Errata to the Second Printing (December 2004)

Preface

"Acknowledgements," p. xxxi

Please change the paragraph at the bottom of p. xxxi (and continuing onto the next page) 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, David Bover, Logan Browne, Terry Brugger, Ralph Bunker, Serdar Cabuk, Raymond Centeno, Yang Chen, Lisa Clark, Michael Clifford, Christopher Clifton, Dan Coming, Kay Connelly, Crispin Cowan, Tom Daniels, Dimitri DeFigueiredo, Joseph-Patrick Dib, Till Dörges, Jeremy Frank, Robert Fourney, Guillermo Francia III, Martin Gagne, Ron Gove, James Hinde, James Hook, Xuxian Jiang, Jesper Johansson, Mark Jones, Calvin Ko, Mark-Neil Ledesma, Ken Levine, Karl Levitt, Yunhua Lu, Gary McGraw, Alexander Meau, Nasir Memon, Katherine Moore, Mark Morrissey, Ather Nawaz, Iulian Neamtiu, Kimberly Nico, Stephen Northcutt, Rafael Obelheiro, Josko Orsulic, Holly Pang, Sean Peisert, Ryan Poling, Sung Park, Ashwini Raina, Jorge Ramos, Brennen Reynolds, Peter Rozental, Christoph Schuba, David Shambroom, Jonathan Shapiro, Clay Shields, Sriram Srinivasan, Andreas Tödter, Mahesh V. Tripunitara, Vinay Vittal, Tom Walcott, James Walden, Dan Watson, Guido Wedig, Chris Wee, Patrick Wheeler, Paul Williams, Bonnie Xu, Charles Yang, Xiaoduan Ye, Lara Whelan, John Zachary, Linfeng Zhang, Aleksandr Zingorenko, and to everyone in my computer security classes, who (knowingly or unknowingly) helped me develop and test this material.

Chapter 4, "Security Policies"

Section 4.1, "Security Policies," p. 46 [Ralph Bunker]

At the beginning of the line just above Definition 4–6, 'Part 6, "Assurance"' should be 'Chapter 17, "Introduction to Assurance"'.

Chapter 5, "Confidentiality Policies"

Section 5.2.1, "Informal Description," p. 63 [Ralph Bunker]

At the beginning of the next-to-last line on the page, "Each security level" should be "Each security classification".

Section 5.2.2.1, "Assigning MAC Labels," p. 67 [Ralph Bunker]

In the fourth line of the paragraph just before the example, "hidden directory under */tmp* with MAC label *MAC_A*" should be "hidden directory under */tmp* with MAC label *MAC_B*".

Chapter 6, "Integrity Policies"

Section 6.2, "Biba Integrity Model," p. 76 [David Bover]

Add the following footnote at the end of the example at the top of the page:

"This is the opposite of the execute rule of the Strict Integrity Policy."

Section 6.3.1, "The Model," p. 78 [Ralph Bunker]

Delete the "*A*" at the end of the second sentence, and change "these relations" to "this relation" in the third.

Section 6.3.1, "The Model," p. 79 [Ralph Bunker]

The paragraph after CR5 should go immediately after ER4, and the paragraph after ER4 should go immediately after CR5.

Section 6.3.3, "Comparison with Other Models," p. 80 [Ralph Bunker]

The last sentence of the last full paragraph on the page should be:

"As with the Bell-LaPadula Model, trusted entities must change the objects' integrity levels, and the method of upgrading need not be certified."

Chapter 8, "Basic Cryptography"

Section 8.3.1, "RSA" p. 115 [Linfeng Zhang]

The last two examples on this page assume that Alice and Bob use the same modulus $n = 77$. This is unrealistic. The following two versions of the example have Alice and Bob using different moduli.

