Recommended Reading for Computer Security

Chapter 1 - Overview 2
Chapter 2 — Cryptographic Tools 3
Chapter 3 — User Authentication 4
Chapter 4 — Access Control 4
Chapter 5 — Database Security 6
Chapter 6 – Malicious Software 8
Chapter 7 — Denial of Service 10
Chapter 8 — Intrusion Detection 10
Chapter 9 — Firewalls 11
Chapter 10 — Buffer Overflow 12
Chapter 11 — Software Security 13
CHAPTER 18 SECURITY AUDITING 14

Supplement to
Cryptography and Network Security, Seventh Edition
© Pearson 2017
http://williamstallings.com/Cryptography/

Chapter 1 - Overview

It is useful to read some of the classic tutorial papers on computer security; these provide a historical perspective from which to appreciate current work and thinking.[1] The papers to read are [WARE79], [BROW72], [SALT75], and [SHAN77]. Two more recent, short treatments of computer security are [ANDR04] and [LAMP04]. [NIST95] is an exhaustive (290 pages) treatment of the subject. Another good treatment is [NRC91]. Also useful is [FRAS97].

NIST SP 800-27 [STON04] and NSA's Information Assurance Technical Framework [NSA02] are two useful discussions of security design principles.

There is an overwhelming amount of material, including books, papers, and online resources, on computer security. Perhaps the most useful and definitive source of information is a collection of standards and specifications from standards-making bodies and from other sources whose work has widespread industry and government approval. We list some of the most important sources in Appendix C.

ANDR04 Andrews, M., and Whittaker, J. "Computer Security." *IEEE Security and Privacy*, September/October 2004.

BROW72 Browne, P. "Computer Security—A Survey." *ACM SIGMIS Database*, Fall 1972.

FRAS97 Fraser, B. *Site Security Handbook.* RFC 2196, September 1997.

LAMP04 Lampson, B. "Computer Security in the Real World." *Computer*, June 2004.

NIST95 National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook.* Special Publication 800-12, October 1995.

[1] These classic papers are available at box.com/CompSec4e.

NRC91 National Research Council. *Computers at Risk: Safe Computing in the Information Age.* Washington, DC: National Academy Press, 1991.

NSA02 National Security Agency. *Information Assurance Technical Framework.* IATF Release 3.1, September 2002.

SALT75 Saltzer, J., and Schroeder, M. "The Protection of Information in Computer Systems." *Proceedings of the IEEE*, September 1975.

SHAN77 Shanker, K. "The Total Computer Security Problem: An Overview." *Computer*, June 1977.

STON04 Stoneburner, G.; Hayden, C.; and Feringa, A. *Engineering Principles for Information Technology Security (A Baseline for Achieving Security).* NIST SP 800-27, June 2004.

WARE79 Ware, W., ed. *Security Controls for Computer Systems.* RAND Report 609-1. October 1979. http://www.rand.org/pubs/reports/R609-1/index2.html

Chapter 2 — Cryptographic Tools

The topics in this chapter are covered in greater detail in [STAL17]. For coverage of cryptographic algorithms, [SCHN96] is a valuable reference work; it contains descriptions of virtually every cryptographic algorithm and protocol in use up to the time of the book's publication. A good classic paper on the topics of this chapter is [DIFF79].

For anyone interested in the history of code making and code breaking, the book to read is [KAHN96]. Although it is concerned more with the impact of cryptology than its technical development, it is an excellent introduction and makes for exciting reading. Another excellent historical account is [SING99].

DIFF79 Diffie, W., and Hellman, M. "Privacy and Authentication: An Introduction to Cryptography." *Proceedings of the IEEE*, March 1979.

KAHN96 Kahn, D. *The Codebreakers: The Story of Secret Writing.* New York: Scribner, 1996.

SCHN96 Schneier, B. *Applied Cryptography.* New York: Wiley, 1996.

SING99 Singh, S. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography.* New York: Anchor Books, 1999.

STAL17 Stallings, W. *Cryptography and Network Security: Principles and Practice, Seventh Edition.* Upper Saddle River, NJ: Pearson, 2014.

