The InfoSec Handbook

An Introduction to Information Security

Umesh Hodeghatta Rao
Umesha Nayak

Selected For intel Intel's Recommended Reading List

Apress open

Contents

About the Authors xxi

Acknowledgments xxiii

Introduction xxv

■Part I: Introduction 1

■Chapter 1: Introduction to Security 3

What is Security? 3

Why is Security Important? 4

What if You Do Not Care About Security? 5

The Evolution of the Computer and Information Security 6

Information Security Today 8

Applicable Standards and Certifications 11

The Role of a Security Program 12

■Chapter 2: History of Computer Security 13

Introduction 13

Communication 14

World Wars and Their Influence on the Field of Security 15

Cypher Machine: Enigma 15

Code Breakers 18

Some Historical Figures of Importance: Hackers and Phreakers 19

Kevin Mitnick 22

Chapter Summary 24

■Part II: Key Principles and Practices 27

■Chapter 3: Key Concepts and Principles 29

Introduction 29

Security Threats 31

External and Internal Threats 31

Information Security Frameworks and Information Security Architecture 35

Pillars of Security 42

People 43

Policies, Procedures, and Processes 48

Technology 49

Information Security Concepts 49

CIA Triad 49

Parkerian Hexad 53

Implementation of Information Security 56

Risk Assessment 56

Planning and Architecture 57

Gap Analysis 57

Integration and Deployment 57

Operations 58

Monitoring 58

Legal Compliance and Audit 58

Crisis Management 59

Principles of Information Security 59

Chapter Summary 61

■Chapter 4: Access Controls 63

Introduction 63

Confidentiality and Data Integrity 64

Who Can Access the Data? 64

What is an Access Control? 64

Authentication and Authorization 65

Authentication and Access Control Layers 65

Access Control Strategies........ 69

Implementing Access Controls........ 72

Access Control Lists (ACLs) 72

AAA Framework........ 74

LDAP and Active Directory........ 75

IDAM 75

Chapter Summary 76

■Chapter 5: Information Systems Management........ 77

Introduction........ 77

Risk........ 78

Incident........ 78

Disaster 78

Disaster Recovery........ 78

Business Continuity........ 78

Risk Management 79

Identification of Risk........ 80

Risk Analysis........ 84

Risk Responses 85

Execution of the Risk Treatment Plans 86

The Importance of Conducting a Periodic Risk Assessment 86

Incident Response........ 87

Incident Response Policy, Plan, and Processes 88

Incident Response Teams........ 91

Ensuring Effectiveness of Incident Response........ 93

Disaster Recovery and Business Continuity........ 102

How to Approach Business Continuity Plan........ 102

Chapter Summary 110

■Part III: Application Security 113

■Chapter 6: Application and Web Security........ 115

Introduction 115

Software Applications 115

Completeness of the Inputs 117

Correctness of the Inputs 118

Completeness of Processing 118

Correctness of Processing 119

Completeness of the Updates 119

Correctness of the Updates 119

Preservation of the Integrity of the Data in Storage 119

Preservation of the Integrity of the Data while in Transmission 120

Importance of an Effective Application Design and Development Life Cycle 120

Important Guidelines for Secure Design and Development 121

Web Browsers, Web Servers, and Web Applications 123

Vulnerabilities in Web Browsers 125

Vulnerabilities of Web Servers 127

Web Applications 129

Chapter Summary 138

■Chapter 7: Malicious Software and Anti-Virus Software........ 141

Introduction 141

Malware Software 142

Introduction to Malware 142

Types of Malware in Detail 143

Spyware 143

Adware 143

Trojans 144

Viruses 144

Worms 144

Backdoors......144
Botnets......144
A Closer Look at Spyware......144
Trojans and Backdoors......145
Rootkits......150
Viruses and Worms......151
Botnets......154
Brief History of Viruses, Worms, and Trojans......155
The Current Situation......156
Anti-Virus Software......156
Need for Anti-Virus Software......157
Top 5 Commercially Available Anti-Virus Software......158
Symantec Norton Anti-Virus Software......159
McAfee Anti-Virus......159
Kaspersky Anti-Virus......159
Bitdefender Anti-Virus......160
AVG Anti-Virus Software......160
A Few Words of Caution......160
Chapter Summary......161
■**Chapter 8: Cryptography......163**
Introduction......163
Cryptographic Algorithms......164
Symmetric Key Cryptography......165
Key Distribution......166
Asymmetric Key Cryptography......167
Public Key Cryptography......168
RSA Algorithm......170
Advantages of Public Key Cryptography......171
Applications of PKC......171
Public Key Infrastructure (PKI)......171

