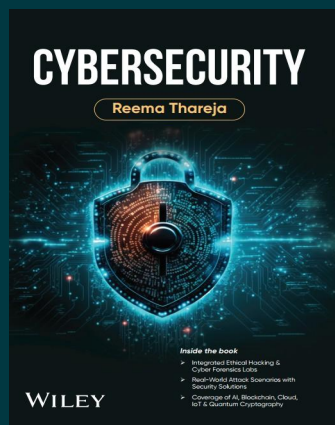




Cybersecurity

By Reema Thareja

Paperback

9789377062897

₹999.00

Pages: 790

Description

Cybersecurity is a comprehensive, classroom-ready introduction to how digital systems are attacked and how they are defended. Banking, healthcare, education, governance, and commerce now run on digital infrastructure, and cybercrime has stopped being an IT department problem. This book is written for the students and professionals who will have to deal with that.

The text is organized into fifteen chapters that move from foundational concepts to advanced and emerging areas. The opening chapters establish what cyber security is, then work through the taxonomy of active, passive, and hardware attacks; malware in all its forms; social engineering; and two full chapters on web application vulnerabilities, from SQL injection and XSS through to clickjacking, session hijacking, and business logic flaws.

From there the book turns to defense. It covers cybercrime techniques and the dark web, the CIA triad and risk management frameworks, access control and authentication, network defense mechanisms from firewalls to onion routing, and threat intelligence through the cyber kill chain, incident response, and honeypots. Three chapters then develop cryptography properly, from classical ciphers to DES, AES, RSA, and Diffie-Hellman, and on to TLS, IPsec, PGP, and email authentication.

The final chapters address cyber threat intelligence, including SIEM, the role of AI and machine learning, and digital, network, and mobile forensics, before closing on security in emerging technologies: blockchain, IoT, cloud, DevSecOps, and quantum cryptography. A full set of laboratory exercises follows the fifteen chapters, giving students hands-on practice in controlled environments. Chapter-wise PowerPoint decks and a solutions manual are available to adopting faculty.

About the Author

Reema Thareja

Reema Thareja is Assistant Professor in the Department of Computer Science, School of Open Learning, University of Delhi, with more than 21 years of teaching experience across undergraduate and postgraduate programmes. She has published over 40 research papers in reputed international journals and filed six patents, with an h-index of 14 and an i10-index of 21. She built Jruma, a computer science learning and quizzing app for Android and iOS, to make learning a fun-based activity.

She serves on the Board of Studies in Computer Science for P.B. Siddhartha College of Arts & Science, Vijayawada and Sri Durga Malleswara Siddhartha Mahila Kalasala, and on the Technical Advisory Board of Refactor Academy. She has spoken at FDPs, conferences, workshops, and webinars in India, the UAE, and the USA, including the Global Virtual Summit in New York in 2021 and an international conference in France in 2023. She has mentored student projects for California-based startups and recorded MOOCs for the School of Open Learning, University of Delhi.

Table of Contents

Preface	v
About the Book	vii
About the Author	ix
Acknowledgments	xi
Chapter 1 Introduction to Cyber Security	1
1.1 What Is Cybersecurity?	2
1.2 Major Cybersecurity Challenges	3
1.3 Components of Cybersecurity Systems	4
1.4 Common Sources of Cyber Threats	7
1.5 Different Types of Cybersecurity	8
1.6 Key Aspects of Cyber Security	14
1.7 The Evolution of the Cybersecurity Threat Landscape	16
1.8 Cybersecurity Trends	18
1.9 Essential Security Technologies	20
1.10 Cybersecurity Myths vs. Facts	22
End-of-chapter assessment	25
Chapter 2 Taxonomy of Attacks: Active, Passive, and Hardware Attacks	31
2.1 Active and Passive Attacks	32
2.2 Types of Active Attacks	35
2.3 Distributed Denial of Service (DDoS)	38
2.4 Passive Attack	46
2.5 Securing Hardware and Software	54
2.6 Hardware Threats	56
2.7 Types of Hardware Attacks	58
2.8 Best Practices for Securing Hardware: A Practical Guide	62
2.9 Cyber Criminals and Their Motives	64
End-of-chapter assessment	70
Chapter 3 Malware Attacks	75
3.1 What Is Malware?	76
3.2 Virus	77
3.3 Worms	83
3.4 Trojan Horse	87
3.5 Ransomware	90
3.6 Adware	92
3.7 Spyware	93
3.8 Keyloggers	96
3.9 Logic Bomb	103
3.10 Rootkits	105