Chapter 3 — User Authentication

[OGOR03] is the paper to read for an authoritative survey of the topics of this chapter. [BURR13] is also a worthwhile survey.

[SCAR09a] is a comprehensive look at many issues related to password selection and management.

BURR13 Burr, W., et al. *Electronic Authentication Guideline.* Gaithersburg, MD: National Institute of Standards and Technology, Special Publication 800-63-2, September 2013.

OGOR03 O'Gorman, L. "Comparing Passwords, Tokens and Biometrics for User Authentication." *Proceedings of the IEEE*, December 2003.

SCAR09a Scarfone, K., and Souppaya, M. *Guide to Enterprise Password Management (Draft).* NIST Special Publication SP 800-118 (Draft), April 2009.

Chapter 4 — Access Control

[DOWN85] provides a good review of the basic elements of DAC. [KAIN87] is a clear discussion of capability-based access control.

[SAND96] is a comprehensive overview of RBAC. [FERR92] also provides some useful insights. [BARK97] looks at the similarities in functionality between RBAC and DAC based on access control lists. [SAUN01] is a more general comparison of RBAC and DAC. [FRAN12] discusses the strengths and weakness of RBAC and its applicability in

various contexts. [FERR01] and [SAND00] present the NIST RBAC standard in detail. [COYN08] describes the INCITS RBAC implementation and interoperability standard, based in the NIST standard.

NIST SP 800-16 [HU13] provides an excellent overview of ABAC models and their application. [CIOC11] is a clear and thorough introduction to ICAM. [RUND10] is a useful overview of OITF. [OIX13] is a much more detailed treatment of trust frameworks and attribute exchange networks.

BARK97 Barkley, J. "Comparing Simple Role-Based Access Control Models and Access Control Lists." *Proceedings of the Second ACM Workshop on Role-Based Access Control*, 1997.

CIOC11 CIO Council. *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance.* cio.gov. December 2011.

COYN08 Coyne, E., and Weil, T. "An RBAC Implementation and Interoperability Standard." *IEEE Security & Privacy*, January/February 2008.

DOWN85 Down, D., et al. "Issues in Discretionary Access Control." *Proceedings of the 1985 Symposium on Security and Privacy*, 1985.

FERR92 Ferraiolo, D., and Kuhn, R. "Role-Based Access Control." *Proceedings of the 15th National Computer Security Conference*, 1992.

FERR01 Ferraiolo, D. et al. "Proposed NIST Standard for Role-Based Access Control." *ACM Transactions on Information and System Security*, August 2001.

FRAN12 Franqueira, V., and Wieringa, R. "Role-Based Access Control in Retrospect." *Computer*, June 2012.

HU13 Hu, V. et al. *Guide to Attribute Based Access Control (ABAC) Definition and Considerations.* NIST SP 800-62, September 2013.

KAIN87 Kain, R., and Landwehr. "On Access Checking in Capability-Based System." *IEEE Transactions on Software Engineering*, February 1987.

OIX13 Open Identity Exchange. *Attribute Exchange Trust Framework Specification.* July 2013. http://openidentityexchange.org

RUND10 Rundle, M., ed. *The Open Identity Trust Framework (OITF) Model.* Microsoft White Paper, March 2010. http://www.microsoft.com/mscorp/twc/endtoendtrust/default.aspx

SAND96 Sandhu, R., et al. "Role-Based Access Control Models." *Computer*, February 1996.

SAND00 Sandhu, R.; Ferraiolo, D.; and Kuhn, R. "The NIST Model for Role-Based Access Control: Towards a Unified Standard." *Proceedings of the Fifth ACM Workshop on Role-Based Access Control*, 2000.

SAUN01 Saunders, G.; Hitchens, M.; and Varadharajan, V. "Role-Based Access Control and the Access Control Matrix." *Operating Systems Review*, October 2001.

Chapter 5 — Database Security

[BERT05] is an excellent survey of database security. Two surveys of access control for database systems are [BERT95] and [LUNT90]. [VIEI05] analyzes ways to characterize and assess security mechanisms in database systems. [DISA05] is a lengthy discussion of database security topics, focusing on the features available in commercial DBMSs.

