Undergraduate Topics in Computer Science

Robin Sharp

# Introduction to Cybersecurity

## A Multidisciplinary Challenge

UTiCS

Springer

# Undergraduate Topics in Computer Science

**Series Editor**

Ian Mackie, University of Sussex, Brighton, UK

**Advisory Editors**

Samson Abramsky, Department of Computer Science, University of Oxford, Oxford, UK

Chris Hankin, Department of Computing, Imperial College London, London, UK

Mike Hinchey, Lero — The Irish Software Research Centre, University of Limerick, Limerick, Ireland

Dexter C. Kozen, Department of Computer Science, Cornell University, Ithaca, NY, USA

Hanne Riis Nielson, Department of Applied Mathematics and Computer Science, Technical University of Denmark, Kongens Lyngby, Denmark

Steven S. Skiena, Department of Computer Science, Stony Brook University, Stony Brook, NY, USA

Iain Stewart, Department of Computer Science, Durham University, Durham, UK

Joseph Migga Kizza, College of Engineering and Computer Science, University of Tennessee at Chattanooga, Chattanooga, TN, USA

Roy Crole, School of Computing and Mathematics Sciences, University of Leicester, Leicester, UK

‘Undergraduate Topics in Computer Science’ (UTiCS) delivers high-quality instructional content for undergraduates studying in all areas of computing and information science. From core foundational and theoretical material to final-year topics and applications, UTiCS books take a fresh, concise, and modern approach and are ideal for self-study or for a one- or two-semester course. The texts are authored by established experts in their fields, reviewed by an international advisory board, and contain numerous examples and problems, many of which include fully worked solutions.

The UTiCS concept centers on high-quality, ideally and generally quite concise books in softback format. For advanced undergraduate textbooks that are likely to be longer and more expository, Springer continues to offer the highly regarded *Texts in Computer Science* series, to which we refer potential authors.

Robin Sharp

# Introduction to Cybersecurity

## A Multidisciplinary Challenge

Springer

Robin Sharp
Department of Applied Mathematics
and Computer Science (DTU Compute)
Technical University of Denmark
Kongens Lyngby, Denmark

ISSN 1863-7310 ISSN 2197-1781 (electronic)
Undergraduate Topics in Computer Science
ISBN 978-3-031-41462-6 ISBN 978-3-031-41463-3 (eBook)
https://doi.org/10.1007/978-3-031-41463-3

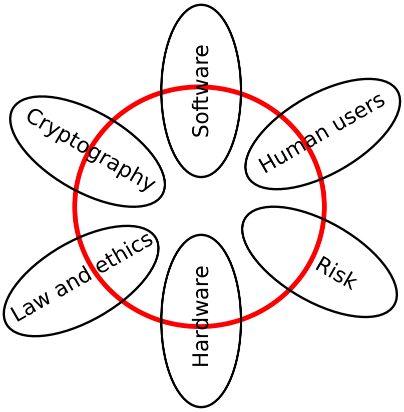
© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2024

This work is subject to copyright. All rights are solely and exclusively licensed 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, expressed 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.

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

Paper in this product is recyclable.

# Preface



This book gives an introduction to cybersecurity for people who would like to know more about the security risks which arise in the modern IT world, where computers and many other electronic devices communicate with one another through networks. The detailed requirements for cybersecurity vary from one application area to another, but in general terms are a matter of achieving some simple aims: that data must not be read, modified, deleted or made unavailable by persons who are not allowed to.

Achievment of such aims is a multidisciplinary challenge, as an IT system consists of both hardware, software and human users, all of which can contribute to the success or failure of efforts to maintain cybersecurity. In this book we therefore look at the most common, both technical and non-technical, ways in which cybersecurity may be threatened, at how you can protect yourself against such threats, and how to deal with situations where this protection fails.

An important topic in any discussion of cybersecurity is the rules which regulate behaviour in an Internet based world. A lack of cybersecurity can have dramatic consequences, both for individuals and for society as a whole. Some activities, such as terrorism or destruction of IT systems which are vital to society, are so harmful, that they must be considered as crimes. Others have consequences, such as disclosure of details of your private life, which are unpleasant but not necessarily illegal. In the last main chapter of the book we give an overview of some of the most important laws and regulations with relevance for cybersecurity.

The book is based on material developed for an elementary course on IT security for a group of students at the Technical University of Denmark (DTU) who were not IT specialists. It is intended particularly for readers starting on a course of study in computer science or engineering who require a general introduction to the subject.

