

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

All rights reserved No part of Publication may be reproduced graphically or electronically, including storage or retrieval system without prior written permission of the Publisher : -

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	1
CHAPTER 1: Introduction	3
THREATS AND STALKING	3
THE NUREMBERG FILES	8
INTERNET FRAUD	12
HACKING	16
CHILD PORNOGRAPHY	24
CYBERTERRORISM	27
TERRORISTS IN CYBERSPACE	27
POLITICALLY AND SOCIALLY MOTIVATED CYBERATTACKS	28
POTENTIAL THREAT	29
FUTURE PROSPECTS	29
REFERENCES:	30
CHAPTER 2: Security (Un-) Usability	31
HUMAN COMPUTER INTERACTION	31
SOFTWARE PSYCHOLOGY	32
ITERATIVE DEVELOPMENT	32
USER MODELS	33
USABILITY ENGINEERING	34
DESIGN RATIONALE	35
ASSESSMENT QUESTIONS	37
COOPERATIVE ACTIVITY	38
REFERENCES	42
CHAPTER 3: Psychology of Security	46
THE TRADE-OFF OF SECURITY	46
CONVENTIONAL WISDOM ABOUT RISK	47
RISK AND THE BRAIN	48
RISK HEURISTICS	49
PROSPECT THEORY	50
OTHER BIASES THAT AFFECT RISK	51
PROBABILITY HEURISTICS	52
THE AVAILABILITY HEURISTIC	52
REPRESENTATIVENESS	54
REFERENCES:	58
CHAPTER 4: Psychology of Hackers	60
THE CLASSICAL CONUNDRUM OF CLASSIFICATION	60
A PSYCHODYNAMIC PERSPECTIVE ON HACKING	61
THE NEW AGE HACKER & FREUD'S PSYCHOANALYSIS	61
HANS EYSENCK'S THEORY	62
NEUTRALIZATION THEORY & HACKING	63
HACKING & COGNITIVE THEORIES	64
RATIONAL CHOICE THEORY OF HACKING	64
REFERENCES:	66
CHAPTER 5: Psychology of Users	67

THE HOME COMPUTER USER	67
PREDICTIVE MODELS	69
SECURITY RISK AND CONSEQUENCES	69
DEFENSIVE SECURITY ACTIONS	72
RECOMMENDATIONS FOR FUTURE WORK	76
REFERENCES	77
CHAPTER 6: Threat Analysis and Management	80
THREAT IDENTIFICATION	81
THREAT / CATEGORY MATRIX	91
CORRELATION OF THREATS TO CATEGORIES	92
THREAT ANALYSIS AND ASSESSMENT	93
SCENARIO GENERATION UTILIZING FOOTPRINTS	95
THREAT ASSESSMENT USING TAME	98
TAME OVERVIEW	98
EXAMPLE SCENARIO	102
PROCESS 1: BUSINESS ANALYSIS	103
PROCESS 2: STAKEHOLDER IDENTIFICATION	104
PROCESS 3: SYSTEM BOUNDARIES IDENTIFICATION	104
PROCESS 4: THREAT AGENT IDENTIFICATION & SELECTION	104
PROCESS 5: ASSET IDENTIFICATION	104
PROCESS 6: THREAT AGENT PREFERENCE STRUCTURING	105
Process 7: Vulnerability Identification & Selection	105
PROCESS 8: THREAT AGENT ATTRIBUTE CALCULATION	105
PROCESS 10: SCENARIO GENERATION	107
PROCESS 13: IMPACT ANALYSIS	107
PROCESS 14: THREAT STATEMENT GENERATION	108
APT EXPLOITATION LIFE CYCLE	109
CHALLENGES	109
INCIDENT RESPONSE AND HANDLING	110
THREAT MANAGEMENT	110
INCENTIVES FOR CHANGE	110
RISK MANAGEMENT APPROACH	111
DECISION ANALYSIS	112
REFERENCES	112
Hacking Techniques in Wireless Networks	113
CASE STUDY	113
WIRELESS LAN OVERVIEW	113
WIRELESS NETWORK SNIFFING	115
WIRELESS SPOOFING	116
WIRELESS NETWORK PROBING	117
AP WEAKNESSES	117
DENIAL OF SERVICE	117
MAN-IN-THE-MIDDLE ATTACKS	118
WAR DRIVING	119
WIRELESS SECURITY BEST PRACTICES	120