[CHAN12] and [SHAR13] are excellent overviews of SQLi attacks and countermeasures.

[FARK02] is a brief overview of the inference problem. For a brief but useful overview of databases, see [LEYT01]. The concepts on which relational databases are based were introduced in a classic paper by Codd [CODD70]. An early survey paper on relational databases is [KIM79].

[JANS11] is a worthwhile, systematic treatment of cloud security issues. Other useful treatments, providing differing perspectives, are [HASS10], [BALA09], [ANTH10], and [CSA11].

ANTH10 Anthes, G. "Security in the Cloud." *Communications of the ACM*, November 2010.

BALA09 Balachandra, R.; Ramakrishna, P.; and Rakshit, A. "Cloud Security Issues." *Proceedings, 2009 IEEE International Conference on Services Computing*, 2009.

BERT95 Bertino, E.; Jajodia, S.; and Samarati, P. "Database Security: Research and Practice." *Information Systems*, Vol. 20, No. 7, 1995.

BERT05 Bertino, E., and Sandhu, R. "Database Security—Concepts, Approaches, and Challenges." *IEEE Transactions on Dependable and Secure Computing*, January–March, 2005.

CODD70 Codd, E. "A Relational Model of Data for Large Shared Data Banks." *Communications of the ACM*, June 1970.

CSA11 Cloud Security Alliance. *Security Guidance for Critical Areas of Focus in Cloud Computing V2.1.* CSA Report, 2011.

DISA05 Defense Information Systems Agency. *Database Security Technical Implementation Guide.* Department of Defense, November 30. 2005. csrc.nist.gov/pcig/STIGs/database-stig-v7r2.pdf

FARK02 Farkas, C., and Jajodia, S. "The Inference Problem: A Survey." *ACM SIGKDD Explorations*, Vol. 4, No. 2, 2002.

HASS10 Hassan, T.; Joshi, J.; and Ahn, G. "Security and Privacy Challenges in Cloud Computing Environments." *IEEE Security&Privacy*, November/December 2010.

JANS11 Jansen, W., and Grance, T. *Guidelines on Security and Privacy in Public Cloud Computing.* NIST Special Publication 800-144, January 2011.

JONG83 Jonge, W. "Compromising Statistical Database Responding to Queries About Means." *ACM Transactions on Database Systems*, March 1983.

KIM79 Kim, W. "Relational Database Systems." *Computing Surveys*, September 1979.

LEYT01 Leyton, R. "A Quick Introduction to Database Systems." *;login*, December 2001.

LUNT90 Lunt, T., and Fernandez, E. "Database Security." *ACM SIGMOD Record*, December 1990.

VIEI05 Vieira, M, and Madeira, H. "Towards a Security Benchmark for Database Management Systems." *Proceedings of the 2005 International Conference on Dependable Systems and Networks*, 2005.

Chapter 6 – Malicious Software

For a thorough understanding of viruses, the book to read is [SZOR05]. Another excellent treatment is [AYCO06]. Good overview articles on viruses and worms are [CASS01], [EGEL12], [KEPH97a], and [KERA16]. [MOOR02] provides a good treatment of the Code Red worm. [WEAV03] supplies a comprehensive survey of worm characteristics. [HYPP06] discusses worm attacks on mobile phones.

[HOLZ05] and [MCLA04] provide overviews of bots. [LEVI06], [LEVI04] [GEER06], and [EMBL08] describe various types of rootkits and their operation.

AYCO06 Aycock, J. *Computer Viruses and Malware.* New York: Springer, 2006.

CASS01 Cass, S. "Anatomy of Malice." *IEEE Spectrum*, November 2001.

EGEL12 Egele, M., Scholte, T., Kirda, E., and Kruegel, C., "A Survey on Automated Dynamic Malware Analysis Techniques and Tools", *ACM Computing Surveys*, Vol. 44, No. 2, Article 6, February 2012.

EMBL08 Embleton, S.; Sparks, S.; and Zou, C. "SMM Rootkits: a New Breed of OS-Independent Malware." *Proceedings of the 4th International Conference on Security and Privacy in Communication Networks*, ACM, September 2008.