3.11 Backdoor	106
3.12 How to Identify if a Device Is Infected with Malware?	109
3.13 How to Protect Against Malware	109
End-of-chapter assessment	111
Chapter 4 Social Engineering Attacks	117
4.1 Social Engineering	118
4.2 How Does Social Engineering Work?	119
4.3 Why It Works: Human Nature and Lack of Awareness	121
4.4 How to Prevent Social Engineering Attacks	124
4.5 Social Engineering Attack Techniques	126
End-of-chapter assessment	138
Chapter 5 Input-Based Vulnerabilities in Web Applications	145
5.1 What Is a Web Application?	146
5.2 SQL Injection	149
5.3 Cross-Site Scripting (XSS)	153
5.4 Cross-Site Request Forgery (CSRF)	157
5.5 Directory Traversal Attack	160
5.6 Command Injection	162
5.7 File Inclusion Attacks	166
5.8 Web Shell Attacks	171
End-of-chapter assessment	175
Chapter 6 Advanced Exploitation and Logic Attacks in Web Security	181
6.1 Clickjacking	183
6.2 Session Hijacking	186
6.3 Man-in-the-Middle (MiTM) Attack	191
6.4 Man-in-the-Browser (MitB)	197
6.5 HTTP Response Splitting Attack	199
6.6 Open Redirect Attack	201
6.7 Business Logic Vulnerabilities	206
6.8 Web Cache Poisoning	209
End-of-chapter assessment	212
Chapter 7 Cybercrime Techniques	219
7.1 Cybercrime	220
7.2 Types of Cybercrimes	221
7.3 Why Are Cybercrimes Increasing?	225
7.4 Impact of Cybercrime	225
7.5 Challenges of Cybercrime	227
7.6 Basic Prevention Measures	228

7.7 Cyberstalking	228
7.8 Cyberharassment	230
7.9 Cyberbullying	230
7.10 Dark Web	233
7.11 Mobile Security	239
7.12 IoT Security	243
7.13 Online Scams	248
7.14 Online Child Sexual Exploitation and Abuse (OCSEA)	252
7.15 Cyberwarfare	254
7.16 Cybercrime-as-a-Service (CaaS)	256
End-of-chapter assessment	261
Chapter 8 Core Concepts in Cybersecurity and Risk Management	267
8.1 The CIA Triad	269
8.2 Cybersecurity Risk Management: A Shared Responsibility	273
8.3 Cybersecurity Risk Management Plan	274
8.4 Risk Appetite and Risk Tolerance	277
8.5 Standards and Frameworks That Require a Cyber Risk Management Plan	279
8.6 Benefits of Cybersecurity Risk Management	283
8.7 Cyber Security Risk Management Best Practices	284
8.8 Common Challenges in Cybersecurity Risk Management	285
8.9 Access Control	286
8.10 Authentication	292
8.11 Authentication Protocols	298
8.12 Kerberos	307
End-of-chapter assessment	310
Chapter 9 Network Defense Mechanisms and Secure Communication	317
9.1 Antivirus Software	319
9.2 Firewall	327
9.3 Intrusion Detection System (IDS)	336
9.4 Intrusion Prevention System (IPS)	343
9.5 Intrusion Detection and Prevention System (IDPS)	346
9.6 Virtual Private Network (VPN)	347
9.7 Wireless Security	352
9.8 Onion Routing	358
End-of-chapter assessment	364
Chapter 10 Advanced Threat Intelligence and Security Planning	371
10.1 Kill Chain	373
10.2 Incident Response	376

10.3 Honeypots	381
10.4 Cybersecurity Plan	391
End-of-chapter assessment	401
Chapter 11 Cryptography	407
11.1 Cryptography	408
11.2 Types of Cryptography	410
11.3 Secure Communications	418
11.4 Classical Encryption Algorithms	420
End-of-chapter assessment	448
Chapter 12 Modern Cryptographic Algorithms	455
12.1 Data Encryption Standard (DES)	456
12.2 Triple DES (3DES)	461
12.3 Advanced Encryption Standard (AES)	463
12.4 RSA (Rivest-Shamir-Adleman) Encryption	472
12.5 Diffie-Hellman Key Exchange and Perfect Forward Secrecy	479
12.6 Hash Functions	485
12.7 Digital Signatures and Certificates	488
End-of-chapter assessment	495
Chapter 13 Cryptographic Protocols and Attacks	503
13.1 Transport Layer Security (TLS)	504
13.2 Secure Socket Layer (SSL)	509
13.3 Hypertext Transport Protocol Secure (HTTPS)	512
13.4 Internet Protocol Security (IPSec)	515
13.5 Internet Key Exchange (IKE)	518
13.6 Pretty Good Privacy (PGP)	521
13.7 Secure/Multipurpose Internet Mail Extensions (S/MIME)	522
13.8 STARTTLS	523
13.9 DNS-Based Authentication of Named Entities (DANE)	524
13.10 How Secure Is Gmail	524
13.11 Simple Mail Transfer Protocol with Security (SMTPS)	525
13.12 Trio of SPF, DKIM, and DMARC	525
13.13 Digital Signatures	527
13.14 Cryptographic Protocol Attacks	527
End-of-chapter assessment	538
Chapter 14 Cyber Threat Intelligence	545
14.1 SIEM Log Management	546
14.2 The Role of AI and ML in Cybersecurity	555
14.3 Digital Multimedia Forensics	565

14.4 Role of Digital Evidence in Investigations	570
14.5 Network Forensics	572
14.6 Wi-Fi Router Data: A Digital Witness in an Investigation	576
14.7 Computer vs. Network Forensics	576
14.8 Mobile Device Forensics	577
End-of-chapter assessment	584
Chapter 15 Security in Emerging Technologies	593
15.1 Blockchain	594
15.2 IoT Security	602
15.3 Security in Cloud Computing	613
15.4 DevSecOps	624
15.5 Quantum Cryptography	633
End-of-chapter assessment	639
Lab Exercises	645

To purchase this product, please visit:

<https://www.wileyindia.com/cybersecurity.html>



Scan to buy