References

[Aleph 1996]
"Aleph One. Smashing the Stack for Fun and Profit." *Phrack 7*(49), 1996.

[Alexander 2003]
Alexander, I. "Misuse Cases: Use Cases with Hostile Intent." *IEEE Software 20*(1): 58–66, 2003.

[Alexandrescu 2010]
Alexandrescu, A. *The D Programming Language*. Upper Saddle River, NJ: Addison-Wesley, 2010.

[Alhazmi 2005a]
Alhazmi, O. H. and Y. K. Malaiya. Modeling the Vulnerability Discovery Process. In *Proceedings of the 16th IEEE International Symposium on Software Reliability Engineering*: ISSRE 2005, *Chicago, November 8–11, 2005*. Los Alamitos, CA: IEEE Computer Society Press, 2005.

[Alhazmi 2005b]
Alhazmi, O.; Y. K. Malaiya; & I. K. Ray. *Security Vulnerabilities in Software Systems: A Quantitative Perspective Technical Report*, CS T&R, AMR05. Fort Collins: Computer Science Department, Colorado State University, 2005.

[Allen 2001]
Allen, J. H. *The CERT Guide to System and Network Security Practices*. Boston: Addison-Wesley, 2001.

[Amarasinghe 2007]
Amarasinghe, S. Lecture 4, "Concurrent Programming," 6.189 IAP 2007. MIT, 2007.

[Andersen 2004]
Andersen, D., D. M. Cappelli, J. J. Gonzalez, M. Mojtahedzadeh, A. P. Moore, E. Rich, J. M. Sarriegui, T. J. Shimeall, J. M. Stanton, E. A. Weaver and A. Zagonel. Preliminary System Dynamics Maps of the Insider Cyber-Threat Problem. In *Proceedings of the 22nd International Conference of the System Dynamics Society*, Oxford, England, July 25–29, 2004. Albany, NY: System Dynamics Society, 2004.

[ANSI 1989]
American National Standards Institute. *American National Standard for Information Systems: Programming Language C* (X3.159-1989). Washington, DC: Author, 1989.

[argp 2012]
argp, huku. "Pseudomonarchia jemallocum." *Phrack* 0x0e, 0x44, Phile #0x0a of 0x13, April 2012.

[Aslani 2008]
Aslani, M, N. Chung, J. Doherty, N. Stockman, and W. Quach. "Comparison of Blackbox and Whitebox Fuzzers in Finding Software Bugs." Presented at the Team for Research in Ubiquitous Secure Technology (TRUST) Autumn 2008 Conference, Nashville, TN, 2008.

[AusCERT 2006]
Australian Computer Emergency Response Team. "Australian Computer Crime and Security Survey," 2006.

[Baratloo 2000]
Baratloo, A., N. Singh, and T. Tsai. Transparent Run-Time Defense against Stack Smashing Attacks. In *Proceedings of 2000 USENIX Annual Technical Conference,* San Diego, CA, June 18–23, 2000, pp. 251–262. Berkeley, CA: USENIX Association, 2000.

[Barbic 2007]
Barbic, J. "Multi-Core Architectures," (class lecture slides), 2007.

[Barney 2012]
Barney, B. "Introduction to Parallel Computing." Livermore Computing, Lawrence Livermore National Laboratory, 2012.

[Bass 2013]
Bass, L., P. Clements, and R. Kazman. *Software Architecture in Practice, 3rd ed.* SEI Series in Software Engineering. Upper Saddle River, NJ: Addison-Wesley Professional, 2013.

[Behrends 2004]
Behrends, R., R. Stirewalt, and L. Dillon. "Avoiding Serialization Vulnerabilities Through the Use of Synchronization Contracts." In *Workshops at the 19th International Conference of Automated Software Engineering*, Linz, Austria, September 20–24, 2004, pp. 207–219. Vienna, Austria: Österreichische Computer Gesellschaft, 2004.

[Bergin 1996]
Bergin, T. J. and R. G. Gibson, eds. *History of Programming Languages II*. New York and Reading, MA: ACM Press/Addison-Wesley, 1996.

[Bessey 2010]
Bessey, A., K. Block, B. Chelf, A. Chou, B. Fulton, S. Hallem, C. Henri-Gros, A. Kamsky, S. McPeak, and D. Engler. "A Few Billion Lines of Code Later: Using Static Analysis to Find Bugs in the Real World." *Communications of the ACM, 53*(2): 66–75, 2010.

[Bier 2011]
Bier, N., M. Lovett, and R. Seacord. "An Online Learning Approach to Information Systems

Security Education." In *Proceedings of the 15th Colloquium for Information Systems Security Education*, June 13–15, 2011, Fairborn, OH. Severn, MD: CISSE, 2011.

[Boehm 2004]
Boehm, H.-J. "The 'Boehm-Demers-Weiser' Conservative Garbage Collector." Hewlett-Packard Development Co., 2004.

[Boehm 2009]
Boehm, H.-J. and M. Spertus. "Garbage Collection in the Next C++ Standard." In *Proceedings of the 2009 ACM SIGPLAN International Symposium on Memory Management (ISMM '09)*, Dublin, Ireland, June 19–20, 2009, pp. 30–38. New York: ACM Press, 2009.

[Boehm 2012]
Boehm H. J. "Threads and Shared Variables in C++11 and Elsewhere." Hewlett-Packard Labs, April 20, 2012.

[Bouchareine 2005]
Bouchareine, P. "__atexit in Memory Bugs—Specific Proof of Concept with Statically Linked Binaries and Heap Overflows," 2005.

[Bourque 2005]
Bourque, P. and R. Dupuis. *Guide to the Software Engineering Body of Knowledge*. Los Alamitos, CA: IEEE Computer Society, 2005.

[Buchanan 2008]
Buchanan, E., R. Roemer, H. Shacham, and S. Savage. "When Good Instructions Go Bad: Generalizing Return-Oriented Programming to RISC." In *Proceedings of the 15th ACM Conference on Computer and Communications Security*, Alexandria, Virginia, October 27–31, 2008. New York: ACM Press, 2008.