GEER06 Geer, D. "Hackers Get to the Root of the Problem." *Computer*, May 2006.

HOLZ05 Holz, T. "A Short Visit to the Bot Zoo." *IEEE Security and Privacy*, May–June 2005.

HYPP06 Hypponen, M. "Malware Goes Mobile." *Scientific American*, November 2006.

KEPH97a Kephart, J.; Sorkin, G.; Chess, D.; and White, S. "Fighting Computer Viruses." *Scientific American*, November 1997.

KERA16, Keragala D., Detecting Malware and Sandbox Evasion Techniques, *SANS Institute InfoSec Reading Room*, 2016.

LEVI04 Levine, J.; Grizzard, J.; and Owen, H. "A Methodology to Detect and Characterize Kernel Level Rootkit Exploits Involving Redirection of the System Call Table." *Proceedings, Second IEEE International Information Assurance Workshop*, 2004.

LEVI06 Levine, J.; Grizzard, J.; and Owen, H. "Detecting and Categorizing Kernel-Level Rootkits to Aid Future Detection." *IEEE Security and Privacy*, January–February 2006.

MCLA04 McLaughlin, L. "Bot Software Spreads, Causes New Worries." *IEEE Distributed Systems Online*, June 2004.

MOOR02 Moore, D,; Shannon, C.; Claffy, K. "Code-Red: A Case Study on the Spread and Victims of an Internet Worm", *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement*, November 2002.

SOUP13 Souppaya, M., and Scarfone, K. *Guide to Malware Incident Prevention and Handling for Desktops and Laptops.* NIST Special Publication SP 800-83, July 2013.

SYMA16 Symantec, "Internet Security Threat Report, Vol. 21." April 2016.

SZOR05 Szor, P. *The Art of Computer Virus Research and Defense.* Reading, MA: Addison-Wesley, 2005.

WEAV03 Weaver, N., et al. "A Taxonomy of Computer Worms." *The First ACM Workshop on Rapid Malcode (WORM)*, 2003.

Chapter 7 — Denial of Service

[PENG07] is an excellent survey of DoS attacks and defenses. Another comprehensive survey is [HAND06]. [CICH12] includes some guidance on types of DoS attacks and how to prepare for and respond to them.

[CHAN02] provides suggestions for defending against DDoS attacks. [LIU09] is a short but useful article on the same subject.

CHAN02 Chang, R. "Defending Against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial." *IEEE Communications Magazine*, October 2002.

CICH12 Cichonksi, P.. *Computer Security Incident Handling Guide*. NIST Special Publication 800-61. Auguste 2012.

HAND06 Handley, M., and Rescorla, E. *Internet Denial-of-Service Considerations.* RFC 4732, November 2006.

LIU09 Liu, S. "Surviving Distributed Denial-of-Service Attacks." *IT Pro*, September/October 2009.

PENG07 Peng, T.; Leckie, C.; and Rammohanarao, K. "Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems." *ACM Computing Surveys*, April 2007.

Chapter 8 — Intrusion Detection

[SCAR12] is a detailed and worthwhile treatment of intrusion detection. Two short but useful survey articles on the subject are [KENT00] and [MCHU00]. [PRED08] gives examples of insider attacks. [LAZA05] and [NING04] survey recent advances in intrusion detection techniques. [CHAN09] is a thorough survey of anomaly detection techniques. A briefer overview is [SAMP13]. [CHEN12] analyzes five evasion techniques used in IDS attacks.

CHAN09 Chandola, V.; Banerjee, A.; and Kumar, V. "Anomaly Detection: A Survey." *ACM Computing Surveys*, July 2009.

CHEN12 Cheng, T., et al. "Evasion Techniques: Sneaking through Your Intrusion Detection/Prevention Systems." *IEEE Communications Surveys & Tutorials*, Fourth Quarter 2012.

KENT00 Kent, S. "On the Trail of Intrusions into Information Systems." *IEEE Spectrum*, December 2000.

LAZA05 Lazarevic, A.; Kumar, V.; and Srivastava, J. "Intrusion Detection: A Survey", in "Managing Cyber Threats: Issues, Approaches and Challenges", Springer, 2005

MCHU00 McHugh, J.; Christie, A.; and Allen, J. "The Role of Intrusion Detection Systems." *IEEE Software*, September/October 2000.