SOFTWARE TOOLS	120
REFERENCES	121
Cyber Storm II–Case Study	121
BACKGROUND	122
PLANNING AND EXECUTION	123
SECURITY POLICY	124
SIGNIFICANT FINDINGS	124
FINDING 1:	124
FINDING 2	125
FINDING 3:	125
FINDING 4	126
FINDING 5	126
FINDING 6	126
ANNEXE A: PARTICIPATING ORGANIZATIONS	127
Using RFID for Cyber Threats Mitigation	127
CASE STUDY	127
SCENARIOS	128
THREAT MODEL	129
LOGISTICS	129
AUDITING	131
TOOLS	133
Case studies	133
ACCESS CONTROL	134
REFERENCES	135
Using RSC for Cyber Threats Mitigation	135
CASE STUDY	135
Description of the FCDS system	135
FCDS use case	137
The Detailed description of the Translator Module	137
Verification and Discussion of results	140
Summary and Futher Work	140
References	141
Mitigating Denial of Service (DoS) Attacks	141
CASE STUDY	141
THREAT ASSESSMENT	142
ATTACK TRENDS	143
THREAT MANAGEMENT	143
PROTECT	144
REACT	144
AVAILABLE RESOURCES	144
CHAPTER 7: Planning for Security	146
STRATEGIC	146
COMPONENTS OF ORGANIZATIONAL PLANNING	147
PLANNING LEVELS	149
PLANNING AND THE CISO	150

PLANNING FOR INFORMATION SECURITY IMPLEMENTATION	150
INTRODUCTION TO THE SYSTEMS DEVELOPMENT LIFE CYCLE	152
INVESTIGATION	152
ANALYSIS	152
LOGICAL DESIGN	152
PHYSICAL DESIGN	152
THE SECURITY SYSTEMS DEVELOPMENT LIFE CYCLE (SECS DLC)	153
INVESTIGATION IN THE SECS DLC	153
ANALYSIS IN THE SECS DLC	153
RISK MANAGEMENT	153
DESIGN IN THE SECS DLC	154
IMPLEMENTATION IN THE SECS DLC	154
MAINTENANCE AND CHANGE IN THE SECS DLC	155
CHAPTER 8: Designing for Securability	157
SIZING A PLANNED DEPLOYMENT	157
SIZING FOR PERFORMANCE	157
SIZING FOR SECURITY	159
SIZING FOR AVAILABILITY	160
SUN CLUSTER	162
SIZING FOR SCALABILITY	163
OPTIMIZING RESOURCES	163
MANAGING RESOURCES	164
SCM Security Architecture–Case Study	165
SECURITY CONSIDERATIONS	166
SAMPLE APPLICATION ARCHITECTURE	166
USAGE SCENARIOS EMPLOYED	166
DEPLOYMENT VIEW	167
SECURITY REQUIREMENTS	168
DATA ORIGIN AUTHENTICATION AND IDENTIFICATION	173
DIGITAL SIGNATURES	174
GETCATALOGREQUEST	184
GETCATALOGRESPONSE	186
SUBMITORDER	188
SUBMITORDERRESPONSE	191
SHIPGOODS	192
ShipGoodsResponse	194
SUBMIT PO	195
ACKPO	197
SECURITY CHECKLIST FOR WEB APPLICATION DESIGN	198
AUTHENTICATION	199
AUTHORIZATION AND ACCESS CONTROL	200
SESSION MANAGEMENT	200
DATA AND INPUT VALIDATION	201
CROSS SITE SCRIPTING (XSS)	201
COMMAND INJECTION FLAWS	201

INSECURE USE OF CRYPTOGRAPHY	202
ERROR HANDLING	202
REMOTE ADMINISTRATION FLAWS	203
WEB APPLICATION AND SERVER CONFIGURATION	203
REFERENCES	203
CHAPTER 9: Cyber Crime Law Making	205
THE RISE OF CRIME IN CYBERSPACE	205
A STUDY OF THE PHENOMENON	206
TERRESTRIAL CRIME VERSUS CYBERCRIME	207
THE SCOPE OF THE PHENOMENON	208
CYBERSPACE MISUSE AND ABUSE	210
HACKING AND RELATED ACTIVITIES	210
VIRUSES AND MALICIOUS CODES	211
ONLINE FRAUD	212
COMPUTER RELATED ECONOMIC CRIMES	218
OFFENCES AGAINST INTELLECTUAL PROPERTY	220
THE INTERNATIONAL DIMENSION	223
USING TECHNOLOGY TO FIGHT CYBERCRIME	225
REFERENCES:	225

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