media to better inform and alert consumers. It involves more than just educating them on security and other defensive or self-help measures. For example, they can provide valuable assistance in reporting, evidence gathering, investigations and enforcement. The existence of counter-scam technology and laws must not be allowed to engender a false sense of security and consumers should be informed and encouraged to report scams to a clearly designated government agency for further investigations and other actions. In turn, country agencies should report to an international agency or coordinator for the problem to be concurrently handled at the global plane.[127]

2. Public/Private Joint Efforts

We have seen some of the more prominent international policy-making and inter-governmental multilateral efforts. However, there is concurrently a network of joint efforts between government agencies and private sector organizations as well as within the private sector itself. There are even non-commercial and non-profit interest groups, many of which operate and have a strong presence online.[128] They can be crime-specific like the Anti-Phishing Working Group (APWG),[129] the Spamhaus Project,[130]

[126] In the context of phishing, see Lauren L. Sullins, *"Phishing" For a Solution: Domestic and International Approaches to Decreasing Online Identity Theft*, 20 Emory Int'l L. Rev. 397, 405-433 (2006). The author focuses on the need for cooperation between law enforcement agencies, legislators, and the private sector (the notion of an "integrated unit"). The proposed solution to phishing depends on cooperation between all three groups and the fight against phishing is dependent upon cooperation in the following three areas: Joint operations among law enforcement agencies, domestic and international legislation, and among the private companies and consumers that are the victims of these attacks.

[127] See, e.g., Interpol on Information Technology Crime at: http://www.interpol.int/Public/TechnologyCrime/default.asp. Interpol's role in international policing is an integral part of the international cooperation and enforcement regime. Its mission is to facilitates cross-border police cooperation, and provide support to public and private sectors in preventing and fighting international crime.

[128] See the "Site Seeing on the Internet" web site at: http://www.pueblo.gsa.gov/cic_text/computers/site-seeing/. The site is interestingly done up like a travel web site.

[129] See the APWG web site at: http://www.antiphishing.org. The APWG is "[a] global pan-industrial and law enforcement association that focuses on eliminating fraud and identity theft that results from phishing and email spoofing of all types."

[130] See the SPAMHAUS web site at: http://www.spamhaus.org.

Hoaxbusters[131] and ScamBusters.org;[132]or they can be non-crime-specific such as the Internet Crime Complaint Centre (ICCC)[133] and the FTC Consumer Alert web sites.[134]

3. Defence Technology[135]

Having the technology to stay safe on-line is just as important as knowing how to spot the signs of trouble when it arises. For example, even defensive technology has to keep one step ahead of phishers who have managed to find ways to get around security and authentication systems ad constantly find new ways and methods to overcome consumer savvy.[136] Hence, secondary-level strategies like having a good defensive technology architecture with the involvement of manufacturers and software makers is very important. It must counter the abuse of 'good technology' (e.g. surveillance or tracking technology) and the creation and use of 'bad technology' (e.g. malware). It should also take advantage of both forms of technology and use them to investigate abuses. Technology is essential to computer forensics, tracing of offenders' identity or location and source of operation, investigations and evidence gathering.

4. Extra-legal Arrangements

Extra-legal arrangements include formal and informal cooperative arrangements between governmental administrative agencies with investigative powers and the exchange of experience and knowledge. The INTERPOL is a good example of such an arrangement. This is important due to the predominantly cross-jurisdictional nature of computer crime and more so for cyber crime. For instance, most phishing and other scams originate overseas. Central agencies and strong international network and cooperative arrangements are essential. Technological know-how, computer forensic capabilities, and sufficient investigative powers within these agencies are important. As time is of the

[131] See the Hoaxbusters web site at: http://hoaxbusters.ciac.org.

[132] See the Scambusters web site at: http://www.scambusters.org.

[133] See the ICCC web site at: http://www.ic3.gov. A partnership between the U.S. Federal Bureau of Investigation and the National White Collar Crime Center (NW3C), it serves as a" vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, local and international level, IC3 provides a central referral mechanism for complaints involving Internet related crimes." See also, the U.S. DOJ Computer Crime and Intellectual Property Section (CCIPS) on Reporting Computer-Related Crimes at: http://www.cybercrime.gov/ and http://www.usdoj.gov/criminal/cybercrime/reporting.htm.

