0.1 Problems

1. Among the fundamental challenges in information security are confidentiality, integrity, and availability, or CIA.

   a. Define each of these terms: confidentiality, integrity, availability.

   b. Give a concrete example where confidentiality is more important than integrity.

   c. Give a concrete example where integrity is more important than confidentiality.

   d. Give a concrete example where availability is the overriding concern.

2. From a bank's perspective, which is usually more important, the integrity of its customer's data or the confidentiality of the data? From the perspective of the bank's customers, which is more important?

3. Instead of an online bank, suppose that Alice provides an online chess playing service known as Alice's Online Chess (AOC). Players, who pay a monthly fee, log into AOC where they are matched with another player of comparable ability.

   a. Where (and why) is confidentiality important for AOC and its customers?

   b. Why is integrity necessary?

   c. Why is availability an important concern?

4. Instead of an online bank, suppose that Alice provides an online chess playing service known as Alice's Online Chess (AOC). Players, who pay a monthly fee, log into AOC where they are matched with another player of comparable ability.

   a. Where should cryptography be used in AOC?

   b. Where should access control used?

   c. Where would security protocols be used?

   d. Is software security a concern for AOC? Why or why not?

5. Some authors distinguish between secrecy, privacy, and confidentiality. In this usage, secrecy is equivalent to our use of the term confidentiality, whereas privacy is secrecy applied to personal data, and

confidentiality (in this misguided sense) refers to an obligation not to divulge certain information.

   a. Discuss a real-world situation where privacy is an important security issue.
   b. Discuss a real-world situation where confidentiality (in this incorrect sense) is a critical security issue.

6. RFID tags are extremely small devices capable of broadcasting a number over the air that can be read by a nearby sensor. RFID tags are used for tracking inventory, and they have many other potential uses. For example, RFID tags are used in passports and it has been suggested that they should be put into paper money to prevent counterfeiting. In the future, a person might be surrounded by a cloud of RFID numbers that would provide a great deal of information about the person.

   a. Discuss some privacy concerns related to the widespread use of RFID tags.
   b. Discuss security issues, other than privacy, that might arise due to the widespread use of RFID tags.

7. Cryptography is sometimes said to be brittle, in the sense that it can be very strong, but when it breaks, it (generally) completely shatters. In contrast, some security features can "bend" without breaking completely—security may be lost as a result of the bending, but some useful level of security remains.

   a. Other than cryptography, give an example where security is brittle.
   b. Provide an example where security is not brittle, that is, the security can bend without completely breaking.

8. Read Diffie and Hellman's classic paper [90].

   a. Briefly summarize the paper.
   b. Diffie and Hellman give a system for distributing keys over an insecure channel (see Section 3 of the paper). How does this system work?
   c. Diffie and Hellman also conjecture that a "one way compiler" might be used to construct a public key cryptosystem. Do you believe this is a plausible approach? Why or why not?

9. The most famous World War II cipher machine was the German Enigma (see also Problem 10).

   a. Draw a diagram illustrating the inner workings of the Enigma.

   b. The Enigma was broken by the Allies and intelligence gained from Enigma intercepts was invaluable. Discuss a significant World War II event where broken Enigma messages played a major role.

10. The German Enigma is the most famous World War II cipher machine (see also Problem 9). The cipher was broken by the Allies and intelligence gained from Enigma messages proved invaluable. At first, the Allies were very careful when using the information gained from broken Enigma messages—sometimes the Allies did not use information that could have given them an advantage. Later in the war, however, the Allies (in particular, the Americans) were much less careful, and they tended to use virtually all information obtained from broken Enigma messages.

    a. The Allies were cautious about using information gained from broken Enigma messages for fear that the Germans would realize the cipher was broken. Discuss two different approaches that the Germans might have taken if they had realized that the Enigma was broken.

    b. At some point in the war, it should have become obvious to the Germans that the Enigma was broken, yet the Enigma was used until the end of the war. Why did the Nazis continue to use the Enigma?

11. When you want to authenticate yourself to your computer, most likely you type in your username and password. The username is considered public knowledge, so it is the password that authenticates you. Your password is something you know.

    a. It is also possible to authenticate based on something you are, that is, a physical characteristic. Such a characteristic is known as a biometric. Give an example of biometric-based authentication.

    b. It is also possible to authenticate based on something you have, that is, something in your possession. Give an example of authentication based on something you have.

c. Two-factor authentication requires that two of the three authentication methods (something you know, something you have, something you are) be used. Give an example from everyday life where two-factor authentication is used. Which two of the three are used?

12. CAPTCHAs [319] are often used in an attempt to restrict access to humans (as opposed to automated processes).

    a. Give a real-world example where you were required to solve a CAPTCHA to gain access to some resource. What do you have to do to solve the CAPTCHA?

    b. Discuss various technical methods that might be used to break the CAPTCHA you described in part a.

    c. Outline a non-technical method that might be used to attack the CAPTCHA from part a.

    d. How effective is the CAPTCHA in part a? How user-friendly is the CAPTCHA?

    e. Why do you hate CAPTCHAs?

13. Suppose that a particular security protocol is well designed and secure. However, there is a fairly common situation where insufficient information is available to complete the security protocol. In such cases, the protocol fails and, ideally, a transaction between the participants, say, Alice and Bob, should not be allowed to occur. However, in the real world, protocol designers must decide how to handle cases where protocols fail. As a practical matter, both security and convenience must be considered. Comment on the relative merits of each of the following solutions to protocol failure. Be sure to consider both the relative security and user-friendliness of each.

    a. When the protocol fails, a brief warning is given to Alice and Bob, but the transaction continues as if the protocol had succeeded, without any intervention required from either Alice or Bob.

    b. When the protocol fails, a warning is given to Alice and she decides (by clicking a checkbox) whether the transaction should continue or not.

    c. When the protocol fails, a notification is given to Alice and Bob and the transaction terminates.

   d. When the protocol fails, the transaction terminates with no explanation given to Alice or Bob.

14. Automatic teller machines (ATMs) are an interesting case study in security. Anderson [14] claims that when ATMs were first developed, most attention was paid to high-tech attacks. However, most real-world attacks on ATMs have been decidedly low tech.

    a. Examples of high-tech attacks on ATMs would be breaking the encryption or authentication protocol. If possible, find a real-world case where a high-tech attack on an ATM has actually occurred and provide the details.
    b. Shoulder surfing is an example of a low-tech attack. In this scenario, Trudy stands behind Alice in line and watches the numbers Alice presses when entering her PIN. Then Trudy bonks Alice in the head and takes her ATM card. Give another example of a low-tech attack on an ATM that has actually occurred.

15. Large and complex software systems invariably have a large number of bugs.

    a. For honest users, such as Alice and Bob, buggy software is certainly annoying but why is it a security issue?
    b. Why does Trudy love buggy software?
    c. In general terms, how might Trudy use bugs in software to break the security of a system?

16. Malware is software that is intentionally malicious, in the sense that it is designed to do damage or break the security of a system. Malware comes in many familiar varieties, including viruses, worms, and Trojans.

    a. Has your computer ever been infected with malware? If so, what did the malware do and how did you get rid of the problem? If not, why have you been so lucky?
    b. In the past, most malware was designed to annoy users. Today, it is often claimed that most malware is written for profit. How could malware possibly be profitable?

17. In the movie *Office Space* [223], software developers attempt to modify company software so that for each financial transaction, any leftover

fraction of a cent goes to the developers, instead of going to the company. The idea is that for any particular transaction, nobody will notice the missing fraction of a cent, but over time the developers will accumulate a large sum of money. This type of attack is sometimes known as a salami attack.

a. Find a real-world example of a salami attack.

b. In the movie, the salami attack fails. Why?

18. Some commercial software is closed source, meaning that the source code is not available to users. On the other hand, some software is open source, meaning that the source code is available to users.

    a. Give an example of software that you use (or have used) that is closed source.

    b. Give an example of software that you use (or have used) that is open source.

    c. For open source software, what can Trudy do to search for security flaws in the software?

    d. For closed source software, what can Trudy do to search for security flaws in the software?

    e. For open source software, what can Alice do to make the software more secure?

    f. For closed source software, what can Alice do to make the software more secure?

    g. Which is inherently more secure, open source software or closed source software? Why?

19. It's sometimes said that complexity is the enemy of security.

    a. Give an example of commercial software to which this statement applies, that is, find an example of software that is large and complex and has had significant security problems.

    b. Find an example of a security protocol to which this statement applies.

20. Suppose that this textbook was sold online (as a PDF) by your money-grubbing author for, say, $5. Then the author would make more money off of each copy sold than he currently does[1] and people who purchase the book would save a lot of money.

[1] Believe it or not.

a. What are the security issues related to the sale of an online book?

b. How could you make the selling of an online book more secure, from the copyright holder's perspective?

c. How secure is your approach in part b? What are some possible attacks on your proposed system?

21. The PowerPoint slides at [255] describe a security class project where students successfully hacked the Boston subway system.

a. Summarize each of the various attacks. What was the crucial vulnerability that enabled each attack to succeed?

b. The students planned to give a presentation at the self-proclaimed "hacker's convention," Defcon 16 [80], where they would have presented the PowerPoint slides now available at [255]. At the request of the Boston transit authority, a judge issued a temporary restraining order (since lifted) that prevented the students from talking about their work. Do you think this was justified, based on the material in the slides?

c. What are war dialing and war driving? What is war carting?

d. Comment on the production quality of the "melodramatic video about the warcart" (a link to the video can be found at [16]).

Annotated Bibliography

[1] 3GPP home page, at www.3gpp.org/
Cited on page ??

[2] @stake LC 5, at en.wikipedia.org/wiki/@stake
Cited on page ??

- Prior to being acquired by Symantec, @stake was a leading security company. At one time they made news for supposedly firing a top-notch security expert for his implicit criticism of Microsoft (see, for example, dc.internet.com/news/article.php/3083901).

[3] M. Abadi and R. Needham, Prudent engineering practice for cryptographic protocols, *IEEE Transactions on Software Engineering*, Vol. 22, No. 1, pp. 6–15, January 1996.
Cited on page ??