Replace the second example on the page with:

EXAMPLE: Suppose Alice wishes to send Bob the message "HELLO WORLD" in confidence and authenticated. Again, assume that Alice's private key is 53. Bob uses $n = 65$ and takes his public key to be 37 (making his private key 13). The plaintext is represented as 07 04 11 11 14 26 22 14 17 11 03. The encipherment is

$(07^{53} \bmod 77)^{37} \bmod 65 = 35$

$(04^{53} \bmod 77)^{37} \bmod 65 = 09$

$(11^{53} \bmod 77)^{37} \bmod 65 = 44$

...

$(03^{53} \bmod 77)^{37} \bmod 65 = 47$

or 35 09 44 44 49 31 22 49 40 44 05.

Replace the third example on the page with:

EXAMPLE: Bob receives the ciphertext above, 35 09 44 44 49 31 22 49 40 44 05. The decipherment is

$(35^{13} \bmod 65)^{17} \bmod 77 = 07$

$(09^{13} \bmod 65)^{17} \bmod 77 = 04$

$(44^{13} \bmod 65)^{17} \bmod 77 = 11$

...

$(05^{13} \bmod 65)^{17} \bmod 77 = 03$

or 07 04 11 11 14 26 22 14 17 11 03. This corresponds to the meessage “HELLO WORLD” from the preceding example.

Section 8.3.1, “RSA” p. 115 [author]

The side bars by the first two examples are too long. Each should stop before the last paragraph of the example; that is, the last paragraph of each of the first two examples are actually text and not part of the examples.

Section 8.8, “Exercises” p. 121 [Katherine Moore]

In exercise 11, “Fermat’s Little Theorem” should be “Euler’s generalization to Fermat’s Theorem”.

Chapter 9, “Key Management”

Section 9.2.1, “Classic Cryptographic Key Exchange and Authentication” p. 125 [Ralph Bunker]

The sentence “If Eve records the second message” in the first full paragraph under the protocol (that begins “This particular protocol”) should read “If Eve records the third message”.

Section 9.2.3, “Public Key Cryptographic Key Exchange and Authentication” p. 130 [Guillermo Francia III]

The sentence “Alice uses her public key to obtain the session key” in the first paragraph under the first item “1” on the page should read “Bob uses her public key to obtain the session key.”

Section 9.3, “Cryptographic Key Infrastructures” p. 130 [Ralph Bunker]

The last paragraph of this section, just before section 9.3.1, should read:

“One immediate problem is that Bob must know Cathy’s public key to validate the certificate. A common solution is to structure certificates into certificate chains.”

Section 9.3.1.2, “PGP Certificate Signature Chains” p. 134 [Ralph Bunker]

Near the bottom of the page, on the first line of item 7, “field 2” should be “field 3”.

Chapter 10, “Cipher Techniques”

Section 10.4, “Example Protocols,” p. 156 [author]

The first paragraph needs to be changed in several places. In its entirety, that paragraph should read:

> Several widely used Internet protocols illustrate different facets of cryptographic techniques. This section examines two such protocols, each at a different layer. PEM is a privacy-enhanced electronic mail protocol at the applications layer and demonstrates the considerations needed when designing such a protocol. Its techniques are similar to those of PGP, another widely used security-enhanced electronic mail protocol. IPsec provides security mechanisms at the network, or IP, layer.

Section 10.4.3, "Conclusion," p. 167 [author]

In the first line of the first paragraph of this section, "three" should be "two".

Section 10.4.3, "Conclusion," p. 168 [author]

In the first line of the first paragraph of this section, "SSL" should be "SSL [340]".

Chapter 13, "Representing Identity"

Section 13.5, "Naming and Certificates," p. 217 [Ralph Bunker]

In the fourth line from the top of the page, "issuance policy" should be "authentication policy".

Chapter 14, "Access Control Mechanisms"

Section 14.1.1, "Abbreviations of Access Control Lists," p. 239 [Ralph Bunker]

In the third line from the bottom of the first full paragraph after the example, "one must create groups of all users *except* Fran" should be "one must create a group of all users *except* Fran".

