Errata to the Seventh Printing (February 2005)

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, David Bover, Logan Browne, Terry Brugger, Gordon Burns, Serdar Cabuk, Raymond Centeno, Yang Chen, HakSoo Choi, Lisa Clark, Michael Clifford, Christopher Clifton, Dan Coming, Kay Connelly, Crispin Cowan, Shayne Czyzewski, Tom Daniels, Dimitri DeFigueiredo, Joseph-Patrick Dib, Till Dörges, Felix Fan, Robert Fourney, Guillermo Francia III, Jeremy Frank, Conny Francke, Martin Gagne, Nina Gholami, Ron Gove, James Hinde, James Hook, Xuxian Jiang, Jesper Johansson, Mark Jones, Calvin Ko, Mark-Neil Ledesma, Ken Levine, Karl Levitt, Luc Longpre, Yunhua Lu, Gary McGraw, Alexander Meau, Nasir Memon, Katherine Moore, Mark Morrissey, Ather Nawaz, Iulian Neamtiu, Dan Nerenburg, 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, night SH, David Shambroom, Jonathan Shapiro, Clay Shields, Sriram Srinivasan, Mahesh V. Tripunitara, Vinay Vittal, Tom Walcott, James Walden, Dan Watson, Guido Wedig, Chris Wee, Han Weili, Patrick Wheeler, Paul Williams, Bonnie Xu, Charles Yang, Xiaoduan Ye, Xiaohui 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 2, "Access Control Matrix"

Section 2.2.2, "Access Controlled by History," p. 36 [night SH]

Add to the line just above the example "The control also restricts the number of questions that can be answered."

Section 2.2.2, "Access Controlled by History," p. 37 [Han Weili]

In the fourth line of the second paragraph on this page, "$|X| > 1$" should read "$|X| < 2$".

Section 2.2.2, "Access Controlled by History," p. 37 [Charles Yang]

The last line of the last paragraph of the example should begin with "A[**asker**, { **Celia**, **Leonard** }] = ∅" and not "A[**asker**, { **Celia**, **Leonard** }] ∅". The equal sign is missing in the current text.

Section 2.3, "Protection State Transitions," p. 39 [Vladimir Berman]

The second postcondition for the primitive command **destroy subject** s reads "$O' = O - \{ o \}$". It should read "$O' = O - \{ s \}$".

Chapter 3, "Foundational Results"

Section 3.2, "Basic Results," p. 51 [Shayne Czyzewski]

In the command $c_{p,A}(s_i, s_{i+1})$, the conditional "`own in a[s_i, s_i]`" should be "`own in a[s_i, s_i+1]`".

Section 3.2, "Basic Results," p. 51 [Lisa Clark]

In the command $crightmost_{p,A}(s_i, s_{i+1})$, the conditional "`end in a[s_i, s_i+1]`" should be "`end in a[s_i, s_i]`".

Section 3.3.2, "Interpretation of the Model," p. 58 [Dan Nerenburg]

In the statement of Theorem 3-11, the phrase "*G* is a finite directed acyclic graph" should be "*G* is a finite directed graph". The word "acyclic" should be dropped.

Section 3.4.1.5, "Safety Analysis," p. 75 [Xiaohui Ye]

In Definition 3-11, the third item should be:

3. $\sigma(\mathbf{X}) = \tau(\mathbf{X})$-surrogate of $\sigma(\mathbf{Y})$ if $\mathbf{Y}$ creates $\mathbf{X}$ and $\tau(\mathbf{Y}) \neq \tau(\mathbf{X})$

Section 3.5.2, "Extending SPM," p. 80 [Nina Gholami]

The *can-create* relation after the example should be:

$$cc(\tau(\mathbf{P}_1), \tau(\mathbf{P}_2), \tau(\mathbf{P}_3), \tau(\mathbf{C})) = Z \subseteq T$$

and the list of creation rules following the example should be:

