

# Practical Information Security



Izzat Alsmadi • Robert Burdwell  
Ahmed Aleroud • Abdallah Wahbeh  
Mahmood Al-Qudah • Ahmad Al-Omari

# Practical Information Security

A Competency-Based Education Course

 Springer

Izzat Alsmadi  
Texas A&M University San Antonio  
One University Way  
San Antonio, TX, USA

Ahmed Aleroud  
Department of Computer  
Information Systems  
Yarmouk University  
Irbid, Jordan

Mahmood Al-Qudah  
Yarmouk University  
Irbid, Jordan

Robert Burdwell  
Texas A&M University San Antonio  
One University Way  
San Antonio, TX, USA

Abdallah Wahbeh  
Slippery Rock University of Pennsylvania  
Slippery Rock, PA, USA

Ahmad Al-Omari  
Schreiner University  
Kerrville, TX, USA

ISBN 978-3-319-72118-7      ISBN 978-3-319-72119-4 (eBook)  
<https://doi.org/10.1007/978-3-319-72119-4>

Library of Congress Control Number: 2017961570

© Springer International Publishing AG 2018, corrected publication 2018

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature  
The registered company is Springer International Publishing AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Contents

<b>1 Introduction to Information Security</b> .....	1
Overview .....	1
Knowledge Sections .....	1
Information Taxonomy .....	2
Information State .....	2
Information Location .....	3
Information Sensitivity .....	4
Security Goals .....	5
Security Risks, Threats, and Vulnerabilities .....	7
Security Countermeasures .....	10
Security Education, Training and Awareness .....	10
Information Security Challenges .....	10
Skills Section .....	12
CIA Triad – Confidentiality, Integrity and Availability .....	12
Information Security Cases .....	12
Applications Section .....	13
Information Security Basics: Testing Your Anti-virus Software Application .....	13
Information Security Basics: Vulnerability Scanning .....	13
References .....	15
<b>2 The Ontology of Malwares</b> .....	17
Overview .....	17
Knowledge Sections .....	17
Spyware .....	18
Adware .....	20
Rootkits .....	22
Ransomware .....	24
Worms .....	26
Trojan Horses .....	29
Backdoors .....	31

Rogue Security Software . . . . .	31
Internet Bots . . . . .	31
Keyloggers . . . . .	32
Crimeware . . . . .	35
Scareware . . . . .	37
Viruses . . . . .	37
Bugs . . . . .	39
Phishing . . . . .	40
Spamming . . . . .	40
Browser Hijacking . . . . .	41
Logic Bombs . . . . .	41
Code Injection . . . . .	41
Pharming . . . . .	43
Skills Section . . . . .	44
General Malware Details . . . . .	44
Applications Section . . . . .	44
Microsoft Safety Scanner . . . . .	44
White Hat: Experience With Keylogger . . . . .	45
Protect Computers from Dangerous Website . . . . .	46
Limit Spam Messages in Your Outlook Account . . . . .	47
Scan for Rootkits Using TDSSKiller . . . . .	48
References . . . . .	50
<b>3 Security and Access Controls: Lesson Plans . . . . .</b>	<b>53</b>
Overview . . . . .	55
Knowledge Sections . . . . .	56
Access Controls in Operating and File Systems . . . . .	56
Access Controls in Database Management Systems . . . . .	59
Access Controls in Websites and Web-Applications . . . . .	60
Identity Management . . . . .	61
Single-Sign-On (SSO) . . . . .	61
Session Time-out . . . . .	62
Kerberos . . . . .	62
Digital Certificates . . . . .	62
Access Control in Distributed and Operating Systems . . . . .	63
RBAC (Role-Based Access Control) . . . . .	64
OBAC (Object-Based Access Control) . . . . .	66
Skills Section . . . . .	67
Tools for Windows SAM Database . . . . .	67
Users Access Control in Linux . . . . .	68
Applications Section . . . . .	69
Access Controls in Different Websites and Web-Applications . . . . .	69
Applications for RBAC (Role-Based Access Control) Systems . . . . .	70
Applications for OBAC (Object-Based Access Control) Systems . . . . .	70
References . . . . .	70