It is assumed that readers have a certain knowledge of computers – at least as computer users. But many aspects of cybersecurity cannot be explained without going somewhat more into detail with technical aspects of IT systems which affect cybersecurity. The book therefore gives an introduction to what computer systems consist of, how networks of various types work, and what operating systems do. These parts of the book are especially intended for readers who do not have a suitable grounding in IT. Certain of the book's topics, especially modern cryptography, require a certain knowledge of mathematics, but not more than you should be able to get from a school-leaving exam. Interested readers can find some more detailed explanations of relevant mathematical topics in an appendix.

A problem for all readers, irrespective of their mother tongue, is that the whole area of cybersecurity is awash with acronyms, most of which are so accepted in technical circles that it is meaningsless to try to avoid using them. To help the reader, a short explanation of all the technical acronyms which are used in this book is provided in an appendix.

The book concludes with a numbered list of references to publicly available documents related to the topics presented in the main text. (References to these documents in the main text appear in square brackets – so for example [34] refers to reference number 34 in the list.)

To get the most out of the book, it is important that the reader doesn't just read the text. All the chapters contain exercises which illustrate important aspects of the topic dealt with in the chapter. There are both theoretical exercises and exercises which involve you in trying something out in practice on a computer. Here it is best if you have an experimental attitude to things, and are willing to throw yourself out into experiments if you do not completely understand what is happening. In this way you will get a much better understanding of how things hang together – and a smaller risk of just becoming a "desktop expert" without any useful practical experience.

The author would like to thank his many students and colleagues at DTU Compute and elsewhere for their helpful comments on various drafts of this book which have seen the light of day. Without their encouragement and feedback the book would never have been written.

Lyngby, *Robin Sharp*
July 2023.

# Acknowledgments

Parts of this textbook have previously appeared in the work “What’s Cybersecurity All About?” (ISBN 978 87 502 0023 9), written by the author and published by Polyteknisk Forlag, Copenhagen, and are reproduced here with their kind permission.

Chapter 3 contains material which is copyright by Carnegie Mellon University[1] and which is reproduced here under the following conditions:

> This textbook has been created by Robin Sharp using, incorporating and/or based on Figure 2 – OCTAVE Phases on page 5 and text from Section 3.1 – OCTAVE Method Processes on pages 11-12 from the User Guide, “Introduction to the OCTAVE Approach” by Christopher J. Alberts, Audrey J. Dorofee, James F. Stevens and Carol Woody © 2003 Carnegie Mellon University and Table 7: Graphical Representation of Threat Trees on page 50 of the Technical Report, “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process” by Richard A. Caralli, James F. Stevens, Lisa R. Young and William R. Wilson, CMU/SEI-2007-TR-012, ESC-TR-2007-012 (c) 2007 Carnegie Mellon University, with special permission from its Software Engineering Institute.
>
> ANY MATERIAL OF CARNEGIE MELLON UNIVERSITY AND/OR ITS SOFTWARE ENGINEERING INSTITUTE CONTAINED HEREIN IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.
>
> This textbook has not been reviewed nor is it endorsed by Carnegie Mellon University or its Software Engineering Institute.

Figure 9.3 comes from my previous colleague Jens Fagertun here at DTU Compute and is reproduced here with his kind permission.

Figures 1.3, 11.8 and 13.3 are original artworks by Peter Heydenreich and are reproduced here with his kind permission.

[1] ™ Carnegie Mellon, CERT and OCTAVE are registered trademarks of Carnegie Mellon University. $^{\text{SM}}$ Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