NING04 Ning, P., et al. "Techniques and Tools for Analyzing Intrusion Alerts." *ACM Transactions on Information and System Security*, May 2004.

PRED08 Predd, J., et al. "Insiders Behaving Badly." *IEEE Security & Privacy*, July/August 2008.

SAMP13 Sample, C., and Schaffer, K. "An Overview of Anomaly Detection." IT Pro, January/February 2013.

SCAR12 Scarfone, K., and Mell, P. *Guide to Intrusion Detection and Prevention Systems.* NIST Special Publication SP 800-94, SP 800-94 rev 1 (draft), July 2012.

Chapter 9 — Firewalls

A classic treatment of firewalls is [CHES03]. [LODI98], [OPPL97], and [BELL94] are good overview articles on the subject. [SCAR09b] is an excellent overview of firewall technology and firewall policies.

IPSs are covered [SCAR12].

BELL94 Bellovin, S., and Cheswick, W. "Network Firewalls." *IEEE Communications Magazine*, September 1994.

CHES03 Cheswick, W., Bellovin, S. , and Rubin, A. *Firewalls and Internet Security: Repelling the Wily Hacker*. Reading, MA: Addison-Wesley, 2003.

LODI98 Lodin, S., and Schuba, C. "Firewalls Fend Off Invasions from the Net." *IEEE Spectrum*, February 1998.

OPPL97 Oppliger, R. "Internet Security: Firewalls and Beyond." *Communications of the ACM*, May 1997.

SCAR09b Scarfone, K., and Hoffman, P. *Guidelines on Firewalls and Firewall Policy*. NIST Special Publication SP 800-41-1, September 2009.

SCAR12 Scarfone, K., and Mell, P. *Guide to Intrusion Detection and Prevention Systems.* NIST Special Publication SP 800-94 rev 1 (draft), July 2012.

ZWIC00 Zwicky, E., Coopers, S., and Chapman, D., E. *Building Internet Firewalls.* Sebastopol, CA: O'Reilly, 2000.

Chapter 10 — Buffer Overflow

[LHEE03] surveys a range of alternative buffer overflow techniques, including a number not mentioned in this chapter, along with possible defensive techniques. Considerably greater detail on specific aspects is given in [HOGL04] and [ANLE07]. The original published description of buffer overflow attacks is given in [LEVY96]. [KUPE05] and [VEEN12] provide broad overviews of this topic.. For much greater detail on the basic organization and operation of computer systems, including details on stack frames and process organization conventions, see [STAL16], or for process and operating systems details, see [STAL15].

ANLE07 Anley, C.; Heasman, J.; Lindner, F.; and Richarte, G. *The Shellcoder's Handbook : Discovering and Exploiting Security Holes*. Hoboken, NJ: John Wiley & Sons, 2007.

HOGL04 Hoglund, G., and McGraw, G. *Exploiting Software: How to Break Code*, Reading, MA: Addison Wesley, 2004.

KUPE05 Kuperman, B., et al. "Detection and Prevention of Stack Buffer Overflow Attacks." *Communications of the ACM*, November 2005.

LEVY96 Levy, E., "Smashing The Stack For Fun And Profit." *Phrack Magazine*, file 14, Issue 49, November 1996.

LHEE03 Lhee, K., and Chapin, S., "Buffer Overflow and Format String Overflow Vulnerabilities." *Software – Practice and Experience*, Volume 33, 2003.

STAL15 Stallings, W. *Operating Systems: Internals and Design Principles, Eighth Edition*. Upper Saddle River, NJ: Pearson, 2015.

STAL16 Stallings, W. *Computer Organization and Architecture: Designing for Performance, Tenth Edition*. Upper Saddle River, NJ: Pearson, 2014.

VEEN12 van der Veen, V., dutt-Sharma, N., Cavallaro, L., and Bos, H. "Memory errors: the past, the present, and the future." in Proceedings of the 15th international conference on Research in Attacks, Intrusions, and Defenses (RAID'12), Springer-Verlag, pp86-106, 2012.

