Information Security: Principles and Practice

Errata

August 23, 2006

1. A note on the PowerPoint slides: Depending on your version of PowerPoint, a few of the slides might have problems. It appears that the most likely problem slides are "Bob's Cave" (Protocols, slide 60) and the buffer overflow slides (Software, slides 17 through 20). A few of the other slides might exhibit slight spacing problems. For example, the interline spacing may be somewhat crowded.

2. Page 5, second full paragraph: "Ideally, by verifying a few simply properties..." should read, "Ideally, by verifying a few simple properties..."

3. Page 12, Figure 2.1: Replace "excrypt" with "encrypt".

4. Page 22, footnote: David Greenglass actually served 10 years (of a 15 year sentence) for his part in the atomic bomb espionage case.

5. Page 26, discussion of Enigma: I should have made clear that the story about Churchill not warning Coventry of the impending bombing is false. Also, the Polish cryptanalysts who initially broke the Enigma continued, after the fall of France, to break messages from unoccupied France. See S. Budiansky's excellent book, *Battle of Wits: The Complete Story of Codebreaking in World War II*, for the definitive treatment of all things Enigma.

6. Page 27, the description of confusion and diffusion: Shannon's definition of confusion is that it obscures the relationship between the *key* and the ciphertext, not the plaintext and the ciphertext, as stated. However, it is clear that what Shannon has in mind is that confusion loosely corresponds to substitution and diffusion loosely corresponds to transposition.

7. Page 71, Figure 4.2: The top arrow from Trudy to Bob should include the label $g^t \bmod p$.

8. Page 89, last paragraph: SHA-1 generates a 160-bit hash, not a 180-bit output.

9. Page 135, second paragraph of Section 6.5.2: Change "beak" to "break".

10. Page 179, Figure 8.1: On the left-hand side, the ACL for file 3 should be, from top to bottom, `(rw,r,r)`. On the right-hand side, Alice's capability should be `(r,w,rw)`, Bob's capability should be `(---,r,r)`, and Fred's capability should be `(r,---,r)`.