# Contents

**1 Introduction: Why Cybersecurity?** . . . . . 1

1.1 Information Security and Cybersecurity . . . . . 1

1.1.1 The Development of the Internet . . . . . 2

1.2 How Do Computers Work Together? . . . . . 3

1.2.1 Systems of Systems . . . . . 4

1.3 Cyberattacks Today . . . . . 5

1.4 Security Targets . . . . . 9

1.4.1 CIA Targets . . . . . 10

1.4.2 Security Policies . . . . . 11

1.5 Reader's Guide . . . . . 13

1.5.1 A Short Note on Notation . . . . . 15

Exercises . . . . . 16

**2 Technique and Human Beings** . . . . . 17

2.1 Psychological Attacks . . . . . 18

2.1.1 Curiosity . . . . . 19

2.1.2 Helpfulness . . . . . 19

2.1.3 Sympathy and Hate . . . . . 20

2.1.4 Belief in Authority . . . . . 20

2.1.5 The Brain's Two Modes of Operation . . . . . 22

2.1.6 Uncertainty in Decision Making . . . . . 23

2.2 Phishing . . . . . 25

2.3 Humans vs. Machines . . . . . 27

2.4 Can Psychological Attacks Be Prevented? . . . . . 29

2.4.1 Motivation . . . . . 30

2.4.2 Training . . . . . 31

Exercises . . . . . 34

**3 Risk** . . . . . 37

3.1 What Is Risk? . . . . . 37

3.2 Threats in IT Systems . . . . . 40

3.3 Countermeasures ... 41
3.4 Risk Management ... 42
3.5 Systematic Security Analysis ... 43
3.5.1 ISO/IEC 27002 ... 43
3.5.2 OCTAVE® ... 45
3.6 Risk Management as a PDCA Process ... 53
Exercises ... 55

**4 Cryptography** ... 57
4.1 Some Central Concepts ... 57
4.1.1 Cryptosystems ... 58
4.1.2 Cryptanalysis ... 59
4.2 Symmetric Encryption ... 60
4.2.1 Substitution Ciphers ... 60
4.2.2 Random Permutation ... 61
4.2.3 Polyalphabetic Ciphers ... 64
4.2.4 Vigenère Ciphers ... 64
4.2.5 Transposition Ciphers ... 65
4.3 Modern Ideas ... 66
4.3.1 One-Time Pads ... 67
4.3.2 Confusion and Diffusion ... 68
4.3.3 DES ... 68
4.3.4 AES ... 72
4.3.5 Symmetric Stream Ciphers ... 73
4.4 Asymmetric Cryptosystems ... 79
4.4.1 Trapdoor Functions ... 80
4.4.2 Modular Arithmetic ... 80
4.4.3 The RSA Cryptosystem ... 82
4.5 A Comparison of PKCS and SKCS ... 88
Exercises ... 90

**5 Applied Cryptography** ... 95
5.1 Integrity ... 95
5.1.1 Cryptographic Hash Functions ... 96
5.1.2 MAC ... 100
5.2 Electronic Signatures ... 102
5.2.1 Verification of Electronic Signatures ... 102
5.2.2 Electronic Signatures with a PKCS ... 103
5.2.3 Digital Signature Standard (DSS) ... 104
5.2.4 Planning for the Future ... 106
5.3 Authentication ... 107
5.3.1 Types of Evidence ... 107
5.3.2 Authentication with an SKCS ... 108
5.3.3 Authentication with a PKCS ... 110
5.4 Key Distribution ... 111

5.4.1 Diffie-Hellman Key Agreement ........ 112
5.4.2 More Secure Key Agreements ........ 113
5.5 Certificates ........ 113
5.5.1 How Are Certificates Issued in a PKI? ........ 115
5.5.2 Access to Certificates ........ 116
5.6 Trust Models ........ 116
5.6.1 The Hierarchical Trust Model ........ 117
5.6.2 The Web-of-trust Model ........ 118
5.6.3 The Reputation-based Trust Model ........ 118
5.7 Establishing an Identity ........ 119
Exercises ........ 122

**6 Communication Networks** ........ 125
6.1 Basic Network Concepts ........ 125
6.1.1 Layered Architectures ........ 126
6.1.2 Services ........ 127
6.1.3 Protocols ........ 128
6.2 Communication in the Internet ........ 130
6.2.1 Data Transfer Between Layers ........ 131
6.2.2 Addressing ........ 132
6.2.3 TCP and UDP Ports ........ 135
6.2.4 Functions in TCP and IP ........ 136
6.2.5 DNS ........ 139
6.2.6 How Do the Layers Work Together? ........ 140
6.3 Technology ........ 141
6.3.1 Shared Cable-based Media ........ 143
6.3.2 Wireless Networks ........ 144
6.3.3 Mobile Telephones on the Net ........ 146
Exercises ........ 150

**7 Network Applications** ........ 153
7.1 Mail Transfer ........ 153
7.1.1 Mail Relays ........ 156
7.1.2 The Structure of a Mail ........ 157
7.1.3 MIME ........ 158
7.2 Transfer of Web Pages ........ 162
Exercises ........ 169

**8 Network Security** ........ 171
8.1 Protection Based on Cryptographic Methods ........ 171
8.1.1 The Application Layer ........ 172
8.1.2 The Transport Layer ........ 173
8.1.3 The Internet Layer ........ 173
8.1.4 The Link Layer ........ 174
8.1.5 The Physical Layer ........ 175