- 4 Security and Risk Management and Planning: Lesson Plans . . . . . 73**
- Overview . . . . . 74
- Knowledge Sections . . . . . 75
  - Security and Risk Management and Planning . . . . . 75
  - Risk Management Approaches . . . . . 76
  - Risk Tolerance. . . . . 76
  - Risk Policies . . . . . 77
  - Risk Assessment and Model . . . . . 79
  - Incident Response Planning . . . . . 79
  - Disaster Recovery . . . . . 80
  - Cyber Security Awareness Plan . . . . . 81
  - Security Risk and Forensics Resources . . . . . 81
  - Common Forensics for Risk . . . . . 82
  - Risk Management Approaches . . . . . 82
  - Risk Tolerance. . . . . 83
  - Incident Response Planning . . . . . 83
  - Potential Risk Self-Assessment Survey . . . . . 84
  - Disaster Recovery . . . . . 85
  - DRP Sections . . . . . 85
  - Cyber Security Awareness Plan . . . . . 86
- Skill’s Section . . . . . 87
  - Discuss Tools for Tracking Risks . . . . . 87
  - Identify Risk Metrics . . . . . 87
  - Identify Types of Security Incident Responses. . . . . 87
  - Discuss why Disaster Recovery Planning Is Necessary . . . . . 87
  - Evaluate Development Process for Risk Management. . . . . 88
  - Create an Incident Response Plan. . . . . 88
  - Develop a Disaster Recovery Plan . . . . . 89
- Applications’ Section . . . . . 89
  - Develop a Risk Assessment or Model. . . . . 89
  - Create a Cyber Security Plan . . . . . 89
- 5 Encryption and Information Protection/Integrity and Concealment Methods: Lesson Plans . . . . . 91**
- Overview . . . . . 93
- Knowledge Sections . . . . . 93
  - Information Hiding and Protection: Cryptography or Encryption . . . . . 93
  - Methods to Break Encrypted Text. . . . . 95
  - Ciphering or Encryption Algorithms . . . . . 95
- Symmetric Encryption Algorithms . . . . . 95
  - Block Ciphers . . . . . 95
  - BlowFish . . . . . 100
  - Stream Ciphers . . . . . 100
- Asymmetric Encryption Algorithms . . . . . 100
  - Encryption Substitution Techniques . . . . . 102

Cryptography Applications . . . . .	104
Encryption for Internet/Online Communications and e-Commerce . . .	104
Encryption in E-Commerce . . . . .	104
Encryption in Email Communication . . . . .	105
Encryption in Browsers. . . . .	105
Encryptions in Telecommunication/Networks . . . . .	107
Encryption in Operating Systems and Disks . . . . .	107
FileVault for Apple OS/X . . . . .	109
Information Integrity and Authentication Techniques and Methods . . . .	111
Information Authentication/Originality Checking . . . . .	113
Information Integrity/Authentication Applications. . . . .	113
Information Concealment/Authenticity Techniques, Methods and Applications . . . . .	115
Skills Section . . . . .	117
Use and Evaluate Encryption Algorithms . . . . .	117
Use and Evaluate Encryption Applications. . . . .	118
Use and Evaluate Information Integrity Algorithms. . . . .	118
Use and Evaluate Information Integrity Applications. . . . .	118
Use and Evaluate Information Concealment Applications. . . . .	119
Experience/Ability Section . . . . .	119
References. . . . .	120
<b>6 Network Security . . . . .</b>	<b>121</b>
Overview . . . . .	121
Knowledge Sections . . . . .	121
Open Systems Interconnection (OSI) . . . . .	121
Application Layer . . . . .	122
Transport Layer. . . . .	122
Network Layer . . . . .	124
Types of the Addresses in the Internet . . . . .	124
Routing and Translation of Addresses . . . . .	125
Network Attacks at Different Layers . . . . .	125
Data Modification Attacks . . . . .	126
Identity Spoofing Attacks . . . . .	126
ARP Spoofing Attacks . . . . .	127
Address Resolution Protocol (ARP) . . . . .	129
Countermeasures. . . . .	129
Denial of Service Attack. . . . .	130
MAC Flooding Attacks. . . . .	131
A TCP SYN Flooding. . . . .	132
Denial of Service Attacks (Smurf Attack) . . . . .	133
Packet Sniffing Attacks. . . . .	134
Skills Section . . . . .	134
Network Traffic Analysis Using Wireshark and Other Tools . . . . .	134
Applications Section. . . . .	137
References. . . . .	138



- 7 Web and Database Security** . . . . . 139
  - Overview . . . . . 139
  - Knowledge Section . . . . . 139
  - Web Applications . . . . . 139
    - The Two Sides of Web Security . . . . . 140
  - Web Threat Models . . . . . 140
    - Cross Site Scripting . . . . . 141
    - Cross Site Request Forgery . . . . . 143
  - Database Security . . . . . 144
  - Access Control . . . . . 145
    - Grant and Revoke . . . . . 145
    - Security through Views . . . . . 145
    - Stored Procedures . . . . . 146
    - Query Modification . . . . . 146
  - Privacy Problems in Databases . . . . . 146
  - SQL Injection Attacks . . . . . 149
    - Using SQL Injection to Steal Data . . . . . 150
    - Mitigation of SQL Injection Attacks . . . . . 152
  - Skills Section . . . . . 152
  - SQL Inject a Web Application . . . . . 154
  - Other Forms of SQL Injection Attacks . . . . . 154
  - Applications Section . . . . . 155
    - Applications for Encryption Techniques for Network Security . . . . . 155
    - Applications of Website Vulnerability Scanners . . . . . 156
    - Applications for Detecting Network Attacks
      - Using Traffic Analysis . . . . . 156
      - Questions . . . . . 156
  - References . . . . . 157
  