$$cr_{\mathbf{P}1}(\tau(\mathbf{P}_1),\tau(\mathbf{P}_2), \tau(\mathbf{P}_3), \tau(\mathbf{C})) = \mathbf{C}/R_{1,1} \cup \mathbf{P}_1/R_{2,1}$$
$$cr_{\mathbf{P}2}(\tau(\mathbf{P}_1),\tau(\mathbf{P}_2), \tau(\mathbf{P}_3), \tau(\mathbf{C})) = \mathbf{C}/R_{1,2} \cup \mathbf{P}_1/R_{2,2}$$
$$cr_{\mathbf{P}3}(\tau(\mathbf{P}_1),\tau(\mathbf{P}_2), \tau(\mathbf{P}_3), \tau(\mathbf{C})) = \mathbf{C}/R_{1,3} \cup \mathbf{P}_1/R_{2,3}$$
$$cr_{\mathbf{C}}(\tau(\mathbf{P}_1),\tau(\mathbf{P}_2), \tau(\mathbf{P}_3), \tau(\mathbf{C})) = \mathbf{C}/R_3 \cup \mathbf{P}_1/R_{4,1} \cup \mathbf{P}_2/R_{4,2} \cup \mathbf{P}_3/R_{4,3}$$

In all cases, the "$\tau(\mathbf{C})$" was omitted.

Section 3.5.2, "Extending SPM," p. 82 [Conny Francke]

In the bulleted list of tickets that the entities have after the creations, the last item should be:

- **C** has $\mathbf{C}/R_3 t$.

Chapter 4, "Security Policies"

Section 4.5.1, "High-Level Policy Languages," p. 109 [Felix Fan]

In the code for domain *d_daemon* in the example,

```
(rxd->t_readable),
(rd->t_generic, t_dte, t_sysbin),
```

should be

```
(rxd->t_sysbin),
(rd->t_generic, t_dte, t_readable),
```

The *t_sysbin* and *t_readable* are reversed.

Section 4.7, "Security and Precision," p. 118 [Nina Gholami]

In the first sentence following Definition 4–21, "either m_1 and m_2" should be "either m_1 or m_2".

Section 4.7, "Security and Precision," p. 119 [night SH]

Replace the top two paragraphs on the page, which are the last two paragraphs of the proof of Theorem 4–3, with the following:

> If, for all inputs x, $T(x) = 0$, then $m(x) = 1$ (because m is secure). If there is an input x' for which $T(x') \neq 0$, then $m(x') = 2$ (again, because m is secure) or is undefined (if p halts before the assignment). But from the definition of T, $T(0) = 0$, so $m(0) = 1$. As m is a constant function, it must be 1 everywhere. Thus, $m(0) = 1$ if and only if $T(x) = 0$ for all x.
>
> If we can effectively determine m, we can effectively determine whether $T(x) = 0$ for all x. This is equivalent to solving the halting problem, which is impossible.

Chapter 5, "Confidentiality Policies"

Section 5.2.2.1, "Assigning MAC Labels," p. 129 [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*".

Section 5.2.3.1, "Basic Security Theorem," p. 135 [Vladimir Berman]

In the first line of the proof of Theorem 5–3, "$z_t = (b_t, a_t, f_t)$" should be "$z_t = (b_t, m_t, f_t, h_t)$". Further down, the Induction Hypothesis line should be:

$$\textit{Induction hypothesis}.\ z_{i-1} = (b_{i-1}, m_{i-1}, f_{i-1}, h_{i-1}) \text{ is secure, for } i < t.$$

Section 5.2.3.2, "Rules of Transformation," p. 138 [Nina Gholami]

In the third line of the proof of Theorem 5–10, "$(s', o', p') \notin b'$" should be "$(s', o', p') \in b'$".

Chapter 6, "Integrity Policies"

Section 6.2.3, "Biba's Model (Strict Integrity Policy)," p. 155 [David Bover]

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

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

Section 6.4.1, "The Model," p. 162 [Ralph Bunker]

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

Chapter 7, "Hybrid Policies"

Section 7.1.1, "Informal Description," p. 171 [Till Dörges]

In item 2 of the *CW-Simple Security Condition, Preliminary Version*, the first "O'" should be "O".

Section 7.1.2, "Formal Model," p. 174 [night SH]

In the second condition of Axiom 7–6, "$l_2(o') \neq l_2(o)$, $l_2(v(o'))$, and $l_2(o') \neq l_2(v(o'))$" should be replaced by "$l_2(o') \neq l_2(o)$, and $v(o') \neq o'$".

Section 7.1.2, "Formal Model," p. 174 [night SH]

Definition 7–4 is poorly named. Change it, and the paragraph before and after, as follows:

> The next definition describes the ability of a subject to read from pairs of objects. This will be useful in determining how information can flow throughout the system.
>
> **Definition 7–4.** A subject may read a pair of objects o, o' in O if there exists a subject s in S such that $H(s, o) = true$ and $H(s, o') = true$.
>
> If information can flow directly from one object o to an object o', written (o, o'), then some subject s must be able to read o and write o'. From the definition of H, $H(s, o) = true$ for this s. As s must be able to write to o', $H(s, o') = true$ by part 1 of Axiom 7–6. Hence s can read the pair of objects o, o'.

