Errata to the the First Printing (December 2, 2002)

"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 Jim Alves-Foss, Bill Arbaugh, Andrew Arcilla, Rebecca Bace, Belinda Bashore, Logan Browne, Terry Brugger, Michael Clifford, Christopher Clifton, Crispin Cowan, Dimitri DeFigueiredo, Jeremy Frank, Robert Fourney, Ron Gove, Jesper Johansson, Mark Jones, Calvin Ko, Karl Levitt, Gary McGraw, Alexander Meau, Nasir Memon, Mark Morrissey, Ather Nawaz, Stephen Northcutt, Holly Pang, Sung Park, Ashwini Raina, Brennen Reynolds,Peter Rozental, Christoph Schuba, Jonathan Shapiro, Clay Shields, Tom Walcott, Dan Watson, Chris Wee, Paul Williams, Bonnie Xu, Xiaoduan Ye, Lara Whelan, 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 1.4, "Assumptions and Trust," p. 12 [Mark Morrissey]

In the second line of the paragraph following Definition 1-3, the statement "$R = A$" should be "$R = Q$".

Chapter 2, "Access Control Matrix"

Section 2.2.2, "Access Control by History," p. 37 [Christopher Clifton]

In the last line of the second paragraph on the page, the subscript for O_{i+1} is wrong. It should be O_{i-1}.

Section 2.8, "Exercises," problem 1, p. 44 [Peter Rosental]

The first paragraph of this problem should read as follows, for clarity:

Consider a computer system with three users: Alice, Bob, and Cyndy. Alice owns the file *alicerc*, and Bob and Cyndy can read it. Cyndy can read and write the file *bobrc*, wich Bob owns, but Alice can only read it. Only Cyndy can read and write the file *cyndyrc*, which she owns. Assume that the owner of each of these files can execute it.

Chapter 3, "Foundational Results"

Section 3.2, "Basic Results," p. 50 [author]

In the second line of the first full paragraph of the page, "q_f;," should be replaced by "q_f,".

Section 3.4.1.2, "Filter Function," p. 68 [Xiaoduam Ye]

Condition 3 should read: $\tau(\mathbf{X})/r{:}c \in f_i(\tau(\mathbf{Y}), \tau(\mathbf{Z}))$

Section 3.4.1.4, "Demand and Create Operations," p. 70 [Ather Nawaz]

In line 4 of the last full paragraph on the page, "**A**/*r*:*c* if **A**/*r*:*c* $\in cr_P(a, b)$" should be "**B**/*r*:*c* if **B**/*r*:*c* $\in cr_P(a, b)$".

Section 3.5.2, "Extending SPM," p. 80 [Ather Nawaz]

In the example, the line "$cc_{\text{proxy}}(a, a, p)$ = Anna/*x* ∪ Bill/*x*" should be "$cr_{\text{proxy}}(a, a, p)$ = Anna/*x* ∪ Bill/*x*". Also, the middle two creation rules in the last indented set of four rules should be:

$cr_{\mathbf{P}2}(\tau(\mathbf{P}_1), \tau(\mathbf{P}_2)\ \tau(\mathbf{P}_3)) = \mathbf{C}/R_{1,2} \cup \mathbf{P}_2/R_{2,2}$

$cr_{\mathbf{P}3}(\tau(\mathbf{P}_1), \tau(\mathbf{P}_2)\ \tau(\mathbf{P}_3)) = \mathbf{C}/R_{1,3} \cup \mathbf{P}_3/R_{2,3}$

Section 3.5.2, "Extending SPM," p. 81 [Ather Nawaz]

In the block of creation rules in the middle of the page, the third through fifth of the rules in the left column should be:

$cr_{Psecond}(p_2, a_1, a_2) = \varnothing$

$cr_{Pfirst}(p_3, a_2, a_3) = \varnothing$

$cr_{Psecond}(p_3, a_2, a_3) = \varnothing$

Chapter 5, "Confidentiality Policies"

Section 5.2.2.2, "Using MAC Labels," p. 131 [Xiaoduan Ye]

In the last line of the example, replace "(TS, { COMP, NUC }) *dom* (S, { ASIA })" with "*not* (TS, { COMP, NUC }) *dom* (S, { ASIA })".

Section 5.2.3, "Formal Model," p. 132 [author]

In the second line of this section, "q" should be "a".

Chapter 9, "Basic Cryptography"

Section 9.2.3, "Data Encryption Standard," p. 230 [Bob Fourney]

In Figure 9-7, the box at the end of the arrow going out of the E ovalshould contain "R_{i-1} (48 bits)".