[134] FTC, FTC Consumer Alert: *How Not to Get Hooked by a 'Phishing' Scam*, available at: http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm

[135] These are also frameworks, whether legal or otherwise, that emphasizes prevention. See, Brian C. Lewis, *Prevention of Computer Crime Amidst International Anarchy*, 41 Am. Crim. L. Rev. 1353 (2004). The author considers reliance solely on an international legal framework for the prosecution of computer-related offences to be inadequate and proposed a framework for prevention as a better alternative. The author endorses a "prevention-based" legal regime utilizing such novel approaches as "privately-sponsored corporate bounties", instituting a tort liability regime for ISPs, "hack-in contests", and a "market trading system" to control private sector solutions, etc. (all involving an active role for ISPs).

[136] See, Gregg Keizer, *Phishers Beat Bank's Two-Factor Authentication* (TechWeb, 14 July 2006), available at: http://news.yahoo.com/s/cmp/20060715/tc_cmp/190400329.

essence and due to the time difference between countries, it is also essential for these agencies to maintain sufficient round-the-clock resources to meet each other's needs. Protocol and operating procedures should be standardized as much as possible and organizations that have experience in this can and should share their know-how and assistance in harmonizing international efforts and in minimizing duplicitous and inefficient processes.

5. Law and Regulation

This has already been dealt with in detail in this paper. Some other suggested models for policing that merit consideration remain, in the foreseeable future at least, only of uncertain potential and even then they can only be supplementary to the current model of sanctioning the offender. Meanwhile, other methods of combating computer-related crimes that are already in existence remain limited and are also secondary to the criminal law model. They include some extent of liability and responsibility on non-offenders, even potential victims;[137] and non-criminal recourse such as the use of tort law to fight computer-related crimes.[138]

Conclusion

As we have seen, computer-related crime, in particular cyber crime such as phishing and its progeny, require a different solution due to the non-terrestrial and non-territorial nature of electronic transactions. In order to fight such crimes effectively, a strong and robust international regime is needed; and one that is as far as possible harmonized.

In order for there to be an effective global system to deal with the problem of computer-related crimes, there must be a multifaceted and multipronged approach using a combination of both legally coercive and non-legal measures. The international legal framework should consist of a dual carriageway approach to the problem with specific treaties for each subject area that is susceptible to universally consistent treatment and model laws in areas that do not, so as to promote as similar and consistent a set of laws as possible for each category of crime. In that way, the overall effect is optimized.

The Cybercrime Convention and other regional and multilateral initiatives are useful insofar as they serve as strong policy statements, and to some extent as undertakings, by

[137] See, Susan W. Brenner and Leo L. Clarke, *Distributed Security: Preventing Cybercrime*, 23 J. Marshall J. Computer & Info. L. (2005). Cyber crime prevention strategy use criminal sanctions and administrative regulations to impose and enforce responsibility on individuals and entities other than the offender to prevent cyber crime.

[138] See, Michael L. Rustad and Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 Berkeley Tech. L.J. 1553 (2005) (Negligence liability); Susan W. Brenner, *Toward a Criminal Law for Cyberspace: A New Model of Law Enforcement?,* 30 Rutgers Computer & Tech. L.J. 1 (2004) (An attenuated assumption of risk principle); Shannon C. Sprinkel, *Global Internet Regulation: The Residual Effects of The "Iloveyou" Computer Virus and the Draft Convention on Cyber-Crime*, 25 Suffolk Transnat'l L. Rev. 491 (2002) (Negligence liability); and Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. Cal. Interdis. L.J. 63 (2001) (Private policing through tort law regime).

governments to tackle what is clearly recognized as a collective problem that requires a collective solution. They also acknowledge and address the requirement for effective prescription, adjudication and enforcement in order for the solution to be truly effective. They serve as a necessary stepping-stone to a more effective and comprehensive treatment and they are often negotiated and discussed in fora that encourage understanding and consensus.

However, more needs to be done in order to effectively deal with the growing problem of computer-related crime. From the above analysis, there are some features that are integral to growing the international order in the cyber realm. Using cyber fraud and identity theft as the case study and in the context of phishing, pharming and related forms of deception, the following requirements are deciphered:

1. Prescriptive jurisdiction – This requires consistent worldwide criminalization of offences through applicable laws that have mutually enforcing effect, whether through extra-territorially applicable laws or a comprehensive network of same or similar laws or both.

2. Adjudicatory jurisdiction – Criminal procedure laws must ensure that offenders cannot avoid being brought to the courts in at least one country; provisions in a treaty requiring either enforcement or extradition can have that effect.[139] This eliminates or at the very least should drastically reduce the possibility of safe havens.

3. Enforcement jurisdiction – Even if a criminal is tried and convicted, effective enforcement of decisions is essential in order for the full effect of the system to work, particularly if the offender or his accomplices, instruments of crime or assets are in other jurisdictions. Consistent and reinforcing mutual legal recognition and enforcement treaties and provisions are required.