[4] E. Aboufadel, Work by the Poles to break the Enigma codes, at faculty.gvsu.edu/aboufade/web/enigma/polish.htm
Cited on page ??

- A brief description of the brilliant work by the Polish cryptanalysts.

[5] Access control matrix, at en.wikipedia.org/wiki/Access_Control_Matrix
Cited on page ??

[6] E. Ackerman, Student skirts CD's piracy guard, SiliconValley.com, at technews.acm.org/articles/2003-5/1008w.html#item2
Cited on page ??

- The classic "hold down the shift key" attack on a DRM system.

[7] AES algorithm (Rijndael) information, at
`csrc.nist.gov/archive/aes/index1.html`
Cited on page **??**

- A good place to tap into the wealth of information available on Rijndael and the AES.

[8] Aleph One, Smashing the stack for fun and profit, *Phrack*, Volume Seven, Issue Forty-Nine, File 14 of 16, at
`www.phrack.com/issues.html?issue=49&id=14&mode=txt`
Cited on page **??**

- The first widely available and hacker-friendly source of information on buffer overflow attacks.

[9] D. Anderson, T. Frivold, and A. Valdes, Next-generation intrusion detection expert system (NIDES): summary, at
`citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.121.5956`
Cited on page **??**

- This is one in a series of papers about NIDES.

[10] R. Anderson and E. Biham, Tiger: a fast new hash function, at
`www.cs.technion.ac.il/~biham/Reports/Tiger/`
Cited on pages **??** and **??**

- Two crypto experts present the details of their hash function.

[11] R. J. Anderson and M. G. Kuhn, Improved differential fault analysis, at `jya.com/akdfa.txt`
Cited on page **??**

- Along with most other security topics under the sun, Ross Anderson is an expert on side channel attacks.

[12] R. Anderson, Security in Open versus Closed Systems — The Dance of Boltzmann, Coase and Moore, at
`www.cl.cam.ac.uk/~rja14/Papers/toulouse.pdf`
Cited on pages **??** and **??**

- This paper gives an interesting and fairly elementary argument that—from a security perspective—there's no significant difference between open and closed source software. This is Ross Anderson at his best.

[13] R. Anderson, TCPA/Palladium frequently asked questions, at `www.cl.cam.ac.uk/~rja14/tcpa-faq.html`
Cited on pages **??**, **??**, and **??**

[14] R. Anderson, *Security Engineering*, Wiley, 2001, at `www.cl.cam.ac.uk/~rja14/book.html`
Cited on pages **??**, 5, **??**, **??**, **??**, **??**, **??**, **??**, **??**, **??**, **??**, **??**, **??**, **??**, **??**, **??**, **??**, and **??**

- Ross Anderson is the reigning God of information security and this book is his Bible. For the nitty-gritty details, you'll have to go elsewhere, but for the big picture, this is very good. There is also a second edition that covers some new ground. However, this first edition is available for free at the given link.

[15] R. Anderson, *Security Engineering* Errata, at `www.cl.cam.ac.uk/~rja14/errata.html`
Cited on page **??**

- This is worth reading just for Anderson's description of the publishing process. Here you'll also learn (among other things) that the MiG-in-the-middle attack never actually occurred.

[16] Z. Anderson, Warcart, at `web.mit.edu/zacka/www/warcart.html`
Cited on page 7

[17] W. A. Arbaugh, N. Shankar, and Y. C. J. Wan, Your 802.11 wireless network has no clothes, at `www.cs.umd.edu/~waa/wireless.pdf`
Cited on page **??**

- Well-written description of the many security flaws in 802.11.

[18] G. Arboit, A method for watermarking Java programs via opaque predicates, at `crypto.cs.mcgill.ca/~garboit/sp-paper.pdf`
Cited on page **??**

[19] D. Aucsmith, Tamper resistant software: an implementation, *Proceedings of the First International Information Hiding Workshop, Lecture Notes in Computer Science 1174*, Springer-Verlag, Cambridge, UK, pp. 317–334, 1996.
Cited on pages **??** and 43

- Difficult to read and impossible for mere mortals like myself to comprehend. I challenge anyone to make sense of this, even with Aucsmith's patent as backup.

[20] Audacity, The free, cross-platform sound editor, at `audacity.sourceforge.net/`
Cited on page **??**

[21] J. Aycock, *Computer Viruses and Malware*, Advances in Information Security, Vol. 22, Springer-Verlag, 2006.
Cited on page **??**

- A well-written, humorous, and easily accessible introduction to malware.

[22] J. Aycock, *Spyware and Adware*, Springer-Verlag, 2010.
Cited on pages **??** and **??**

- Another excellent malware book from John Aycock.

[23] D. V. Bailey, Inside eBook security, *Dr. Dobb's Journal*, November 2001, at `www.drdobbs.com/184404845`
Cited on page **??**

- The weakness of eBook security is exposed.

[24] I. Balepin, Superworms and cryptovirology: a deadly combination, at `wwwcsif.cs.ucdavis.edu/~balepin/files/worms-cryptovirology.pdf`
Cited on page **??**

- The future of malware is considered.

[25] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan and K. Yang, On the (im)possibility of obfuscating programs (extended abstract), in J. Kilian, editor, Advances in Cryptology – CRYPTO 2001, Lecture Notes in Computer Science 2139, at `www.iacr.org/archive/crypto2001/21390001.pdf`
Cited on page **??**

- This paper created quite a stir when published. The upshot is that, in some sense, obfuscation can probably never "really" be secure. There is some debate as to whether the model used is realistic, and what "really" really means.

[26] E. Barkan, E. Biham, and N. Keller, Instant ciphertext-only cryptanalysis of GSM encrypted communication, at
`cryptome.org/gsm-crack-bbk.pdf`
Cited on page **??**

- Attacks on the GSM protocol as well as attacks on A5/2 and A5/1.

[27] M. Barrett and C. Thomborson, Using NGSCB to mitigate existing software threats, at `www.cs.auckland.ac.nz/~cthombor/Pubs/cses.pdf`
Cited on pages **??** and **??**

[28] BBC News, Afghan girl found after 17 years, at
`news.bbc.co.uk/1/hi/world/south_asia/1870382.stm`
Cited on page **??**

[29] Beale Screamer, Microsoft's digital rights management scheme—technical details, at
`web.elastic.org/~fche/mirrors/cryptome.org/beale-sci-crypt.htm`
Cited on pages **??** and **??**

- Interesting and well written, at least by hacker standards.

[30] D. J. Bernstein, The IPv6 mess, at `cr.yp.to/djbdns/ipv6mess.html`
Cited on page **??**

[31] P. Biddle et al., The darknet and the future of content distribution, at
`crypto.stanford.edu/DRM2002/darknet5.doc`
Cited on page **??**

- A true classic. Anyone interested in DRM must read this.

[32] Biometrics comparison chart, at
`ctl.ncsc.dni.us/biomet%20web/BMCompare.html`
Cited on page **??**

[33] A. Biryukov, A. Shamir, and D. Wagner, Real time cryptanalysis of A5/1 on a PC, at
`home.in.tum.de/~gerold/KryptDokumente/a5_Angriff/a51-bsw.htm`
Cited on pages **??** and **??**

- An efficient attack on A5/1 that requires huge amounts of storage.

[34] M. Bishop, *Computer Security: Art and Science*, Addison Wesley, 2003.
Cited on pages **??** and **??**

- In my humble opinion, this book often crosses the line into the realm of theory for the sake of theory. The book is definitely not an easy read. The best sections are those on topics that are theoretical by their very nature. For example, the discussion of security modeling is excellent.

[35] I. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press, 2000.
Cited on page **??**

- The mathematical results are all there but without the proofs.

[36] blexim, Basic Integer Overflows, *Phrack Magazine*, Volume `0x0b`, Issue `0x3c`, Phile #`0x0a` of `0x10`, at
`www.phrack.com/issues.html?issue=60&id=10`
Cited on page **??**

[37] L. Boettger, The Morris worm: how it affected computer security and lessons learned by it, at
`hackersnews.org/hackerhistory/morrisworm.html`
Cited on page **??**

[38] N. Borisov, I. Goldberg, and D. Wagner, Intercepting mobile communications: the insecurity of 802.11, at
`www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf`
Cited on pages **??** and **??**

- A good source for information concerning the many flaws of WEP.

[39] Botnet, at `en.wikipedia.org/wiki/Botnet`
Cited on page **??**

[40] J. Bowen, Formal methods, *The World Wide Web Virtual Library*, at
`formalmethods.wikia.com/wiki/Jonathan_Bowen`
Cited on page **??**

[41] D. Brumley and D. Boneh, Remote timing attacks are practical, at
`crypto.stanford.edu/~dabo/papers/ssl-timing.pdf`
Cited on pages **??** and **??**

- A nice paper describing a side-channel attack on the RSA implementation in OpenSSL.

[42] S. Budiansky, *Battle of Wits: The Complete Story of Codebreaking in World War II*, The Free Press, 2000.
Cited on page **??**

- An excellent and highly readable book. The historical accuracy is first rate, and the author has good insight into both the technical aspects and the human side of intelligence gathering. My only quibble is that the subtitle is somewhat misleading, since the focus is clearly on the Enigma and the British.

[43] D. M. Burton, *Elementary Number Theory*, fourth edition, Wm. C. Brown, 1998.
Cited on pages **??**, **??**, **??**, and **??**

[44] Cafebabe bytecode editor, at
`cafebabe.sourceforge.net/index.html`
Cited on page **??**

- If you want to see just how easy it is to reverse engineer a Java program, try this tool on your favorite `class` file.

[45] K. W. Campbell and M. J. Wiener, DES is not a group, *Advances in Cryptology*, CRYPTO '92, Springer-Verlag, 1993, pp. 512–520.
Cited on page **??**

- Definitive proof—though late in coming—that triple DES really is more secure than single DES.

[46] P. Capitant, Software tamper-proofing deployed 2-year anniversary report, Macrovision Corporation, at
`www.cs.sjsu.edu/faculty/stamp/DRM/`
`DRM%20papers/Software_Tamper-Proofing.ppt`
Cited on page **??**

- Some good information on DRM techniques, based on real-world experiences.

