Errata to the Fifth Printing (August 2004) and the Sixth Printing (November 2004)

Preface

"Acknowledgements," p. xl

Please change the paragraph at the bottom of p. xl to the following. The list of names has several additions:

Many others contributed to this book in various ways. Special thanks to Steven Alexander, Jim Alves-Foss, Bill Arbaugh, Andrew Arcilla, Alex Aris, Rebecca Bace, Belinda Bashore, Vladimir Berman, Rafae Bhatti, Ziad El Bizri, Logan Browne, Terry Brugger, Serdar Cabuk, Raymond Centeno, Lisa Clark, Michael Clifford, Christopher Clifton, Dan Coming, Kay Connelly, Crispin Cowan, Tom Daniels, Dimitri DeFigueiredo, Joseph-Patrick Dib, Jeremy Frank, Robert Fourney, Martin Gagne, Ron Gove, James Hinde, Xuxian Jiang, Jesper Johansson, Mark Jones, Calvin Ko, Mark-Neil Ledesma, Ken Levine, Karl Levitt, Yunhua Lu, Gary McGraw, Alexander Meau, Nasir Memon, Mark Morrissey, Ather Nawaz, Iulian Neamtiu, Kimberly Nico, Stephen Northcutt, Rafael Obelheiro, Josko Orsulic, Holly Pang, Ryan Poling, Sung Park, Ashwini Raina, Jorge Ramos, Brennen Reynolds, Peter Rozental, Christoph Schuba, David Shambroom, Jonathan Shapiro, Clay Shields, Sriram Srinivasan, Mahesh V. Tripunitara, Vinay Vittal, Tom Walcott, James Walden, Dan Watson, Guido Wedig, Chris Wee, Patrick Wheeler, Paul Williams, Bonnie Xu, Xiaoduan Ye, Lara Whelan, John Zachary, Aleksandr Zingorenko, and to everyone in my computer security classes, who (knowingly or unknowingly) helped me develop and test this material.

Chapter 1, "An Overview of Computer Security"

Section 1.1.1, "Confidentiality," p. 4 [author]

The first word in this section, "Confidentiality", should be italicized.

Section 1.1.2, "Integrity," p. 5 [author]

The first word in this section, "Integrity", should be italicized.

Section 1.1.3, "Availability," p. 6 [author]

The first word in this section, "Availability", should be italicized.

Section 1.3, "Policy and Mechanism," p. 10 [author]

In the last sentence of this section, just above section 1.3.1, "Internet Service Provider" should be "Internet service provider" (note the change in case for two of the words).

Section 1.3.1, "Goals of Security," p. 10 [author]

In the third line of the third paragraph, "underway" should be "under way".

Section 1.3.1, "Goals of Security," p. 11 [author]

In the second line of the first full paragraph on this page, "underway" should be "under way".

Section 1.5.3, "Implementation," p. 14 [author]

The fifth word in this section, "implementation", should be italicized.

Section 1.6.3, "Laws and Customs," p. 18 [author]

In the first example, the word "manufacturer" in the second to last line should be "manufacturer's".

Section 1.6.3, "Laws and Customs," p. 19 [author]

In the fourth line of the first paragraph after the second full example on this page, "social security" should be "Social Security" (note the capitalization).

Section 1.12, "Exercises," p. 25 [author]

In exercise 2a, "password changing" should be "password-changing".

Chapter 2, "Access Control Matrix"

Section 2.1, "Protection State," p. 31 [author]

In the third line of the second paragraph, "P–Q^1," should be "P–Q,[1]" (the comma and the footnote reference should be transposed).

Section 2.3, "Protection State Transitions," p. 39 [Vinay Vittal]

In the third line (postconditions) of item 5, "$O' = O - \{ o \}$" should be "$O' = O - \{ s \}$".

Section 2.3.1, "Conditional Commands," p. 41 [author]

The next to last paragraph

if *r* **not in** ***A*[*p, f*]**

should be

if *r* **not in** *a*[*p, f*].

Note the trailing period, as well as the changes in bold, italics, and the lower-case "*a*".

Section 2.3.1, "Conditional Commands," p. 41 [Vinay Vittal]

The two commands in the middle of the page should be "*grant•read•file•1*" and "*grant•read•file•2*", not "*grant•write•file•1*" and "*grant•write•file•2*", respectively. Further, the line

grant•write•file•1(*p, f, q*); *grant•write•file•2*(*p, f, q*)

should be

grant•read•file•1(*p, f, q*); *grant•read•file•2*(*p, f, q*)

Chapter 6, "Integrity Policies"

Section 6.4.1, "The Model," p. 163 [author]

In the second line of the paragraph between Certification rule 4 and Certification rule 5, "Automated Teller Machine" should be "automated teller machine" (no capitalization).

Chapter 7, “Hybrid Policies”

Section 7.4, “Role-Based Access Control,” p. 183 [Rafae Bhatti]

In the third line from the bottom of the first paragraph of the first example on the page, “containing” should be “contained in”.

