# REFERENCES

## ABBREVIATIONS

ACM         Association for Computing Machinery
IEEE        Institute of Electrical and Electronics Engineers
NIST        National Institute of Standards and Technology
RFC         Request for Comments

**ACM04**   The Association for Computing Machinery. USACM Policy Brief: Digital Millennium Copyright Act (DMCA). February 6, 2004. acm.org/usacm/Issues/DMCA.htm

**ADAM89**  Adam, N., and Wortmann, J. "Security-Control Methods for Statistical Databases: A Comparative Study." *ACM Computing Surveys*, December 1989.

**ADSD06**  Australian Defence Signals Directorate, "ACSI33—Australian Communications-Electronic Security Instruction 33," ISB DSD, 2006.

**AGOS06**  Agosta, J., et al. "Towards Autonomic Enterprise Security: Self-Defending Platforms, Distributed Detection, and Adaptive Feedback." *Intel Technology Journal*, November 9, 2006. developer.intel.com/technology/itj

**ALEX04**  Alexander, S. "Password Protection for Modern Operating Systems." *;login*, June 2004.

**ANDE80**  Anderson, J. *Computer Security Threat Monitoring and Surveillance.* Fort Washington, PA: James P. Anderson Co., April 1980.

**ANDE93**  Anderson, R., et al. "Using the New ACM Code of Ethics in Decision Making." *Communications of the ACM*, February 1993.

**ANDE95**  Anderson, D., et al. *Detecting Unusual Program Behavior Using the Statistical Component of the Next-generation Intrusion Detection Expert System (NIDES).* Technical Report SRI-CSL-95–06, SRI Computer Science Laboratory, May 1995. www. csl.sri.com/programs/intrusion

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

**ANTE06**  Ante, S., and Grow, B. "Meet the Hackers." *Business Week*, May 29, 2006.

**ANTH07**  Anthes, G. "Computer Security: Adapt or Die." *ComputerWorld*, January 8, 2007.

**AUDI04**  Audin, G. "Next-Gen Firewalls: What to Expect." *Business Communications Review*, June 2004.

**AXEL00**  Axelsson, S. "The Base-Rate Fallacy and the Difficulty of Intrusion Detection." *ACM Transactions and Information and System Security*, August 2000.

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

**BACE00**  Bace, R. *Intrusion Detection.* Indianapolis, IN: Macmillan Technical Publishing, 2000.

**BAIL05**  Bailey, M., et al. "The Internet Motion Sensor: A Distributed Blackhole," *Proceedings of the Network and Distributed System Security Symposium Conference*, February 2005.

**BALA98**  Balasubramaniyan, J., et al. "An Architecture for Intrusion Detection Using Autonomous Agents." *Proceedings, 14th Annual Computer Security Applications Conference*, 1998.

**BARH80**    Bar-Hillel, M. "The Base-Rate Fallacy in Probability Judgements." *Acta Psychologica*, May 1980.

**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.

**BARR03**    Barreto, P., and Rijmen, V. "The Whirlpool Hashing Function." *Submitted to NESSIE*, September 2000, revised May 2003.

**BAUE88**    Bauer, D., and Koblentz, M. "NIDX—An Expert System for Real-Time Network Intrusion Detection." *Proceedings, Computer Networking Symposium*, April 1988.

**BAUE04**    Bauer, M. "Linux Filesystem Security, Part I and Part II." *Linux Journal*, October and November 2004.

**BAUE05**    Bauer, M. *Linux Server Security, Second Edition*. Sebastopol, CA: O'Reilly Media, 2005.

**BAUE06**    Bauer, M. "An Introduction to Novell AppArmor." *Linux Journal*, August 2006.

**BAUE07**    Bauer, M. "Introduction to SELinux." *Linux Journal*, February 2007.

**BELL73**    Bell, D., and LaPadula, L. "Secure Computer Systems: Mathematical Foundations." *MTR–2547, Vol. I*, The MITRE Corporation, Bedford, MA, 1 March 1973. (ESD–TR–73–278–I)

**BELL75**    Bell, D., and LaPadula, L. "Secure Computer Systems: Unified Exposition and Multics Interpretation." *MTR–2997*, The MITRE Corporation, Bedford, MA, July 1975. (ESD–TR–75–306)

**BELL94a**   Bellare, M, and Rogaway, P. "Optimal Asymmetric Encryption—How to Encrypt with RSA." *Proceedings, Eurocrypt '94*, 1994.

**BELL94b**   Bellovin, S., and Cheswick, W. "Network Firewalls." *IEEE Communications Magazine*, September 1994.

**BELL96**    Bellare, M.; Canetti, R.; and Krawczyk, H. "Keying Hash Functions for Message Authentication." *Proceedings, CRYPTO '96*, August 1996; published by Springer-Verlag. An expanded version is available at http://www-cse.ucsd.edu/users/mihir

**BELL05**    Bell, D. "Looking Back at the Bell-Lapadula Model." *Proceedings, 21st Annual IEEE Computer Security Applications Conference*, 2005.

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

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

**BHAT03**    Bhatkar, S.; DuVarney, D.; and Sekar, R. "Address Obfuscation: An Efficient Approach to Combat a Broad Range of Memory Error Exploits." *Proceedings, 12th Unix Security Symposium*, 2003.

**BHAT07**    Bhatti, R.; Bertino, E.; and Ghafoor, A. "An Integrated Approach to Federated Identity and Privilege Management in Open Systems." *Communications of the ACM*, February 2007.

**BIBA77**    Biba, K. "Integrity Considerations for Secure Computer Systems," *ESD-TR-76–372*, ESD/AFSC, Hanscom AFB, Bedford, Mass., April 1977

**BIDG06**    Bidgoli, H., editor. *Handbook of Information Security*. New York: Wiley, 2006.

**BLOO70**    Bloom, B. "Space/time Trade-offs in Hash Coding with Allowable Errors." *Communications of the ACM,* July 1970.

**BLUM86**   Blum, L.; Blum, M.; and Shub, M. "A Simple Unpredictable Pseudo-Random Number Generator." *SIAM Journal on Computing*, No. 2, 1986.