[Bulba 2000]
Bulba and Kil3r. "Bypassing StackGuard and StackShiel." *Phrack*, vol. 0xa, no. 0x38 05.01.2000 0x05[0x10, 2000.

[Burley 2011]
Burley, D. and M. Bishop. "Summit on Education in Secure Software: Final Report," June 2011.

[Burrell 2011]
Burrell, T. "Compiler Security Enhancements in Visual Studio 11," December, 2011.

[Burrell 2012]
Burrell, T. "Enhancements to /GS in Visual Studio 11," January 2011.

[Callaghan 1995]
Callaghan, B., B. Pawlowski, and P. Staubach. "IETF RFC 1813 NFS Version 3 Protocol Specification," June 1995.

[Capelli 2012]
Capelli, D. M., A. P. Moore, and R. F. Trzeciak. *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. SEI Series in Software Engineering. Boston: Addison-Wesley Professional, 2012.

[Cesare 2000]
Cesare, S. "Shared Library Call Redirection via ELF PLT Infection." *Phrack*, vol. 0xa, no. 0x38, 05.01.2000, 0x07[0x10], 2000.

[Chari 2009]
Chari, S., S. Halevi, and W. Venema. "Where Do You Want to Go Today? Escalating Privileges by Pathname Manipulation," March 2009.

[Charney 2003]
Charney, S. "Prepared Testimony of Scott Charney," Chief Trustworthy Computing Strategist, Microsoft Corporation, before the Subcommittee on Commerce, Trade and Consumer Protection House Committee on Energy and Commerce. U.S. House of Representatives, Hearing on Cybersecurity and Consumer Data: What's at Risk for the Consumer? November 19, 2003.

[Chen 2002]
Chen, H., D. Wagner, and D. Dean. "Setuid Demystified." In *Proceedings of the 11th USENIX Security Symposium*, San Francisco, CA, August 5–9, 2002, pp. 171–190, Dan Boneh (Ed.). Berkeley, CA: USENIX Association, 2002.

[Chen 2004]
Chen, P., M. Dean, D. Ojoko-Adams, H. Osman, L. Lopez, N. Xie, and N. Mead. *Systems Quality Requirements Engineering (SQUARE) Methodology: Case Study on Asset Management System* (CMU/SEI-2004-SR-015, ADA431068). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004.

[Choi 2000]
Choi S.-E. and E. C. Lewis. "A Study Of Common Pitfalls In Simple Multi-Threaded Programs." In *SIGCSE'00: Proceedings of the 31st SIGCSE Technical Symposium on Computer Science Education*, Austin, TX, March 7–12, 2000, pp. 325–329. New York: ACM Press, 2000.

[Conover 1999]
Conover, M. "w00w00 on Heap Overflows," 1999.

[Conover 2004]
Conover, M. and O. Horowitz. "Reliable Windows Heap Exploits," (PowerPoint presentation). CanSecWest, April 21–23, 2004.

[Cowan 2000]
Cowan, C., P. Wagle, C. Pu, S. Beattie, and J. Walpole. "Buffer Overflows: Attacks and Defenses for the Vulnerability of the Decade." In *Proceedings of the DARPA Information*

Survivability Conference and Exposition (DISCEX'00), Hilton Head Island, SC, January 25–27, 2000, pp. 119–129. Los Alamitos, CA: IEEE Computing Society, 2000.

[Cowan 2001]
Cowan, C., M. Barringer, S. Beattie, G. Kroah-Hartman, M. Frantzen, and J. Lokier. "FormatGuard: Automatic Protection from printf Format String Vulnerabilities." In *Proceedings of the Tenth USENIX Security Symposium*, Washington, DC, August 13–17, 2001, pp. 191–199. Berkeley, CA: USENIX Association, 2001.

[Cox 1986]
Cox, B. J. *Object-Oriented Programming: An Evolutionary Approach*. Reading, MA: Addison-Wesley, 1986.

[CSI 2011]
Computer Security Institute. "15th Annual 2010/2011 Computer, Crime and Security Survey 2011," 2011.

[CSIS 2008]
Center for Strategic and International Studies (CSIS). "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency." Washington, DC: CSIS, 2008.

[CSO 2010]
CSO Magazine. "2010 CyberSecurity Watch Survey—Survey Results. Conducted by CSO in Cooperation with the U.S. Secret Service," Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, 2010.

[Dannenberg 2010]
Dannenberg, R. B., W. Dormann, D. Keaton, R. C. Seacord, D. Svoboda, A. Volkovitsky, T. Wilson and T. Plum. "As-If Infinitely Ranged Integer Model." In *Proceedings of the 2010 IEEE 21st International Symposium on Software Reliability Engineering (ISSRE '10)*, Washington, DC, pp. 91–100. Los Alamitos, CA: IEEE Computer Society, 2010.

[Davis 2003]
Davis, N. and J. Mullaney. *The Team Software Process (TSP) in Practice: A Summary of Recent Results* (CMU/SEI-2003-TR-014, ADA418430). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003.

[de Kere 2003]
de Kere, C. "'MSBlast' / LovSan Write up," 2003.

[Deloitte 2011]
Deloitte Touche Tohmatsu Limited's (DTTL). "Raising the Bar: 2011 TMT Global Security Study—Key Findings." Fifth edition of DTTL's Global Security Study for the Technology, Media and Telecommunications (TMT) Industry, 2011.

[Dennelly 2000]
Donnelly, J. M. *Navy Names Nations Posing Cyber Threats*. King Communications Group. Navy News Week, September 11, 2000, p. 1.

[Denning 2000]
Denning, D. E. "Cyberterrorism," 2000.

[Dewhurst 2005]
Dewhurst, S.C. *C++ Common Knowledge: Essential Intermediate Programming*. Upper Saddle River, NJ: Addison-Wesley, 2005.