Chapter 10, "Key Management"

Section 10.2.1, "Classical Cryptographic Key Exchange and Authentication," p. 247 [Mark Jones]

The second step of the first protocol in this section should read:

2. Cathy → Alice: $\{ k_{session} \}k_{Alice} \| \{ \{ k_{session} \}k_{Bob}$

The "||" were omitted. Similarly, the second step of the Needham-Schroeder protocol (the last line on the page) should read:

2. Cathy → Alice: { Alice || Bob || $rand_1$ || $k_{session}$ || { Alice || $k_{session}$ }k_{Bob} }k_{Alice}

The first $k_{session}$ is followed by a "," rather than a "||".

Section 10.2.1, "Classical Cryptographic Key Exchange and Authentication," p. 249 [Mark Jones]

The Otway-Rees protocol (in the middle of the page) has several typos in which "||"s, ","s, and juxtaposition are used interchangeably. The protocol should look like this:

1. Alice → Bob: *num* || Alice || Bob || { $rand_1$ || *num* || Alice || Bob }k_{Alice}
2. Bob → Cathy: *num* || Alice || Bob || { $rand_1$ || *num* || Alice || Bob }k_{Alice} ||
   { $rand_2$ || *num* || Alice || Bob }k_{Bob}
3. Cathy → Bob: *num* || { $rand_1$ || $k_{session}$ }k_{Alice} || { $rand_2$ || $k_{session}$ }k_{Bob}
4. Bob → Alice: *num* || { $rand_1$ || $k_{session}$ }k_{Alice}

Chapter 11, "Cipher Techniques"

Section 11.2.1.1, "Synchronous Stream Ciphers," p. 278 [Bob Fourney]

The second sentence of Definition 11-3 should begin: "To obtain a key bit, r_{n-1} is used" rather than r_0 being used (as is there now).

Section 11.2.1.1, "Synchronous Stream Ciphers," p. 279 [Bob Fourney]

The second sentence of Definition 11-4 should begin: "To obtain a key bit, r_{n-1} is used" rather than r_0 being used (as is there now)

Section 11.4.2.3, "Upper Layer: SSL Handshake Protocol," p. 296 [Mark Jones]

The fifth step of the handshake protocol (in the middle of the page) should read:

5. *S* → *C*: { *cert_type* || *good_cert_authorities* }

Chapter 17, "Confinement Problem"

Section 17.2.2, "Sandboxes," p. 445 [Paul Williams]

The Janus configuration file example has a typographical error in one of the comments. In the third comment (before the first line that begins with "path"), the comment should say:

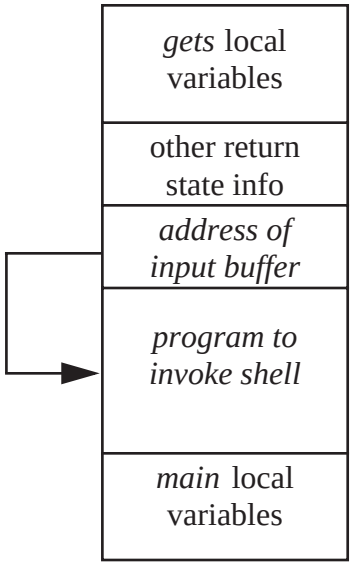
```
# deny access to everything except files under /usr
```

and not "allow".

Chapter 23, “Vulnerability Analysis”

Section 23.3.1, “Two Security Flaws,” p. 663 [Bonnie Xu]

Figure 23-7(b) should be as shown here. Note the arrow is moved to point into the square labeled “program to invoke shell”.



Chapter 24, “Auditing”

Section 24.3, “Designing an Audit System,” p. 699 [Bob Fourney]

In the next-to-last line on this page, the parenthetical expression should be changed to read “similar to a pseudonymous remailer; see Definition 14–5” rather than what is there now, namely “similar to a Cypherpunk remailer; see Definition 14–6”.

Chapter 29, “Program Security”

Section 29.5.6.1, “Bounds Checking,” p. 903 [author]

The last line in the last paragraph of this section should have a closing parenthesis (")") after the "57" footnote indicator.

Chapter 36, “Bibliography”

Reference 907, p. 1051 [author]

This reference should read:

[907] A. Shamir, “How to Share a Secret,” *Communication of the ACM* **22** (11), pp. 612–613 (Nov.1979).

Reference 936, p. 1053 [author]

[936] K. Smith and M. Winslett, “Entity Modelling in the MLS Relational Model,” *Proceedings of the 18th International Conference on Very Large Data Bases*, pp. 199–210 (Aug. 1992).