8.2 Encryption in the Application Layer .......... 175
8.3 Virtual Private Networks .......... 178
8.3.1 Tunneling .......... 178
8.4 Secure Socket Layer .......... 182
8.4.1 SSL Protocol Architecture .......... 183
8.4.2 SSL/TLS Security Parameter Sets .......... 184
8.4.3 Protocols Secured with SSL/TLS .......... 185
8.5 Risks in Using Certificates .......... 187
8.6 Firewalls .......... 189
8.6.1 Types of Firewall .......... 189
8.6.2 Placement of Firewalls .......... 192
8.6.3 Residual Risks Connected with Firewalls .......... 195
8.6.4 Personal Firewalls .......... 195
8.7 Intrusion Detection Systems (IDS) .......... 196
8.7.1 Principles of Operation .......... 196
8.7.2 Network IDSs (NIDS) .......... 198
8.7.3 Host IDSs (HIDS) .......... 198
8.8 Security in Wireless Networks .......... 199
8.8.1 Original WiFi Security (WEP) .......... 200
8.8.2 Development of Security in IEEE 802.11 .......... 201
8.8.3 Security in Bluetooth .......... 202
8.9 Security in the Mobile Telephone Network .......... 204
8.9.1 Security in GSM .......... 204
8.9.2 Can the A5 Functions Be Broken in Practice? .......... 206
8.9.3 Security in UMTS .......... 207
8.9.4 False BTSs and Surveillance .......... 208
8.9.5 Is Your Mobile Device Secure? .......... 209
8.10 Denial of Service (DoS) Attacks .......... 211
8.10.1 DoS Attacks in the Application Layer .......... 211
8.10.2 DoS Attacks in the Transport Layer .......... 213
8.10.3 DoS Attacks in the Internet Layer .......... 214
8.10.4 DoS Attacks in the Link and Physical Layers .......... 215
8.10.5 Distributed DoS Attacks .......... 216
8.10.6 Permanent DoS Attacks .......... 217
8.10.7 Risks and Countermeasures for DOS Attacks .......... 218
8.11 Security in DNS .......... 218
8.11.1 Countermeasures for Use in DNS .......... 219
8.12 Security in SMTP .......... 220
8.12.1 SPF .......... 220
8.12.2 DKIM .......... 222
8.13 Security in SNMP .......... 224
8.13.1 Risks and Countermeasures in Using SNMP .......... 225
8.14 Critical Infrastructure Protection .......... 226
8.15 Evaluation of Network Security .......... 228
Exercises .......... 231

**9 Security in Operating Systems** . . . . . 235
9.1 User Authentication . . . . . 236
9.1.1 Biometric Authentication . . . . . 237
9.1.2 Passwords . . . . . 241
9.1.3 Pattern Locks . . . . . 246
9.1.4 Trends in User Authentication . . . . . 247
9.1.5 Authentication Through the Net . . . . . 247
9.2 Authorisation, Protection & Rights . . . . . 250
9.2.1 Who Decides? . . . . . 251
9.2.2 Access Control Matrices . . . . . 252
9.2.3 Access Control Lists . . . . . 252
9.2.4 Directories . . . . . 253
9.2.5 Capabilities . . . . . 253
9.3 Access Control in File Systems . . . . . 254
9.3.1 Unix-style File Protection . . . . . 255
9.3.2 setuid and setgid . . . . . 257
9.3.3 Windows NT ACLs . . . . . 258
9.4 Access Control for Other System Components . . . . . 259
9.4.1 Access Control in the Memory . . . . . 260
9.4.2 Access Control for Hardware Units . . . . . 263
9.4.3 Access Control for the CPU . . . . . 264
9.4.4 Access Control in Android . . . . . 265
9.4.5 Bypassing Access Control: Rootkits . . . . . 266
9.4.6 The Reference Monitor revisited . . . . . 267
9.5 Encryption in the Operating System . . . . . 268
9.6 Job Scheduling . . . . . 270
9.7 Updating the Operating System . . . . . 271
9.8 Is Your OS Genuine? . . . . . 272
9.9 What the OS Cannot Do . . . . . 273
Exercises . . . . . 276

**10 Software security** . . . . . 281
10.1 Classes of Security Failure in Software . . . . . 281
10.1.1 Buffer Overflow . . . . . 282
10.1.2 Buffer Overflow Vulnerabilities . . . . . 283
10.1.3 Buffer Overread . . . . . 284
10.1.4 Incomplete Mediation . . . . . 285
10.1.5 Time-of-check to Time-of-use (TOCTTOU) . . . . . 285
10.1.6 Detection of Programming Errors . . . . . 286
10.2 Malicious Code . . . . . 289
10.2.1 Virus Attacks . . . . . 290
10.2.2 Worm attacks . . . . . 292
10.2.3 Antivirus Systems . . . . . 293
10.3 SQL Injection . . . . . 296
10.3.1 Countermeasures . . . . . 298