**BOSW02**   Boasworth, S., and Kabay, M., eds. *Computer Security Handbook*. New York: Wiley, 2002.

**BOWE06**   Bowen, P.; Hash, J.; and Wilson, M. *Information Security Handbook: A Guide for Managers*. NIST Special Publication 800-100. October 2006.

**BRAU01**   Braunfeld, R., and Wells, T. "Protecting Your Most Valuable Asset: Intellectual Property." *IT Pro*, March/April 2000.

**BREW89**   Brewer, D., and Nash, M. "The Chinese Wall Security Policy." *IEEE Symposium on Security and Privacy*, 1989.

**BRIG79**   Bright, H., and Enison, R. "Quasi-Random Number Sequences from Long-Period TLP Generator with Remarks on Application to Cryptography." *Computing Surveys*, December 1979.

**BR0095**   Brooks, F. *The Mythical Man-Month: Essays on Software Engineering*. Reading, MA: Addison-Wesley, 1995.

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

**BRYA88**   Bryant, W. *Designing an Authentication System: A Dialogue in Four Scenes*. Project Athena document, February 1988. Available at http://web.mit.edu/kerberos/www/ dialogue.html

**BURR04**   Burr, W.; Dodson, D.; and Polk, W. *Electronic Authentication Guideline*. Gaithersburg, MD: National Institute of Standards and Technology, Special Publication 800-63, September 2004.

**CALA99**   Calabrese, C. "The Trouble with Biometrics."*; login*, August 1999.

**CAMP03**   Camp, L. " First Principles of Copyright for DRM Design." *IEEE Internet Computing*, May/June 2003.

**CAMP05**   Campbell, P. "The Denial-of-Service Dance." *IEEE Security and Privacy*, November–December 2005.

**CARL06**   Carl, G., et al. "Denial-of-Service Attack-Detection Techniques." *IEEE Internet Computing*, January–February 2006.

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

**CCPS04a**   Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model*. CCIMB-2004-01-001, January 2004.

**CCPS04b**   Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements*. CCIMB-2004-01-002, January 2004.

**CCPS06**   Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components*. CCIMB-2006-09-003, September 2006.

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

**CHAN05**   Chandra, A., and Calderon, T. "Challenges and Constraints to the Diffusion of Biometrics in Information Systems." *Communications of the ACM*, December 2005.

**CHAP00**   Chapman, D., and Zwicky, E. *Building Internet Firewalls*. Sebastopol, CA: O'Reilly, 2000.

**CHAP06** Chapman, C. "Fundamental Ethics in Information Systems." *Proceedings of the 39th Hawaii International Conference on System Sciences*, 2006.

**CHEN98** Cheng, P., et al. "A Security Architecture for the Internet Protocol." *IBM Systems Journal,* Number 1, 1998.

**CHEN04** Chen, S., and Tang, Y. "Slowing Down Internet Worms," *Proceedings of the 24th International Conference on Distributed Computing Systems*, 2004.

**CHES97** Chess, D. "The Future of Viruses on the Internet." *Proceedings, Virus Bulletin International Conference*, October 1997.

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

**CHEU06** Cheling, S. "Denial of Service Against the Domain Name System." *IEEE Security and Privacy*, January–February 2006.

**CHIN05** Chinchani, R., and Berg, E. "A Fast Static Analysis Approach to Detect Exploit Code Inside Network Flows." *Recent Advances in Intrusion Detection, 8th International Symposium*, 2005.

**CHOK92** Chokhani, S. "Trusted Products Evaluation." *Communications of the ACM*, July 1992.

**CLAR87** Clark, D., and Wilson, D. "A Comparison of Commercial and Military Computer Security Policies." *IEEE Symposium on Security and Privacy*, 1987.

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

**COHE94** Cohen, F. *A Short Course on Computer Viruses.* New York: Wiley, 1994.

**COKE05** Coker, F., and Coker, R. " Taking Advantage of SELinux in Red Hat® Enterprise Linux®." *Red Hat Magazine*, April 2005. redhat.com/magazine/006apr05/features/selinux

**COLL06** Collett, S. "Encrypting Data at Rest." *Computerworld*, March 27, 2006.

**COMP06** Computer Associates International. *The Business Value of Identity Federation.* White Paper, January 2006.

**CONR02** Conry-Murray, A. "Behavior-Blocking Stops Unknown Malicious Code." *Network Magazine*, June 2002.

**CORM01** Cormen, T.; Leiserson, C.; Rivest, R.; and Stein, C. *Introduction to Algorithms.* Cambridge, MA: MIT Press, 2001.

**COST05** Costa, M., et al. "Vigilante: End-to-end Containment of Internet Worms." *ACM Symposium on Operating Systems Principles*. 2005.

**COVE03** Coventry, L.; Angeli, A.; and Johnson, G. "Usability and Biometric Verification at the ATM Interface." *Proceedings, 2003 ACM Conference on Human Factors in Computing*, 2003.

**CREM06** Cremonini, M. "Network-Based Intrusion Detection Systems." In [BIDG06].

**CURR94** Curry, T. "Profiling and Tracing Dynamic Library Usage Via Interposition." *USENIX Summer 1994 Technical Conference*, Summer 1994.

**CYMR06** Team Cymru, "Cybercrime: An Epidemic." *ACM Queue*, November 2006.

**DAMG89** Damgard, I. "A Design Principle for Hash Functions." *Proceedings, CRYPTO '89*, 1989; published by Springer-Verlag.

**DAMI03** Damiani, E., et al. " Balancing Confidentiality and Efficiency in Untrusted Relational Databases." *Proceedings, Tenth ACM Conference on Computer and Communications Security*, 2003.

**DAMI05**   Damiani, E., et al. " Key Management for Multi-User Encrypted Databases." *Proceedings, 2005 ACM Workshop on Storage Security and Survivability*, 2005.

**DAMR03**   Damron, J. "Identifiable Fingerprints in Network Applications."*; login*, December 2003.

**DAUG06**   Daugman, J. "Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons." *Proceedings of the IEEE*, November 2006.

**DAVI89**   Davies, D., and Price, W. *Security for Computer Networks.* New York: Wiley, 1989.

**DAVI93**   Davies, C., and Ganesan, R. "BApasswd: A New Proactive Password Checker." *Proceedings, 16th National Computer Security Conference,* September 1993.