Certificate Authority (CA) 172

Digital Certificate 172

Hash Function Cryptography 172

Popular Hashes 174

Digital Signatures 174

Summary of Cryptography Standard Algorithms 174

Disk / Drive Encryption 180

Attacks on Cryptography 181

Chapter Summary 181

■Part IV: Network Security 183

■Chapter 9: Understanding Networks and Network Security 187

Introduction 187

Networking Fundamentals 187

Computer Communication 188

Network and its Components 189

Network Protocols 191

Network Vulnerabilities and Threats 195

Vulnerabilities 196

Threats 198

Attacks 199

Chapter Summary 203

■Chapter 10: Firewalls 205

Introduction 205

How Do You Protect a Network? 206

Firewall 208

Basic Functions of Firewall 209

Packet Filtering 209

Stateful Packet Filtering 213

Network Address Translation (NAT)....214

Application Level Gateways (Application Proxy)....216

Firewall Deployment Architecture....217

Option 1: Bastion Host....218

Option 2: Staging Area or Demilitarized Zone (DMZ)....218

Personal Firewall....219

Firewall Best Practices....219

Auditing of Firewall....221

Chapter Summary....222

■Chapter 11: Intrusion Detection and Prevention Systems....225

Introduction....225

Why Use IDS?....225

Types of IDS....226

How Does Detection Work?....229

Signature-Based Detection....229

Anomaly-Based Detection....230

IDS/IPS System Architecture and Framework....234

Appliance (Sensors)....235

Signature Update Server....235

IDS/IPS in Context....242

Chapter Summary....243

■Chapter 12: Virtual Private Networks....245

Introduction....245

Advantages of VPN....246

VPN Types....247

Remote Access (Host-to-Site) VPN....247

Site-to-Site (Intranet and Extranet) VPN....248

VPN and Firewall....249

VPN Protocols....250

Tunneling....250

Data Authentication and Data Integrity.......251
Anti-Replay Services.......251
Data Encryption.......251
Layer Two Tunneling Protocol (L2TPv3).......252
Generic Routing Encapsulation (GRE).......253
Internet Protocol Security (IPSec).......253
MPLS (Multi-Protocol Label Switching).......257
MPLS VPN.......258
MPLS VPN Security.......259
Important IETF Standards and RFCs for VPN Implementation.......259
A Few Final Thoughts about VPN.......260
Chapter Summary.......262
■**Chapter 13: Data Backups and Cloud Computing.......263**
Introduction.......263
Need for Data Backups.......263
Types of Backups.......264
Category 1: Based on current data on the system and the data on the backups.......264
Category 2: Based on what goes into the backup.......265
Category 3: Based on storage of backups.......266
Category 4: Based on the extent of the automation of the backups.......266
RAID Levels.......267
Other Important Fault Tolerance Mechanisms.......267
Role of Storage Area Networks (SAN) in providing Backups and Disaster Recovery.......269
Cloud Infrastructure in Backup Strategy.......269
Database Backups.......270
Backup Strategy.......270
Restoration Strategy.......271
Important Security Considerations.......271
Some Inherent Issues with Backups and Restoration.......272
Best Practices Related to Backups and Restoration.......272

