Rule AA. References

[Abadi 1996] Martin Abadi and Roger Needham, Prudent Engineering Practice for Cryptographic Protocols, *IEEE Transactions on Software Engineering*, Volume 22, Issue 1, 1996, 6–15.

[Aho 1986] Aho, Alfred V.; Sethi, Ravi; Ullman, Jeffrey D. "Compilers: Principles, Techniques, and Tools" (2nd ed.), 1986.

[Android API 2013] *Android API*. Package Index, Android, 2013.

[Android Guide 2013] *Android API Guides*, Introduction to Android, Android, 2013.

[Android Security] Security Tips, Android Training.

[Apache 2014] Apache Tika: A Content Analysis Toolkit, Apache Software Foundation, 2014.

[Apache 2015] Apache Tomcat, Apache Software Foundation, 2015.

[API 2006] Java Platform, Standard Edition 6 API Specification, Oracle, 2011.

[API 2012] Java Platform, Standard Edition 7 API Specification, Oracle, 2012.

[API 2013] Java Platform, Standard Edition 7 API Specification, Oracle, 2013.

[J2EE API 2013] Java Platform, Extended Edition 7 API Specification, Oracle, 2013.

[API 2014] Java Platform, Standard Edition 8 API Specification, Oracle, 2014.

[Arnold 2006] Ken Arnold, James Gosling, and David Holmes. *The Java™ Programming Language*, 4th ed., Addison-Wesley, Boston, 2006.

[Austin 2000] Calvin Austin and Monica Pawlan, *Advanced Programming for the Java 2 Platform*, Addison-Wesley Longman, Boston, 2000.

[Black 2004] Paul E. Black and Paul J. Tanenbaum, partial order, in *Dictionary of Algorithms and Data Structures* [online], Paul E. Black, ed., U.S. National Institute of Standards and Technology, December 17, 2004.

[Black 2006] Paul E. Black and Paul J. Tanenbaum, total order, in *Dictionary of Algorithms and Data Structures* [online], Paul E. Black, ed., U.S. National Institute of Standards and Technology. March 30, 2006.

[Bloch 2001] Joshua Bloch, *Effective Java: Programming Language Guide*, Addison-Wesley Professional, Boston, 2001.

[Bloch 2005a] Joshua Bloch and Neal Gafter, *Java™ Puzzlers: Traps, Pitfalls, and Corner Cases*, Addison-Wesley Professional, Boston, 2005.

[Bloch 2005b] Joshua Bloch and Neal Gafter, Yet More Programming Puzzlers, JavaOne Conference, 2005.

[Bloch 2007] Joshua Bloch, Effective Java™ Reloaded: This Time It's (Not) for Real, JavaOne Conference, 2007.

[Bloch 2008] Joshua Bloch, *Effective Java™: Programming Language Guide*, 2nd ed., Addison-Wesley Professional, Boston, 2008.

[Bloch 2009] Joshua Bloch and Neal Gafter, Return of the Puzzlers: Schlock and Awe, JavaOne Conference, 2009.

[Boehm 2005] Hans-J. Boehm, Finalization, Threads, and the Java™ Technology-Based Memory Model, JavaOne Conference, 2005.

[Campione 1996] Mary Campione and Kathy Walrath, *The Java Tutorial: Object-Oriented Programming for the Internet*, Addison-Wesley, Reading, MA, 1996.

[CCITT 1988] International Telegraph and Telephone Consultative Committee (CCITT). *CCITT Blue Book*, Recommendation X.509 and IS0 9594-8: The Directory-Authentication Framework, International Telecommunication Union, Geneva, 1988.

[Chan 1999] Patrick Chan, Rosanna Lee, and Douglas Kramer, *The Java Class Libraries: Supplement for the Java 2 Platform*, Volume 1.2, 2nd ed., Prentice Hall, Upper Saddle River, NJ, 1999.

[Chess 2007] Brian Chess and Jacob West, *Secure Programming with Static Analysis*, Addison-Wesley Professional, Boston, 2007.

[Chen 14] Eric Chen, Yutong Pei, Shuo Chen, Yuan Tian, Robert Kotcher, and Patrick Tague. "OAuth Demystified for Mobile Application Developers.", 2014.

[Chin 2011] Erika Chin, Adrienne Porter Felt, Kate Greenwood, and David Wagner, Analyzing Inter-Application Communication in Android, *Proc. MobiSys '11: Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services*, pp. 239–252, ACM, New York, 2011.

[Christudas 2005] Internals of Java Class Loading, ONJava, 2005.

[Cohen 1981] On Holy Wars and a Plea for Peace, *IEEE Computer*, Volume 14, Issue 10, 1981.

[Conventions 2009] Code Conventions for the Java Programming Language, Sun Microsystems, 2009.