**DAWS96**   Dawson, E., and Nielsen, L. "Automated Cryptoanalysis of XOR Plaintext Strings." *Cryptologia*, April 1996.

**DEFW96**   Dean, D., Felten, E., and Wallach, D. "Java Security: From HotJava to Netscape and Beyond." *Proceedings IEEE Symposium on Security and Privacy*, IEEE, May 1996.

**DENN71**   Denning, P. "Third Generation Computer Systems." *ACM Computing Surveys*, December 1971.

**DENN79**   Denning, D., and Denning P. "The Tracker: A Threat to Statistical Database Security." *ACM Transactions on Database Systems*, March 1979.

**DENN82**   Denning, D. *Cryptography and Data Security.* Reading, MA: Addison-Wesley, 1982.

**DENN85**   Denning, D. "Commutative Filters for Reducing Interference Threats in Multilevel Database Systems." *Proceedings of 1985 IEEE Symposium on Security and Privacy*, 1985.

**DENN87**   Denning, D. "An Intrusion-Detection Model." *IEEE Transactions on Software Engineering,* February 1987.

**DHEM01**   Dhem, J., and Feyt, N. "Hardware and Software Symbiosis Help Smart Cart Evolution." *IEEE Micro*, November/December 2001.

**DIFF76**   Diffie, W., and Hellman, M. "New Directions in Cryptography." *Proceedings of the AFIPS National Computer Conference*, June 1976.

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

**DIFF88**   Diffie, W. "The First Ten Years of Public-Key Cryptography." *Proceedings of the IEEE*, May 1988. Reprinted in [SIMM92].

**DINU03**   Dinur, I., and Nissim, K. "Revealing Information while Preserving Privacy." *Proceedings of the 22nd ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, 2003.

**DISA95**   Defense Information Systems Agency. *Database Security Technical Implementation Guide.* Department of Defense, 30 November 2005. csrc.nist.gov/pcig/STIGs/database-stig-v7r2.pdf

**DOBB96**   Dobbertin, H. "The Status of MD5 After a Recent Attack." *CryptoBytes*, Summer 1996.

**DOJ00**   U.S. Department of Justice. *The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet.* March 2000. usdoj.gov/criminal/cybercrime/ unlawful.htm

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

**DWOR06**    Dwork, C., et al. "Our Data, Ourselves: Privacy via Distributed Noise Generation." *Advances in Cryptology — Eurocrypt 2006*, 2006.

**EFF98**    Electronic Frontier Foundation. *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design.* Sebastopol, CA: O' Reilly, 1998

**ENGE80**    Enger, N., and Howerton, P. *Computer Security.* New York: Amacom, 1980.

**ENGL03**    England, P., et al. "A Trusted Open Platform." *Computer*, July 2003.

**EVFI03**    Evfimievski, A., et al. "Limiting Privacy Breaches in Privacy Preserving Data Mining." *Proceedings of the 22nd ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, 2003.

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

**FEIS73**    Feistel, H. "Cryptography and Computer Privacy." *Scientific American*, May 1973.

**FELT03**    Felten, E. "Understanding Trusted Computing: Will Its Benefits Outweigh Its Drawbacks?" *IEEE Security and Privacy*, May/June 2003.

**FEMA03**    Federal Emergency Management Administration. *Emergency Management Guide for Business and Industry.* FEMA 141, October 1993.

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

**FERR98**    Ferrari, J, and Poh, S. *Smart Cards: A Case Study.* IBM Redbook SG24–5239–00. http://www.redbooks.ibm.com, October 1998.

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

**FLUH01**    Fluhrer, S.; Mantin, I.; and Shamir, A. "Weakness in the Key Scheduling Algorithm of RC4." *Proceedings, Workshop in Selected Areas of Cryptography,* 2001.

**FORR97**    Forrest, S.; Hofmeyr, S.; and Somayaji, A. "Computer Immunology." *Communications of the ACM*, October 1997.

**FORR06**    Forristal, J. "Physical/Logical Convergence." *Network Computing*, November 23, 2006.

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

**GARD77**    Gardner, M. "A New Kind of Cipher That Would Take Millions of Years to Break." *Scientific American*, August 1977.

**GARR06**    Garris, M.; Tabassi, E.; and Wilson, C. "NIST Fingerprint Evaluations and Developments." *Proceedings of the IEEE*, November 2006.

**GASS88**    Gasser, M. *Building a Secure Computer System*. New York: Van Nostrand Reinhold, 1988.

**GAUD00**    Gaudin, S. "The Omega Files." *Network World*, June 26, 2000.

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

**GIBB00**    Gibbs, J. "The Digital Millennium Copyright Act." *ACM Ubiquity*, August 2000.

**GOTT99**    Gotterbarn, D. " How the New Software Engineering Code of Ethics Affects You." *IEEE Software*, November/ December 1999.

**GOWA01**    Goldberg, I., and Wagner, D. "Randomness and the Netscape Browser." *Dr. Dobb's Journal*, July 22, 2001.

**GOYE99**    Goyeneche, J., and Souse, E. "Loadable Kernel Modules." *IEEE Software*, January/ February 1999.

**GRAH72**    Graham, G., and Denning, P. "Protection—Principles and Practice." *Proceedings, AFIPS Spring Joint Computer Conference*, 1972.

**GRAN04**    Grance, T.; Kent, K.; and Kim, B. *Computer Security Incident Handling Guide.* NIST Special Publication SP 800-61, January 2004.

**GRIF76**    Griffiths, P., and Wade, B. "An Authorization Mechanism for a Relational Database System." *ACM Transactions on Database Systems*, September 1976.

**GUTM96**    Gutmann, P. "Secure Deletion of Data from Magnetic and Solid-State Memory." *Proceedings of the Sixth USENIX Security Symposium*, San Jose, California, July 22–25, 1996.

**GUTM02**    Gutmann, P. "PKI: It's Not Dead, Just Resting." *Computer*, August 2002.

**HACI02**    Hacigumus, H., et al. "Executing SQL over Encrypted Data in the Database-Service-Provider Model." *Proceedings, 2002 ACM SIGMOD International Conference on Management of Data*, 2002.

