INFORMATION
SECURITY

Volume
2

PSYCHOLOGY OF SECURITY AND THREAT ANALYSIS

MUHAMMAD ADEEL JAVAID

Nexus Academic Publishers (NAP)
Lahore Pakistan

Psychology of Security and Threat Analysis

Volume–2

INFORMATION SECURITY

Psychology of Security
and
Threat Analysis

http://nexusacademicpublishers.com/books

For a full list of contents, please see the *complete table* of contents on page 227

INFORMATION SECURITY

Volume 2

Psychology of Security and Threat Analysis

Muhammad Adeel Javaid

Nexus Academic Publishers (NAP)
Lahore Pakistan

First Published in Pakistan in 2013

The first edition published in 2013 by

Nexus Academic Publishers (NAP)

1–B Opposite School –4, Gate # 2, Old Officer Colony Zarar Shaheed Road, Sadar Lahore Cantt. Lahore, Pakistan Phone: 0092 322 4742353

email: info@nexusacademicpublishers.com

Nexus Academic Publishers (NAP)

1–B Opposite School –4, Gate # 2, Old Officer Colony Zarar Shaheed Road, Sadar Lahore Cantt. Lahore, Pakistan Phone: 0092 322 4742353

email: info@nexusacademicpublishers.com

Whilst the advice and information in this book are believed to be true and accurate at the date of going to press, neither the author(s) nor the publisher can accept any legal responsibility or liability for any errors or omissions that may be made. In particular (but without limiting the generality of the preceding disclaimer) every effort has been made to check information; however it is still possible that errors have been missed.

Nexus Academic Library Cataloguing in Publication Data
A catalogue record for this book is available for the Nexus Academic Publishers

Price :	Inland	Rs. 1500
	Foreign	USD 30

Typeset in 8.5 Californian FB by Nexus Academic Publishers, Punjab, Lahore Cantt (Pakistan)
Printed and bound in Pakistan

What do you think about this book? Or any other Hodder Arnold title? Please send your comments to info@nexusacademicpublishers.com

"Security is, I would say, our top priority because for all the exciting things you will be able to do with computers- organizing your lives, staying in touch with people, being creative- if we don't solve these security problems, then people will hold back."

– Bill Gates

Contents

PREFACE

Every day, the news media give more and more visibility to the effects of computer security on our daily lives. For example, on a single day in June 2006, the *Washington Post* included three important articles about security. On the front page, one article discussed the loss of a laptop computer containing personal data on 26.5 million veterans. A second article, on the front page of the business section, described Microsoft's new product suite to combat malicious code, spying, and unsecured vulnerabilities in its operating system. Further back, a third article reported on a major consumer electronics retailer that inadvertently installed software on its customers' computers, making them part of a web of compromised slave computers. The sad fact is that news like this appears almost every day, and has done so for a number of years. There is no end in sight.

Even though the language of computer security—terms such as virus, Trojan horse, phishing, spyware—is common, the application of solutions to computer security problems is uncommon. Moreover, new attacks are clever applications of old problems. The pressure to get a new product or new release to market still in many cases overrides security requirements for careful study of potential vulnerabilities and countermeasures. Finally, many people are in denial, blissfully ignoring the serious harm that insecure computing can cause.

Why Read This Book?

Admit it. You know computing entails serious risks to the privacy and integrity of your data, or the operation of your computer. Risk is a fact of life: Crossing the street is risky, perhaps more so in some places than others, but you still cross the street. As a child you learned to stop and look both ways before crossing. As you became older you learned to gauge the speed of oncoming traffic and determine whether you had the time to cross. At some point you developed a sense of whether an oncoming car would slow down or yield. We hope you never had to practice this, but sometimes you have to decide whether darting into the street without looking is the best means of escaping danger. The point is all these matters depend on knowledge and experience. We want to help you develop the same knowledge and experience with respect to the risks of secure computing.

How do you control the risk of computer security?

- Learn about the threats to computer security.
- Understand what causes these threats by studying how vulnerabilities arise in the development and use of computer systems.
- Survey the controls that can reduce or block these threats.
- Develop a computing style—as a user, developer, manager, consumer, and voter—that balances security and risk.

The field of computer security changes rapidly, but the underlying problems remain largely unchanged. In this book you will find a progression that shows you how current complex attacks are often instances of more fundamental concepts.

Users and uses of this Book

This book is intended for the study of computer security. Many of you want to study this topic: college and university students, computing professionals, managers, and users of all kinds of computer–based systems. All want to know the same thing: how to control the risk of computer security. But you may differ in how much information you need about particular topics: Some want a broad survey, while others want to focus on particular topics, such as networks or program development.

This book should provide the breadth and depth that most readers want. The book is organized by general area of computing, so that readers with particular interests can find information easily. The chapters of this book progress in an orderly manner, from general security concerns to the particular needs of specialized applications, and finally to overarching management and security and data breach issues and suggested ways and techniques to prevent them. Thus, the book covers all key areas of interest.

The home computer user is often said to be the weakest link in computer security. They do not always follow security advice, and they take actions, as in phishing, that compromise themselves. In general, we do not understand why users do not always behave safely, which would seem to be in their best interest. This book reviews the factors that influence security decisions for home computer users. The review is organized in four sections: understanding of threats, perceptions of risky behavior, efforts to avoid security breaches and attitudes to security interventions. These studies reveal a lot of reasons why current security measures may not match the needs or abilities of home computer users and suggest future work needed to inform how security is delivered to this user group.

What Background should you have to Appreciate this Book?

The only assumption is an understanding of programming and computer systems. Someone who is an advanced undergraduate or graduate student in computer science certainly has that background, as does a professional designer or developer of computer systems. A user who wants to understand more about how programs work can learn from this book, too; we provide the necessary background on concepts of operating systems or networks, for example, before we address the related security concerns.

This book can be used as a textbook in a one– or two–semester course in computer security. The book functions equally well as a reference for a computer professional or as a supplement to an intensive training course. And the index and extensive bibliography make it useful as a handbook to explain significant topics and point to key articles in the literature

Muhammad Adeel Javaid
Dated: 5–10–2013