Introduction to Cloud Computing....................273
What is Cloud Computing? 274
Fundamentals of Cloud Computing....................275
Cloud Service Models....................275
Important Benefits of Cloud Computing 278
Upfront Capital Expenditure (CAPEX) versus Pay as you use Operational Expenditure (OPEX)....................278
Elasticity or Flexibility....................278
Reduced need for specialized resources and maintenance services....................278
On-Demand Self-Service Mode versus Well-Planned Time-Consuming Ramp Up....................278
Redundancy and Resilience versus Single Points of Failure....................279
Cost of traditional DRP and BCP versus the DRP & BCP through Cloud Environment 279
Ease of use on the Cloud Environment....................279
Important Enablers of Cloud Computing 279
Four Cloud Deployment Models 280
Private Cloud 281
Public Cloud....................281
Community Cloud 281
Hybrid Cloud....................281
Main Security and Privacy Concerns of Cloud Computing 282
Compliance....................282
Lack of Segregation of Duties 282
Complexity of the Cloud Computing System....................282
Shared Multi-tenant Environment 282
Internet and Internet Facing Applications....................283
Control of the Cloud Consumer on the Cloud Environment....................283
Types of Agreements related to Service Levels and Privacy with the Cloud Provider....................283
Data Management and Data Protection....................283
Insider Threats....................284
Security Issues on account of multiple levels 284
Physical security issues related to Cloud Computing environment....................284
Cloud Applications Security....................284

Threats on account of Virtual Environment....284

Encryption and Key Management....284

Some Mechanisms to address the Security and Privacy Concerns in Cloud Computing Environment....285

Understand the Cloud Computing environment and protect yourself....285

Understand the Technical Competence and segregation of duties of the Cloud Provider....285

Protection against Technical Vulnerabilities and Malicious Attacks....285

Regular Hardening and Appropriate Configurations of the Cloud Computing Environment....286

Data Protection....286

Encryption....286

Good Governance Mechanisms....286

Compliance....286

Logging and Auditing....286

Patching / Updating....287

Application Design and Development....287

Physical Security....287

Strong Access Controls....287

Backups....287

Third-Party Certifications / Auditing....287

Chapter Summary....287

■Part V: Physical Security....289

■Chapter 14: Physical Security and Biometrics....293

Introduction....293

Physical and Technical Controls....294

ID Cards and Badges....295

Photo ID cards....295

Magnetic Access Cards....295

Other Access Mechanisms....296

Locks and Keys....297

Electronic Monitoring and Surveillance Cameras....297

Alarms and Alarm Systems 297

Biometrics 297

Some of the important biometric mechanisms 298

How the biometric system works 300

Enrollment 301

Recognition 301

Performance of the Biometrics System 301

The test of a good biometric system 301

Possible information security issues with the Biometric Systems 302

Multimodal biometric system 302

Advantages of Biometric systems 302

Administrative Controls 303

Fire Safety Factors 303

Interception of Data 304

Mobile and Portable Devices 305

Visitor Control 305

Chapter Summary 306

■**Chapter 15: Social Engineering 307**

Introduction 307

Social Engineering Attacks: How They Exploit Human Nature 309

Helping Nature 309

Trusting Nature 310

Obeying the Authority 310

Fear 311

Social Engineering: Attacks Caused by Human Beings 312

Social Engineering: Attacks Caused by Computers or Other Automated Means 314

Social Engineering: Methods that are Used for Attacks 316

Social Engineering: Other Important Attack Methods 319

Social Engineering: How to Reduce the Possibility of Falling Prey to Attacks 320

Chapter Summary 323

■Chapter 16: Current Trends in Information Security 325
Wireless Security 325
Bluetooth Technology and Security 327
Mobile Security 328
Chapter Summary 329
■Bibliography 331
Chapter 1 331
Footnotes 331
References 331
Chapter 2 332
Footnotes 332
Additional References 333
Chapter 3 334
Footnotes 334
Chapter 4 335
Footnotes 335
Chapter 5 335
Footnotes 335
Chapter 6 335
Footnotes 335
Additional References 336
Chapter 7 336
Footnotes 336
Chapter 8 337
Footnotes 337
Additional References 339
Chapter 9 340
Footnotes 340
Additional References 341

Chapter 10 341

Footnotes 341

Additional References 341

Chapter 11 342

Footnotes 342

Additional References 342

Chapter 12 343

Footnotes 343

Additional References 344

Chapter 13 345

Footnotes 345

References 346

Chapter 14 346

Footnotes 346

References 346

Additional References 346

Chapter 15 346

Footnotes 346

Additional References 347

Chapter 16 347

Footnotes 347

Index 349