Errata to the the Second Printing (March 25, 2003)

Preface

"Graduate Level," p. xxxix [Steven Alexander]

In the footnote after the bottom of the page, all reference numbers except the first are off by 2 or 3. The correct reference numbers (includng the first) are "[240, 590, 695, 702, 888, 897, 998]".

"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, Ziad El Bizri, Logan Browne, Terry Brugger, Raymond Centeno, Michael Clifford, Christopher Clifton, Dan Coming, Crispin Cowan, Dimitri DeFigueiredo, Joseph-Patrick Dib, Jeremy Frank, Robert Fourney, Martin Gagne, Ron Gove, James Hinde, Jesper Johansson, Mark Jones, Calvin Ko, Mark-Neil Ledesma, Ken Levine, Karl Levitt, Gary McGraw, Alexander Meau, Nasir Memon, Mark Morrissey, Ather Nawaz, Iulian Neamtiu, Kimberly Nico, Stephen Northcutt, Rafael Obelheiro, Holly Pang, Ryan Poling, Sung Park, Ashwini Raina, Jorge Ramos, Brennen Reynolds, Peter Rozental, Christoph Schuba, David Shambroom, Jonathan Shapiro, Clay Shields, Tom Walcott, Dan Watson, Chris Wee, Paul Williams, Bonnie Xu, Xiaoduan Ye, Lara Whelan, John Zachary, and to everyone in my computer security classes, who (knowingly or unknowingly) helped me develop and test this material.

Chapter 2, "Access Control Martix"

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

In the fourth line of the second paragraph of the example, "*read*" should be "{ *read* }" (adding set braces) and "$|O_i| > 1$" should be "$|O_i| < 2$". In the last line of that paragraph, "{ *o* }" should be "*o*" (the set braces should be removed). The next paragraph (last one in the example) should read:

> When C_1 is referenced, $|O_1| = 0$ and A[**asker**, **{ Celia**, **Leonard**, **Matt }**] = { *read* }, so the query is answered. When C_2 is used, $|O_2| = 1$ and A[**asker**, **{ Matt }**] = { *read* }, so that query is also answered. But with query C_3, $|O_3| = 2$, so A[**asker**, **{ Celia, Leonard }**] = ∅, and the query is not answered.

Section 2.3, "Protection State Transitions," p. 37 [author]

The first paragraph ends with "where the notation λ ⊢, and the expression", but should end with "where the notation". The "λ ⊢, and the expression" is extraneous.

Section 2.3, "Protection State Transitions," p. 38 [Iulian Neamtiu]

The precondition of item 1 should read "$s \notin S$".

Section 2.3, "Protection State Transitions," p. 39 [John Zachary]

In the second line of the postconditions of **destroy object**, the comma just before the ∅ should be deleted, and $O' = O - \{ s \}$ should be $O' = O - \{ o \}$.

Chapter 3, "Foundational Results"

Section 3.2, "Basic Results," pp. 51–52 [author]

In the command $crightmost_{p,A}$, every occurrance of the subscript k (and k+1) should be replaced by i (and i+1, respectively). The actual command should be:

```
command crightmost_{p,A}(s_i, s_{i+1})
    if end in a[s_i, s_{i+1}] and p in a[s_i, s_i] and A in a[s_i,
s_i]
    then
        delete end from a[s_i, s_i];
        create new subject s_{i+1};
        enter own into a[s_i, s_{i+1}];
        enter end from a[s_{i+1}, s_{i+1}];
        delete p from a[s_i, s_i];
        delete A from a[s_i, s_i];
        enter B into a[s_i, s_i];
        enter q into a[s_{i+1}, s_{i+1}];
end
```

Section 3.3.4, "Conspiracy," p. 65 [Ziad El Bizri]

In the example, the "**y**" in each of the 5 steps of the witness should be "**z**".

Just above the steps, the predicate *can*•*share*(*r*, **x**, **y**, G_0) should be *can*•*share*(*r*, **x**, **z**, G_0).