**HAMD06**    Hamdi, M.; Boudriga, N.; and Obaidat, M. "Security Policy Guidelines." In [BIDG06].

**HAMM91**    Hamming, R. *The Art of Probability for Scientists and Engineers.* Reading, MA: Addison-Wesley, 1991.

**HARR76**    Harrison, M.; Ruzzo, W.; and Ullman, J. "Protection in Operating Systems." *Communications of the ACM*, August 1976.

**HARR90**    Harrington, S., and McCollum, R. "Lessons from Corporate America Applied to Training in Computer Ethics." *Proceedings of the ACM Conference on Computers and the Quality of Life (SIGCAS and SIGCAPH)*, September 1990.

**HAYE02**    Hayes, B.; Judy, H.; and Ritter, J. "Privacy in Cyberspace." In [BOSW02].

**HAYE06**    Hayes, B., and Marshall, M. "The Real Inside Man." *Redspin White Paper*, Redspin, Inc. April 2006. www.redspin.com

**HEBE92**    Heberlein, L.; Mukherjee, B.; and Levitt, K. "Internetwork Security Monitor: An Intrusion-Detection System for Large-Scale Networks." *Proceedings, 15th National Computer Security Conference,* October 1992.

**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.

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

**HONE01**    The Honeynet Project. *Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community.* Reading, MA: Addison-Wesley, 2001.

**HONE05**    Honeynet Project. *Knowing Your Enemy: Tracking Botnets.* Honeynet White Paper, March 2005. http://honeynet.org/papers/bots

**HOWA98**    Howard, J., and Longstaff, T. *A Common Language for Computer Security Incidents.* Sandia Report SAND98-8667, Sandia National Laboratories, October 1998.

**HOWA02a** Howard, M., and LeBlanc, D. *Writing Secure Code, Second Edition,* Redmond, WA: Microsoft Press, 2002.

**HOWA02b** Howard, J., and Meunier, P. "Using a Common Language for Computer Security Incident Information." In [BOSW02].

**HOWA04** Howard, M. "Browsing the Web and Reading E-mail Safely as an Administrator." *MSDN Library*, November 15, 2004. http://msdn2.microsoft.com/en-us/library/ ms972827.aspx

**HOWA06** Howard, M., and Lipner, S. *The Security Development Lifecycle.* Redmond, WA: Microsoft Press, 2006.

**HOWA07** Howard, M., and LeBlanc, D. *Writing Secure Code for Windows Vista .* Redmond, WA: Microsoft Press, 2006.

**HUIT98** Huitema, C. *IPv6: The New Internet Protocol.* Upper Saddle River, NJ: |Prentice Hall, 1998.

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

**IANN06** Iannella, R. "Digital Rights Management." In [BIDG06].

**ILGU95** Ilgun, K.: Kemmerer, R.; and Porras, P. "State Transition Analysis: A Rule-Based Intrusion Detection Approach." *IEEE Transaction on Software Engineering,* March 1995.

**ISAT02** Information Science and Technology Study Group. "Security with Privacy," *DARPA Briefing on Security and Privacy*, Dec. 2002. www.cs.berkeley.edu/~tygar/papers/ISAT-final-briefing.pdf

**ISF05** Information Security Forum. *The Standard of Good Practice for Information Security.* 2005. www.securityforum.org

**ISO12207** ISO/IEC, *ISO/IEC 12207:1997—Information technology—Software lifecycle processes*.

**ISO13335** ISO/IEC, "ISO/IEC 13335—1:2004—Information technology—Security techniques—Management of information and communications technology security—Part 1: Concepts and models for information and communications technology security management." Part 2 on operational guidance for ICT security management will be released soon.

**ISO17799** ISO/IEC, "ISO/IEC 17799:2005—Information technology—Security techniques—Code of practice for information security management." Will be replaced by ISO27002.

**ISO27001** ISO/IEC, "ISO/IEC 27001:2005—Information technology—Security Techniques—Information security management systems—Requirements." This replaces the older Australian and British national standards AS7799.2 and BS7799.2.

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

**JAIN91** Jain, R. *The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, Simulation, and Modeling.* New York: Wiley, 1991.

**JAIN00** Jain, A.; Hong, L.; and Pankanti, S. "Biometric Identification." *Communications of the ACM*, February 2000.

**JAKO98**    Jakobsson, M.; Shriver, E.; Hillyer, B.; and Juels, A. "A Practical Secure Physical Random Bit Generator." *Proceedings of The Fifth ACM Conference on Computer and Communications Security*, November 1998.

**JAME06**    James, A. "UTM Thwarts Blended Attacks." *Network World*, October 2, 2006.

**JANS01**    Jansen, W. *Guidelines on Active Content and Mobile Code.* NIST Special Publication SP 800-28, October 2001.

**JAVI91**    Javitz, H., and Valdes, A. "The SRI IDES Statistical Anomaly Detector." *Proceedings, 1991 IEEE Computer Society Symposium on Research in Security and Privacy*, May 1991.

**JHI07**    Jhi, Y., and Liu, P. "PWC: A Proactive Worm Containment Solution for Enterprise Networks." To appear.

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

**JUEN85**    Jueneman, R.; Matyas, S.; and Meyer, C. "Message Authentication." *IEEE Communications Magazine*, September 1988.

**JUN99**    Jun, B., and Kocher, P. *The Intel Random Number Generator.* Intel White Paper, April 22, 1999.

**JUNG04**    Jung, J.; et al. "Fast Portscan Detection Using Sequential Hypothesis Testing," *Proceedings, IEEE Symposium on Security and Privacy*, 2004.

**KABA02a**    Kabay, M. "Security Policy Guidelines." In [BOSW02].

**KABA02b**    Kabay, M. "Employment Practices and Policies." In [BOSW02].

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

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

**KAND05**    Kandula, S. "Surviving DDoS Attacks."*; login*, October 2005.

**KELL06**    Kelly, C. "Cutting through the Fog of Security Data." *ComputerWorld*, September 25, 2006.

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

**KENT05**    Kenthapadi, K.; Mishra, N.; and Nissim, K. "Simulatable Auditing." *Proceedings of the 24th ACM Symposium on Principles of Database Systems*, 2005.