[Dhurjati 2006]
Dhurjati, D. and V. Adve. "Backwards-Compatible Array Bounds Checking for C with Very Low Overhead." In *Proceedings of the 28th International Conference on Software Engineering (ICSE)*, May 20–28, 2006, Shanghai, China, pp. 162–171. New York: ACM Press, 2006.

[Dormann 2008]
Dormann, W. and D. Plakosh. "Vulnerability Detection in ActiveX Controls through Automated Fuzz Testing," 2008.

[Vulnerability Note VU#444213]
Vulnerability Notes Database. "AVI video codec image height heap overflow," September 5, 2009.

[Dormann 2012a]
Dormann, W. "Microsoft Indeo Video codecs Contain Multiple Vulnerabilities," [Vulnerability Note VU#228561], January 12, 2012.

[Dormann 2012b]
Dormann, W. "Adobe Flash ActionScript AVM2 newfunction Vulnerability,"[Vulnerability Note VU#486225], January 12, 2012.

[Dougherty 2009]
Dougherty, C., K. Sayre, R. Seacord, D. Svoboda, and K. Togashi. *Secure Design Patterns* (CMU/SEI-2009-TR-010). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2009.

[Dowd 2006]
Dowd, M., J. McDonald, and J. Schuh. *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities*. Boston: Addison-Wesley, 2006 (updates and errata).

[Dowd 2007]
Dowd, M., J. McDonald, and J. Schuh. "The Art of Software Security Assessment: Attacking delete and delete[] in C++," 2007.

[Drepper 2004]
Drepper, U. "Security Enhancements in Red Hat Enterprise Linux (Beside SELinux)," 2004.

[Ellis 1990]
Ellis, M. A. and B. Stroustrup. *The Annotated C++ Reference Manual*. Reading, MA: Addison-Wesley, 1990.

[Ergonul 2012]
Ergonul, M. Research. "NYU Poly Application Security Discussions/Exploiting Concurrency Vulnerabilities in System Call Wrappers," April 2012.

[Etoh 2000]
Etoh, H. and K. Yoda. "Protecting from Stack-Smashing Attacks." IBM Research Division, Tokyo Research Laboratory, 2004.

[Evans 1998]
Evans, C. "Nasty Security Hole in 'lprm'" (Bugtraq Archive), 1998.

[Evans 2006]
Evans, J. A. "Scalable Concurrent malloc(3) Implementation for FreeBSD" 2006.

[Fallon 2012]
Fallon, E. "Experience Report: Applying and Introducing TSP to Electronic Design Automation." In *Proceedings of the 2012 Team Software Process Symposium*, St. Petersburg, FL, September 17–20, 2012.

[FFmpeg 2012]
FFmpeg Developers. Website of FFmpeg.org, 2012.

[Firesmith 2003]
Firesmith, D. G. "Security Use Cases." *Journal of Object Technology 2*(3): 53–64, 2003.

[Fisher 2010]
Fisher, K., Y. Mandelbaum, and D. Walker. The Next 700 Data Description Languages. *Journal of the ACM 57*(2): article 10, 2010.

[Fithen 2004]
Fithen, W. L, S. V. Hernan, P. F. O'Rourke, and D. A. Shinberg. "Formal Modeling of Vulnerability." *Bell Labs Technical Journal 8*(4): 173–186, 2004.

[Foote 2011]
Foote, J. JasPer Memory Corruption Vulnerabilities [Vulnerability Note #VU887409], December 9, 2011.

[Forrester 2000]
Forrester, J. E, B. P. Miller, and USENIX Association. "An Empirical Study of the Robustness

of Windows NT Applications Using Random Testing." In *Proceedings of the 4th Conference on USENIX Windows Systems Symposium*—Vol. 4. Berkeley, CA: USENIX Association, 2000.

[Forrester 2000]
Forrester, J. E. and B. P. Miller. "An Empirical Study of the Robustness of Windows NT Applications Using Random Testing." In *Proceedings of the 4th USENIX Windows System Symposium*, August 3–4, 2000, Seattle, WA, pp.9–68. Berkeley, CA: USENIX Association, 2000.

[FSF 2004]
Free Software Foundation. "GCC Online Documentation," 2004.

[Gamma 1995]
Gamma, E., R. Helm, R. Johnson, and J. M. Vlissides. *Design Patterns: Elements of Reusable Object-Oriented Software*. Boston: Addison-Wesley, 1995.

[Garfinkel 1996]
Garfinkel, S., and G. Spafford. *Practical UNIX & Internet Security, 2nd ed.* Sebastopol, CA: O'Reilly Media, 1996.

[Gehani 1989]
Gehani, N. H., and W. D. Roome. *Concurrent C*. Summit, NJ: Silicon Press, 1989.

[gera 2002]
gera, and riq. "Advances in Format String Exploitation." *Phrack* 0x0b, Issue 0x3b, Phile #0x07 of 0x12, 2002.

[Godefroid 2008]
P. Godefroid, M. Y. Levin, and D. Molnar. "Automated Whitebox Fuzz Testing." In *Proceedings of the Network and Distributed System Security Symposium*, February 10–13, 2008, San Diego, CA. Reston, VA: The Internet Society, 2008.

[Godefroid 2010]
Godefroid, P. "From Blackbox Fuzzing to Whitebox Fuzzing Towards Verification." In *Proceedings of the 19th International Symposium on Software Testing and Analysis (ISSTA)*, Trento, Italy, July 12–16, 2010, pp. 1–38. New York: ACM Press, 2010.

[Graff 2003]
Graff, M. G. and K. R. van Wyk. *Secure Coding Principles & Practices: Designing and Implementing Secure Applications*. Sebastopol, CA: O'Reilly, 2003.

[Griffiths 2006]
Griffiths, A. 2006. "Clutching at Straws: When You Can Shift the Stack Pointer." *Phrack* 0x0b(0x3f), phile #0x0e of 0x14.