[47] CAPTCHA, at
`en.wikipedia.org/wiki/CAPTCHA`
Cited on page **??**

[48] A. Carlson, Simulating the Enigma cypher machine, at
`homepages.tesco.net/~andycarlson/enigma/simulating_enigma.html`
Cited on page **??**

- Describes the double stepping well.

[49] J. Carr, Strategies & issues: thwarting insider attacks, *Network Magazine*, September 4, 2002.
Cited on page **??**

[50] L. Carroll, *Alice's Adventures in Wonderland*, at
`www.sabian.org/alice.htm`
Cited on page **??**

[51] CERT coordination center, at `www.cert.org/`
Cited on page **??**

[52] Certicom Corporation, Certicom ECC Challenge, November 1997, at
`www.certicom.com/index.php/the-certicom-ecc-challenge`
Cited on page **??**

[53] P. Červeň, *Crackproof Your Software: Protect Your Software Against Crackers*, No Starch Press, 2002.
Cited on page **??**

- Easily the best available book for information on anti-disassembly and anti-debugging techniques. A new edition would be valuable since the material is heavily focused on Windows 98.

[54] H. Chang and M. J. Atallah, Protecting software code by guards, *Workshop on Security and Privacy in Digital Rights Management 2001.*
Cited on pages **??** and 27

- Surprisingly similar to the paper [145], which was presented at the same conference.

[55] G. Chapman et al., *The Complete Monty Python's Flying Circus: All the Words*, vols. 1 and 2, Pantheon, 1989.
Cited on pages **??** and **??**

[56] K. Chellapilla, K. Larson, P. Simard, and M. Czerwinski, Computers beat Humans at Single Character Recognition in Reading based Human Interaction Proofs (HIPs), Microsoft Research, at

www.ceas.cc/2005/papers/160.pdf
Cited on pages **??** and **??**

- A very interesting paper that shows that computers are better than humans at solving all of the basic visual CAPTCHA/HIP problems, with the exception of the segmentation problem. The obvious implication is that a strong CAPTCHA must rely primarily on the segmentation problem for its security.

[57] T. Cipresso, Software Reverse Engineering Education, Master's Thesis, Department of Computer Science, San Jose State University, 2009, at
reversingproject.info/
Cited on pages **??** and **??**

- An excellent overview of the uses of SRE (both good and bad), along with several detailed examples (with complete, animated solutions). I've used these examples as the basis for a software reverse engineering course, and they are also ideal for self-study.

[58] T. Cipresso, Java bytecode anti-reversing exercise, at
reversingproject.info/?page_id=65
Cited on page **??**

[59] Clipper chip, at en.wikipedia.org/wiki/Clipper_chip
Cited on page **??**

[60] F. B. Cohen, Experiments with computer viruses, 1984, at
www.all.net/books/virus/part5.html
Cited on page **??**

- Discussion of early virus experiments by the father of the computer virus.

[61] F. B. Cohen, Operating system protection through program evolution, at all.net/books/IP/evolve.html
Cited on pages **??** and **??**

- A fascinating idea, that has implications far beyond operating systems.

[62] F. B. Cohen, *A Short Course on Computer Viruses*, second edition, Wiley, 1994.
Cited on page **??**

- A nice book, but the material is dated.

[63] C. Collberg, SandMark: a tool for the study of software protection mechanisms, at `sandmark.cs.arizona.edu/`
Cited on page **??**

[64] C. S. Collberg and C. Thomborson, Watermarking, tamper-proofing and obfuscation—tools for software protection, *IEEE Transactions on Software Engineering*, Vol. 28, No. 8, August 2002.
Cited on page **??**

- These authors are the originators of most of the sophisticated methods of software obfuscation.

[65] Common Criteria — The Common Criteria portal, at
`www.commoncriteriaportal.org/`
Cited on page **??**

[66] Computer Knowledge, Virus tutorial, at
`www.cknow.com/cms/vtutor/cknow-virus-tutorial.html`
Cited on page **??**

- A wide ranging and fairly thorough discussion of many issues related to malware. Robert Slade's history of viruses—which is current up to about the year 2000—is included.

[67] M. Cooney, IBM touts encryption innovation: New technology performs calculations on encrypted data without decrypting it, *ComputerWorld*, June 25, 2009, at
`www.computerworld.com/action/article.do?command=viewArticle`
`Basic&articleId=9134823&source=CTWNLE_nlt_security_2009-06-25`
Cited on page **??**

[68] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities, *Journal of Cryptology*, Vol. 10, 1997, pp. 233–260.
Cited on page **??**

[69] Coventry blitz, at `en.wikipedia.org/wiki/Coventry_Blitz`
Cited on page **??**

[70] S. Craver, The underhanded C contest, at
`underhanded.xcott.com/`
Cited on page **??**

- An amusing contest with some incredible examples of innocent-looking code doing malicious things.

[71] S. A. Craver et. al., Reading between the lines: lessons learned from the SDMI challenge, *Proceedings of the 10th USENIX Security Symposium*, Washington, DC, August 13–17, 2001, at
`www.usenix.org/events/sec01/craver.pdf`
Cited on pages **??**, **??**, and **??**

- One of the best security papers you'll ever read. The authors demolish the security of the proposed SDMI system. If you think watermarking is easy, or if you're tempted to ignore Kerckhoffs' Principle, you'll change your mind after reading this.

[72] R. X. Cringely, Calm before the storm, at
`www.pbs.org/cringely/pulpit/2001/pulpit_20010730_000422.html`
Cited on page **??**

[73] Cryptographer's Panel, RSA Conference 2002, at
`www.cs.sjsu.edu/~stamp/cv/tripreports/RSA2002.html`
Cited on page **??**

[74] Cryptographer's Panel, RSA Conference 2004, at
`www.cs.sjsu.edu/~stamp/cv/tripreports/RSA04.html`
Cited on pages **??**, **??**, and **??**

[75] J. Daemen and V. Rijmen, The Rijndael block cipher, at
`csrc.nist.gov/archive/aes/index.html`
Cited on page **??**

[76] J. Daugman, How iris recognition works, at
`www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf`
Cited on page **??**

[77] D. Davis, Defective sign & encrypt in S/MIME, PKCS#7, MOSS, PEM, PGP, and XML, at
`world.std.com/~dtd/sign_encrypt/sign_encrypt7.html`
Cited on page **??**

[78] E. X. DeJesus, SAML brings security to XML, *XML Magazine*, Volume 3, No. 1, January 11, 2002, pp. 35–37.
Cited on page **??**

[79] Defcon 11, at www.cs.sjsu.edu/~stamp/cv/tripreports/defcon11.html
Cited on pages ??, ??, ??, and ??

- My “trip report” about Defcon 11.

[80] Defcon 16, at www.defcon.org/html/defcon-16/dc-16-post.html
Cited on page 7

[81] Definition of John Anthony Walker, at
www.wordiq.com/definition/John_Anthony_Walker
Cited on page ??

[82] Definition of Purple code, at www.wordiq.com/definition/Purple_code
Cited on page ??

[83] Definition of Zimmermann Telegram, at
www.wordiq.com/definition/Zimmermann_Telegram
Cited on page ??

[84] M. Delio, Linux: fewer bugs than rivals, *Wired*, December 2004, at
www.wired.com/software/coolapps/news/2004/12/66022
Cited on page ??

[85] D. E. Denning and D. K. Branstad, A taxonomy for key escrow encryption systems, *Communications of the ACM*, Vol. 39, No. 3, March 1996, at
www.cosc.georgetown.edu/~denning/crypto/Taxonomy.html
Cited on page ??

[86] D. E. Denning, Descriptions of key escrow systems, at
www.cosc.georgetown.edu/~denning/crypto/Appendix.html
Cited on page ??

[87] Denver International Airport, at
en.wikipedia.org/wiki/Denver_International_Airport
Cited on page ??

[88] Y. Desmedt, What happened with knapsack cryptographic schemes?, *Performance Limits in Communication, Theory and Practice*, J. K. Skwirzynski, ed., Kluwer, pp. 113–134, 1988.
Cited on page ??

[89] J. F. Dhem et. al., A practical implementation of the timing attack, at

www.cs.jhu.edu/~fabian/courses/CS600.624/Timing-full.pdf
Cited on page ??

[90] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, Vol. IT–22, No. 6, pp. 644–654, November 1976, at
www.cs.jhu.edu/~rubin/courses/sp03/papers/diffie.hellman.pdf
Cited on pages **??**, **??**, and 35

- Diffie and Hellman's classic paper, where they argue (correctly, as it turned out) that public key cryptography is possible.

[91] DI Management, RSA Algorithm, at
www.di-mgt.com.au/rsa_alg.html#pkcs1schemes
Cited on page **??**

[92] I. Dubrawsky, Effects of Internet worms on routing, RSA Conference 2004, at
www.cs.sjsu.edu/faculty/stamp/cv/tripreports/RSA04.html
Cited on page **??**

[93] I. Dubrawsky and L. Hayden, Wireless LANs and privacy, at
www.isoc.org/inet2002/inet-technologyprogram.shtml
Cited on page **??**

[94] D. Dumars, Stephen King's The Plant withers, at
www.mania.com/stephen-kings-plant-withers_article_26476.html
Cited on page **??**

[95] J. E. Dunn, Encrypted image backups open to new attack, *Techworld*, October 2008, at
www.techworld.com/security/news/index.cfm?newsid=105263
Cited on page **??**

[96] P. Earley, Family of spies: The John Walker Jr. spy case, *The Crime Library*, at www.crimelibrary.com/spies/walker/
Cited on page **??**

[97] Easy solution to bypass latest CD-audio protection, at
www.cdfreaks.com/news/4068
Cited on page **??**

- The classic "felt-tip pen" attack.

[98] EFF DES cracker, at
`en.wikipedia.org/wiki/EFF_DES_cracker`
Cited on page **??**

[99] E. Eilam, *Reversing: Secrets of Reverse Engineering*, Wiley, 2005.
Cited on pages **??**, **??**, 27, and 38

- The best book available on reversing—at least until your humble author finishes his reverse engineering textbook...