Section 7.1.2, "Formal Model," p. 175 [author]

In the statement and proof of Theorem 7–3, "$l_2(o) = l_2(v(o))$" should be replaced by "$v(o) \neq o$". Also, the paragraph after the definition of F should read:

> is the set of all pairs of objects that any subject can read, by Definition 7–4. Let F^* be its transitive closure, which includes all possible information flows (allowed or not).

Chapter 8, "Nonnterference and Policy Composition"

Section 8.2.1, "Unwinding Theorem" p. 196 [author]

Lemma 8–2, and its proof, should be deleted.

Section 8.9, "Exercises" p. 212 [author]

Exercise 2 should be deleted.

Chapter 9, "Basic Cryptography"

Section 9.3.2, "RSA" p. 236 [Linfeng Zhang]

The 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 first 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 second 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 9.8, "Exercises" p. 242 [HakSoo Choi]

In exercise 10, "25" should be "26".

Section 9.8, "Exercises" p. 242 [Katherine Moore]

In exercise 12, "Fermat's Little Theorem" should be "Euler's generalization to Fermat's Theorem".

Chapter 10, "Key Management"

Section 10.2.3, "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 10.4.2.2, "PGP Certificate Signature Chains" p. 259 [Ralph Bunker]

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

Chapter 10, "Key Management"

Section 10.2.3, "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."

Chapter 15, "Access Control Mechanisms"

Section 15.1.1, "Abbreviations of Access Control Lists," p. 383 [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 15.1.2, "Control and Maintenance of Access Control Lists," p. 385 [Ralph Bunker]

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

Section 15.1.2.4, "Conflicts," p. 387 [Ralph Bunker]

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

Chapter 16, "Information Flow"

Section 16.3.2.4, "Iterative Statements," p. 421 [author]

In the last line of the last paragraph of the example in this section, "$lub\{ \underline{i}, \underline{n} \} \leq glb\{ \underline{a}[\underline{i}], \underline{i} \}$" should be "$lub\{ \underline{b}[\underline{i}], \underline{i}, \underline{n} \} \leq glb\{ \underline{a}[\underline{i}], \underline{i} \}$". In the third line of that paragraph, "$lub\{ \underline{b}[\underline{i}], \underline{i}, \underline{n} \} \leq glb\{ \underline{a}[\underline{i}], \underline{i} \}$" should be "$lub\{ \underline{i}, \underline{n} \} \leq glb\{ \underline{a}[\underline{i}], \underline{i} \}$". Note this error was corrected in the errata sheet for the third and fourth printings, but the correction was unclear.

Section 16.4.1, "Fenton's Data Mark Machine," p. 432 [Yang Chen]

In the paragraph after the example at the top of the page, the last sentence should read: "If $z = 0$, then the *else* branch of statement 1 must have been taken, meaning that $x = 1$ initially."

Section 16.9, "Exercises," p. 437 [Conny Francke]

The second sentence of exercise 2 should read: "Prove that the structure $IL = (S_{IL}, \leq_{IL})$ is a lattice, where:".

Chapter 22, "Malicious Logic"

Section 22.7.2.3, "Sandboxing," p. 636 [Ralph Bunker]

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

Chapter 26, "Network Security"

Section 26.3.4, "In the Internal Network," p. 791 [Ralph Bunker]

In the last line on the page, change "mechanism" to "privilege".

Chapter 27, "System Security"

Section 27.3.2, "The Development System," p. 814 [Ralph Bunker]

In the first line of the example, put "is" between "[1012]" and "host-based".

Chapter 30, "Lattices"

Section 30.1, "Basics," p. 926 [Luc Longpre]

In Definition 30–5, change "there is no $t \in U$ for which tRu" , to "for every $t \in U$, uRt". Similarly, definition 30–7 should read "for every $m \in L$, mRl" rather than "there is no $m \in L$ for which lRm".

"Bibliography"

Reference 26, p. 994 [Sean Peisert]

The year of this reference is 1972, not 1974.

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 739, p. 691 [Ralph Bunker]

This reference appears in volume 7 number 2, dated April 1988.

"Index"

T, p. 1081 [Gordon Burns]

The item "Termite and stay resident virus, 620" should be "Terminate and stay resident virus, 620".