Errata to the Third Printing (July 2003) and the Fourth Printing (November 2003)

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, 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, 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 2, "Access Control Matrix"

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

The first two sentences of the second paragraph on this page are fine. But the rest of that paragraph, and the paragraph following it, should read as follows:

"The function *f(X)* is *read* if $|X| > 1$ and is $\varnothing$ otherwise. Thus, the *read* right corresponds to the database being able to answer the query for that particular query set. Let O_i be the union of the objects referenced in accesses 1 through i, inclusive. The elements of the matrix corresponding to this control are $A[s, C_i] = f(O_{i-1} \cap C_i)$ for query i, where $1 \leq i$ and $O_0 = \varnothing$.

When C_1 is referenced, $|O_0 \cap C_1| = 0$ and A[**asker**, {**Celia**, **Leonard**, **Matt }**] = { *read* }, so the query is answered. When C_2 is used, $|O_1 \cap C_2| = 1$ and A[**asker**, **{ Matt }**] = { *read* }, so that query is also answered. But with query C_3, $|O_2 \cap C_3| = 2$, so A[**asker**, **{ Celia, Leonard }**] = $\varnothing$, and the query is not answered."

Chapter 3, “Foundational Results”

Section 3.2, “Basic Results,” p. 51 [Serdar Cabuk]

In the middle of the last paragraph on the page, “s_k is given *own* rights over the new subject s_{k+1} and *end* rights over itself” should be “s_k is given *own* rights over the new subject s_{k+1}, s_{k+1} is given *end* rights over itself”.

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 3.2, “Basic Results,” p. 52 [Serdar Cabuk]

In the first line of the page, “**from**” should be “**into**”.

Section 3.4.1.4, “Demand and Create Operations,” p. 71 [Xuxian Jiang]

In the example, “*cr*(*subject*, *object*) = { *object*/*tc*, *object*/*gc*, *object*/*rc*, *object*/*wc* }” should be “*cr*(*subject*, *object*) = { *object*/*rc*, *object*/*wc* }”.

Section 3.5.1, “Brief Comparison of HRU and SPM,” p. 78 [Lisa Clark]

The *multicreate* command is garbled. The correct command, at the bottom of the page, should be:

```
command multicreate($s_0$, $s_1$, $o$)
     if $p$ in $a[s_0, s_1]$ and $p$ in $a[s_1, s_0]$
     then
          create object $o$;
          enter $r$ into $a[s_0, o]$;
          enter $r$ into $a[s_1, o]$;
end
```

Section 3.5.2, “Extending SPM,” p. 79 [Sriram Srinivasan]

In the last line of the page, “cr_P” should be “cr_{P_i}” (the P in the subscript should itself have a subscript i).

Section 3.5.2, “Extending SPM,” p. 80 [Xuxian Jiang]

In the first line of the page, “$\mathbf{X}_i/R_{4,1}$” should be “$\mathbf{X}_1/R_{4,1}$” (the i in the subscript of **X** should be 1). In the example, the sentence “We model the rights that Anna and Bill have over the proxy by the right x in R” should be “We model the rights that the proxy has by the right x in R”.

Section 3.5.2, “Typed Access Marix Model,” p. 88 [Lisa Clark]

In the fourth line of the statement of the **create subject** *s* **of type** *ts* primitive operation, “$\tau'(s') = ts$” should be “$\tau'(s) = ts$”. Similarly, in the fourth line of the statement of the **create object** *o* **of type** *to* primitive operation, “$\tau'(o') = to$” should be “$\tau'(o) = to$”.

Chapter 4, “Security Policies”

Section 4.7, “Security and Precision,” p. 118 [author]

In Definition 4–21, there should be an equals sign “=” after $m_3(i_1, ..., i_n)$ and before the curly brace.

Section 4.7, “Security and Precision,” p. 118 [Tom Daniels]

The first sentence after Definition 4–21 should be “This definition says that for inputs on which either m_1 or m_2 return the same value as p, their union does also.”.

Chapter 5, “Confidentiality Policies”

Section 5.2.3.2, “Rules of Transformation,” p. 137 [Xuxian Jiang]

In the last line of Definition 5–8, “$\rho_i(r, v) = (d, v')$” should be “$\rho_i(r, v') = (d, v)$”. This maintains consistency with the definition of W.