[100] G. Ellison, J. Hodges, and S. Landau, Risks presented by single sign-on architectures, October 18, 2002, at
`research.sun.com/liberty/RPSSOA/`
Cited on page **??**

[101] C. Ellison and B. Schneier, Ten risks of PKI: what you're not being told about public key infrastructure, *Computer Security Journal*, Vol. 16, No. 1, pp. 1–7, 2000, at `www.schneier.com/paper-pki.html`
Cited on page **??**

[102] P. England et. al., A trusted open platform, *IEEE Computer*, pp. 55–62, July 2003.
Cited on page **??**

- A general description of NGSCB/TCG at an early stage in its development.

[103] A. C. Engst, Mac OS X trojan technique: beware of geeks bearing gifts, *TidBITS*, No. 726, April 2004, at
`db.tidbits.com/getbits.acgi?tbart=07636`
Cited on pages **??** and 29

- A proof-of-concept trojan for the Mac. See [160] for additional context.

[104] Enigma machine, at `en.wikipedia.org/wiki/Enigma_machine`
Cited on pages **??** and **??**

[105] U. Erlingsson, Y. Younan, and F. Piessens, Low-level Software Security by Example, to appear in *Handbook of Communications Security*, Springer-Verlag, 2009.
Cited on page **??**

- An excellent survey of low-level software vulnerabilities and defenses.

[106] Evaluation assurance level, at
`en.wikipedia.org/wiki/Evaluation_Assurance_Level`
Cited on page **??**

[107] D. B. Everett, Trusted computing platforms, at
`www.netproject.com/presentations/TCPA/david_everett.pdf`
Cited on page **??**

[108] Exploit Systems, Inc., at `www.exploitsystems.com/`
Cited on page **??**

- An unsuccessful—yet clever—approach to making money from the pirates who inhabit peer-to-peer networks.

[109] W. Feller, *An Introduction to Probability Theory and Its Applications*, third edition, Wiley, 1968.
Cited on page **??**

- The best source for information on discrete probability.

[110] Fernflower — Java Decompiler, at
`www.reversed-java.com/fernflower/`
Cited on page **??**

[111] U. Fiege, A. Fiat, and A. Shamir, Zero knowledge proofs of identity, *Proceedings of the Nineteenth Annual ACM Conference on Theory of Computing*, pp. 210–217, 1987.
Cited on page **??**

[112] S. Fluhrer, I. Mantin and A. Shamir, Weaknesses in the key scheduling algorithm of RC4, at `www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf`
Cited on pages **??**, **??**, **??**, **??**, **??**, 34, and 50

- Several attacks on RC4 are discussed, including a devastating attack on the encryption in WEP. This paper suffers from some typos and a lack of detail. See Mantin's thesis [195] for a more readable and complete version.

[113] B. A. Forouzan, *TCP/IP Protocol Suite*, second edition, McGraw Hill, 2003.
Cited on page **??**

- Forouzan has digested the relevant RFCs and provides the important points in a readable form—no mean feat.

[114] S. Forrest, S. A. Hofmeyr, and A. Somayaji, Computer immunology, *Communications of the ACM*, Vol. 40, No. 10, pp. 88–96, October 1997.
Cited on page **??**

- A somewhat “far out” view of the role that biological analogies can play in security.

[115] S. Forrest, A. Somayaji, and D. H. Ackley, Building diverse computer systems, at `www.cs.unm.edu/~forrest/publications/hotos-97.pdf`
Cited on page **??**

[116] L. Fraim, SCOMP: A solution to the multilevel security problem, *IEEE Computer*, pp. 26–34, July 1983.
Cited on page **??**

- One of the few serious attempts to develop a trusted operating system.

[117] J. Fraleigh, *A First Course in Abstract Algebra*, Addison Wesley, seventh edition, 2002.
Cited on page **??**

[118] K. Gaj and A. Orlowski, Facts and myths of Enigma: breaking stereotypes, at
`ece.gmu.edu/courses/ECE543/viewgraphs_F03/EUROCRYPT_2003.pdf`
Cited on page **??**

[119] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP–Completeness*, W. H. Freeman & Company, 1979.
Cited on page **??**

[120] B. Gates, Keynote address, RSA Conference 2004, at
`www.cs.sjsu.edu/faculty/stamp/cv/tripreports/RSA04.html`
Cited on page **??**

[121] D. Geer, comments from “Who will kill online privacy first—the lawyers or the techies?”, at
`www.cs.sjsu.edu/~stamp/cv/tripreports/RSA2002.html`
Cited on page **??**

[122] W. W. Gibbs, Software's chronic crisis, Trends in Computing, *Scientific American*, September 1994, p. 86, at
`www.cis.gsu.edu/~mmoore/CIS3300/handouts/SciAmSept1994.html`
Cited on page **??**

[123] R. Glenn and S. Kent, RFC 2410 — The NULL encryption algorithm and its use with IPsec, at `www.faqs.org/rfcs/rfc2410.html`
Cited on page **??**

- Good nerdy humor.

[124] D. B. Glover, *Secret Ciphers of the 1876 Presidential Election*, Aegean Park Press, 1991.
Cited on page **??**

[125] D. Gollmann, *Computer Security*, Wiley, 1999.
Cited on page **??**

- A fairly theoretical treatment of most topics. Includes an excellent discussion of security modeling.

[126] S. W. Golomb, *Shift Register Sequences*, Aegean Park Press, 1982.
Cited on page **??**

[127] D. Goodin, Buggy 'smart meters' open door to power-grid botnet: Grid-burrowing worm only the beginning, *The Register*, at
`www.theregister.co.uk/2009/06/12/smart_grid_security_risks/`
Cited on page **??**

[128] S. Goodwin, Internet gambling software flaw discovered by Reliable Software Technologies software security group, at
`www.cigital.com/news/index.php?pg=art&artid=20`
Cited on page **??**

- A nice description of an attack on an online version of Texas hold 'em poker.

[129] E. Grevstad, CPU-based security: the NX bit, at
`hardware.earthweb.com/chips/article.php/3358421`
Cited on page **??**

[130] GSM cloning, at `www.isaac.cs.berkeley.edu/isaac/gsm.html`
Cited on page **??**

[131] A guide to understanding covert channel capacity analysis of a trusted system, National computer security center, November 1993, at
`www.fas.org/irp/nsa/rainbow/tg030.htm`
Cited on pages **??** and **??**

[132] A guide to understanding data remanence in automated information systems, NCSC–TG–025, at
`www.cerberussystems.com/INFOSEC/stds/ncsctg25.htm`
Cited on page **??**

[133] B. Guignard, How secure is PDF?, at
`www-2.cs.cmu.edu/~dst/Adobe/Gallery/PDFsecurity.pdf`
Cited on page **??**

- A brief explanation of the ElcomSoft utility to remove PDF security. Correctly concludes that "your encrypted PDF files offer about as much strength as dried egg shells!"

[134] E. Guisado, Secure random numbers, at
`erngui.com/articles/rng/index.html`
Cited on page **??**

[135] A. Guthrie, "Alice's Restaurant," lyrics at
`www.arlo.net/lyrics/alices.shtml`
Cited on page **??**

[136] Hacker may be posing as Microsoft, *USA Today*, February 6, 2002, at
`www.usatoday.com/tech/techinvestor/2001-03-22-microsoft.htm`
Cited on page **??**

- Discusses a Microsoft certificate that went astray.

[137] D. Hamer, Enigma: actions involved in the 'double-stepping' of the middle rotor, *Cryptologia*, Vol. 21, No. 1, January 1997, pp. 47–50, at
`www.eclipse.net/~dhamer/downloads/rotorpdf.zip`
Cited on page **??**

[138] Hand based biometrics, *Biometric Technology Today*, pp. 9–11, July & August 2003.
Cited on page **??**

[139] N. Hardy, The confused deputy (or why capabilities might have been invented), at

`www.skyhunter.com/marcs/capabilityIntro/confudep.html`
Cited on page **??**

- This paper is itself confusing, but it's worth understanding.

[140] D. Harkins and D. Carrel, RFC 2409 — The Internet key exchange (IKE), at `www.faqs.org/rfcs/rfc2409.html`
Cited on page **??**

[141] B. Harris, Visual cryptography, two levels, personal correspondence.
Cited on page **??**

[142] History of GSM, at `www.cellular.co.za/gsmhistory.htm`
Cited on page **??**

[143] G. Hoglund and G. McGraw, *Exploiting Software*, Addison Wesley, 2004.
Cited on pages **??**, **??**, and 29

- In spite of some good reviews, this book is, in your author's humble opinion, not on par with Kaspersky's book [161] or Eilam's fine book [99].

[144] J. J. Holt and J. W. Jones, Discovering number theory, Section 9.4: Going farther: RSA, at
`www.math.mtu.edu/mathlab/COURSES/holt/dnt/phi4.html`
Cited on page **??**

- A small part of an excellent set of number theory notes—all available online.

[145] B. Horne et, al., Dynamic self-checking techniques for improved tamper resistance, *Workshop on Security and Privacy in Digital Rights Management 2001.*
Cited on pages **??** and 16

- Very similar to the "guards" paper [54]. Interestingly, both papers were presented at the same conference and both are undoubtedly patented.

[146] HotBots '07, USENIX first workshop on hot topics in understanding botnets, at `www.usenix.org/event/hotbots07/tech/`
Cited on page **??**

[147] IDA Pro disassembler, at www.hex-rays.com/idapro/
Cited on page **??**

- The best disassembler in the known universe, it also includes a good debugger.

[148] Index of Coincidence, Wikipedia, at
en.wikipedia.org/wiki/Index_of_coincidence
Cited on page **??**

[149] Iridian Technologies, Iris recognition: science behind the technology, at
www.l1id.com/pages/383-science-behind-the-technology
Cited on pages **??** and **??**

[150] D. Isbell, M. Hardin, and J. Underwood, Mars climate team finds likely cause of loss, at
science.ksc.nasa.gov/mars/msp98/news/mco990930.html
Cited on page **??**

[151] A. Jain, L. Hong, and S. Pankanti, Biometric Identification, *Communications of the ACM*, Vol. 43, No. 2, pp. 91–98, 2000.
Cited on page **??**

[152] A. Jain, A. Ross, and S. Pankanti, *Proceedings of the 2nd AVBPA Conference*, Washington, DC, March 22–24, pp. 166–171, 1999.
Cited on page **??**

[153] C. J. A. Jansen, *Investigations on Nonlinear Streamcipher Systems: Construction and Evaluation Methods*, PhD thesis, Technical University of Delft, 1989.
Cited on page **??**

- An unusual and hard to find manuscript. Some very difficult research problems are discussed.