Section 3.5.2, "Extending SPM," p. 81 [Joseph-Patrick Dib]

In the block of *cc* rules following "Augment the *can-create* rules as follows:", "$cc(p_i) = a_1$" should be "$cc(p_1) = a_1$". In the block of *link* rules at the bottom of the page, the third rule should begin "$link_2(\mathbf{S}, \mathbf{A}_3)$" and not "$link_2(\mathbf{S}, \mathbf{A}_2)$".

Chapter 4, "Security Policies"

Section 4.5.1, "High-Level Policy Languages," p. 105 [Ather Nawaz]

In the example, the last three "deny" statements should read:

```
deny(s |→ c_1.f) when b_1
deny(s |→ c_2.f) when b_2
```

and

```
deny(s |→ c_2.f) when b_1 ∨ b_2
```

Section 4.5.1, "High-Level Policy Languages," p. 108 [Raymond Centeno]
In the next to last line of the assign statements near the bottom of the page, "`dte_t`" should be "`t_dte`".

Section 4.5.2, "Low-Level Policy Languages," p. 109 [Ryan Poling]
In the third line of the example at the bottom of the page, "*xhosts*" should be "*xhost*".

Section 4.11, "Exercises," problem 5, p. 121 [Alex Aris]
In part b, the word "author's" should be "creator's".

Chapter 5, "Confidentiality Policies"

Section 5.2.3, "Formal Model," p. 133 [Alex Aris]
In the second line of the next to last paragraph, "Becauses" should be "Because".

Section 5.2.3.1, "Basic Security Theorem," p. 134 [Ather Nawaz]
In the second condition of Definition 5–2, "$f_c(s)\ dom\ f_o(o)$" should be "$f_s(s)\ dom\ f_o(o)$".

Section 5.2.3.2, "Rules of Transformation," p. 137 [Ather Nawaz]
On the second line of Theorem 5–7, "$\Sigma(R, D, W, z_0)$" should be "$\Sigma(R, D, W(\omega), z_0)$". On the second line of Theorem 5–9, "$\Sigma(R, D, W, z_0)$" should be "$\Sigma(R, D, W(\omega), z_0)$".

Section 5.2.3.2, "Rules of Transformation," p. 137 [author]
In the first line of the proof of Theorem 5–8, "Definition 5–3" should be "Definition 5–2".

Section 5.2.3.2, "Rules of Transformation," p. 138 [Ather Nawaz]
On the second line of Theorem 5–11, "$\Sigma(R, D, W, z_0)$" should be "$\Sigma(R, D, W(\omega), z_0)$".

Section 5.2.3.2, "Rules of Transformation," p. 138 [Jim Hinde]
In Theorem 5–10, "$v' = (b', a, f, h)$" should be "$v' = (b', m, f, h)$". Also, the theorem should have a fourth condition:
d. $p = \underline{e}$.

Section 5.2.3.2, "Rules of Transformation," p. 138 [author]
The proof for Theorem 5–10 should read as follows:
Proof If v' satisfies the *-property, then the claim follows from Definition 5–3 and the definition of $\underline{e}$. Conversely, assume that condition (a) holds. Let $(s', o', p') \notin b'$. If $(s', o', p') \in b$, the assumption that v satisfies the *-property means that v' also satisfies the *-property. Otherwise, $(s', o', p') = (s, o, p)$ and, by condition (a) and Definition 5–3, the *-property holds. The proof for each of the other conditions is similar. Thus, v' satisfies the *-property.

Section 5.2.4.2, "The *give-read* Rule," p. 141 [Christopher Clifton]

In the definition of ρ_6, which is the indented text following the third paragraph of this section, the three occurrences of ρ_1 (in the first line after "**then**", in the fifth line after "**then**", and in the sixth line after "**else**") should all be ρ_6.

Chapter 6, "Integrity Policies"

Section 6.3.2, "Lipner's Full Model," p. 159 [Kimberly Nico]

In the table in the middle of the page, the "Security clearance" entry for "System controllers" should be "(SL, { SP, SD, SSD }) and downgrade privilege". The "SSD" is missing.