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

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

**KEPH97b**    Kephart, J.; Sorkin, G.; Swimmer, B.; and White, S. "Blueprint for a Computer Immune System." *Proceedings, Virus Bulletin International Conference*, October 1997.

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

**KIRK06**    Kirk, J. "Tricky New Malware Challenges Vendors." *Network World*, October 30, 2006.

**KING06**    King, N. "E-Mail and Internet Use Policy." In [BIDG06].

**KLEI90**    Klein, D. "Foiling the Cracker: A Survey of, and Improvements to, Password Security." *Proceedings, UNIX Security Workshop II*, August 1990.

**KOBL92**    Koblas, D., and Koblas, M. "SOCKS." *Proceedings, UNIX Security Symposium III*, September 1992.

**KOCH96**    Kocher, P. "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems." *Proceedings, Crypto '96*, August 1996.

**KOHL94**    Kohl, J.; Neuman, B.; and Ts'o, T. "The Evolution of the Kerberos Authentication Service." In Brazier, F., and Johansen, D. *Distributed Open Systems.* Los Alamitos, CA: IEEE Computer Society Press, 1994. Available at http://web.mit.edu/kerberos/ www/papers.html

**KOZI04**    Koziol, J. *The Shellcoder's Handbook : Discovering and Exploiting Security Holes*. Hoboken, NJ: John Wiley & Sons, 2004.

**KSHE06**    Kshetri, N. "The Simple Economics of Cybercrimes." *IEEE Security and Privacy*, January/February 2006.

**KUMA97**    Kumar, I. *Cryptology.* Laguna Hills, CA: Aegean Park Press, 1997.

**KUPE99**    Kuperman, B., and Spafford, E. "Generation of Application Level Audit Data via Library Interposition." *CERIAS Tech Report 99–11*. Purdue U., October 1999. www.cerias.purdue.edu

**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/

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

**LAMP69**    Lampson, B. "Dynamic Protection Structures." *Proceedings, AFIPS Fall Joint Computer Conference*, 1969.

**LAMP71**    Lampson, B. "Protection." Proceedings, *Fifth Princeton Symposium on Information Sciences and Systems*, March 1971; Reprinted in *Operating Systems Review*, January 1974.

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

**LAND81**    Landwehr, C. "Formal Models for Computer Security." *Computing Surveys*, September 1981.

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

**LEHM51**    Lehmer, D. "Mathematical Methods in Large-Scale Computing." *Proceedings, 2nd Symposium on Large-Scale Digital Calculating Machinery,* Cambridge, MA: Harvard University Press, 1951.

**LEUT94**    Leutwyler, K. "Superhack." *Scientific American*, July 1994.

**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*, May–June 2005.

**LEVY96**    Levy, E., "Smashing The Stack for Fun and Profit." *Phrack Magazine*, Vol. 7, Issue 49, November 1996. insecure.org/stf/smashstack.html

**LEVY05**    Levy, E., and Arce, I. "A Short Visit to the Bot Zoo." *IEEE Security and Privacy*, January–February 2006.

**LEWI69**    Lewis, P.; Goodman, A.; and Miller, J. "A Pseudo-Random Number Generator for the System/360." *IBM Systems Journal*, No. 2, 1969.

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

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

**LINN06**    Linn, J. "Identity Management." In [BIDG06].

**LIPM00**    Lipmaa, H.; Rogaway, P.; and Wagner, D. "CTR Mode Encryption." *NIST First Modes of Operation Workshop*, October 2000. http://csrc.nist.gov/encryption/modes

**LITC03**    Litchfield, D. "Defeating the Stack Based Buffer Overflow Prevention Mechanism of Microsoft Windows 2003 Server." *NGS Software White Paper*, 8 September 2003. ngssoftware.com/papers/defeating-w2k3-stack-protection.pdf

**LIU01**    Liu, S., and Silverman, M. "A Practical Guide to Biometric Security Technology." *IT Pro*, January/February 2001,

**LIU03**    Liu, Q.; Safavi-Naini, R.; and Sheppard, N. "Digital Rights Management for Content Distribution." *Proceedings, Australasian Information Security Workshop 2003 (AISW2003),* 2003.

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

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

**LUNT89**    Lunt, T. "Aggregation and Inference: Facts and Fallacies." *Proceedings, 1989 IEEE Symposium on Security and Privacy*, 1989,

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

**MAEK87**    Maekawa, M.; Oldehoeft, A.; and Oldehoeft, R. *Operating Systems: Advanced Concepts.* Menlo Park, CA: Benjamin Cummings, 1987.

**MAIW02**    Maiwald, E. and Sieglein, W. *Security Planning & Disaster Recovery*, Berkeley, CA: McGraw-Hill/Osborne, 2002.

**MANS01**    Mansfield, T.; et al. Biometric Product Testing Final Report. National Physics Laboratory, United Kingdom, March 2001. www.cesg.gov.uk/site/ast/biometrics/media/Biometric TestReportpt1.pdf

**MARK97**    Markham, T. "Internet Security Protocol." *Dr. Dobb's Journal*, June 1997.

**MART73**    Martin, J. *Security, Accuracy, and Privacy in Computer Systems.* Englewood Cliffs, NJ: Prentice Hall, 1973.

**MAYE07**    Mayer, F., MacMillan, K., and Caplan, D. *SELinux by Example: Using Security Enhanced Linux*. Upper Saddle River, NJ: Prentice Hall, 2007.

**MCCA05**    McCarty, B. *SELinux: NSA's Open Source Security Enhanced Linux*. Sebastopol, CA: O'Reilly Media, 2005.

**MCGO02**    McGovern, M. "Opening Eyes: Building Company-Wide IT Security Awareness." *IT Pro*, May/June 2002.

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

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

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

**MEIN01**    Meinel, C. "Code Red for the Web." *Scientific American*, October 2001.

**MENE97**    Menezes, A.; van Oorschot, P.; and Vanstone, S. *Handbook of Applied Cryptography.* Boca Raton, FL: CRC Press, 1997.