4. Administrative cooperation – Mutual legal assistance and cooperation in investigations, collection of evidence and other police matters are important. A strong international system of cooperation such as through Interpol as well as regional networks and a robust national infrastructure are important in this respect in order to

[139] In some Terrorism Conventions, for example, there is a provision that requires parties that have custody of offenders to either extradite the offender or submit the case for prosecution. Other provisions of note are provisions that require “severe penalties” or that require parties to assist each other in connection with criminal proceedings brought under the Convention. See the list of Conventions Against Terrorism at the UN Office on Drugs and Crimes web site at: http://www.unodc.org/unodc/terrorism_conventions.html. See in particular article 7 of the Hague Convention for the Suppression of Unlawful Seizure of Aircraft of 1970 and the Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation of 1971 (“The Contracting State in the territory of which the alleged offender is found shall, if it does not extradite him, be obliged, without exception whatsoever and whether or not the offence was committed in its territory, to submit the case to its competent authorities for the purpose of prosecution…”). See also, Chapter II, Section 3 on jurisdiction and Chapter III, Section 1, Title 2 of the Cybercrime Convention on the principles relating to extradition. It is submitted that cyberspace is no different from its physical analogue (i.e. the world) when it comes to commonality of certain subject matters (e.g. terrorism and cyber-terrorism) and due to the commonality in nature and effect of human communication and intercourse (i.e. transnational interaction and extraterritorial effects).

successfully identify, capture, try and convict cyber criminals. A network of domestic central specialized authorities connected to one another through one centralized international agency will be ideal.[140]

5. Pre-emptive measures – As far as possible, substantive law should have the effect of deterring and preventing offences from occurring rather than merely punish for offences that have occurred. This can be done through providing legal sanctions for preparation to commit offences that prescribes offences irrespective of its successful commission.[141]

6. Applicable laws (substantive) – Substantive laws must be rendered applicable to electronic transactions and digital assets including money and products; preferably through specific stand-alone legislation or new provisions, but otherwise through amendment of existing laws and definitions.

7. Applicable laws (procedural) – Procedural laws should be enacted or amended to facilitate the gathering of evidence and investigation of computer related crimes (i.e. computer forensics), and investigators and detectives must be equipped and skilled with the necessary expertise and technological know-how to investigate and deal with such offences and offenders.

8. Appropriate remedies – The law should create a credible and effective deterrent effect and sufficient punishment to suit the nature and severity of the offence.[142] Also where relevant, provisions allowing for rehabilitation could be useful, particularly if previous offenders, with their expertise, knowledge and connections, can be inducted into the system to aid and assist in future investigations and in the development of computer forensics.

9. Technological neutrality – The law should be drafted in such a way as to ensure its applicability to changing technology and techniques used to perpetrate criminal offences as far as possible. If technologically neutral provisions are not possible for a particular subject matter, then fast and reactive amendments or updates to the law are the only other alternative.

[140] Consider the 24/7 Network under Chapter III, Section 2, Title 3 of the Cybercrime Convention. See also Chapter III, Section 1, Title 1 (on the general principles relating to international co-operation) and Titles 3 to 4 (on the general principles relating to mutual assistance and procedures pertaining to mutual assistance requests in the absence of international agreements) as well as Section 2, Titles 1 to 3 of the Convention.

[141] Note that this may only be appropriate in some cases such as in the case of cyber fraud and identity theft through phishing and similar methods. Such legislation must be carefully drafted so that it is not ambiguous or encounter problems such as an over-incursion into civil liberty rights.

[142] See Chapter II, Section 1, Title 5, Article 13 of the Cybercrime Convention, which states that each party "…shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty…[and] shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions."

10. One-step Recourse – For the sake of clarity, transparency and ease of recourse, legislation directly dealing with computer and cyber crime that are preferably labeled as such and that contains provisions, illustrations and explanatory notes on point will be useful to potential offenders, possible victims and law enforcement officers. This is preferable to a messy and confusing array of different laws that may be applicable such as theft, fraud, identity theft and other legislation.

International connectivity and ease of transacting through information technology is valuable and, if mismanaged, will be squandered as an asset for human progress and interaction. As it is, computer crimes, cyber crimes and other abuses of the Internet, mobile and broadcast networks have damaged the trust and confidence in their use. This has adversely affected the full utility and potential of the cyber realm as another dimension, and the use of electronic media as a means, for humans to communicate and transact. Constant vigilance and efforts to manage these resources can and will reverse this trend and reinstate a lawful and orderly cyber society for the benefit of all.