[Grossman 2005]
Grossman, D., M. Hicks, J. Trevor, and G. Morrisett. "Cyclone: A Type-safe Dialect of C." *C/C++ Users Journal, 23*(1): 6–13,2005.

[Hocevar 2007]
Hocevar, S. "Zzuf—Multiple Purpose Fuzzer". Presented at the Free and Open Source Software Developers' European Meeting (FOSDEM), Brussels, Belgium, 2007.

[Hoogstraten 2003]
Van Hoogstraten, J. SANS Malware FAQ: What Is W32/Blaster Worm? 2003.

[Horovitz 2002]
Horovitz, O. Big Loop Integer Protection. *Phrack* Vol. 0x0b, Issue 0x3c, Phile #0x09 of 0x10, 2002.

[Householder 2012a]
Householder, A. *Well There's Your Problem: Isolating the Crash-Inducing Bits in a Fuzzed File* (CMU/SEI-2012-TN-018). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2012.

[Householder 2012b]
Householder, A. and J. Foote. *Probability-Based Parameter Selection for Black-Box Fuzz Testing* (CMU/SEI-2012-TN-019). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2012.

[Howard 1997]
Howard, J. D. An Analysis of Security Incidents on the Internet 1989–1995. PhD Diss. Carnegie Mellon University, 1997.

[Howard 2002]
Howard, M. and D. C. LeBlanc. *Writing Secure Code, 2nd ed*. Redmond, WA: Microsoft Press, 2002.

[Howard 2003a]
Howard, M. "An Overlooked Construct and an Integer Overflow Redux," 2003.

[Howard 2003b]
Howard, M., J. Pincus, and J. M., Wing. "Measuring Relative Attack Surfaces." In *Proceedings of Workshop on Advanced Developments in Software and Systems Security*, Taipei, Taiwan, December 5–7, 2003. 2003.

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

[Howard 2011]
Howard, M., M. Miller, J. Lambert, and M. Thomlinson. "Windows ISV Software Security Defenses." MSDN, 2011.

[huku 2012]
huku, argp. "The Art of Exploitation: Exploiting VLC, A jemalloc Case Study." *Phrack*, Vol. 0x0e, Issue 0x44, Phile #0x0d of 0x13, April 2012.

[Humphrey 2002]
Humphrey, W. S. *Winning with Software: An Executive Strategy*. Boston: Addison-Wesley, 2002.

[IBM 2004]
IBM. "Rational PurifyPlus," 2004.

[IBM 2012]
IBM. Writing Reentrant and Thread-Safe Code, 2012.

[IEEE Std 1003.1-2008]
IEEE Standard for Information Technology. *Portable Operating System Interface (POSIX) Base Specifications*," Issue 7, IEEE Std 1003.1-2008 (revision of IEEE Std 1003.1-2004), pp. c1–3826, December 1, 2008.

[Intel 2004]
Intel Corporation. IA-32 Intel® Architecture Software Developer's Manual, 2004.

[Intel 2010]
Intel Corporation. "Intel® 64 and IA-32 Architectures Software Developer's Manual, Instruction Set Reference, A-M, Volume 2A," 2010.

[Internet Society 2000]
The Internet Society. "Internet Security Glossary (RFC 2828)," 2000.

[Internet Society 2007]
Network Working Group, R. Shirey. "Internet Security Glossary (RFC 4949), Version 2 (Obsoletes: 2828)," August 2007.

[ISO/IEC 14882: 2011]
ISO/IEC (International Organization for Standardization, International Electrotechnical Commission). "Programming Languages—C++," 2011. (ISO/IEC 14882-1998).

[ISO/IEC 1998]
ISO/IEC. *Programming Languages—C++* (ISO/IEC 14882-1998). Geneva, Switzerland: ISO/IEC, 1998.

[ISO/IEC 1999]
ISO/IEC. *Programming Languages—C, 2nd ed.* (INCITS/ISO/IEC 9899-1999). Geneva, Switzerland: ISO/IEC, 1999.

[ISO/IEC 2005]
ISO/IEC. "Extensions to the C Library—Part I," (ISO/IEC WDTR 24731). Geneva, Switzerland: ISO/IEC, 2005.

[ISO/IEC 2007]
ISO/IEC. *Extensions to the C Library—Part I: Bounds-Checking Interfaces* (ISO/IEC TR 24731-1: 2007). Geneva, Switzerland: ISO/IEC, 2007.

[ISO/IEC 9945: 2003]
ISO/IEC. "Information Technology—Programming Languages, Their Environments and System Software Interfaces—Portable Operating System Interface (POSIX®)," (ISO/IEC 9945: 2003) (including Technical Corrigendum 1). Geneva, Switzerland: ISO/IEC, 2003.

[ISO/IEC TR 24731-2: 2010]
ISO/IEC. "Extensions to the C Library—Part II: Dynamic Allocation Functions," (ISO/IEC TR 24731-2). Geneva, Switzerland: ISO/IEC, 2010.

[ISO/IEC/IEEE 9945: 2009]
ISO/IEC/IEEE. "IEEE Standard for Information Technology—Portable Operating System Interface (POSIX®) Base Specifications," Issue 7. Geneva, Switzerland: ISO/IEC, 2009.

[Jack 2007]
Jack, B. Vector. "Rewrite Attack" (White Paper). Juniper Networks, May 2007.

[Johnson 1973]
Johnson, S. C. and B. W. Kernighan. *The Programming Language B* (Computing Science Technical Report No. 8). Murray Hill, NJ: Bell Labs, 1973.

[Jones 1997]
Jones, R. W. M. and P. H. J. Kelley. "Backwards-Compatible Bounds Checking for Arrays and Pointers in C Programs." In *Proceedings of the Third International Workshop on Automatic Debugging (AADEBUG'97)*, Linkoping, Sweden, May 26–27, 1997, pp. 13–26. Linkoping, Sweden: Linkopings Universitet, 1997.