Chapter 9, “Basic Cryptography”

Section 9.2, “Classical Cryptosystems,” p. 218 [Mark Morrissey]

On the last line of the page, “for all $E_k \in C$” should be “for all $E_k \in E$”.

Section 9.8, “Exercises,” p. 242 [author]

In exercise 8, delete the comma “,” after the word “key” in the second line of the exercise.

Chapter 10, “Key Management”

Section 10.2.2, “Kerberos,” p. 248 [author]

In the third line of the first paragraph, add a comma “,” after “First”.

Section 10.2.3, “Public Key Cryptographic Key Exchange and Authentication,” p. 252 [author]

In the second line of the first paragraph following item 6, the word “attack” should be “*attack*” (that is, italicized).

Chapter 11, “Cipher Techniques”

Section 11.3, “Networrks and Cryptography,” p. 286 [author]

Change “*curley*” to “*curly*” on the second and fifth lines from the top.

Chapter 12, “Authentication”

Section 12.2.2.5, “Guessing Through Authentication Functions,” p. 322 [author]

In the third line of the last paragraph of this section, “Containment” should be “Contanment Phase” to match the name of the section referred to.

Section 12.6, “Multiple Methods,” p. 332 [author]

In the first paragraph of the second example, change ““pluggable authentication modules” (PAM)” to “*pluggable authentication modules* (PAM)”. Note the quotation marks are to be removed.

Section 12.10, “Exercises,” p. 335 [author]

In the second line of exercise 3, “where” should be “in which”.

Chapter 13, “Design Principles”

Section 13.1, “Overview,” p. 343 [author]

At the end of the second line of the example, “source” should be “source’s”.

Chapter 14, “Representing Identity”

Section 14.6.3.1, “Anonymity for Better or Worse,” p. 377 [author]

At the end of the first paragraph on the page (the one that continues from the previous page), the comma “,” should be a period “.”.

Section 14.9, “Further Reading,” p. 378 [author]

In the second line of the last paragraph on the page, “best known” should be “best-known”.

Section 14.9, “Further Reading,” p. 379 [author]

In the first line on the page, “In” should be “in”.

Chapter 21, “Evaluating Systems”

There should be a period “.” after the page numbers in the cite to Shakespeare.

Chapter 22, “Malicious Logic”

There should be a period “.” after the page numbers in the cite to Shakespeare.

Section 22.7.5.1, “Proof-Carrying Code,” p. 639 [author]

Delete “; see Section 17.2.2” in the parentheses at the end of the first paragraph of this page.

Section 22.11, “Exercises” p. 642 [author]

In exercises 4 and 5, delete the colon “:” in the sentence fragment “How would a virus spread if:” just before the two parts in each question.

Chapter 23, “Vulnerability Analysis”

Section 23.1, “Introduction,” p. 646 [author]

In the first line of the first full paragraph, “property-based testing” should be “penetration testing”.

Chapter 24, “Auditing”

Section 24.2.1, “Logger,” p. 692 [author]

In the paragraph following the output, “the Administrator successfully executing” should be “the Administrator’s successfully executing”.

Chapter 25, “Intrusion Detection”

Section 25.2, “Basic Intrusion Detection,” p. 726 [author]
Add a comma “,” after the word “Often” in the second line of item 2.

Chapter 27, “System Security”

Section 27.6.2, “The Development System,” p. 830 [author]
Replace “*A Posteriori*” with “A Posteriori” in footnote 63.

Chapter 28, “User Security”

Section 28.5.3, “Sending Unexpected Content,” p. 866 [author]
Transpose the period “.” and the reference “[47]” at the end of the example in this section.

Chapter 32, “Entropy and Uncertainty”

Section 32.3.2, “Conditional Entropy,” p. 939 [author]
On this page, every occurrence of “$p(X = x_i / Y = y_j)$” should be replaced by “$p(X = x_i \mid Y = y_j)$”. The “|” should not be italicized. This occurs in every equation on the page.

Chapter 36, “Bibliography”

Reference 19, p. 994 [author]
Add a comma “,” after MM88-37 at the end of the second line.

Reference 347, p. 1015 [author]
Add a comma “,” after “Thompson” on the first line.

Reference 377, p. 1017 [author]
Capitalize the “a” in “a Decision” at the end of the first line.

Reference 431, p. 1020 [author]
Delete the comma “,” after “MA” on the last line.

Reference 450, p. 1022 [author]
The title of the paper is “Protection in Operating Systems”. The “operating systems” there now should be capitalized, as indicated.

References 610–617, p. 1032 [Rafael Obelheiro]
These references are out of (alphabetical) order. Reference 612 should be numbered 610. Reference 613 should be numbered 611. Reference 614 should be numbered 612. Reference 615 should be numbered 613. Reference 611 should be numbered 614. Reference 616 should be numbered

615. Reference 617 should be numbered 616. Reference 610 should be numbered 617. The references should be reordered accordingly, and the reference numbers in the text fixed up.

Reference 656, p. 1035 [author]
Delete the comma "," after "176" on the last line.

Reference 966, p. 1055 [author]
Change "Addison-Wesley Publishing Co.," to "Addison-Wesley,".