10.4 LDAP Injection . . . . . . . . 299
10.4.1 LDAP Searches . . . . . . . . 302
10.5 HTTP-based Applications . . . . . . . . 304
10.5.1 HTTP Authentication . . . . . . . . 305
10.5.2 HTTP Cookies . . . . . . . . 309
10.5.3 SessionIDs . . . . . . . . 312
10.5.4 Webforms . . . . . . . . 313
10.5.5 Mobile code . . . . . . . . 316
10.5.6 Web Server Vulnerabilities . . . . . . . . 317
10.6 Targets for Software Security . . . . . . . . 320
Exercises . . . . . . . . 322

**11 Incident Handling and System Availability** . . . . . . . . 325
11.1 Reacting to Security Incidents . . . . . . . . 325
11.1.1 Incident Reporting . . . . . . . . 326
11.1.2 Investigation of Security Incidents . . . . . . . . 327
11.2 Business Continuity Planning . . . . . . . . 333
11.2.1 The BCP Process . . . . . . . . 334
11.2.2 BCP Analysis . . . . . . . . 334
11.2.3 BCP Resource Requirements . . . . . . . . 335
11.3 Disaster Recovery Planning . . . . . . . . 335
11.3.1 Phases of Recovery . . . . . . . . 336
11.3.2 DRP Strategies . . . . . . . . 337
11.3.3 DRP Testing . . . . . . . . 341
11.4 Security Awareness . . . . . . . . 342
Exercises . . . . . . . . 344

**12 Law and Ethics** . . . . . . . . 347
12.1 Computer Crime . . . . . . . . 348
12.1.1 Which Acts Must Be Considered Illegal? . . . . . . . . 349
12.1.2 Which Powers Must Be Available? . . . . . . . . 350
12.1.3 Jurisdiction . . . . . . . . 351
12.1.4 International Rules in the Convention . . . . . . . . 352
12.1.5 Anti-terror Laws . . . . . . . . 352
12.2 Protection of Personal Data . . . . . . . . 353
12.2.1 Important Concepts . . . . . . . . 355
12.2.2 General Rules . . . . . . . . 355
12.2.3 Classes of Personal Data . . . . . . . . 356
12.2.4 Transfer of Personal Data to Third Countries . . . . . . . . 358
12.2.5 The Data Subject's Rights . . . . . . . . 358
12.2.6 Security of Processing . . . . . . . . 359
12.2.7 Leakages . . . . . . . . 360
12.2.8 Authorities . . . . . . . . 360
12.2.9 Codes of Conduct and Certification . . . . . . . . 361
12.2.10 Legal Responsibility and Penalties . . . . . . . . 362

12.3 Protection of Healthcare Data . . . 363
12.3.1 Who Has Access to Health Data? . . . 363
12.4 Ethics . . . 364
12.4.1 Datamining . . . 365
12.4.2 Tracking . . . 366
12.4.3 Protection Against Breaches of Privacy . . . 368
Exercises . . . 370

**13 Epilogue** . . . 373

**A What's in the Box?** . . . 381
A.1 Hardware . . . 381
A.1.1 Disks . . . 384
A.1.2 Input and Output (I/O) Units . . . 387
A.1.3 Attachment of I/O Units . . . 388
A.1.4 Communication Units . . . 389
A.1.5 Power Supplies . . . 390
A.2 Software . . . 390
A.2.1 The Operating System . . . 391
A.2.2 Firmware . . . 392
A.2.3 Utility Programs . . . 393
A.2.4 Application Programs . . . 393
Exercises . . . 395

**B Mathematics** . . . 397
B.1 Basic Concepts . . . 397
B.2 Fermat's Factorisation Algorithm . . . 401
B.3 Euclid's Algorithm . . . 403
B.4 Euclid's Extended Algorithm . . . 404
B.4.1 Calculation of an Inverse modulo *n* . . . 405
B.5 The Chinese Remainder Theorem . . . 406
B.6 Why Does RSA Work? . . . 407
B.7 A Common-modulus Attack on RSA . . . 409
B.8 The Birthday Paradox . . . 410

**C Acronyms** . . . 411

**References** . . . 421

**Index** . . . 427