[Jones 2007]
Jones, M. T. "Anatomy of the Linux File System: A Layered Structure-Based Review," October 2007.

[Kaminsky2011]
Kaminsky, D. "Fuzzmarking: Towards Hard Security Metrics for Software Quality? March 2011.

[Kamp 1998]
Kamp, P. H. Malloc(3) Revisited. In *Proceedings of 1998 USENIX Annual Technical Conference: Invited Talks and Freenix Track*, New Orleans, LA, June 15–19, 1998, pp. 93–198. Berkeley, CA: USENIX Association, 1998.

[Kath 1993]
Kath, R. Managing Virtual Memory in Win32, 1993.

[Kernighan 1978]
Kernighan, B. W. and D. M. Ritchie. *The C Programming Language*. Englewood Cliffs, NJ: Prentice-Hall, 1978.

[Kernighan 1988]
Kernighan, B. W. and D. M. Ritchie. *The C Programming Language, 2nd ed*. Englewood Cliffs, NJ: Prentice-Hall, 1988.

[Kerr 2004]
Kerr, K. "Putting Cyberterrorism into Context," 2004.

[Kirwan 2004]
Kirwan, M. "The Quest for Secure Code," 2004.

[Knuth 1997]
Knuth, D. E. Ch. 2, "Information Structures." In *Art of Computer Programming, Vol. 1: Fundamental Algorithms, 3rd ed.*, pp. 438–442. Reading, MA: Addison-Wesley, 1997.

[Landwehr 2008]
Landwehr, C. "IARPA STONESOUP Proposers Day." IARPA, 2008.

[Lanza 2003]
Lanza, J. P. Multiple FTP Clients Contain Directory Traversal Vulnerabilities, March 14, 2003.

[LaRue 2012]
LaRue, M. and J. Lee. "Attack Surface Analyzer 1.0," (released August 2012).

[Leiserson 2008]
Leiserson, C. E., and I. B. Mirman. *How to Survive the Multicore Software Revolution (or at Least Survive the Hype)* [e-book]. Santa Clara, CA: Cilk Arts, 2008.

[Lemos 2004]
Lemos, R. "MSBlast Epidemic Far Larger than Believed," 2004.

[Linux 2008]
"Linux Programmer's Manual." October 2008.

[Lipner 2005]
Lipner, S., and M. Howard. The Trustworthy Computing Security Development Lifecycle. In *Proceedings of 20th Annual Computer Security Applications Conference*, Tucson, AZ, December 6–10, 2004, pp. 2–13. Los Alamitos, CA: IEEE Computer Society, 2004 (updated 2005).

[Litchfield 2003a]
Litchfield, D. Variations in Exploit Methods between Linux and Windows, 2003.

[Litchfield 2003b]
Litchfield, D. Defeating the Stack-Based Buffer Overflow Prevention Mechanism of Microsoft Windows 2003 Server, 2003.

[Liu 2010]
Liu, V. Concurrency vs. Multi-Threading Blog, May 2010.

[Long 2011]
Long, F. The CERT Oracle Secure Coding Standard for Java, 2012.

[Manadhata 2010]
Manadhata, P. K. and J. M. Wing. "An Attack Surface Metric." *IEEE Transactions on Software Engineering 36*(1), 2010.

[McAndrews 2000]
McAndrews, D. *The Team Software Process (TSP): An Overview and Preliminary Results of Using Disciplined Practices* (CMU/SEI-2000-TR-015, ADA387260). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2000.

[McDermott 1999]
McDermott, J. and C. Fox. "Using Abuse Case Models for Security Requirements Analysis." In *Proceedings 15th Annual Computer Security Applications Conference*, Scottsdale, AZ, December 6–10, 1999, pp. 55–64. Los Alamitos, CA: IEEE Computer Society Press, 1999.

[McDermott 2001]
McDermott, J. Abuse-Case-Based Assurance Arguments. In *Proceedings of the 17th Annual Computer Security Applications Conference*, New Orleans, LA, December 10–14, 2001, pp. 366–374. Los Alamitos, CA: IEEE Computer Society Press, 2001.

[Mead 2010]
Mead, N. R., T. B. Hilburn, and R. C. Linger. *Software Assurance Curriculum Project Volume II: Undergraduate Course Outlines*, 2010. (CMU/SEI-2010-TR-019), 2010.

[Meier 2003]
Meier, J. D., A. Mackman, S. Vasireddy, R. Escamilla, and A. Murukan. Improving Web Application Security Threats and Countermeasures, 2003.

[Meyer 1988]
Meyer, B. *Object-Oriented Software Construction*. New York: Prentice-Hall, 1988.

[Meyers 1998]
Meyers, S. *Effective C++: 50 Specific Ways to Improve Your Programs and Designs, 2nd ed.* Reading, MA: Addison-Wesley, 1998.

[Michael 1996]
Michael, M. M. and M. L. Scott. "Simple, Fast, and Practical Non-Blocking and Blocking Concurrent Queue Algorithms." In *Proceedings of 15th Annual ACM Symposium Principles of Distributed Computing*, Philadelphia, PA, May 23–26, 1996, pp. 267–275, New York: ACM Press, 1996.

[Microsoft 2009]
Microsoft Corporation. Microsoft Security Research & Defense. "Safe Unlinking in the Kernal Pool," 2009.

[Microsoft 2010]
Microsoft Corporation. "Simplified Implementation of the Microsoft SDL," November 4, 2010.

[Microsoft 2011]
Microsoft Corporation. "Microsoft Secure Development Lifecycle (SDL) Process Guidance Version 5.1," June, 3, 2011.

[Microsoft 2012]
Microsoft Corporation. "Dev-Center Desktop, Introduction," 2012.

[MISRA 2005]
MISRA (Motor Industry Software Reliability Association). "MISRA-C: 2004: Guidelines for the Use of the C Language in Critical Systems." Nuneaton, UK: MIRA, 2005.

