Security-Specific Bibliography

Carol Dekkers
James McCurley
Dave Zubrow

February 2007

ABSTRACT: Content area bibliography specific to security.

Alhazmi, O. H. and Y. K. Malaiya, "Quantitative Vulnerability Assessment of Systems Software," Proc. Ann. IEEE Reliability and Maintainability Symposium, 2005, pp. 615-620.

Anderson, Ross J. Security Engineering: A Guide to Building Dependable Distributed Systems. New York, NY: Wiley, 2001 (ISBN 0471389226).

Application Security, Inc. Database Security: A Key Component of Application Security. New York, NY: Application Security, Inc., 2004.

Austin, Bob. “The OWASP Application Security Metrics Project,” October 2006.

Biszick-Lockwood, Bar. IEEE P1074/D5, Jan 2006 - Standard for Developing Project Life Cycle Processes. QualityIT, Jan 2006.

Brown, Keith. The .NET Developer's Guide to Windows Security. Boston, MA: Addison Wesley Professional, Microsoft .NET Development Series, 2004 (ISBN 0321228359).

Cannon, J. C. Privacy: What Developers and IT Professionals Should Know. Boston, MA: Addison-Wesley Professional, 2004 (ISBN 0321224094).

Chew, Elizabeth; Swanson, Marianne; Steine, Kevin; Bartol, Nadya; Brown, Anthony; & Robinson, Will. Contingency Planning Guide for Information Technology Systems; Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-34, Revision 1. U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology (2010).

Cohen, Fred. “Security Metrics,” CSI Conference presentation, Nov. 14, 2005.

Corporate Information Security Working Group. Report of the Best Practices and Metrics Teams. Subcommittee on Technology and Information Policy, Intergovernmental Relations and the Census, Government Reform Committee, U.S. House of Representatives (Rev. Jan. 10, 2005).

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

Phone: 412-268-5800
Toll-free: 1-888-201-4479

www.sei.cmu.edu

DISAnet. DoD Information Technology Security Certification & Accreditation Process. Dec. 20, 2000.

Fortify. Metrics That Matter: Quantifying Software Security Risk.

Fortify. Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors.

Foundstone. Hacme Bank™ v2.0, released 5/19/2006 by Foundstone, Inc.

Foundstone. Validator.NET™, released 3/08/2005 by Foundstone, Inc. http://www.foundstone.com.

Geer, Dan. Measuring Security.

Geer, Dan; Soohoo, K.; & Jaquith, A. "Information Security: Why the Future Belongs to the Quants." IEEE Security and Privacy Magazine 1, 4 (July-August 2003): 24-32.

Germanow, Abner; Wysopal, Chris; Geer, Dan; & Darby, Chris.The Injustice of Insecure Software, @stake Security Briefing, February 2002.

Gilliam, D.; Kelly, J.; Powell, J.; & Bishop, M. "Development of a Software Security Assessment Instrument to Reduce Software Security Risk," 144-149. Proceedings of the 10th IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises. Cambridge, MA, June 20-22, 2001. Los Alamitos, CA: IEEE Computer Society, 2001.

Goertzel, K., et al. Software Security Assurance: A State-of-the-Art Report (SOAR). Herndon, VA: Information Assurance Technology Analysis Center (IATAC) and Defense Technical Information Center (DTIC), July 31, 2007.

Graf, Kenneth. Addressing Challenges in Application Security, A WatchFire whitepaper, 2005.

Graff, Mark G. & Van Wyk, Kenneth R. Secure Coding: Principles and Practices. Cambridge, MA: O'Reilly, 2003 (ISBN 0596002424).

Grance, Tim; Hash, Joan; & Stevens, Marc. Security Considerations in the Information System Development Life Cycle; Recommendations of the National Institute of Standards and Technology, NIST SPECIAL PUBLICATION 800-64 REV. 1,Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, (June 2004), U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology.

Hoglund, Greg & McGraw, Gary. Exploiting Software: How to Break Code. Boston, MA: Addison-Wesley, 2004 (ISBN 0201786958).

Howard, Michael. Fending Off Future Attacks by Reducing Attack Surface (2003).