Section 14.1.2, "Control and Maintenance of Access Control Lists," p. 241 [Ralph Bunker]

In the first line of the first paragraph after the list, "isues" should be "issues".

Section 14.1.2.4, "Conflicts," p. 243 [Ralph Bunker]

In the last line of the second example, "second approach" should be "third approach".

Section 14.5, "Propagated Access Control Lists," p. 257 [Ralph Bunker]

In thesecond line below the first example, "subject o'" should be "object o'"..

Chapter 15, "Information Flow"

Section 15.2.1, "Declarations," p. 266 [James Hook]

The last two sentences of the paragraph at the top of the page (beginning with "Information flows into $a[i]$" and continuing to the end of the paragraph) are wrong. They should read as follows:

> Information flows into $a[i]$ affect only the value in $a[i]$, but may cause information about i to flow into $a[i]$ (as, for example, when all elements of a are 0, and $a[i]$ is assigned 1). Thus, for information flows into and from $a[i]$, the class involved is $lub\{ \underline{a[i]}, \underline{i} \}$.

Section 15.3.1, "Fenton's Data Mark Machine," p. 280 [Yang Chen]

In the fourth and fifth lines of the example at the top of the page, the "$\underline{x}$" in the fifth column should be "$\underline{z}$". In the following paragraph, third sentence, "fifth step" should be "fourth step". The last sentence of that paragraph should read: "If $z = 0$, then the *else* branch of statement 1 must have been taken, meaning that $x = 1$ initially."

Chapter 16, "Confinement Problem"

Section 16.3.1, "Detection of Covert Channels," p. 297 [James Hook]

In the example, delete the second line of the comment before *Lockfile*, and the return type. *Lockfile* is a procedure, not a function. It should look like this:

```
(* lock the file if it is not locked and not opened *)
procedure Lockfile(f: file);
begin
  if not f.locked and empty(f.inuse) then
     f.locked := true;
end;
```

Section 16.3.1, "Detection of Covert Channels," p. 298 [Andreas Tödter]

In the table, the entry for row "modify" and column "Unlockfile" should be "locked". The function "Unlockfile" modifies the file attribute "locked" (by setting it to "false").

Section 16.3.1, "Detection of Covert Channels," p. 298 [Ralph Bunker]

The paragraph beginning "The first step in constructing" should not be part of the first example. The example bar to the left should stop before that paragraph.

Section 16.3.1, "Detection of Covert Channels," p. 303 [Ralph Bunker]

Change "The shared resource matrix model and covert flow trees" to "Covert flow trees".

Chapter 19, "Malicious Logic"

Section 19.6.2.3, "Sandboxing," p. 381 [Ralph Bunker]

Change "rebounded" to "rebound" in the third line of the first example.

Section 19.6.3, "Malicious Logic Crossing Protection Domain Boundaries by Sharing," p. 381 [author]

In the first line of the example, "see Section 22.7.1" should be "see Section 19.6.1".

Chapter 20, "Vulnerability Analysis"

Section 20.1, "Introduction," p. 390 [author]

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

Section 20.2.8, "Example: Penetrating a UNIX System," p. 400 [author]

At the bottom of the page, the caption of Figure 20–3 should read "The output of the UNIX port scan. These are the ports that provide network services." The words "network services." are omitted.

Chapter 23, "Network Security"

Section 23.3.2, "Analysis of the Network Infrastructure," p. 497 [Ralph Bunker]
In footnote 23, "Definition 15–1" should be "Definition 16–1".

Section 23.3.4, "In the Internal Network," p. 505 [Ralph Bunker]
In the last line on the page, change "mechanism" to "privilege".

Chapter 24, "System Security"

Section 24.3.2, "The Development System," p. 527 [Ralph Bunker]
In the first line of the example, put "is" between "[912]" and "host-based".

"Bibliography"

Reference 25, p. 650 [Sean Peisert]
The year of this reference is 1972, not 1974.

Reference 659, p. 691 [Ralph Bunker]
This reference appears in volume 7 number 2, dated April 1988.