Chapter 7, "Hybrid Policies"

Section 7.1.2, "Formal Model," p. 174 [Martin Gagne]

The second condition in Axiom 7–6 should read:

2. There is no $o' \in O$ with $H(s, o') = true$, $l_2(o) \neq l_2(o')$, $l_2(o) \neq l_2(v(o))$, and $l_2(o') \neq l_2(v(o'))$.

Chapter 9, "Basic Cryptography"

Section 9.3.2, "RSA," p. 235 [author]

In the next to last line, the number "93" should be "24".

Section 9.3.2, "RSA," p. 236 [Dan Coming]

In the next to last line of the second example, "meesage" should be "message".

Chapter 10, "Key Management"

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

In the second step of the Otway-Rees protocol (in the middle of the page), there is an extraneous comma after the second "Bob". The comma should be deleted.

Section 10.6.2.2, "El Gamal Digital Signature," p. 269 [Mark-Neil Ledesma]

In the second paragrah of the section, the equation spanning the end of line 2 to the beginning of line3 is "$a = m^k \bmod p$", but it should be "$a = g^k \bmod p$".

Section 10.6.2.2, "El Gamal Digital Signature," p. 270 [Ken Levine]

In the second line of the first paragraph after the first example, "x, Alice's public key" should read "d, Alice's private key".

Chapter 11, "Cipher Techniques"

Section 11.4.2.1, "Supporting Cryptographic Mechanisms," p. 293 [David Shambroom]

In Table 11–3, column 1, the word "Algorithm" should be deleted.

Chapter 12, "Authentication"

Section 12.2.2.2, "Pronounceable and Other Computer-Generated Passwords," p. 315 [Alex Aris]

The line before Definition 12-4 should read "One way to increase the size of the set of allowed passwords is through *key crunching* [417]."

Chapter 14, "Representing Identity"

Section 14.5, "Naming and Certificates," p. 359 [Ken Levine]

In the fourth line of the page, "This CA had the same issuance policy" should read "This CA had the same authentication policy".

Section 14.6.1.1, "Static and Dynamic Identifiers," p. 368 [Alex Aris]

In the fifth line of the second paragraph on the page, "When the gateway" should read "When that gateway".

Section 14.6.3, "Anonymity on the Web," p. 374 [Alex Aris]

In Figure 14-2, the innermost box is slightly wider than the box containing it. The innermost box should be completely enclosed by the next box out.

Chapter 15, "Access Control Mechanisms"

Section 15.3.2, "Sharing Secrets," p. 399 [Rafael Obelheiro]

In Definition 15–3, "threshhold" should be spelled "threshold". In the second line of the second paragraph after Definition 15–3, "polymonials" should be "polynomials". In the first line of the example at the bottom of the page, "threshhold" should be "threshold".

Section 15.5, "Propagated Access Control Lists," p. 403 [Ken Levine]

In the second line of the third paragraph on the page, "subject o'" should be "object o'".

Section 15.9, "Exercises," p. 405 [author]

In exercise 1, "ACLs and C-List entries" should be "ACLs".

Section 15.9, "Exercises," p. 406 [Raymond Centeno]

In exercise 9, part c, "q" should be "d".

Chapter 16, "Information Flow"

Section 16.2.3, "Nontransitive Information Flow Policies," p. 414 [Ken Levine]

In the definition of h_R in Definition 16.5, "$y \in S_P$" should be "$y \in SC_R$". Also, in the last line of the proof of Theorem 16-1, "Thus, $a \in S_P$ and $a \leq_R b$" should read "Thus, $a \leq_R b$".

Section 16.3.1, "Declaraions," p. 417 [Ken Levine]

In the two lines showing the output parameter o_s and the input/output parameter io_s declarations, io_k should be io_m.

Section 16.3.2.3, "Conditional Statements," p. 420 [Christopher Clifton]

In the last line of the example, "$lub\{ \underline{y}, \underline{z} \} \leq \underline{x}$" should be "$lub\{ \underline{b}, \underline{c}, \underline{x} \} \leq \underline{d}$" and "$\underline{b} \leq a$" should be "$\underline{b} \leq \underline{a}$".