[154] D. Jao, Elliptic curve cryptography, in *Handbook of Communication and Information Security*, Springer-Verlag, 2009.
Cited on page **??**

[155] H. S. Javitz and A. Valdes, The NIDES statistical component description and justification.
Cited on page **??**

- One of many NIDES papers available online.

[156] John Gilmore on the EFF DES cracker, at
`www.computer.org/internet/v2n5/w5news-des.htm`
Cited on page **??**

[157] John the Ripper password cracker, at `www.openwall.com/john/`
Cited on page **??**

[158] M. E. Kabay, Salami fraud, *Network World Security Newsletter*, July 24, 2002, at
`www.nwfusion.com/newsletters/sec/2002/01467137.html`
Cited on page **??**

[159] D. Kahn, *The Codebreakers: The Story of Secret Writing*, revised edition, Scribner, 1996.
Cited on pages **??** and **??**

- *The* source for crypto history prior to its original publication date of 1967. Supposedly, it was updated in 1996, but little new information was added.

[160] L. Kahney, OS X trojan horse is a nag, at
`www.wired.com/news/mac/0,2125,63000,00.html?tw=rss.TEK`
Cited on pages **??** and 22

- Additional discussion of this harmless trojan can be found at [103].

[161] K. Kaspersky, *Hacker Disassembling Uncovered*, A-List, 2003.
Cited on pages **??**, **??**, 27, and 38

- A good resource for anyone interested in software reverse engineering. Far superior to [143], although it does suffer somewhat from poor writing, as do most "hacker" publications.

[162] C. Kaufman, R. Perlman, and M. Speciner, *Network Security*, second edition, Prentice Hall, 2002.
Cited on pages **??**, **??**, **??**, **??**, **??**, and **??**

- Excellent coverage of networking protocols as well as good—though brief—coverage of many relevant crypto topics. Chapter 11 alone is worth the price of the book. Overall, the content is consistently first rate, with the possible exception of the IPSec chapters.

[163] J. Kelsey, B. Schneier, and D. Wagner, Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA, *ICICS '97 Proceedings*, Springer-Verlag, November 1997.
Cited on page **??**

[164] A. Kerckhoffs, La cryptographie militaire, *Journal des Sciences Militaires*, Vol. IX, pp. 5–83, January 1883, pp. 161–191, February 1883.
Cited on page **??**

[165] Kerckhoffs' law, at `en.wikipedia.org/wiki/Kerckhoffs'_law`
Cited on page **??**

[166] P. C. Kocher, Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems, at
`www.cryptography.com/resources/whitepapers/TimingAttacks.pdf`
Cited on pages **??**, **??**, and **??**

[167] P. Kocher, J. Jaffe, and B. Jun, Differential power analysis, *Advances in Cryptology — CRYPT0 '99*, Vol. 1666 of Lecture Notes in Computer Science, M. Wiener, editor, Springer-Verlag, pp. 388–397, 1999, at
`www.cryptography.com/resources/whitepapers/DPA.html`
Cited on page **??**

- One of the few papers written by Kocher on side channel attacks. This is curious, since he is clearly a leader in the field.

[168] Kodak research and development, at
`www.kodak.com/US/en/corp/researchDevelopment/worldwide/index.jhtml`
Cited on page **??**

[169] F. Koeune, Some interesting references about LLL, at
`www.dice.ucl.ac.be/~fkoeune/LLL.html`
Cited on page **??**

[170] D. Kopel, Pẽna's new airport still a failure, at
`davekopel.org/Misc/OpEds/op021997.htm`
Cited on page **??**

[171] D. P. Kormann and A. D. Rubin, Risks of the Passport single signon protocol, at `avirubin.com/passport.html`
Cited on page **??**

[172] M. Kotadia, Spammers use free porn to bypass Hotmail protection, *ZD Net UK*, May 6, 2004, at
`news.zdnet.co.uk/internet/security/0,39020375,39153933,00.htm`
Cited on page **??**

[173] J. Koziol et al., *The Shellcoder's Handbook*, Wiley, 2004.
Cited on pages **??** and **??**

- For a long time, there were few books that made any serious attempt to discuss hacking techniques. Of course, hackers knew (or could learn) about such techniques, so this lack of information only hindered the good guys while doing little or nothing to deter the bad guys. Recently, however, there has been a flood of "hacking" books and this book is among the best of the genre.

[174] H. Krawczyk, M. Bellare and R. Canetti, RFC 2104 — HMAC: Keyed-hashing for message authentication, at
`www.faqs.org/rfcs/rfc2104.html`
Cited on page **??**

[175] D. L. Kreher and D. R. Stinson, *Combinatorial Algorithms*, CRC Press, 1999.
Cited on page **??**

- The best available mathematical discussion of the lattice reduction attack on the knapsack. However, be forewarned that this book has many typos, which is death for an algorithms book.

[176] M. Kuhn, Security—biometric identification, at
`www.cl.cam.ac.uk/Teaching/2003/Security/guestslides/`
`slides-biometric-4up.pdf`
Cited on page **??**

[177] J. F. Kurose and K. W. Ross, *Computer Networking*, Addison Wesley, 2003.
Cited on pages **??** and **??**

- A good textbook for an introduction to networking class. For self-study, I prefer Tanenbaum [298].

[178] P. B. Ladkin, Osprey, cont'd, *The Risks Digest*, Vol. 21, issue 41, 2001, at `catless.ncl.ac.uk/Risks/21.41.html#subj7`
Cited on page **??**

[179] M. K. Lai, Knapsack cryptosystems: the past and the future, March 2001, at `www.cecs.uci.edu/~mingl/knapsack.html`
Cited on page **??**

[180] B. W. Lampson, Computer security in the real world, *IEEE Computer*, pp. 37–46, June 2004.
Cited on page **??**

[181] S. Landau, Standing the test of time: the Data Encryption Standard, *Notices of the AMS*, Vol. 47, No. 3, pp. 341–349, March 2000.
Cited on page **??**

- A good technical description of DES. As the title suggests, this paper should have (finally) put to rest all of the nonsense about a back door in DES.

[182] S. Landau, Communications security for the twenty-first century: the Advanced Encryption Standard, *Notices of the AMS*, Vol. 47, No. 4, pp. 450–459, April 2000.
Cited on page **??**

- This paper has good detail on the Rijndael algorithm, as well as an overview of the other AES finalists.

[183] C. E. Landwehr et al., A taxonomy of computer program security flaws, with examples, *ACM Computing Surveys*, Vol. 26, No. 3, pp. 211–254, September 1994.
Cited on page **??**

[184] M. Lee, Cryptanalysis of the SIGABA, Master's Thesis, University of California, Santa Barbara, June 2003.
Cited on page **??**

- An excellent overview of rotors as cryptographic elements and a good description of Sigaba. However, the cryptanalysis only covers reduced-rotor versions of the cipher, which are qualitatively much different than the full Sigaba.

[185] H.-H. Lee and M. Stamp, P3P privacy enhancing agent, *Proceedings of the 3rd ACM Workshop on Secure Web Services* (SWS'06), Alexandria, Virginia, November 3, 2006, pp. 109–110, at
`www.cs.sjsu.edu/faculty/stamp/papers/sws10p-lee.pdf`
Cited on page **??**

[186] H.-H. Lee and M. Stamp, An agent-based privacy enhancing model, *Information Management & Computer Security*, Vol. 16, No. 3, 2008, pp. 305–319, at `www.cs.sjsu.edu/faculty/stamp/papers/PEA_final.doc`
Cited on page **??**

[187] R. Lemos, Spat over MS 'flaw' gets heated, *ZD Net UK News*, at `news.zdnet.co.uk/software/developer/0,39020387,2104559,00.htm`
Cited on pages **??** and 40

- The debate over the implementation of Microsoft's buffer overflow prevention technique. It is claimed that the "cure" was worse than the disease.

[188] C. J. Lennard and T. Patterson, History of fingerprinting, at `www.policensw.com/info/fingerprints/finger01.html`
Cited on page **??**

[189] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovàsz, Factoring polynomials with rational coefficients, *Math. Ann.*, 261, 1982.
Cited on page **??**

- The LLL lattice reduction algorithm.

[190] J. Lettice, Bad publicity, clashes trigger MS Palladium name change, *The Register*, at `www.theregister.co.uk/content/4/29039.html`
Cited on page **??**

- What's in a name? That which we call NGSCB by any other name would smell like Palladium.

[191] S. Levy, The open secret, *Wired*, issue 7.04, April 1999, at `www.wired.com/wired/archive/7.04/crypto_pr.html`
Cited on pages **??**, **??**, and **??**

- So you think Diffie, Hellman, Merkle, Rivest, Shamir, and Adleman invented public key cryptography? Think again.

[192] Liberty alliance project, at `www.projectliberty.org/`
Cited on page **??**

[193] D. Lin, Hunting for undetectable metamorphic viruses, Master's Thesis, Department of Computer Science, San Jose State University, 2010, at

www.cs.sjsu.edu/faculty/stamp/students/lin_da.pdf
Cited on page ??

- This paper gives a metamorphic generator that produces variants that cannot be detected using signature detection or the machine learning techniques discussed in [330].

[194] A. Main, Application security: building in security during the development stage, at www.cloakware.com/downloads/news/
Cited on page ??

[195] I. Mantin, Analysis of the stream cipher RC4, at www.wisdom.weizmann.ac.il/~itsik/RC4/Papers/Mantin1.zip
Cited on pages ??, ??, and 23

- A clearer and more detailed description of the RC4 attacks presented in [112].

[196] J. L. Massey, Design and analysis of block ciphers, *EIDMA Minicourse 8–12 May 2000.*
Cited on page ??

- Some excellent insights by one of the lesser-known giants of cryptography.