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

**MERK79**    Merkle, R. *Secrecy, Authentication, and Public Key Systems.* Ph.D. Thesis, Stanford University, June 1979.

**MERK89**    Merkle, R. "One Way Hash Functions and DES." *Proceedings, CRYPTO '89*, 1989; published by Springer-Verlag.

**MESS02**    Messner, E. "Behavior Blocking Repels New Viruses." *Network World*, January 28, 2002.

**MESS06**    Messner, E. " All-in-one Security Devices Face Challenges." *Network World*, August 14, 2006.

**MEYE82**    Meyer, C., and Matyas, S. *Cryptography: A New Dimension in Computer Data Security.* New York: Wiley, 1982.

**MICH06a**    Michael, M. "Physical Security Threats." In [BIDG06].

**MICH06b**    Michael, M. "Physical Security Measures." In [BIDG06].

**MILL06**    Miller, B.; Cooksey, G.; and Moore, F. "An Empirical Study of the Robustness of MacOS Applications Using Random Testing." *First International Workshop on Random Testing*. Portland, Maine, ACM, 2006.

**MIRA05**    Michael, C., and Radosevich, W. *Black Box Security Testing Tools*, US DHS BuildSecurityIn, Cigital, December 2005.

**MIRK04**    Mirkovic, J., and Relher, P. "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms." *ACM SIGCOMM Computer Communications Review*, April 2004.

**MIRK05**    Mirkovic, J., et al. *Internet Denial of Service: Attack and Defense Mechanisms.* Upper Saddle River, NJ: Prentice Hall, 2005.

**MOFF99**    Moffett, J., and Lupu, E. "The Uses of Role Hierarchies in Access Control." *Proceedings of the Fourth ACM Workshop on Role-Based Access Control*, 1999.

**MOOR06**    Moore, D., et al. "Inferring Internet Denial-of-Service Activity." *ACM Transactions on Computer Systems*, May 2006.

**MORG87**    Morgenstern, M. "Security and Inference in Multilevel Database and Knowledge-Base Systems." *ACM SIGMOD Record*, December 1987.

**MORR79**    Morris, R., and Thompson, K. "Password Security: A Case History." *Communications of the ACM*, November 1979.

**NACH97**    Nachenberg, C. "Computer Virus-Antivirus Coevolution." *Communications of the ACM*, January 1997.

**NACH02**    Nachenberg, C. "Behavior Blocking: The Next Step in Anti-Virus Protection." *White Paper*, SecurityFocus.com, March 2002.

**NAI01**    NAI Labs, "Windows Data Protection." *MSDN Library*, October 2001. msdn2. microsoft.com/en-us/library/ms995355.aspx

**NEGI00**    Negin, M., et al. "An Iris Biometric System for Public and Personal Use." *Computer*, February 2000.

**NEME06** Nemeth, E., Snyder, G., and Hein, T. *Linux Administration Handbook,* Edition. Upper Saddle River, NJ: Prentice Hall, 2006.

**NEUM99** Neumann, P., and Porras, P. "Experience with EMERALD to Date." *Proceedings, 1st USENIX Workshop on Intrusion Detection and Network Monitoring*, April 1999.

**NEWS05** Newsome, J.; Karp, B.; and Song, D. "Polygraph: Automatically Generating Signatures for Polymorphic Worms." *IEEE Symposium on Security and Privacy*, 2005.

**NIAP05** National Information Insurance Partnership. Microsoft Windows Server 2003 and Microsoft Windows XP Common Criteria Validation. 6 November 2005. niap.bahialab. com/cc-scheme/st/ST_VID4025.cfm

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

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

**NIST02** National Institute of Standards and Technology. *Risk Management Guide for Information Technology Systems*. Special Publication 800-30. July 2002.

**NIST04a** National Institute of Standards and Technology. *Computer Security Incident Handling Guide*. Special Publication 800–61. January 2004.

**NIST04b** 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.

**NIST05** National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems.* Special Publication 800-53. February 2005.

**NIST06** National Institute of Standards and Technology. *Guide for Developing Security Plans for Federal Information Systems*. Special Publication 800-18 Revision 1. February 2006.

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

**NRC02** National Research Council. *Cybersecurity: Today and Tomorrow.* Washington, DC: National Academy Press, 2002.

**OECH03** Oechslin, P. " Making a Faster Cryptanalytic Time-Memory Trade-Off." *Proceedings, Crypto 03*, 2003.

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

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

**OPPL05** Oppliger, R., and Rytz, R. "Does Trusted Computing Remedy Computer Security Problems?" *IEEE Security and Privacy*, March/April 2005.

**ORMA03** Orman, H. "The Morris Worm: A Fifteen-Year Perspective." *IEEE Security and Privacy*, September/October 2003.

**OSBO00** Osborn, S.; Sandhu, R.; and Munawer, Q. " Configuring Role-Based Access Control to Enforce Mandatory and Discretionary Access Control Policies." *ACM Transactions on Information and System Security*, May 2000,

**PARK88a**    Park, S., and Miller, K. "Random Number Generators: Good Ones are Hard to Find." *Communications of the ACM*, October 1988.

**PARK88b**    Parker, D.; Swope, S.; and Baker, B. *Ethical Conflicts in Information and Computer Science, Technology and Business.* Final Report, SRI Project 2609, SRI International1988.

**PELT07**    Peltier, J. "Identity Management." *SC Magazine*, February 2007.

**PERL99**    Perlman, R. "An Overview of PKI Trust Models." *IEEE Network*, November/December 1999.

**PERR03**    Perrine, T. "The End of crypt() Passwords . . . Please?"*; login*, December 2003.

**PIAT91**    Piattelli-Palmarini, M. "Probability: Neither Rational nor Capricious." *Bostonia*, March 1991.

**PIAT94**    Piattelli-Palmarini, M. *Inevitable Illusions: How Mistakes of Reason Rule Our Minds.* New York: Wiley, 1994.

**PLAT02**    Platt, F. "Physical Threats to the Information Infrastructure." In [BOSW02].

**POPP06**    Popp, R., and Poindexter, J. "Countering Terrorism through Information and Privacy Protection Technologies." *IEEE Security and Privacy*, November/December 2006.