Chapter 11 — Software Security

[MCGR06] updates and extends [VIEG01**],** and both are widely cited as key references discussing the general topic of software security. [HOWA07] discusses many specific details on writing secure code for Microsoft Windows systems, and [WHEE03] provides similar details for Linux and UNIX systems. [NIST04] provides a set of general principles for IT security that can be applied specifically to software security. [SIMP11] describes a set of industry best secure development practices, successfully used by SAFECode members. [MILL07] is the latest in a series of papers by these authors discussing the use of fuzzing to test applications running on common operating systems. [LAND94] is a useful compilation of security flaws in program code, well worth studying.

HOWA07 Howard, M., and LeBlanc, D. *Writing Secure Code for Windows Vista*, Redmond, WA: Microsoft Press, 2007.

LAND94 Landwehr, C., et al. "A Taxonomy of Computer Program Security Flaws." *ACM Computing Surveys*, September 1994.

MCGR06 McGraw, G. *Software Security: Building Security In*. Reading, MA: Addison-Wesley, 2006.

MILL07 Miller, B.; Cooksey, G.; and Moore, F. "An Empirical Study of the Robustness of MacOS Applications Using Random Testing." *ACM SIGOPS Operating Systems Review*, Volume 41 Issue 1, January 2007.

NIST04 National Institute of Standards and Technology, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*. Special Publication 800-27 Rev A, June 2004.

SIMP11 Simpson, S. (ed) "Fundamental Practices for Secure Software Development" 2/e, SAFECode, February 2011.

VIEG01 Viega, J., and McGraw, G. *Building Secure Software: How to Avoid Security Problems the Right Way*. Reading, MA: Addison-Wesley, 2001.

WHEE03 Wheeler, D. *Secure Programming for Linux and UNIX HOWTO*, Linux Documentation Project, 2003.

CHAPTER 18 SECURITY AUDITING

[CCPS12b], [FRAS97], and [NIST95] each has a useful chapter or section on security auditing. The following standards documents cover the topics of this chapter: [KENT06] and [ITUT95]. [KUPE04] is a lengthy treatment of the topic.

[EATO03] is an excellent treatment of syslog.

[MERC03] discusses audit trails and their proper use. [SING04] provides a useful description of both UNIX syslog and the Windows Event Log. [ZHOU04] describes techniques for application-level auditing that do not require recompilation. [HELM93] provides statistical models of misuse

detection based on analysis of audit trails and shows that careful selection of transaction attributes can improve detection accuracy.

CCPS12b Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements.* CCIMB-2004-01-002, January 2012.

EATO03 Eaton, I. *The Ins and Outs of System Logging Using Syslog.* SANS Institute InfoSec Reading Room, February 2003.

FRAS97 Fraser, B. *Site Security Handbook.* RFC 2196, September 1997.

HELM93 Helman, P., and Liepins, G. "Statistical Foundations of Audit Trail Analysis for the Detection of Computer Misuse." *IEEE Transactions on Software Engineering*, September 1993.

ITUT95 Telecommunication Standardization Sector of the International Telecommunications Union (ITU-T). *Security Audit and Alarms Framework.* X.816, November 1995.

KENT06 Kent, K., and Souppaya, M. *Guide to Computer Security Log Management.* NIST Special Publication 800-92, September 2006.

KUPE04 Kuperman, B. *A Categorization of Computer Security Monitoring Systems and the Impact on the Design of Audit Sources.* CERIAS Tech Report 2004-26; Purdue U. Ph.D. Thesis, August 2004. www.cerias.purdue.edu/

MERC03 Mercuri, R. "On Auditing Audit Trails." *Communications of the ACM*, January 2003.

NIST95 National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook.* Special Publication 800-12, October 1995.

SING04 Singer, A., and Bird, T. *Building a Logging Infrastructure.* Short Topics in System Administration, Published by USENIX Association for Sage, 2004. sageweb.sage.org

ZHOU04 Zhou, J., and Vigna, G. "Detecting Attacks that Exploit Application-Logic Errors Through Application-Level Auditing." *Proceedings of the 20th Annual Computer Security Applications Conference (ACSAC'04),* 2004.