Section 16.4.1, "Fenton's Data Mark Machine," p. 430 [Christopher Clifton]

In line 4 of the paragraph labeled "2", the "PC = *lub*(PC, *x*)" in

```
if x = 0 then { push(PC, PC); PC = lub(PC, x); PC := n; }
```

should be "PC := *lub*(PC, *x*)". The colon ":" is missing.

Section 16.4.1, "Fenton's Data Mark Machine," p. 431 [Ken Levine]

The first line of the sample should end with "in which *x* initially contains 0 or 1,[2] and *y* and *z* contain 0."

Section 16.4.1, "Fenton's Data Mark Machine," p. 432 [Jorge Ramos]

In the example's table at the top of the page, the values of PC when PC is 6 and 7 should be $\underline{z}$ rather than $\underline{x}$. In the second line of the paragraph right after the example, both occurences of $\underline{x}$ should be $\underline{z}$, and "at the fifth step" should be changed to "at the fourth step (statement 6)".

Section 16.6, "Summary," p. 436 [Ken Levine]

In the last sentence of the first paragraph, "antecedent" should be "consequent".

Chapter 17, "Confinement Problem"

Section 17.3.1.1, "Noninterference," p. 450 [Ken Levine]

The first full paragraph should begin "Next, because *o* exists in σ_2" rather than "σ_1".

Section 17.1.3.4, "Covert Flow Trees," p. 456 [Ken Levine]

The second line of the first comment in the code sample should be deleted.

Section 17.1.3.4, "Covert Flow Trees," p. 456 [Alex Aris]

In the example code, the procedure *Lockfile* is defined as returning a *boolean* value. Procedures do not return values. The first line of the definition of that procedure should read:

```
procedure Lockfile(f: File);
```

and the comment immediately above this declaration should read:

```
(* lock the file if it is not locked and not opened *)
```

(the second line of the comment should be deleted).

Section 17.1.3.4, "Covert Flow Trees," p. 457 [Ken Levine]

The table entry for (modified, *Unlockfile*) should be *locked*.

Section 17.1.3.4, "Covert Flow Trees," p. 459 [Alex Aris]

In the second line on the page, "*and*" should be "*or*".

Section 17.1.3.4, "Covert Flow Trees," p. 462 [Ken Levine]

The last two sentences of the example should read "If the file is opened, the *High* process did not lock the file (a 1 bit). If the file is not opened, the *High* process did lock the file (a 0 bit)." In the book, the 1 and the 0 are reversed.

Chapter 19, "Building Systems with Assurance"

Section 19.2.2.2, "External Functional Specification," p. 514 [author]

In the first and second lines of the example, "describes a routine for an error handling subsystem" should be "describes a routine, *logevent*(), for an error handling subsystem".

Section 19.3.3.2, "Security Testing Using PGWG," p. 540 [Ken Levine]

In the first line of the example, "stime_1" should be "stime_2", the *Test case name* should be "K_MIS_stime_2", and the "Event" in the second line from the bottom of the page should be "SETTHETIME_2".

Chapter 20, "Formal Methods"

Section 20.3.1, "The Hierarchical Development Methodology," p. 552 [Ken Levine]

The first sentence of the second full paragraph should end with"the next lower machine". Currently, it ends with "the next higher machine".

Section 20.3.1.2, "The Boyer-Moore Theorem Prover," p. 556 [Ken Levine]

The word "one" in the next-to-last line in the first paragraph should be "done".

Chapter 22, "Malicious Logic"

Section 22.3.2, "Executable Infectors," p. 619 [Iulian Neamtiu]

In the third line of the last paragraph of the example, the file name "COMND.COM" should be "COMMAND.COM".

Section 22.6.1, "Theory of Computer Viruses," p. 626 [Ken Levine]

In Definition 22-16, *V* is defined as "a sequence of symbols on the machine tape". It should be defined as "a set of sequences of symbols on the machine tape".