[Molnar 2009]
Molnar, D., X. C. Li, D. A. Wagner, and USENIX Association. "Dynamic Test Generation to Find Integer Bugs in x86 Binary Linux Programs," 2009.

[Morrow 2012]
Morrow, T., R. Seacord, J. Bergey, and P. Miller. *Supporting the Use of CERT® Secure Coding Standards in DoD Acquisitions* (CMU/SEI-2012-TN-016). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2012.

[Moscibroda 2007]
Moscibroda, T. and O. Mutlu. "Memory Performance Attacks: Denial of Memory Service in Multi-Core Systems." In *Proceedings of the 16th USENIX Security Symposium*, Boston, MA, August 6–10, 2007, pp. 257–274, 2007.

[Nagarakatte 2009]
Nagarakatte, S., J. Zhao, M. M. K. Martin, and S. Zdancewic. "SoftBound: Highly Compatible and Complete Spatial Memory Safety for C." In *Proceedings of ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI)*, Dublin, Ireland, June 15–21, 2009. New York: ACM Press, 2009.

[Nelson 1991]
Nelson, G. *Systems Programming with Modula-3.* EnglewoodCliffs, NJ: Prentice-Hall, 1991.

[Netzer 1990]
Netzer, R. and B. Miller. "On the Complexity of Event Ordering for Shared-Memory Parallel Program Executions." In *Proceedings of the 1990 International Conference on Parallel Processing*, Pennsylvania State University, University Park, PA, August 1–17, 1990, pp. 93–97. University Park: Pennsylvania State University Press, 1990.

[NIST 2002]
National Institute of Standards and Technology. "Software Errors Cost U.S. Economy $59.5 Billion Annually, (NIST 2002-10), 2002.

[Nowak 2004]
Nowak, T. "Functions for Microsoft Windows NT/2000," 2004.

[Okun 2009]
Okun, V., R. Gaucher, and P. E. Black, eds. Static Analysis Tool Exposition (SATE) *2008*. (NIST Special Publication 500-279). Gaithersburg, MD: National Institute of Standards and Technology, 2009.

[Parasoft 2004]
Parasoft. "Automating C/C++ Application Testing with Parasoft Insure++ (Insure++ Technical Papers)," 2004.

[Pethia 2003a]
Pethia, R. D. "Cyber Security—Growing Risk from Growing Vulnerability." Testimony before the House Select Committee on Homeland Security Subcommittee on Cybersecurity, Science, and Research and Development. Hearing on Overview of the Cyber Problem—A Nation Dependent and Dealing with Risk, 2003.

[Pethia 2003b]
Pethia, R. D. "Viruses and Worms: What Can We Do about Them?" Testimony before the House Committee on Technology, Information Policy, Intergovernmental Relations and the Census. Hearing on Worm and Virus Defense: How Can We Protect the Nation's Computers From These Threats?, 2003.

[Pfenning 2004]
Pfenning, F. "Lectures Notes on Type Safety: Foundations of Programming Languages," Lecture 6, pp. 15–312. Carnegie Mellon University, 2004.

[Pincus 2002]
Pincus, J. "Infrastructure for Correctness Tools," (PowerPoint Presentation), 2002.

[Pincus 2004]
Pincus, J. and B. Baker. "Beyond Stack Smashing: Recent Advances in Exploiting Buffer Overruns." *IEEE Security & Privacy 2*(4): 20–27, 2004.

[Plakosh 2009]
Plakosh, D. "Developing Multicore Software." Paper presented at the Systems and Software Technology Conference, Salt Lake City, UT, April 23, 2009.

[Plum 2005]
Plum, T. and D. M. Keaton. "Eliminating Buffer Overflows, Using the Compiler or a Standalone Tool." In *Proceedings of the Workshop on Software Security Assurance Tools, Techniques, and Metrics*, National Institute of Standards and Technology (NIST), Long Beach, CA, November 7–8, 2005.

[Plum 2008]
Plum, T. and A. Barjanki. "Encoding and Decoding Function Pointers," (SC22/WG14/N1332), 2008.

[Provos 2003a]
Provos, N., M. Friedl, and P. Honeyman. "Preventing Privilege Escalation." In *Proceedings of the 12th USENIX Security Symposium*, Washington, DC, August 4–8, 2003, pp. 231–242. Berkeley, CA: USENIX Association, 2003.

[Provos 2003b]
Provos, N. "Improving Host Security with System Call Policies." In *Proceedings of the 12th USENIX Security Symposium*, Washington, DC, August 4–8, 2003, pp. 257–272. Berkeley, CA: USENIX Association, 2003.

[Purczynski 2002]
Purczynski, W. "GNU Fileutils—Recursive Directory Removal Race Condition (Bugtraq Archive)," 2002.

[Randazzo 2004]
Randazzo, M. R., M. Keeney, D. Cappelli, A. Moore, and E. Kowalski. Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector, 2004.

[Rational 2003]
Rational Software Corporation. "Rational® PurifyPlus, Rational® Purify®, Rational® PureCoverage®, Rational® Quantify®, Installing and Getting Started," Version: 2003.06.00, Part Number: 800-026184-000 (Product Manual), 2003.

[Reinders 2007]
James, R. *Intel Threading Building Blocks*. Sebastopol, CA: O'Reilly, 2007.

[Richards 1979]
Richards, M. and C. Whitby-Strevens. *BCPL: The Language and Its Compiler*. New York: Cambridge University Press, 1979.

[Richarte 2002]
Richarte, G. "Four Different Tricks to Bypass StackShield and StackGuard Protection," 2002.

[Richter 1999]
Richter, J. *Programming Applications for Microsoft*, 4th ed. Redmond, WA: Microsoft Press, 1999.

[Rivas 2001]
Rivas, J. M. B. "Overwriting the .dtors Section," 2001.

[rix 2000]
rix. "Smashing C++ Vptrs." *Phrack*, Vol. 0xa, Issue 0x38, 05.01.2000, 0x08[0x10], 2000.