- 8 Mobile and Wireless Security: Lesson Plans** . . . . . 159
  - Overview . . . . . 161
  - Knowledge Sections . . . . . 161
  - Users/Software Security in Mobile/Smart Devices . . . . . 162
    - Application Code Signing (Vetting) . . . . . 162
    - Bring your Own Device (BYOD) and Security Issues . . . . . 162
    - Theft and Loss/Unauthorized Access Issues . . . . . 163
    - Mobile Security/Malware Threats . . . . . 164
    - Installing Mobile Applications from Unknown or Un-trusted Stores . . . . . 167
    - Mobile Anti-malware Systems . . . . . 168
    - Online Social Networks (OSNs) . . . . . 169
    - Operating Systems Security Issues in Mobile/Smart Devices . . . . . 170
    - Sandboxing . . . . . 171
    - Mobile Jail-Breaking . . . . . 172
    - Operating System Updates . . . . . 172
    - Prepare for Phone Physical Theft . . . . . 172

Hardware/Network Security Issues in Mobile/Smart Devices . . . . .	173
A Secure Phone Booting Process . . . . .	173
AES Crypto-Engine . . . . .	174
Access Control Models . . . . .	174
Connecting to Unsecured Wireless Networks . . . . .	175
Wireless Networks and Platforms Security Issues . . . . .	175
Transport Layer Security (TLS) . . . . .	175
Remote Wipe Feature . . . . .	176
Location-Based Services and Privacy Control . . . . .	176
Skills Section . . . . .	177
Software Security Issues in Smart Devices . . . . .	177
Smart Devices Operating Systems and Security Issues . . . . .	177
Applications Section . . . . .	178
Evaluating Access Controls in Smart Devices and Wireless Networks . . . . .	178
<b>9 Software Code Security: Lesson Plans . . . . .</b>	<b>181</b>
Overview . . . . .	183
Knowledge Sections . . . . .	183
Software Code Security and Vulnerability Issues . . . . .	184
Buffer and Stack Overflows . . . . .	184
Memory Leak and Violation Issues . . . . .	185
Invalidated Inputs (SQL Injection and XSS) . . . . .	185
Race Conditions . . . . .	187
Software Vulnerability/Penetration Testing . . . . .	188
Static and Dynamic Security Analysis . . . . .	188
Secure Software Design Principles and Practices . . . . .	190
Common Software Security Design Flaws . . . . .	192
Software Secure Construction and Defensive Programming, Exceptions and Error Handling . . . . .	194
Software Malware Analysis . . . . .	194
Anti-malware Detection Techniques . . . . .	195
Manual Malware Analysis . . . . .	197
Skills Section . . . . .	197
Software Security Testing . . . . .	197
Static Software Security Code Reviews . . . . .	198
Malware Analysis . . . . .	198
Applications Section . . . . .	198
Evaluating Software Programs for Security Vulnerabilities . . . . .	198
Software Security Assessment Based on Predefined Security Requirements . . . . .	199
<b>10 Disk and Computer Forensics: Lesson Plans . . . . .</b>	<b>201</b>
Overview . . . . .	204
Knowledge Sections . . . . .	204
Disk Forensic Activities . . . . .	205
Image Acquisition . . . . .	205