Section 22.6.1, "Theory of Computer Viruses," p. 627 [Ken Levine]
In the first line of the third paragraph of the proof of Theorem 22-1, the "*d*" should be "δ".

Section 22.6.1, "Theory of Computer Viruses," p. 627-630 [author]
The proof of Theorem 22-1 (from after the statement of the theorem on p. 627 to the end of the paragraph at the top of p. 630) should be indented, as the other proofs in the book are.

Section 22.7.2.2, "Reducing the Rights," p. 632 [Ken Levine]
In the last line of the page, "o_1" should be "o_3".

Section 22.7.2.2, "Reducing the Rights," p. 633 [Ken Levine]
In the second equation line for $PD(s_{12})$, the symbol $\cup_j$ should be $\cup_{j \neq 1}$.

Section 22.7.4, "Malicious Logic Altering Files," p. 637 [Ken Levine]
In the next-to-last line of the first example, "file" should be "database".

Chapter 23, "Vulnerability Analysis"

Section 23.2.4.3, "Flaw Generalization," p. 652 [Ken Levine]
The word at the end of the last paragraph, which is "supervisor", should be "*administrator*".

Section 23.2.4.4, "Flaw Elimination," p. 652 [Ken Levine]
The word "phase" in the third line from the end of this section should be "phases".

Chapter 24, "Auditing"

Section 24.3, "Designing an Audit System," p. 695 [Ken Levine]
In the second paragraph of the example, at the fourth line, $\exists O'(CD(O') \in CD_H(S))$ should be $CD(O) \in CD_H(S)$. The same change should be made to Equation 1 following the paragraph.
In the seventh line of the same paragraph, "$COI(O) = COI(O')$" should be "$CD(O) \neq CD(O')$". The same change should be made to Equation 2 following the paragraph.

Chapter 25, "Intrusion Detection"

Section 25.3.1, "Anomaly Modeling," p. 730 [Ken Levine]
At the end of the first paragraph of the example on this page, the "about 26%" should be "about 28%".

Section 25.3.2, "Misuse Modeling," p. 737 [Ken Levine]
In the third line of the second paragraph on the page (after the second table), "–*x*" should be "–*s*".

Section 25.6.2.3, "Follow-Up Phase," p. 763 [Ken Levine]
In the second line of the page, "Evaluating" should be "Solving".

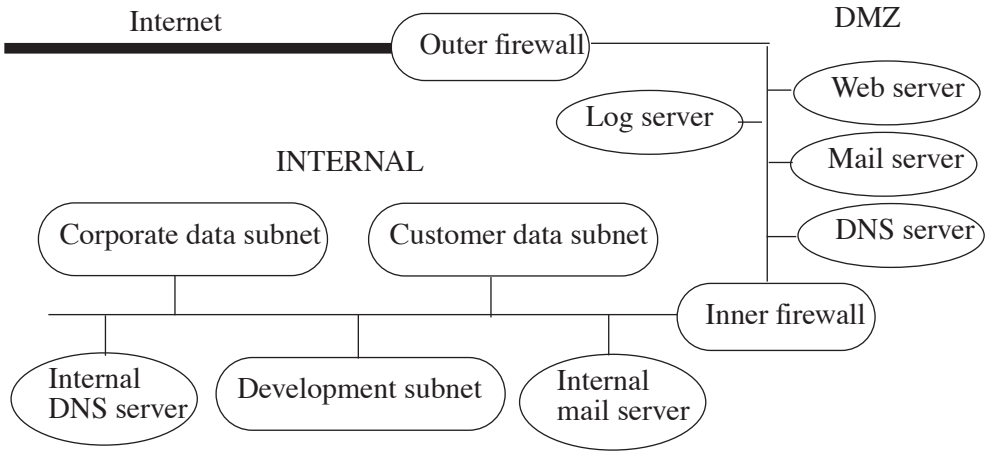
Section 25.6.2.3, "Follow-Up Phase," p. 764 [Ken Levine]

The first sentence of the example says "see page 586". It should say "see page 614".