**PORR92**    Porras, P. *STAT: A State Transition Analysis Tool for Intrusion Detection.* Master's Thesis, University of California at Santa Barbara, July 1992.

**PRAB03**    Prabhakar, S.; Pankanti, S.; and Jain, A. "Biometric Recognition: Security and Privacy Concerns." *IEEE Security and Privacy*, March/April 2003.

**PROC01**    Proctor, P., *The Practical Intrusion Detection Handbook.* Upper Saddle River, NJ: Prentice Hall, 2001.

**PROV99**    Provos, N., and Mazieres, D. "A Future-Adaptable Password Scheme." *Proceedings of the 1999 USENIX Annual Technical Conference*, 1999.

**RADC04**    Radcliff, D. "What Are They Thinking?" *Network World*, March 1, 2004.

**RAJA05**    Rajab, M., Monrose, F., and Terzis, A., "On the Effectiveness of Distributed Worm Monitoring," *Proceedings, 14th USENIX Security Symposium*, 2005.

**RAND55**    Rand Corporation. *A Million Random Digits.* New York: The Free Press, 1955. http://www.rand.org/publications/classics/randomdigits

**RAND05**    Randall, J. *Hash Function Update Due to Potential Weakness Found in SHA-1.* RSA Laboratories Tech Notes, March 11, 2005.

**RIBE96**    Ribenboim, P. *The New Book of Prime Number Records.* New York: Springer-Verlag, 1996.

**RIVE78**    Rivest, R.; Shamir, A.; and Adleman, L. "A Method for Obtaining Digital Signatures and Public Key Cryptosystems." *Communications of the ACM*, February 1978.

**ROBB06a**    Robb, D. "Desktop Defenses." *ComputerWorld*, May 22, 2006.

**ROBB06b**    Robb, D. "Better Security Pill Gets Suite-r." *Business Communications Review*, October 2006.

**ROBS95a**    Robshaw, M. *Stream Ciphers.* RSA Laboratories Technical Report TR-701, July 1995. http://www.rsasecurity.com/rsalabs

**ROBS95b**    Robshaw, M. *Block Ciphers.* RSA Laboratories Technical Report TR-601, August 1995. http://www.rsasecurity.com/rsalabs

**ROS06**    Ros, S. "Boosting the SOA with XML Networking." *The Internet Protocol Journal*, December 2006. cisco.com/ipj

**ROTH05**    Roth, D., and Mehta, S. "The Great Data Heist." *Fortune*, May 16, 2005.

**SA04**    Standards Australia, "HB 231:2004—Information Security Risk Management Guidelines." 2004.

**SADO03**    Sadowsky, G., et al. *Information Technology Security Handbook.* Washington, DC: The World Bank, 2003. http://www.infodev-security.net/handbook

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

**SAND94**    Sandhu, R., and Samarati, P. "Access Control: Principles and Practice." *IEEE Communications Magazine*, February 1996.

**SAND96**    Sandhu, R., et al. "Role-Based Access Control Models." *Computer*, September 1994.

**SASN04**    Standards Australia and Standards New Zealand, "AS/NZS 4360:2004: Risk Management." 2004.

**SAUE81**    Sauer, C., and Chandy, K. *Computer Systems Performance Modeling.* Englewood Cliffs, NJ: Prentice Hall, 1981.

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

**SAYD04**    Saydjari, O. "Multilevel Security: Reprise." *IEEE Security and Privacy*, September/October 2004.

**SCAR07**    Scarfone, K., and Mell, P. *Guide to Intrusion Detection and Prevention Systems.* NIST Special Publication SP 800–94, February 2007.

**SCHA01**    Scjaad. A.; Moffett, J.; and Jacob, J. "The Role-Based Access Control System of a European Bank: A Case Study and Discussion." *Proceedings, SACMAT '01*, May 2001.

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

**SCHN00**    Schneier, B. *Secrets and Lies: Digital Security in a Networked World.* New York: Wiley, 2000.

**SEI06**    Software Engineering Institute, *Capability Maturity Model for Development Version 1.2*, Carnegie-Mellon, August 2006.

**SEQU03**    Sequeira, D. "Intrusion Prevention Systems: Security's Silver Bullet?" *Business Communications Review*, March 2003.

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

**SHAS04**    Shasha, D., and Bonnet, P. "Database Systems: When to Use Them and How to Use Them Well." *Dr. Dobb's Journal*, December 2004.

**SHEL02**    Shelfer, K., and Procaccion, J. "Smart Card Evolution." *Communications of the ACM*, July 2002.

**SHIE98**    Shieh, S.; Lin, C.; and Juang, Y. "Controlling Inference and Information Flows in Secure Databases." *1998 Information Security Conference*, May 1998.

**SHIM05**    Shim, S.; Bhalla, G.; and Pendyala, V. "Federated Identity Management." *Computer*, December 2005.

**SIDI05**    Sidiroglou, S., and Keromytis, A. "Countering Network Worms Through Automatic Patch Generation." *IEEE Security and Privacy*, November–December 2005.

**SILB04**    Silberschatz, A.; Galvin, P.; and Gagne, G. *Operating System Concepts with Java.* Reading, MA: Addison-Wesley, 2004.

**SIMM92**    Simmons, G., ed. *Contemporary Cryptology: The Science of Information Integrity.* Piscataway, NJ: IEEE Press, 1992.

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

**SING03**    Singer, A. "Life without Firewalls."*; login*, December 2003,

**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

**SIPO01**    Siponen, N. "Five Dimensions of Information Security Awareness." *Computers and Society*, June 2001.

**SLAY06**    Slay, J., and Koronios, A. *Information Technology Security & Risk Management*, Milton, Qld: John Wiley & Sons Australia, 2006.

**SMIT97**    Smith, R. *Internet Cryptography.* Reading, MA: Addison-Wesley, 1997.

**SNAP91**    Snapp, S., et al. "A System for Distributed Intrusion Detection." *Proceedings, COMPCON Spring '91,* 1991.

**SPAF89**    Spafford, E. "Crisis and Aftermath." *Communications of the ACM*, June 1989.

**SPAF92a**   Spafford, E. "Observing Reusable Password Choices." *Proceedings, UNIX Security Symposium III*, September 1992.