Section 5.2.4.1, “The *get-read* Rule,” p. 140 [Xuxian Jiang]

In the fifth line of the paragraph after the *get-read* rule, the phrase “simple security property” should be “*-property”. In the fourth line of the second paragraph of the proof of Theorem 5-14, “$f_c(s)$ *dom* $f_o(o)$” should be “$f_s(s)$ *dom* $f_o(o)$”.

Section 5.8, “Exercises,” p. 150 [author]

In exercise 2, on the third line, “(read, write, or both)” should be “(read, write, both, or neither)”.

Chapter 6, “Integrity Policies”

Section 6.2.1, “Low-Water-Mark Policy,” p. 154 [Lisa Clark]

In the last line of Theorem 6–1, “$n > 1$” should be “$n \geq 1$”.

Section 6.2.2, “Ring Policy,” p. 155 [Xuxian Jiang]

In the last paragraph of this section, delete the sentence “Hence. Theorem 6-1 holds for this model, too.”.

Section 6.3.2, “Lipner’s Full Model,” p. 159 [Xuxian Jiang]

In the table in the middle of the page, the “Integrity clearance” entry for “System controllers” should be “(ISP, { IP, ID })”. In the table at the bottom of the page, the “Integrity level” entry for “Development code/test data” should be “(ISL, { ID })”.

Section 6.3.2, “Lipner’s Full Model,” p. 159 [Kay Connelly]

In the table in the middle of the page, the “Integrity clearance” entry for “System managers and auditors” should be “(ISL, ∅)”. In the table at the bottom of the page, the “Integrity level” entry for “Repair” should be “(ISP, { IP })”.

Section 6.8, “Exercises,” p. 167 [Xuxian Jiang]

In exercise 3, “subject levels and categories” should be “security levels and categories”.

Section 6.8, “Exercises,” p. 167 [Aleksandr Zingorenko]

In exercise 3, “a system” should be “a system implementing Biba’s model (the strict integrity policy”.

Chapter 7, “Hybrid Policies”

Section 7.1.2, “Formal Model,” p. 174 [Xuxian Jiang]

In Theorem 7-2, “$l_1(o_i) = d$” should be “$l_1(o_i) = c$”.

Section 7.1.2, “Formal Model,” p. 174 [Xuxian Jiang]

In Theorem 7-3, “$\{ (o, o') \mid o \in O \wedge o' \in O \wedge l_2(o) = l_2(o') \vee l_2(o) = l_2(v(o)) \}$” should be “$\{ (o, o') \mid o \in O \wedge o' \in O \wedge (l_2(o) = l_2(o') \vee l_2(o) = l_2(v(o))) \}$”. It is clear from the proof that this is what was intended, but the parentheses make the statement of the theorem clearer.

Section 7.4, “Role-Based Access Control,” p. 183 [Guido Wedig]

In the last line of the first example, “$r_j > r_i$” should be “$r_i > r_j$”.

Section 7.4, “Role-Based Access Control,” p. 183 [Xuxian Jiang]

In the first line of Definition 7-12, “$r \in auth(s)$” should be “$r \in authr(s)$”.

Chapter 8, “Noninterference and Policy Composition”

Section 8.1, “The Problem,” p. 190 [Kay Connelly]

In the example, the transitive closure $AS(X \cup Y)^+$ does not include (Lilith, Alice). It should:

$AS(X \cup Y)^+$ = { (Bob, Eve), (Bob, Lilith), (Bob, Alice), (Eve, Lilith), (Eve, Alice), (Lilith, Eve), (Lilith, Alice) }

The same is true for $AS(X \cup Y)^-$, which should be:

$AS(X \cup Y)^-$ = { (Bob, Eve), (Bob, Lilith), (Eve, Lilith), (Eve, Alice), (Lilith, Eve), (Lilith, Alice) }

Section 8.2, “Deterministic Noninterference,” p. 194 [Xuxian Jiang]

In Definition 8–5A, the “for *M*” at the end of the definition should be omitted.

Section 8.2, “Deterministic Noninterference,” p. 195 [Xuxian Jiang]

In the statement of Lemma 8–1, “$T^*(\pi_d(c_s), \sigma_0)$” should be “$T^*(\pi'_d(c_s), \sigma_0)$”.´Similarly, in the second line of the proof, “$T^*(\pi_{dom(c)}(c_s), \sigma_0)$” should be “$T^*(\pi'_{dom(c)}(c_s), \sigma_0)$”.