[197] D. Maughan et al., RFC 2408 — Internet security association and key management protocol (ISAKMP), at www.faqs.org/rfcs/rfc2408.html
Cited on page ??

[198] J. McLean, A comment on the "basic security theorem" of Bell and LaPadula, *Information Processing Letters*, Vol. 20, No. 2, February 1985.
Cited on page ??

- McLean attacks BLP.

[199] J. McNamara, The complete, unofficial TEMPEST information page, at www.eskimo.com/~joelm/tempest.html
Cited on page ??

[200] T. McNichol, Totally random: how two math geeks with a lava lamp and a webcam are about to unleash chaos on the Internet, *Wired*, Issue 11.08, August 2003, at
www.wired.com/wired/archive/11.08/random.html
Cited on page ??

[201] A. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997, Chapter 7, at
`www.cacr.math.uwaterloo.ca/hac/about/chap7.pdf`
Cited on page **??**

- More precise than Schneier's book [258], but in need of a second edition.

[202] R. Merkle, Secure communications over insecure channels, *Communications of the ACM*, April 1978, pp. 294–299 (submitted in 1975), at
`www.itas.fzk.de/mahp/weber/merkle.htm`
Cited on page **??**

- Given its submission date, this paper should be at least as famous as Diffie and Hellman's [90]. However, due to its absurdly late publication date, it's not.

[203] Microsoft .NET Passport: one easy way to sign in online, at
`www.passport.net`
Cited on page **??**

[204] Microsoft shared source initiative, at
`www.microsoft.com/resources/ngscb/default.mspx`
Cited on page **??**

[205] D. Miller, Beware the prophet seeking profit, at
`www.exercisereports.com/2009/11/27/`
`"beware-the-prophet-seeking-profit-"/`
Cited on page **??**

[206] M. S. Miller, K.-P. Yee, and J. Shapiro, Capability myths demolished, at `zesty.ca/capmyths/`
Cited on page **??**

- Capabilities are loved by academics, as this paper illustrates. However, in typical academic fashion, the paper ignores the significant practical challenges that arise when capabilities are actually implemented.

[207] E. Mills, Twitter, Facebook attack targeted one user, *CNET News*, at
`news.cnet.com/8301-27080_3-10305200-245.html`
Cited on page **??**

[208] F. Mirza, Block ciphers and cryptanalysis
Cited on pages **??** and **??**

- A good paper that uses STEA (simplified TEA) as an example to illustrate certain cryptanalytic attacks.

[209] D. Moore et al., The spread of the Sapphire/Slammer worm, at `www.caida.org/publications/papers/2003/sapphire/sapphire.html`
Cited on page **??**

[210] A. Muchnick, Microsoft nearing completion of Death Star, at `bbspot.com/News/2002/05/deathstar.html`
Cited on page **??**

- Geeky humor at its best.

[211] D. Mulani, How smart is your Android smartphone?, Master's Thesis, Department of Computer Science, San Jose State University, 2010, at `www.cs.sjsu.edu/faculty/stamp/students/mulani_deepika.pdf`
Cited on page **??**

[212] G. Myles and C. Collberg, Software watermarking via opaque predicates, at `sandmark.cs.arizona.edu/ginger_pubs_talks/icecr7.pdf`
Cited on page **??**

[213] MythBusters, excerpt at `www.metacafe.com/watch/252534/myth_busters_finger_print_lock/`
Cited on page **??**

- A very interesting series of attacks on fingerprint biometrics, including successful attacks on a system that the manufacturer (foolishly) claimed had "never been broken."

[214] M. Naor and A. Shamir, Visual cryptography, Eurocrypt '94, at `www.wisdom.weizmann.ac.il/~naor/topic.html#Visual_Cryptography`
Cited on page **??**

[215] National Security Agency, at `en.wikipedia.org/wiki/NSA`
Cited on page **??**

[216] National Security Agency, Centers of Academic Excellence, at `www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml`
Cited on page **??**

[217] R. Needham and M. Schroeder, Using encryption for authentication in large networks of computers *Communications of the ACM*, Vol. 21, No. 12, pp. 993–999, 1978.
Cited on page **??**

- This is the foundation on which Kerberos was built.

[218] R. M. Needham and D. J. Wheeler, Tea extensions, at
`www.cl.cam.ac.uk/ftp/users/djw3/xtea.ps`
Cited on page **??**

- An "extended" version of TEA that eliminates an obscure related key attack.

[219] Next-generation secure computing base, at
`www.microsoft.com/resources/ngscb/default.mspx`
Cited on page **??**

[220] NGSCB: Trusted computing base and software authentication, at
`www.microsoft.com/resources/ngscb/documents/ngscb_tcb.doc`
Cited on page **??**

[221] J. R. Nickerson et al., The encoder solution to implementing tamper resistant software, at
`www.cert.org/research/isw/isw2001/papers/Nickerson-12-09.pdf`
Cited on page **??**

[222] A. M. Odlyzko, The rise and fall of knapsack cryptosystems, at
`www.dtc.umn.edu/~odlyzko/doc/arch/knapsack.survey.pdf`
Cited on page **??**

[223] Office Space, at `en.wikipedia.org/wiki/Office_Space`
Cited on page 5

[224] G. Ollmann, Size matters — measuring a botnet operator's pinkie, *Virus Bulletin: VB2010*, at
`www.virusbtn.com/conference/vb2010/abstracts/Ollmann.xml`
Cited on page **??**

[225] OllyDbg, at `www.ollydbg.de/`
Cited on page **??**

[226] Optimal asymmetric encryption padding, at
`en.wikipedia.org/wiki/Optimal\_Asymmetric\_Encryption\_Padding`
Cited on page **??**

[227] Our Documents—High-resolution PDFs of Zimmermann Telegram (1917), at `www.ourdocuments.gov/doc.php?flash=true&doc=60&page=pdf`
Cited on page **??**

[228] P. S. Pagliusi, A contemporary foreword on GSM security, in G. Davida, Y. Frankel, and O. Rees, editors, *Infrastructure Security: International Conference—InfraSec 2002*, Bristol, UK, October 1–3, 2002, Lecture Notes in Computer Science 2437, pp. 129–144, Springer-Verlag, 2002.
Cited on pages **??**, **??**, and **??**

- This is a comprehensive and highly readable description of the major security flaws in GSM.

[229] J. C. Panettieri, Who let the worms out? — the Morris worm, *eWeek*, March 12, 2001, at `www.eweek.com/article2/0,1759,1245602,00.asp`
Cited on page **??**

[230] D. B. Parker, Automated crime, at
`www.windowsecurity.com/whitepapers/Automated_Crime_.html`
Cited on page **??**

[231] D. B. Parker, Automated security, at
`www.windowsecurity.com/whitepapers/Automated_Crime_.html`
Cited on page **??**

- A security guru discusses the use of metamorphism to enhance security.

[232] Passwords revealed by sweet deal, *BBC News*, April 20, 2004, at
`news.bbc.co.uk/2/hi/technology/3639679.stm`
Cited on page **??**

- Most users reveal passwords for a candy bar.

[233] C. Peikari and A. Chuvakin, *Security Warrior*, O'Reilly, 2004.
Cited on page **??**

- A reasonably interesting book with some real software hacking examples. However, Kaspersky's book [161] is much more thorough, and much better, as is Eilam's book [99].

[234] S. Petrovic and A. Fúster-Sabater, Cryptanalysis of the A5/2 algorithm, at `eprint.iacr.org/2000/052/`
Cited on page **??**

[235] C. P. Pfleeger and S. L. Pfleeger, *Security in Computing*, third edition, Prentice Hall, 2003.
Cited on pages **??**, **??**, **??**, **??**, **??**, **??**, **??**, and **??**

- Particularly good for OS security and some software issues. However, much of the information is dated—the book is ancient by computing standards, having been originally published in 1989.

[236] M. Pietrek, An in-depth look into the Win32 portable executable file format, at `msdn.microsoft.com/en-us/magazine/cc301805.aspx`
Cited on page **??**

[237] D. Piper, RFC 2407 — The Internet IP security domain of interpretation for ISAKMP, at `www.faqs.org/rfcs/rfc2407.html`
Cited on page **??**

[238] Platform for Privacy Preferences Project (P3P), at `www.w3.org/p3p`
Cited on page **??**

[239] PMC Ciphers, at
`www.turbocrypt.com/eng/content/TurboCrypt/Backup-Attack.html`
Cited on page **??**

[240] A. Pressman, Wipe 'em out, then sue for back pay, at
`www.internetwright.com/drp/RiskAssess.htm`
Cited on page **??**

- An interesting description of an insider attack. Most interesting of all is the response by the company, which probably remains fairly typical today.

[241] P. Priyadarshini and M. Stamp, Digital rights management for untrusted peer-to-peer networks, *Handbook of Research on Secure Multimedia Distribution*, IGI Global, March 2009, at
`www.cs.sjsu.edu/faculty/stamp/papers/Pallavi_paper.doc`
Cited on page **??**

[242] J. Raley, Ali Baba Bunny — 1957, Jenn Raley's Bugs Bunny page, at
`www.jenn98.com/bugs/1957-1.html`
Cited on page **??**

- Bugs Bunny and Daffy Duck in Ali Baba's cave.

[243] J. R. Rao, et al., Partitioning attacks: or how to rapidly clone some GSM cards, *2002 IEEE Symposium on Security and Privacy*, May 12–15, 2002.
Cited on page **??**

[244] A real MD5 collision, *Educated Guesswork*, August 2004 archives, at `www.rtfm.com/movabletype/archives/2004_08.html#001055`
Cited on pages **??** and **??**

[245] C. Ren, M. Weber, and G. McGraw, Microsoft compiler flaw technical note, at `www.cigital.com/news/index.php?pg=art&artid=70`
Cited on page **??**

- A discussion of an attack on Microsoft's buffer overflow prevention technique. Microsoft argued that the claimed attack was exaggerated [187].

[246] G. Richarte, Four different tricks to bypass StackShield and StackGuard protection
Cited on page **??**

[247] R. L. Rivest et al., The RC6 block cipher, at `www.secinf.net/cryptography/The_RC6_Block_Cipher.html`
Cited on page **??**

[248] Robert Morris, at `www.rotten.com/library/bio/hackers/robert-morris/`
Cited on page **??**

- The creator of the Morris Worm.