Chapter 26, "Network Security"

Section 26.3, "Network Organization," p. 780 [Ken Levine]

Figure 26-1 should look like:



Note the "Log server" oval hanging off the DMZ.

Section 26.3.3.5, "Summary," p. 790 [Ken Levine]

In line four of the second paragraph of this section, "techniques,[58]" should be "techniques[58])".

Chapter 27, "System Security"

Section 27.5.2, "Development Network System," p. 823 [author]

The title of the section should read "Development System". The word "Network" should not be in the title.

Section 27.5.2, "Development Network System," p. 824 [Ken Levine]

The last sentence of the second paragraph should read, "Unlike the Web server system, the development system uses a password hashing scheme based on the DES. This maintains compatibility with NIS.".

Chapter 29, "Program Security"

Section 29.2.2.1, "Group 1: Unauthorized Users Accessing Role Accounts," p. 872 [Ken Levine]

In the next-to-bottom line of the next-to-end paragraph of this section, "that trusted users" should be "that only trusted users".

Section 29.3.2.3, "Storage of the Access Control Data," p. 878 [Ken Levine]

In the last line of the page, the "l" following "'*any*'" should be deleted.

Section 29.4.1, "First-Level Refinement," p. 881 [Ken Levine]

The part of the program between "repeat" and "until" is mis-indented and has some typographical errors. The following is the correct indentation, with the typos fixed:

```
repeat
        rec ← get next record from file; EOF if none
        if rec ≠ EOF then
                stat ← match(rec, rname, cmd, user, timeday, entry)
until rec = EOF or stat = true
```

The indentation in the book should be 4 characters rather than a mixture of 4 and 8 characters, and uses "nonw" rather than "none". Also, the next-to-last line of the code has "sccess" rather than "access".

Section 29.4.2, "Second-Level Refinement," p. 883 [Ken Levine]

The next-to-last line of the last segment of code on the page is:

```
stat = match(rec, rname, cmd, user, timeday, entry);
```

It should be:

```
stat = match(acrec, rname, cmd, userid, timeday, entry);
```

(the "rec" should be "acrec" and the "user" should be "userid").

Section 29.5.1.3, "Memory Protection," p. 891 [Ken Levine]

In the line immediately above Implementation Rule 29.5.3, the word "types" should be "typed".

Chapter 30, "Lattices"

Section 30.1, "Basics," p. 926 [Ken Levine]

In the last example of the section, the set of lower bounds should be
$\{ 1 + 0i, 1 + 1i, 1 + 2i, 1 + 3i, 0 + 0i, 0 + 1i, 0 + 2i, 0 + 3i \}$ and the greatest lower bound is $1 + 3i$.

Chapter 34, "Symbolic Logic"

Section 34.3.1, "Syntax of CTL," p. 955 [Ken Levine]

Near the end of the second bullet, "AF" should be "AFϕ".

Section 34.3.2, "Semantics of CTL," p. 955 [Ken Levine]

In the first line, "syntax" should be "semantics". Near the middle of the page, the paragraph beginning "Let M be a model, let s_is be states of M" should begin "Let M be a model, let s and s_i be states of M". In the last bullet on the page, "disjunction" should be "conjunction".

Section 34.3.2, "Semantics of CTL," p. 956 [Ken Levine]

In the first bullet, "conjunction" should be "disjunction". In the second bullet, "satisfies neither the first nor the second" should be "does not satisfy the first".

Chapter 36, "Bibliography"

Reference 602, p. 1031 [Rafael Obelheiro]

The work "CrptoLib" should be "CryptoLib".

Reference 1033, p. 1059 [Ken Levine]

This reference should be changed to the newer PERL reference:

1033. L. Wall, T. Christiansen, and J. Orwant, *Programming Perl*, 3rd Edition, O'Reilly and Associates, Sebastopol, CA (July, 2000).

Index

"Operational Assurance", p. 1076 [Raymond Centeno]

The index entry for "operational assurance" should refer to pages 480 and 484, not pages 452 and 456.