Section 8.2.1, “Unwinding Theorem,” p. 196–197 [author]

Throughout the proof of Theorem 8–1, every occurrance of “π’” should be replaced by “π'”. The apostrophe should be a prime.

Section 8.2.2, “Access Control Matrix Interpretation,” p. 198 [Kay Connelly]

In the second line of item 2 at the very top of the page, “*POW*” should be “*P*”.

Section 8.2.2, “Access Control Matrix Interpretation,” p. 199 [Xuxian Jiang]

In the second paragraph of Theorem 8-2’s proof, “$(dom(c),d) \in r$” should be “$(dom(c),d) \notin r$”.

Section 8.2.3, “Security Policies That Change over Time,” p. 200 [Xuxian Jiang]

At the end of definition 8-9, “and all $s \in G$” should be “and all $s \in G'$”.

Section 8.2.3, “Security Policies That Change over Time,” p. 201 [Xuxian Jiang]

The second sentence of the second paragraph says “thus, $cando(\nu, s_2, z)$ is true” when it should say “thus, $cando(\nu, s_2, z)$ is false”.

Chapter 9, “Basic Cryptography”

Section 9.8, “Exercises,” p. 242 [Mahesh Tripunitara]

In exercise 15, part a, “$a \bmod n + b \bmod n$” should be “$(a \bmod n + b \bmod n) \bmod n$”.

Chapter 10, “Key Management”

Section 10.5.1.3, “The Yaksha Security System,” p. 264 [Patrick Wheeler]

The equation “$d_{AliceA}d_{AliceY} = d_{Alice} \bmod n_{Alice}$” is wrong (although it is indeed what is in the referenced paper). The correct equation is “$d_{AliceA}d_{AliceY} \bmod \phi(\bmod n_{Alice}) = d_{Alice}$”. This can be verified either by working out the math (see exercise 2 of this chapter) or by referring to the paper by C. Boyd, “Digital Multisignatures,” *Cryptography and Coding*, H. Beker and F. Piper, *eds*., Clarendon Press, Oxford (1989) pp. 241–246; the relevant part is section 2.

Section 10.6, “Digital Signatures,” p. 266 [author]

In the second line of the paragraph after Definition 10-10, “$m \{ m \}k$” should be “$m \| \{ m \}k$”. The vertical bars (for concatenation) are missing.

Section 10.6, “Digital Signatures,” p. 267 [author]

In the second line of the first full paragraph on the page, “$m \{ m \}d_{Alice}$” should be “$m \| \{ m \}d_{Alice}$”. The vertical bars (for concatenation) are missing.

Chapter 11, “Cipher Techniques”

Section 11.1.1, “Synchronous Stream Ciphers,” pp. 275–276 [Lisa Clark]

The two sentences that cross the page boundaryuse Bob as the attacker, but the previous sentence make Cathy the attacker. So, change “When Alice sends the message, Bob intercepts it and compares the ciphertext with the two he computed. From this, he knows which message Alice sent.” to “When Alice sends the message, Cathy intercepts it and compares the ciphertext with the two she computed. From this, she knows which message Alice sent.”

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

In the example, the fourth line of the computation of key bits is wrong, and that makes the rest wrong. The key bit computation should be:

Current register	*Key*	*New bit*	*New register*
1100	0	$f(1, 1, 0, 0) = (1 \text{ and } 0) \text{ or } 0 = 0$	0110
0110	0	$f(0, 1, 1, 0) = (0 \text{ and } 1) \text{ or } 0 = 0$	0011
0011	1	$f(0, 0, 1, 1) = (0 \text{ and } 1) \text{ or } 1 = 1$	1001
1001	1	$f(1, 0, 0, 1) = (1 \text{ and } 0) \text{ or } 1 = 1$	1100
1100	0	$f(1, 1, 0, 0) = (1 \text{ and } 0) \text{ or } 0 = 0$	0110
0110	0	$f(0, 1, 1, 0) = (0 \text{ and } 1) \text{ or } 0 = 0$	0011
0011	1	$f(0, 0, 1, 1) = (0 \text{ and } 1) \text{ or } 1 = 1$	1001
1001	1	$f(1, 0, 0, 1) = (1 \text{ and } 0) \text{ or } 1 = 1$	1100
1100	0	$f(1, 1, 0, 0) = (1 \text{ and } 0) \text{ or } 0 = 0$	0110
0110	0	$f(0, 1, 1, 0) = (0 \text{ and } 1) \text{ or } 0 = 0$	0011

Also, in the immediately following text, "(with an initial nonrepeating sequence of length 4) and is $0011\overline{0010}$... (the overstruck part repeats indefinitely)" should be "and is 0011".

