Information Security: Principles and Practice

Errata

April 20, 2008

A note on the PowerPoint slides: There is one set of PowerPoint slides for Windows users and one for Mac users (and also a set of slides in PDF). Of course, the Mac slides work on Windows and vice versa, but some of the spacing and animation will not display correctly.

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

2. Page 11, 1st quote. The "quote" that appears is ciphertext, so it might be more accurate to say, "corresponding plaintext from...", or something like that.

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

4. Page 13, the last line before Section 2.3.1: It is probably more reasonable to describe the one-time pad as "semi-practical" instead of "pratical".

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

6. 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 book, *Battle of Wits: The Complete Story of Codebreaking in World War II*, for the definitive treatment of most things Enigma.

7. 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 had in mind is that confusion loosely corresponds to substitution and diffusion loosely corresponds to transposition.

8. Page 45, 2nd line: Replace "that is in table." with "that is in the table."

9. Page 47, 3rd line: Replace "the EAS equivalent" with "the AES equivalent".

10. Page 53, last paragraph, 2nd line: Replace "will receive \$10" with "will receive \$2".

11. Page 61, 2nd line: Change "know" to "known".

12. Page 62, 2nd full paragraph, 3rd line: Change "trap door" to "one way".

13. Page 63, 1st sentence: It is stated that Diffie and Hellman "...offered no viable system" in [67]. In their seminal paper, New directions in cryptography, Diffie and Hellman did not provide a solution to the general public key problem (i.e., encryption and signatures), but they did, of course, provide details on the Diffie-Hellman key exchange.

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

15. Page 73, elliptic curve example: This is not a good example, since $4a^3 + 27b^2 = 0$, which implies the curve is not "smooth". This should be replaced with an example where $4a^3 + 27b^2 \neq 0$.

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

17. Page 96, 2nd paragraph: It is not immediately obvious that 2^N hashes, on average, are needed to obtain an output that begins with N zeros. Verifying this is a good exercise.

18. Page 135, 2nd paragraph of Section 6.5.2: Change "beak" to "break".

19. Page 154, 2nd line: Change "find-grained" to "fine-grained".

20. Page 179, first line of the last paragraph: Change "since the simply provide" to "since they simply provide".

21. 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)`.

22. Page 203, Problem 1: Change "advantaged" to "advantages".

23. Page 215, Section 9.3.1, second paragraph: Change "Authenticate" to "Authentication".

24. Page 222, Section 9.35, 2nd paragraph, 3rd line: Replace "the efficiency is some other way" with "the efficiency in some other way".

25. Page 224, Figure 9.27: Replace "SYN,ACK" with "SYN-ACK".

26. Page 225, Figure 9.28: Replace "SYN,ACK" with "SYN-ACK".

27. Page 259, first paragraph, 6th line: Replace "a call to the the" with "a call to the".