[249] S. Robinson, Up to the challenge: computer scientists crack a set of AI-based puzzles, *SIAM News*, Vol. 35, No. 9, November 2002, at `www.siam.org/siamnews/11-02/gimpy.htm`
Cited on page **??**

[250] M. J. Rose, Stephen King's 'Plant' uprooted, *Wired*, November 28, 2000, at `www.wired.com/news/culture/0,1284,40356,00.html`
Cited on page **??**

[251] M. Rosing, *Implementing Elliptic Curve Cryptography*, Manning Publications, 1998.
Cited on page **??**

- A good elementary introduction to elliptic curve cryptography.

[252] RSA SecurID, at `www.rsa.com/node.aspx?id=1156`
Cited on page **??**

[253] Rsync Open source software project, at `samba.anu.edu.au/rsync/`
Cited on page **??**

[254] R. A. Rueppel, *Analysis and Design of Stream Ciphers*, Springer-Verlag, 1986.
Cited on page **??**

- This book is a classic, which Rueppel wrote when he was Massey's student.

[255] R. Ryan, Z. Anderson, and A. Chiesa, Anatomy of a subway hack, at `tech.mit.edu/V128/N30/subway/Defcon_Presentation.pdf`
Cited on page 7

- A fascinating security analysis of the Boston subway system.

[256] R. Sanchez-Reillo, C. Sanchez-Avila and Ana Gonzalez-Marcos, Biometric identification through hand geometry measurements, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 22, No. 10, pp. 1168–1171, 2000.
Cited on page **??**

[257] W. Schindler, A timing attack against RSA with the Chinese Remainder Theorem, *CHES 2000*, LNCS 1965, Ç. K. Koç and C. Paar, Eds., Springer-Verlag, 2000, pp. 109–124.
Cited on page **??**

[258] B. Schneier, *Applied Cryptography*, second edition, Wiley, 1996.
Cited on pages **??**, **??**, **??**, and 35

- This book is, for better or for worse, the crypto bible for working security professionals.

[259] B. Schneier, Attack trees, *Dr. Dobb's Journal*, December 1999, at `www.schneier.com/paper-attacktrees-ddj-ft.html`
Cited on page **??**

- A practical and intuitive approach to "hazard analysis."

[260] B. Schneier, Biometrics: truths and fictions, at
`www.schneier.com/crypto-gram-9808.html`
Cited on pages **??** and **??**

[261] B. Schneier, Risks of relying on cryptography, Inside Risks 112, *Communications of the ACM*, Vol. 42, No. 10, October 1999, at
`www.schneier.com/essay-021.html`
Cited on page **??**

- Schneier, in his own inimitable style, emphasizes the point that attackers don't necessarily play by the rules.

[262] B. Schneier, The Blowfish encryption algorithm, at
`www.schneier.com/blowfish.html`
Cited on page **??**

- Schneier describes his favorite crypto algorithm.

[263] H. Shacham, et al, On the Effectiveness of Address-Space Randomization, at `crypto.stanford.edu/~nagendra/papers/asrandom.ps`
Cited on page **??**

[264] A. Shamir, How to share a secret, *Communications of the ACM*, Vol. 22, No. 11, pp. 612–613, November 1979, at
`szabo.best.vwh.net/secret.html`
Cited on page **??**

[265] A. Shamir, A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem, *IEEE Transactions on Information Theory*, Vol. IT–30, No. 5, pp. 699–704, September 1984.
Cited on pages **??** and **??**

- Shamir's clever attack on the original knapsack cryptosystem.

[266] A. Shamir and N. van Someren, Playing hide and seek with stored keys
Cited on pages **??** and **??**

- This paper includes a simple and effective statistical test for distinguishing random from non-random.

[267] C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, Vol. 28–4, pp. 656–715, 1949.
Cited on page **??**

- The paper that started it all. Most of this paper remains surprisingly relevant after more than $3/5^{\text{ths}}$ of a century.

[268] K. Skachkov, Tamper-resistant software: design and implementation, at `www.cs.sjsu.edu/faculty/stamp/students/TRSDIfinal.doc`
Cited on page **??**

- Discusses some of the issues related to tamper-resistant software of Aucsmith [19] variety. A toy implementation is presented.

[269] S. Skorobogatov and R. Anderson, Optical fault induction attacks, *IEEE Symposium on Security and Privacy*, 2002.
Cited on page **??**

[270] E. Skoudis, *Counter Hack*, Prentice Hall, 2002.
Cited on page **??**

- An excellent book that includes plenty of details on how a sophisticated hacker analyzes and attacks a target. A must read for the system administrators of the world.

[271] SSL 3.0 specification, at
`www.lincoln.edu/math/rmyrick/ComputerNetworks/InetReference/ssl-draft/3-SPEC.HTM`
Cited on page **??**

[272] Sonogram, Visible speech, at
`www.dontcrack.com/freeware/downloads.php/id/266/software/Sonogram/`
Cited on page **??**

[273] Staff Report, U. S. Senate Select Committee on Intelligence, Unclassified summary: involvement of NSA in the development of the Data Encryption Standard, Staff Report, 98th Congress, 2nd Session, April 1978.
Cited on pages **??** and **??**

- Senate report that cleared NSA of any wrongdoing in the design of DES. Needless to say, this did not convince the critics.

[274] M. Stamp, Digital rights management: for better or for worse?, *ExtremeTech*, May 20, 2003.
Cited on page **??**

- Tries to make the case that, in spite of its technical shortcomings, DRM can facilitate e-commerce if the business model is right.

[275] M. Stamp, Digital rights management: the technology behind the hype, *Journal of Electronic Commerce Research*, Vol. 4, No. 3, 2003, at
`www.csulb.edu/web/journals/jecr/issues/20033/paper3.pdf`
Cited on pages **??** and **??**

- Perhaps the most detailed description of a fielded commercial DRM system ever published.

[276] M. Stamp, Risks of digital rights management, Inside Risks 147, *Communications of the ACM*, Vol. 45, No. 9, p. 120, September 2002, at
`www.csl.sri.com/users/neumann/insiderisks.html#147`
Cited on page **??**

- This article highlights some of the obvious difficulties of doing DRM in software.

[277] M. Stamp, Risks of monoculture, Inside Risks 165, *Communications of the ACM*, Vol. 47, No. 3, p. 120, March 2004, at
`www.csl.sri.com/users/neumann/insiderisks04.html#165`
Cited on page **??**

- An intuitive discussion of the potential security benefits of diverse software.

[278] M. Stamp, A revealing introduction to hidden Markov models, at
`www.cs.sjsu.edu/faculty/stamp/RUA/HMM.pdf`
Cited on page **??**

[279] M. Stamp, S. Attaluri, and S. McGhee, Profile hidden Markov models and metamorphic virus detection, *Journal in Computer Virology*, Vol. 5, No. 2, May 2009, pp. 151–169.
Cited on page **??**

[280] M. Stamp and W. O. Chan, SIGABA: Cryptanalysis of the full keyspace, *Cryptologia*, Vol. 31, No. 3, July 2007, pp. 201–222.
Cited on page **??**

[281] M. Stamp and X. Gao, Metamorphic software for buffer overflow mitigation, *Proceedings of the 2005 Conference on Computer Science and*

its Applications, at
`www.cs.sjsu.edu/faculty/stamp/papers/BufferOverflow.doc`
Cited on page **??**

[282] M. Stamp and D. Holankar, Secure streaming media and digital rights management, *Proceedings of the 2004 Hawaii International Conference on Computer Science*, January 2004, at
`www.cs.sjsu.edu/~stamp/cv/papers/hawaii.pdf`
Cited on page **??**

- A nice protocol (OK, I'm biased...) for delivering DRM-protected streaming media that includes many of the software protection tricks discussed in this book.

[283] M. Stamp and A. Hushyar, Multilevel security models, *The Handbook of Information Security*, H. Bidgoli, editor, Wiley, 2006.
Cited on page **??**

- This paper gives an overview of many different security models. It likely contains more than you'll ever want to know about security modeling.

[284] M. Stamp and R. M. Low, *Applied Cryptanalysis: Breaking Ciphers in the Real World*, Wiley, 2007.
Cited on pages **??**, **??**, **??**, and **??**

- A personal favorite of mine...

[285] M. Stamp and P. Mishra, Software uniqueness: how and why, *Proceedings of the 2003 Conference on Computer Science and its Applications*, at
`www.cs.sjsu.edu/~stamp/cv/papers/iccsaPuneet.html`
Cited on page **??**

[286] M. Stamp and E. J. Sebes, Enterprise digital rights management: Ready for primetime?, *Business Communications Review*, pp. 52–55, March 2004.
Cited on page **??**

- Makes the case that DRM within an enterprise is a much different beast than DRM for e-commerce.

[287] M. Stamp, M. Simova, and C. Pollett, Stealthy ciphertext, *Proceedings of 3rd International Conference on Internet Computing (ICOMP'05)*, Las Vegas, Nevada, June 27–30, 2005, at
`www.cs.sjsu.edu/faculty/stamp/papers/stealthy.pdf`
Cited on page **??**

[288] M. Stamp and S. Thaker, Software watermarking via assembly code transformations, *Proceedings of the 2004 Conference on Computer Science and its Applications*, June 2004, at
`www.cs.sjsu.edu/faculty/stamp/papers/iccsaSmita.doc`
Cited on page **??**

[289] S. Staniford, V. Paxson, and N. Weaver, How to 0wn the Internet in your spare time, at
`www.icir.org/vern/papers/cdc-usenix-sec02/`
Cited on page **??**

- Excellent article on the future of malware.

[290] M. Stigge, et al, Reversing CRC — Theory and Practice, at
`sar.informatik.hu-berlin.de/research/publications/SAR-PR-2006-05/SAR-PR-2006-05_.pdf`
Cited on page **??**

[291] H. L. Stimson and M. Bundy, *On Active Service in Peace and War*, Hippocrene Books, 1971.
Cited on page **??**

[292] D. Stinson, Doug Stinson's visual cryptography page, at
`www.cacr.math.uwaterloo.ca/~dstinson/visual.html`
Cited on page **??**

- An excellent introduction to a fascinating topic.