Section 11.4.2, "Security at the Transport Layer: SSL," p. 291 [Josko Orsulic]

In the middle of the page, the first item 5 should say that the master secret is 48 bytes, not 48 bits.

Chapter 12, "Authentication"

Section 12.3.2, "One-Time Passwords," p. 326 [James Walden]

In step 4 of the S/Key protocol, near the middle of the page, "p_{i+1}" should be "p_{i-1}".

Chapter 15, "Access Control Mechanisms"

Section 15.9, "Exercises," p. 405 [Vladimir Berman]

In exercise 1, "Both ACLs" should read "In general, ACLs".

Chapter 16, "Information Flow"

Section 16.2.1, "Confinement Flow Model," p. 412 [Yunhua Lu]

In the second line of the page, "$x \rightarrow y$, $x \rightarrow z$, $y \rightarrow z$, and $z \rightarrow x$" should be "$x \rightarrow y$, $x \rightarrow z$, $y \rightarrow z$, $z \rightarrow x$, and $z \rightarrow y$". The "$z \rightarrow y$" is missing.

Section 16.3.1, "Declarations," p. 417 [author]

The text from the second full paragraph (that begins "Because information can flow ...") to the example is imprecise. It should read as follows:

Let r_1, ..., r_p be the set of input and input/output variables from which information flows to the output variable o_s. The declaration for the type must capture this:

o_s: *type* **class** { r_1, ..., r_p }

(We implicitly assume that any output-only parameter is initialized in the procedure.) The input/output parameters are like output parameters, except that the initial value (as input) affects the allowed security classes. Again, let r_1, ..., r_p be defined as above. Then:

io_s: *type* **class** { r_1, ..., r_p, io_s }

Section 16.3.2.4, “Iterative Statements,” p. 421 [author]

In the last paragraph of the example in this section, “$lub\{ \underline{i}, \underline{n} \} \le glb\{ \underline{a[i]}, \underline{i} \}$” should be “$lub\{ \underline{b[i]}, \underline{i}, \underline{n} \} \le glb\{ \underline{a[i]}, \underline{i} \}$”.

Section 16.3.2.5, “Goto Statements,” p. 421 [author]

The declaration for variables in the procedure *transmatrix* should not include the variable *tmp*. Here is the right declaration:

var *i*, *j*: *int* **class** { *i* };

Section 16.3.2.5, “Goto Statements,” p. 423 [author]

At the end of the second paragraph of the second example (the one after the line beginning “b_6:”), “$lub\{\underline{x}, \underline{tmp}\} \le \underline{y}$” should be “$lub\{\underline{x}, \underline{i}\} \le \underline{y}$”. The last sentence of the next paragraph should read “In other words, $\underline{i} \le glb\{ \underline{i}, \underline{y} \}$, or $\underline{i} \le \underline{y}$”. In the last sentence of the example, “$lub\{ \underline{x}, \underline{tmp} \} \le \underline{y}$” should be “$lub\{ \underline{x}, \underline{i} \} \le \underline{y}$”.

Chapter 22, “Malicious Logic”

Section 22.1, “Introduction,” p. 613 [Tom Daniels]

In the line with *chmod* in the example, “`o+s,w+x`” should be “`u+s,o+x`”.

Chapter 24, “Auditing”

Section 24.3, “Designing an Audit System,” p. 694 [Lisa Clark]

In the second example, “$L(S) \le L(O)$” in the third line should be “$L(S) < L(O)$”. In the fourth line, “$L(S) \ge L(O)$” should be “$L(S) > L(O)$”.

Chapter 36, “Bibliography”

Reference 199, p. 1006 [author]

The volume number of this paper is incorrect. The volume number should be **8**, not **1**.

Reference 298, p. 1012 [author]

The title of this paper is mispunctuated. It should be “The Structure of the ‘THE’-Multiprogramming System”.

Reference 531, p. 1027 [author]

The title of this paper is wrong. It should be “Identity Authentication Based on Keystroke Latencies” (the word “Authentication” is currently “Authorization”).

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.