Howard, Michael & LeBlanc, David C. Writing Secure Code, 2nd ed. Redmond, WA: Microsoft Press, 2002 (ISBN 0735617228).

Institute for Security and Open Methodologies (ISECOM). SPSMM - The Secure Programming Standards Methodology Manual (2001).

ISO. ISO/IEC 27004 Information technology - Security techniques - Information security management measurement.

Jaquith, Andrew. The Security of Applications: Not All Are Created Equal, @stake Security Research Report (2002).

Kimbell, John & Walrath Marjorie. "Life Cycle Security and DITSCAP," IA Newsletter, vol. 4, no. 2, Spring, 2001.

Kleinfeld, Abe. "Measuring Security." EDPACS, Volume 34, Issue 4 October 2006,10-16.

Knorr, Konstantin and Susanne Röhrig. "Security of Electronic Business Applications - Structure and Quantification." Proceedings of the 1st International Conference on Electronic Commerce and Web Technologies EC-Web 2000.

Koziol, Jack; Litchfield, D.; Aitel, D.; Anley, C.; Eren, S.; Mehta, N.; & Riley. H. The Shellcoder's Handbook: Discovering and Exploiting Security Holes. Indianapolis, IN: Wiley Pub, 2004 (ISBN 0764544683).

La, Thien. Secure Software Development and Code Analysis Tools. GIAC Certification: Practical Assignment v1.4b, Option 1, SANS Institute, 2003.

Letteer, Ray A. Information Operations and the DAA (Designated Approving Authority), DISA/IPMO D253 [SAIC] (2001).

Levine, Matthew. The Importance of Application Security. @atstake Security Briefing, January 2003.

Liu, Yanguo and Issa Traore. "UML-based Security Measures of Software Products." Proceedings of MOMPES'04, 1st International Workshop on Model-Based Methodologies for Pervasive and Embedded Software, Hamilton, Ontario, Canada, June 15, 2004.

Manadhata, Pratyusa & Wing, Jeannette M. Measuring a System's Attack Surface CMU-CS-04-102. Pittsburgh, PA: School of Computer Science, Carnegie Mellon University, January 2004.

McGibbon, Thomas; Fedchak, Elaine; & Vienneau, Robert. Software Project Management for Software Assurance: A DACS State of the Art Report, 30 September 2007.

McGraw, Gary. Software Security: Building Security In. Boston, MA: Addison-Wesley Professional, 2006 (ISBN 0-321-35670-5).

Mead, Nancy R. International Liability Issues for Software Quality (CMU/SEI-2003-SR-001, ADA416434). Pittsburgh, PA: CERT Research Center, Software Engineering Institute, Carnegie Mellon University, July 2003.

Microsoft TechNet. Threats and Countermeasures Guide (2003).

Microsoft Developer Network (MSDN).Threat Modeling: Patterns and Practices(2004).

MITRE Corporation. Common Attack Pattern Enumeration and Classification (CAPEC).

MITRE Corporation. Common Vulnerabilities and Exposures (CVE).

MITRE Corporation. Common Weakness Enumeration (CWE).

MITRE Corporation. Making Security Measurable.

National Institute of Standards and Technology.Revised NIST SP 800-26 (Security Self-Assessment Guide for Information Technology Systems, November 2001) System Questionnaire with NIST SP800-53 (Recommended Security Controls for Federal Information Systems, February 2005 (Including updates through 04-22-2005)) References and Associated Security Control Mappings (2005).

National Institute of Standards and Technology. Information Security in the System Development Life Cycle (SDLC) Brochure (2004).

National Security Agency. INFOSEC Assurance Capability Maturity Model (IA-CMM), Version 3.1, Infosec Assurance Training and Rating Program (2004).

Nichols, Betsy and Julia Allen. Building a Security Metrics Program, Transcript, CERT Podcast, Feb 2008.

NIST SP 800-55, Revision 1, Performance Measurement Guide for Information Security, July 2008.

Ounce Labs. Product Overview (2005).

OWASP. CLASP (Comprehensive, Lightweight Application Security Process) Project, Best Practice: Define and Monitor Metrics.