[293] B. Stone, Breaking Google captchas for some extra cash, *New York Times*, March 13, 2008, at
`bits.blogs.nytimes.com/2008/03/13/breaking-google-captchas-for-3-a-day/`
Cited on page **??**

[294] A. Stubblefield, J. Ioannidis, and A. D. Rubin, Using the Fluhrer, Mantin and Shamir attack to break WEP, at
`www.isoc.org/isoc/conferences/ndss/02/papers/stubbl.pdf`
Cited on pages **??** and **??**

[295] C. Swenson, *Modern Cryptanalysis: Techniques for Advanced Code Breaking*, Wiley, 2008.
Cited on page **??**

[296] P. Ször, *The Art of Computer Virus Defense and Research*, Symantec Press, 2005.
Cited on page **??**

[297] P. Ször and P. Ferrie, Hunting for metamorphic, Symantec Corporation White Paper, at `www.peterszor.com/metamorp.pdf`
Cited on page **??**

- An excellent discussion of polymorphism and metamorphism, along with various detection techniques.

[298] A. S. Tanenbaum, *Computer Networks*, fourth edition, Prentice Hall, 2003.
Cited on pages **??**, **??**, and 31

- Probably the best networking book for self-study or casual reading. The book is comprehensive, yet Tanenbaum has plenty of stories to keep the reader interested and awake.

[299] TechnoLogismiki, Hackman, at
`www.technologismiki.com/en/index-h.html`
Cited on page **??**

[300] D. Terdiman, Vegas gung-ho on gambling tech, *Wired*, September 19, 2003, at `www.wired.com/news/print/0,1294,60499,00.html`
Cited on page **??**

[301] The Warhol, at `www.warhol.org/`
Cited on page **??**

[302] C. Thomborson and M. Barrett, NGSCB: a new tool for securing applications, at
`www.cs.auckland.ac.nz/~cthombor/Pubs/barrettNZISF120804.pdf`
Cited on pages **??**, **??**, and **??**

[303] K. Thompson, Reflections on trusting trust, *Communication of the ACM*, Vol. 27, No. 8, pp. 761–763, August 1984.
Cited on pages **??** and **??**

- A classic paper that probes the limits of security in software.

[304] B. C. Tjaden, *Fundamentals of Secure Computing Systems*, Franklin, Beedle & Associates, 2004.
Cited on page **??**

- An introductory information security textbook. The chapter on intrusion detection is well worth the (modest) price of the book.

[305] W. A. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory*, Prentice Hall, 2002.
Cited on pages **??** and **??**

- An excellent and mathematically sound introduction to many aspects of cryptography.

[306] Trusted Computing Group, at `www.trustedcomputinggroup.org/home`
Cited on page **??**

[307] B. W. Tuchman, *The Zimmermann Telegram*, Ballantine Books, 1985.
Cited on page **??**

- An entertaining historical account by one of the better writers of popular history.

[308] Ultra, at `en.wikipedia.org/wiki/Ultra`
Cited on page **??**

[309] United States Department of Defense, *Trusted Computing System Evaluation Criteria*, 1983, at
`csrc.nist.gov/publications/history/dod85.pdf`
Cited on pages **??**, **??**, **??**, and **??**

- The infamous "orange book." Like most government publications, this one is a sure cure for insomnia.

[310] US v. ElcomSoft & Sklyarov FAQ, at
`www.eff.org/IP/DMCA/US_v_Elcomsoft/us_v_elcomsoft_faq.html`
Cited on page **??**

[311] R. Vamosi, Windows XP SP2 more secure? Not so fast, at
`reviews.zdnet.co.uk/software/os/0,39024180,39163696,00.htm`
Cited on pages **??** and **??**

[312] S. Venkatachalam, Detecting undetectable computer viruses, Master's Thesis, Department of Computer Science, San Jose State University,

2010, at
`www.cs.sjsu.edu/faculty/stamp/students/venkatachalam_sujandharan.pdf`
Cited on page ??

[313] R. Venkataramu, Analysis and enhancement of Apple's Fairplay digital rights management, Master's Thesis, Department of Computer Science, San Jose State University, 2007, at
`www.cs.sjsu.edu/faculty/stamp/students/RamyaVenkataramu_CS298Report.pdf`
Cited on page ??

[314] R. Venkataramu and M. Stamp, P2PTunes: A peer-to-peer digital rights management system, *Handbook of Research on Secure Multimedia Distribution*, IGI Global, March 2009, at
`www.cs.sjsu.edu/faculty/stamp/papers/Ramya_paper.doc`
Cited on page ??

[315] VENONA, at `www.nsa.gov/public_info/declass/venona/index.shtml`
Cited on page ??

- VENONA is an interesting topic, both for the crypto and for the historical material. Many of those who vehemently denied they had any role in espionage are implicated by VENONA decrypts. Also, of the hundreds of traitors mentioned (by cover name) in the decrypts, the true identities of most remain unknown.

[316] VeriSign, Inc., at `www.verisign.com/`
Cited on page ??

- The leading commercial certificate authority (CA).

[317] J. Viega and G. McGraw, *Building Secure Software*, Addison Wesley, 2002.
Cited on pages ??, ??, ??, ??, ??, and ??

- This is a worthwhile book that provides considerable detail on issues related to secure software development. About the only conceivable criticism is that it provides no evidence of the effectiveness of its suggestions.

[318] VMware is virtual infrastructure, at `www.vmware.com/`
Cited on page ??

[319] L. von Ahn, M. Blum, and J. Langford, Telling humans and computers apart automatically, *Communications of the ACM*, Vol. 47, No. 2, pp. 57–60, February 2004, at
`www.cs.cmu.edu/~biglou/captcha_cacm.pdf`
Cited on pages 4 and **??**

- A fascinating, informative and entertaining article. This is the place to start your research into CAPTCHAs.

[320] L. von Ahn et al., The CAPTCHA project, at `www.captcha.net/`
Cited on page **??**

[321] J. R. Walker, Unsafe at any key size; an analysis of the WEP encapsulation, at `www.dis.org/wl/pdf/unsafe.pdf`
Cited on pages **??** and **??**

- A clever title and a good description of the some of the problems created by WEP's use of IVs. However, one of the most serious problems is the devastating cryptanalytic attack discussed in [112], which is not mentioned here.

[322] What is reCAPTCHA?, at
`recaptcha.net/learnmore.html`
Cited on page **??**

[323] D. J. Wheeler and R. M. Needham, TEA, a tiny encryption algorithm, at `www.cix.co.uk/~klockstone/tea.pdf`
Cited on page **??**

- Less than four pages to present TEA in all of its wonderful simplicity.

[324] O. Whitehouse, An Analysis of Address Space Layout Randomization on Windows Vista, at
`www.symantec.com/avcenter/reference/`
`Address_Space_Layout_Randomization.pdf`
Cited on page **??**

- A readable analysis of the randomness (or lack thereof) in ASLR as implemented in Windows Vista.

[325] Wi-Fi Protected Access, at
`en.wikipedia.org/wiki/Wi-Fi_Protected_Access`
Cited on page **??**

[326] R. N. Williams, A painless guide to CRC error detection algorithms, at
`www.ross.net/crc/crcpaper.html`
Cited on pages **??** and **??**

[327] N. Winkless and I. Browning, *Robots on Your Doorstep*, Robotics Press, 1978.
Cited on page **??**

- While it seems dated today, this classic and off-beat book presents the conventional wisdom of its time in an unconventional way.

[328] Wireshark, at `www.wireshark.org/`
Cited on pages **??** and **??**

[329] W. Wong, Revealing your secrets through the fourth dimension, *ACM Crossroads*, at
`www.cs.sjsu.edu/faculty/stamp/students/wing.html`
Cited on page **??**

- An elementary and highly readable description of the basic ideas behind RSA timing attacks.

[330] W. Wong and M. Stamp, Hunting for metamorphic engines, *Journal in Computer Virology*, Vol. 2, No. 3, December 2006, pp. 211–229.
Cited on pages **??**, **??**, and 34

- This paper covers some research problems related to metamorphic malware. A number of real-world metamorphic generators are analyzed and a reasonably practical detection technique is given.

[331] T. Ylonen, The Secure Shell (SSH) Authentication Protocol, RFC 4252, at `www.ietf.org/rfc/rfc4252.txt`
Cited on page **??**

[332] B. Yee, et al., Native client: a sandbox for portable, untrusted x86 native code, at
`nativeclient.googlecode.com/svn/data/docs_tarball/nacl/`
`googleclient/native_client/documentation/nacl_paper.pdf`
Cited on page **??**

[333] T. Ylonen, The Secure Shell (SSH) Transport Layer Protocol, RFC 4253, at `www.ietf.org/rfc/rfc4253.txt`
Cited on page **??**

[334] G. Yuval, How to swindle Rabin, *Cryptologia*, Vol. 3, No. 3, 1979, pp. 187–189.
Cited on page **??**

[335] M. Zalewski, Strange attractors and TCP/IP sequence number analysis—one year later, at `lcamtuf.coredump.cx/newtcp/`
Cited on page **??**

- Fascinating scatter plots of the distribution of TCP initial sequence numbers for many different vendor's products. Many are extremely non-random.

[336] L. Zeltser, Reverse engineering malware, at
`www.zeltser.com/sans/gcih-practical/`
Cited on pages **??** and 52

- An excellent discussion of malware as well as reverse engineering principles. Highly recommended. See also [337].

[337] L. Zeltser, SANS malware FAQ: reverse engineering `srvcp.exe`, at
`www.sans.org/resources/malwarefaq/srvcp.php`
Cited on pages **??** and 52

- Much overlap with [336], but this one also includes a link to the malware executable that is reverse engineered.

[338] J. Zhang, Improved software activation using multithreading, Master's Thesis, Department of Computer Science, San Jose State University, 2010, at
`www.cs.sjsu.edu/faculty/stamp/students/zhang_jianrui.pdf`
Cited on page **??**

[339] M. Zorz, Basic security with passwords, at
`www.net-security.org/article.php?id=117`
Cited on page **??**