**SPAF92b**   Spafford, E. "OPUS: Preventing Weak Password Choices." *Computers and Security*, No. 3, 1992.

**SPAF00**    Spafford, E., and Zamboni, D. "Intrusion Detection Using Autonomous Agents." *Computer Networks*, October 2000.

**SPIT03**    Spitzner, L. "The Honeynet Project: Trapping the Hackers." *IEEE Security and Privacy*, March/April 2003.

**STAL05**    Stallings, W. *Operating Systems: Internals and Design Principles, Fifth Edition*. Upper Saddle River, NJ: Prentice Hall, 2005.

**STAL06a**   Stallings, W. *Cryptography and Network Security: Principles and Practice, Fourth Edition.* Upper Saddle River, NJ: Prentice Hall, 2003.

**STAL06b**   Stallings, W. *Computer Organization and Architecture: Designing for Performance, Seventh Edition*. Upper Saddle River, NJ: Prentice Hall, 2006.

**STAL06c**   Stallings, W. "The Whirlpool Secure Hash Function." *Cryptologia*, January 2006.

**STEP93**    Stephenson, P. "Preventive Medicine." *LAN Magazine*, November 1993.

**STIN06**    Stinson, D. *Cryptography: Theory and Practice.* Boca Raton, FL: CRC Press, 2006.

**SUEH05**    Suehring, S., and Ziegler, R. *Linux Firewalls, 3rd.* Upper Saddle River, NJ: Novell Press, 2005.

**SUMM84**    Summers, R. "An Overview of Computer Security." *IBM Systems Journal*, Vol. 23, No. 4, 1984.

**SYMA01**    Symantec Corp. *The Digital Immune System.* Symantec Technical Brief, 2001.

**SYMA07**    Symantec. "Security Implications of Microsoft Windows Vista." Symantec Research Paper, 2007. symantec.com

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

**SZUB98**    Szuba, T. *Safeguarding Your Technology.* National Center for Education Statistics, NCES 98–297, 1998. nces.ed.gov/pubsearch/pubsinfo.asp?pubid=98297

**TAVA00**    Tavani, H. " Defining the Boundaries of Computer Crime: Piracy, Break-Ins, and Sabotage in Cyberspace." *Computers and Society*, September 2000.

**THOM84**    Thompson, K. "Reflections on Trusting Trust (Deliberate Software Bugs)." *Communications of the ACM*, August 1984.

**THUR05**    Thuraisingham, B. *Database and Applications Security*. New York: Auerbach, 2005.

**TIME90**    Time, Inc. *Computer Security, Understanding Computers Series*. Alexandria, VA: Time-Life Books, 1990.

**TIPP27**    Tippett, L. *Random Sampling Numbers*. Cambridge, England: Cambridge University Press, 1927.

**TOXE02**    Toxen, B. *Real World Linux Security, 2nd*. Upper Saddle River, NJ: Prentice Hall, 2002.

**TUNS06**    Tunstall, M.; Petit, S.; and Porte, S. "Smart Card Security." In [BIDG06].

**TSUD92**    Tsudik, G. "Message Authentication with One-Way Hash Functions." *Proceedings, INFOCOM '92,* May 1992.

**VACC89**    Vaccaro, H., and Liepins, G. "Detection of Anomalous Computer Session Activity." *Proceedings of the IEEE Symposium on Research in Security and Privacy,* May 1989.

**VANO94**    van Oorschot, P., and Wiener, M. "Parallel Collision Search with Application to Hash Functions and Discrete Logarithms." *Proceedings, Second ACM Conference on Computer and Communications Security*, 1994.

**VENE06**    Venema, W. "Secure Programming Traps and Pitfalls – The Broken File Shredder." *Proceedings of the AusCERT2006 IT Security Conference*, Gold Coast, Australia, May 2006.

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

**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.

**VIGN02**    G. Vigna, G.; Cassell, B.; and Fayram, D. "An Intrusion Detection System for Aglets." *Proceedings of the International Conference on Mobile Agents*, October 2002.

**VIME06**    Vimercati, S., and Paraboschi, S. "Access Control: Principles and Solutions." In [BIDG06].

**WACK02**    Wack, J.; Cutler, K.; and Pole, J. *Guidelines on Firewalls and Firewall Policy*. NIST Special Publication SP 800-41, January 2002.

**WAGN00**    Wagner, D., and Goldberg, I. "Proofs of Security for the UNIX Password Hashing Algorithm." *Proceedings, ASIACRYPT '00*, 2000.

**WANG05**    Wang, X.; Yin, Y.; and Yu, H. "Finding Collisions in the Full SHA-1. *Proceedings, Crypto '05*, 2005; published by Springer-Verlag.

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

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

**WEIP06**    Weippl, E. "Security in E-Learning." In [BIDG06].

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

**WHIT99**    White, S. *Anatomy of a Commercial-Grade Immune System*. IBM Research White Paper, 1999.

**WIEN90**   Wiener, M. "Cryptanalysis of Short RSA Secret Exponents." *IEEE Transactions on Information Theory,* vol. IT-36, 1990.

**WILS98**   Wilson, M., ed. *Information Technology Security Training Requirements: A Role- and Performance-Based Model.* NIST Special Publication 800–16. April 1998.

**WILS05**   Wilson, J. "The Future of the Firewall." *Business Communications Review*, May 2005.

**WORL04**   The World Bank. *Technology Risk Checklist.* May 2004.

**WYK06**   Wyk, K., and Steven, J. " Essential Factors for Successful Software Security Awareness Training." *IEEE Security and Privacy*, September/October 2006.

**YAN04**   Yan, J., et al. "Password Memorability and Security: Empirical Results." *IEEE Security and Privacy*, September/October 2004.

**YONG05**   Yongzheng, W., and Yap, H. "A User-Level Framework for Auditing and Monitoring*." Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005)*, 2005.

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

**ZOU05**   Zou, C., et al. "The Monitoring and Early Detection of Internet Worms." *IEEE/ACM Transactions on Networking*, October 2005.