OWASP. A Revised Guide to Building Secure Web Applications and Web Services, 2.1.0 OWASP/vgr Edition. The Open Web Application Security Project (OWASP) (2010).

Payne, Shirley C. A Guide to Security Metrics, SANS Security Essentials GSEC Practical Assignment Version 1.2e, June 19, 2006.

Peikari, Cyrus & Chuvakin, Anton. Security Warrior. Sebastopol, CA :O'Reilly & Associates, Inc, 2004 (ISBN 0596005458).

President's Information Technology Advisory Committee (PITAC), Cyber Security: A Crisis of Prioritization, National Coordination Office for Information Technology Research and Development, Arlington, VA (2005).

Practical Software and Systems Measurement (PSM). Security Measurement, White Paper v3.0 (2006).

Reavis, Jim.Developing Secure Software: The State of the Industry as Determined by the Secure Software Forum. Chief Security Officer White Paper Series for SPI Dynamics, 2006.

Ross, Ron; Swanson, Marianne; Stoneburner, Gary; Katzke, Stu; & Johnson, Arnold. Guide for the Security Certification and Accreditation of Federal Information Systems, NIST Special Publication 800-37, Revision 1, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD. U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology (2010).

Sademies, Anni. Process Approach to Information Security Metrics in Finnish Industry and State Institutions, VTT Electronics, Oulu, Finland (2004).

Schechter, Stuart Edward. Computer Security Strength & Risk: A Quantitative Approach, Doctoral Thesis, Computer Science, Harvard University, Cambridge, Massachusetts, May 2004 (2004).

Seacord, Robert C. Secure Coding in C and C++. Boston, MA: Addison-Wesley, 2005 (ISBN 0321335724).

SecureSoftware, Inc. A Special Report for Managers: Why Application Security Is the New Business Imperative – and How to Achieve It., Secure Software, Inc., McLean VA (2004).

Soo Hoo, Kevin; Jaquith, Andrew; & Geer, Dan. The Security of Applications, Reloaded, @atstake Security Briefing, July, 2003.

Stoneburner, Gary; Hayden, Clark; & Feringa, Alexis. Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, NIST Special Publication 800-27 Rev A, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, and Booz-Allen and Hamilton U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology (2004).

Swanson, Marianne; Bartol, Nadya; Sabato, John; Hash, Joan; & Graffo, Laurie. Security Metrics Guide for Information Technology Systems, NIST Special Publication 800-55, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology (2003).

Trocino, Douglas P. Developing Secure Applications: Best Practices for Writing Secure Code. Boca Raton, Fla.: Auerbach , 2004 (ISBN 0849319900).

Viega, John & McGraw, Gary. Building Secure Software: How to Avoid Security Problems the Right Way. Boston, MA: Addison-Wesley, 2002 (ISBN 020172152X).

Viega, John & Messier, Matt. Secure Programming Cookbook for C and C++. Sebastopol, CA : O'Reilly, 2003 (ISBN 0596003943).

Wheeler, David A., Secure Programming for Linux and UNIX HOWTO, v3.010, (March 3, 2003).

Whittaker, James A. & Thompson, Herbert H. How to Break Software Security: Effective Techniques for Security Testing. Boston: Pearson/Addison Wesley, 2004 (ISBN 0321194330).

IBM Developer Works Series:

Wheeler, David A. Secure programmer: Call components safely (December 16, 2004).

Wheeler, David A. Secure programmer: Prevent race conditions (October 7, 2004).

Wheeler, David A. Secure programmer: Minimizing privileges (May 20, 2004).

Wheeler, David A. Secure programmer: Countering buffer overflows (January 27, 2004).

Wheeler, David A. Secure programmer: Keep an eye on inputs (December 19, 2003).

Wheeler, David A. Secure programmer: Validating input (October 23, 2003).

Wheeler, David A. Secure programmer: Developing secure programs (August 21, 2003).

Woody, Carol; Hall, Anthony; & Clark, John. "Can Secure Systems Be Built Using Today's Development Processes?" Panel presentation at the European SEPG in London, England, June 17, 2004.

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0001120