[Rodrigues 2008]
Rodrigues, G. "Taming the OOM Killer." LWN.net, 2008.

[Ruwase 2004]
Ruwase, O. and M. S. Lam. "A Practical Dynamic Buffer Overflow Detector." In *Proceedings of the 11th Annual Network and Distributed System Security Symposium*, San Diego, CA, February 5–6 2004, pp. 159–169. Reston, VA: Internet Society, 2004.

[Saltzer 1974]
Saltzer, J. H. "Protection and the Control of Information Sharing in Multics." *Communications of the ACM 17*(7): 388–402, 1974.

[Saltzer 1975]
Saltzer, J. H. and M. D. Schroeder. "The Protection of Information in Computer Systems." *Proceedings of the IEEE* 63(9): 1278–1308, 1975.

[Schneider 1999]
Schneider, F. B., ed., National Research Council, Committee on Information Systems Trustworthiness. *Trust in Cyberspace*. Washington, DC: National Academy Press, 1999.

[Schneier 2004]
Schneier, B. *Secrets and Lies: Digital Security in a Networked World*. Indianapolis, IN: Wiley, 2004.

[Scut 2001]
Scut/Team Teso. "Exploiting Format String Vulnerabilities," 2001.

[Seacord 2005a]
Seacord, R. C. *Secure Coding in C and C++*. Boston: Addison-Wesley, 2005.

[Seacord 2005b]
Seacord, R. C. and A. Householder. *A Structured Approach to Classifying Security Vulnerabilities* (CMU/SEI-2005-TN-003). Software Engineering Institute, Carnegie Mellon University, 2005.

[Seacord 2005c]
Seacord, R. C. "Wide-Character Format String Vulnerabilities Strategies for Handling Format String Weaknesses." *Dr. Dobb's Journal 30*(12): 63–66, 2005.

[Seacord 2008]
Seacord, R. C. *The CERT C Secure Coding Standard*. Boston: Addison-Wesley, 2008.

[Seacord 2010]
Seacord, R., W. Dormann, J. McCurley, P. Miller, R. Stoddard, D. Svoboda, and J. Welch. Source Code Analysis Laboratory (SCALe) for Energy Delivery Systems (CMU/SEI-2010-TR-021). Software Engineering Institute, Carnegie Mellon University, 2010.

[Seacord 2012]
Seacord, R., et al. "ISO/IEC TS 17961 Draft. Information Technology—Programming Languages, Their Environments and System Software Interfaces—C Secure Coding Rules," 2012.

[SEI 2012a]
Software Engineering Institute. *Secure Coding Standards*, 2012.

[SEI 2012b]
Software Engineering Institute. "CERT C++ Secure Coding Standard, 2012."

[SEI 2012c]
Software Engineering Institute. "CERT Perl Secure Coding Standard," 2012.

[SEI 2012d]
Software Engineering Institute. "CERT C Secure Coding Standard," 2012.

[Shacham 2007]
Shacham, H. (2007). "The Geometry of Innocent Flesh on the Bone: Return-Into-Libc Without Function Calls (on the x86)." In *Proceedings of the 14th ACM Conference/Computer and Communications Security (CCS '07),* Whistler, Canada, October 28–31, 2007. New York: ACM Press.

[Shankar 2001]
Shankar, U., K. Talwar, J. S. Foster, and D. Wagner. "Detecting Format String Vulnerabilities with Type Qualifiers." In *Proceedings of the 10th USENIX Security Symposium, Washington, DC, August 13–17, 2001, pp.* 201–218. Berkeley, CA: USENIX Association, 2001.

[Shannon 2011]
Shannon, G. E. "Statement of Gregory E. Shannon," Chief Scientist for Computer Emergency Readiness Team (Cert). In Examining the Homeland Security Impact of the Obama Administration's Cybersecurity Proposal. Hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security. House of Representatives, One Hundred Twelfth Congress, First Session, Serial No. 112–33. June 24, 2011. Software Engineering Institute, Carnegie Mellon University, 2011.

[Sheridan 2012]
Sheridan, F. Deploying Static Analysis. *Dr. Dobb's Journal*, August 2012.

[Sindre 2000]
Sindre, G. and A. Opdahl. "Eliciting Security Requirements by Misuse Cases." In *Proceedings of TOOLS Pacific 2000*, Sydney, Australia, November 20–23, 2000, pp. 120–130. Los Alamitos, CA: IEEE Computer Society Press, 2000.

[Sindre 2002]
Sindre, G., S. Opdahl, and B. Brevik. "Generalization/Specialization as a Structuring Mechanism for Misuse Cases (CD-ROM)." In *Proceedings of the Second Symposium on Requirements Engineering for Information Security (SREIS 2002)*, Raleigh, NC, October 16, 2002. Lafayette, IN: CERIAS, Purdue University, 2002.

[Sindre 2003]
Sindre, G., D. G. Firesmith, and A. L. Opdahl. "A Reuse-Based Approach to Determining Security Requirements." In *Proceedings of the 9th International Workshop on Requirements Engineering: Foundation for Software Quality (REFSQ'03)*, Klagenfurt/Velden, Austria, June 16–17, 2003, pp. 127–136. Essen, Germany: Essener Informatik Beitrage, 2003.

[Sinha 2005]
Sinha, P. "A Memory-Efficient Doubly Linked List." *Linux Journal 129*: 38, 2005.

[Smashing 2005]
BSD Heap Smashing, 2005.

[Solar 2000]
Solar Designer. "JPEG COM Marker Processing Vulnerability in Netscape Browsers," 2000.

[Soo Hoo 2001]
Soo Hoo, K., J. W. Sudbury, and J. R. Jaquith. "Tangible ROI through Secure Software Engineering." *Secure Business Quarterly 1*(2): 1–3, 2001.

[Stein 2001]
Stein, L. D. *Network Programming with Perl*. Boston: Addison-Wesley, 2001.