- Data Recovery . . . . . 207
- Forensic Analysis . . . . . 208
- Disk Forensics in FAT Systems . . . . . 209
- Why and How Much Technical Detail a Forensic Investigator Needs to Know? . . . . . 213
- Disk Forensics in NTFS Systems . . . . . 214
- ADS (Alternate Data Stream) . . . . . 216
- ADS Detection Tools . . . . . 217
- Disk Forensics in Ext. Systems . . . . . 218
- File Recovery in Ext File Systems . . . . . 220
- Disk Forensics in HFS+ Systems . . . . . 221
- Volume Headers . . . . . 222
- Memory Forensics . . . . . 223
- Forensic Relevant Information That Can Be Found in Memory . . . . . 223
- Memory Forensic Tools . . . . . 225
- Forensic Investigations in Windows Operating Systems . . . . . 227
- Windows Registry . . . . . 229
- Internet Traces . . . . . 229
- Event Viewer . . . . . 232
- Web Logs . . . . . 233
- Forensic Investigations in Linux Operating Systems . . . . . 233
- Forensic Investigations in MAC Operating Systems . . . . . 236
- Skills Section . . . . . 237
  - Disk Forensic Tools . . . . . 237
- Disk Forensics . . . . . 238
  - Raw Format Image Acquisition . . . . . 238
  - Using Hex-Editors . . . . . 238
  - Foremost and File Carving . . . . . 238
- Applications Section . . . . . 240
- Memory Analysis with Volatility . . . . . 240
- Linux Logs . . . . . 241
- Kali Linux . . . . . 241
- Windows Registry . . . . . 241
- Linux Rootkit Checker . . . . . 242
- References . . . . . 243
- 11 Network Forensics: Lesson Plans . . . . . 245**
  - Overview . . . . . 246
  - Knowledge Section . . . . . 247
    - Traffic Analysis . . . . . 247
    - Wire Tapping . . . . . 250
    - Wireless Tapping . . . . . 250
    - Wireshark . . . . . 252
    - Packet Filtering . . . . . 254
    - Foremost . . . . . 259
    - Switches' Forensics . . . . . 261
    - Port Mirroring . . . . . 264

- Routers’ Forensics . . . . . 265
- Firewalls’ Forensics . . . . . 267
- IDS/IPS Forensics . . . . . 267
- Wireless Forensics . . . . . 269
- Skills’ Sections . . . . . 272
  - Traffic Analysis . . . . . 272
  - Foremost . . . . . 273
  - ARP Spoofing . . . . . 273
- Applications’ Section . . . . . 273
  - NIC Promisc Mode . . . . . 273
  - SDN Switches . . . . . 273
  - Switch Forensics . . . . . 274
  - IDS/IPS Forensics . . . . . 274
- References . . . . . 282
- 12 Web Forensics-Chapter Competencies . . . . . 283**
  - Overview . . . . . 284
  - Knowledge Section . . . . . 284
    - Web Forensics . . . . . 284
      - Email . . . . . 284
      - Email Protocols . . . . . 285
      - Email Forensics Tools . . . . . 286
      - Email Headers . . . . . 287
      - Email Files . . . . . 289
      - Email File Reports . . . . . 291
      - Web Browsers . . . . . 291
      - Criminal Cases with Web . . . . . 291
  - Skill Activities . . . . . 292
    - Understand the Process of Evidence Handling of Emails  
and Browsers Information . . . . . 292
    - Review Email Headers . . . . . 293
    - Scan for Archived Files from Mail Client . . . . . 293
    - Review and Examine the Web Browsing History . . . . . 294
    - Locate Essential Artifacts for Investigation (IE, Firefox,  
Chrome, and Safari) . . . . . 294
    - Discuss the Criminal and Civil Cases Associated  
with Electronic Communications or Web Activities . . . . . 295
  - Application Activities . . . . . 295
    - Review and Examine the Web Browsing History . . . . . 295
    - Utilize a Web Forensics Software . . . . . 295
- 13 Mobile Forensics . . . . . 297**
  - Overview . . . . . 297
  - Knowledge Section . . . . . 298
    - Mobile Forensics . . . . . 298
    - Mobile Device Hardware and Software . . . . . 299
    - Operating Systems . . . . . 299

- Device States . . . . . 300
- SIM Card . . . . . 300
- GPS . . . . . 301
- Device Seize . . . . . 301
- Mobile Forensics Tools . . . . . 301
- Skill Activities . . . . . 304
  - Know the Different Operating Systems for the Mobile Devices . . . . . 304
  - Identify the Layers of an Operating System for a Mobile Device . . . . . 304
  - Outline the Steps for Examining the Device Folders  
on a Mobile Device . . . . . 305
  - Identify the States of a Mobile Device . . . . . 305
  - Understand how the SIM Card Can Be Used for the Investigation . . . . . 306
  - Understand How GPS Coordinates Can Be Used  
in an Investigation . . . . . 306
  - Create a Process for a Company to Seize a Mobile Device  
from an Employee . . . . . 307
- Application Activities . . . . . 307
  - Examine the Device Information, Installed Apps, Call History,  
Contacts, and Messaging . . . . . 307
- References . . . . . 308
- Erratum to: Practical Information Security . . . . . E1**
- Index . . . . . 309**

---

The original version of this book was revised. An erratum to this book can be found at [https://doi.org/10.1007/978-3-319-72119-4\\_14](https://doi.org/10.1007/978-3-319-72119-4_14)