[Stroustrup 1986]
Stroustrup, B. *The C++ Programming Language*. Reading, MA: Addison-Wesley, 1986.

[Stroustrup 1997]
Stroustrup, B. *The C++ Programming Language, 3rd ed*. Reading, MA: Addison-Wesley, 1997.

[Stroustrup 2012]
Stroustrup, B. C++11—The Recently Approved New ISO C++ Standard, 2012.

[Sutter 2005]
Sutter, H. and Alexandrescu, A. *C++ Coding Standards: 101 Rules, Guidelines, and Best Practices*. Boston: Addison-Wesley, 2005.

[Sutter 2008]
Sutter, H. Lock-Free Code: A False Sense of Security. *Dr. Dobb's Journal*, September 2008. Retrieved 9/25/2012.

[Swiderski 2004]
Swiderski, F. and W. Snyder. *Threat Modeling. Redmond*, WA: Microsoft Press, 2004.

[Taylor 2012]
Taylor, B., M. Bishop, D. Burley, S. Cooper, R. Dodge, and R. Seacord. "Teaching Secure Coding: Report From Summit on Education in Secure Software." In *Proceedings of the 43rd ACM Technical Symposium on Computer Science Education (SIGCSE '12), Raleigh, NC, February 29–March 3, 2012*, pp. 581–582, New York: ACM Press.

[Thinking 1990]
Thinking Machines Corporation. *Getting Started in C*. Cambridge, MA: Thinking Machines Corporation, 1990.

[Thomas 2002]
Thomas, D. "Cyber Terrorism and Critical Infrastructure Protection." Testimony Before the Committee on House Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations. July 24, 2002.

[TIS 1995]
Tool Interface Standard Committee. "Tool Interface Standard (TIS) Executable and Linking Format (ELF) Specification, Version 1.2," 1995.

[Tsai 2001]
Tsai, T. and N. Singh. "Libsafe 2.0: Detection of Format String Vulnerability Exploits." White paper, Avaya Labs, February 6, 2001.

[Valgrind 2004]
Valgrind. "Valgrind Latest News," 2004.

[van de Ven 2004]
van de Ven, A. "New Security Enhancements in Red Hat Enterprise Linux v.3," update 3, 2004.

[Viega 2000]
Viega, J., J. T. Bloch, Y. Kohno, and G. McGraw. "ITS4: A Static Vulnerability Scanner for C and C++ Code." In *Proceedings of the 16th Annual Computer Security Applications Conference (ACSAC'00)*, New Orleans, LA, December 11–15, 2000, pp. 257–267. Los Alamitos, CA: IEEE Computer Society Press, 2000.

[Viega 2002]
Viega, J. and G. McGraw. *Building Secure Software: How to Avoid Security Problems the Right Way*. Boston, MA: Addison-Wesley, 2002.

[Viega 2003]
Viega, J. and M. Messier. *Secure Programming Cookbook for C and C++: Recipes for Cryptography, Authentication, Networking, Input Validation & More*. Sebastopol, CA: O'Reilly, 2003.

[Wagle 2003]
Wagle, P. and C. Cowan. "StackGuard: Simple Stack Smash Protection for GCC." In *Proceedings of the GCC Developers Summit*, Ottawa, Ontario, Canada, May 25–27, 2003, pp. 243–256.

[Wallnau 2002]
Wallnau, K. C., S. Hissam, and R. C. Seacord. *Building Systems from Commercial Components*. Boston: Addison-Wesley, 2002.

[Warren 2003]
Warren, Jr., H. S. *Hacker's Delight*. Boston: Addison-Wesley, 2003.

[Watson 2007]
Watson, R. N. M. "Xploiting Concurrency Vulnerabilities in System Call Wrappers." In *Proceedings of 1st USENIX Workshop on Offensive Technologies, Boston, MA, August 6–10, 2007*. Berkeley, CA: USENIX Association, 2007.

[Weaver 2004]
Weaver, N. and V. Paxson. "A Worst-Case Worm." The Third Annual Workshop on Economics and Information Security (WEIS04), *Minneapolis, MN, May 13–14, 2004*.

[Wheeler 2003]
Wheeler, D. "Secure Programming for Linux and Unix HOWTO—Creating Secure Software," 2003.

[Wheeler 2004]
Wheeler, D. A. "Secure Programmer: Countering Buffer Overflows," 2004.

[Wikipedia 2012a]
Wikipedia. "Amdahl's Law," 2012 (retrieved 9/25/2012).

[Wikipedia 2012b]
Wikipedia. "Concurrency (Computer Science)," 2012.

[Wikipedia 2012c]
Wikipedia. "Concurrent Computing," 2012.

[Wilander 2003]
Wilander, J. and M. Kamkar. "A Comparison of Publicly Available Tools for Dynamic Buffer Overflow Prevention." In *Proceedings of the 10th Network and Distributed System Security Symposium*, San Diego, California, February 6–7, 2003, pp. 149–162. Reston, VA: Internet Society, 2003.

[Wilson 2003]
Wilson, M. "Generalized String Manipulation: Access Shims and Type Tunneling." C/C++. Users Journal 21(8): 24–35, 2003.

[Wojtczuk 1998]
Wojtczuk, R. "Defeating Solar Designer Non-Executable Stack Patch (Bugtraq Archive)," 1998.

[Xie 2004]
Xie, N., N. R. Mead, P. Chen, M. Dean, L. Lopez, D. Ojoko-Adams, and H. Osman. *SQUARE Project: Cost/Benefit Analysis Framework for Information Security Improvement Projects in Small Companies* (CMU/SEI-2004-TN-045, ADA431118). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2004.

[Yu 2009]
Yu, F., T. Bultan, and O. H. Ibarra. "Symbolic String Verification: Combining String Analysis and Size Analysis." In *Proceedings of the 15th International Conference on Tools and Algorithms for the Construction and Analysis of Systems: Held as Part of the Joint European Conferences on Theory and Practice of Software*, York, UK, March 22–29, 2009. Series Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2009.