[Coomes 2007] John Coomes, Peter Kessler, and Tony Printezis, Garbage Collection-Friendly Programming, Java SE Garbage Collection Group, Sun Microsystems, JavaOne Conference, 2007.

[Core Java 2004] Cay S. Horstmann and Gary Cornell, *Core Java™ 2, Volume I, Fundamentals*, 7th ed., Prentice Hall PTR, Boston, 2004.

[Coverity 2007] Coverity Prevent User's Manual (3.3.0). Coverity, 2007.

[Cunningham 1995] Ward Cunningham, The CHECKS Pattern Language of Information Integrity, in *Pattern Languages of Program Design*, James O. Coplien and Douglas C. Schmidt (eds.), Addison-Wesley Professional, Reading, MA, 1995.

[CVE 2011] Common Vulnerabilities and Exposures, MITRE Corporation, 2011.

[Daconta 2000] Michael C. Daconta, When Runtime.exec() Won't, JavaWorld.com, 2000.

[Daconta 2003] Michael C. Daconta, Kevin T. Smith, Donald Avondolio, and W. Clay Richardson, *More Java Pitfalls*, Wiley, New York, 2003.

[Darwin 2004] Ian F. Darwin, *Java Cookbook*, O'Reilly, Sebastopol, CA, 2004.

[Davis 2008a] Mark Davis and Ken Whistler, Unicode Standard Annex #15, Unicode Normalization Forms, 2008.

[Davis 2008b] Mark Davis and Michel Suignard, Unicode Technical Report #36, Unicode Security Considerations, 2008.

[Dennis 1966] Jack B. Dennis and Earl C. Van Horn, Programming Semantics for Multiprogrammed Computations, *Communications of the ACM*, Volume 9, Issue 3, March 1966, pp. 143–155, DOI=10.1145/365230.365252.

[DHS 2006] Build Security In, U.S. Department of Homeland Security, 2006.

[Dormann 2008] Will Dormann, Signed Java Applet Security: Worse than ActiveX?, CERT Vulnerability Analysis Blog, 2008.

[Doshi 2003] Gunjan Doshi, Best Practices for Exception Handling, ONJava.com, 2003.

[Dougherty 2009] Chad Dougherty, Kirk Sayre, Robert C. Seacord, David Svoboda, and Kazuya Togashi, *Secure Design Patterns*, CMU/SEI-2009-TR-010, Defense Technical Information Center, Ft. Belvoir, VA, 2009.

[Eclipse 2008] The Eclipse Platform, 2008.

[Egele 2013] Manuel Egele, David Brumley, Yanick Fratantonio, and Christopher Kruegel. An Empirical Study of Cryptographic Misuse in Android Applications, Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, pp.73–84, 2013.

[EMA 2014] Java SE Documentation, Extension Mechanism Architecture, Oracle, 1993, 2014.

[Enck 2009] William Enck, Machigar Ongtang, Patrick Drew McDaniel, and others. Understanding Android Security, *IEEE Security & Privacy,* vol. 7, 1, p. 50–57, 2009.

[Encodings 2014] Supported Encodings, Oracle, 2014.

[Enterprise 2003] The O'Reilly Java Authors, *Java Enterprise Best Practices*, O'Reilly, Sebastopol, CA, 2003.

[ESA 2005] Java Coding Standards, prepared by European Space Agency (ESA) Board for Software Standardisation and Control (BSSC), 2005.

[Fahl 2012] Fahl, Sascha, et al. "Why Eve and Mallory love Android: An analysis of Android SSL (in) security." *Proceedings of the 2012 ACM Conference on Computer and Communications Security*. ACM, 2012.

[Fairbanks 2007] *Design Fragments*, Defense Technical Information Center, Ft. Belvoir, VA, 2007.

[FindBugs 2008] FindBugs Bug Descriptions, 2008.

[Fisher 2003] Maydene Fisher, Jon Ellis, and Jonathan Bruce, *JDBC API Tutorial and Reference*, 3rd ed., Addison-Wesley, Boston, 2003.

[Flanagan 2005] David Flanagan, *Java in a Nutshell*, 5th ed., O'Reilly, Sebastopol, CA, 2005.

[Forman 05] Ira R. Forman and Nate Forman, *Java Reflection in Action*, Manning Publications, Greenwich, CT, 2005.

[Fortify 2014] A Taxonomy of Coding Errors That Affect Security, Java/JSP, Fortify Software, 2014.

[Fox 2001] Joshua Fox, When Is a Singleton Not a Singleton?, Sun Developer Network, 2001.

[Fritz 2014] C. Fritz, S. Arzt, S. Rasthofer, E. Bodden, A. Bartel, J. Klein,Y. le Traon, D. Octeau, and P. McDaniel. FlowDroid: Precise Context, Flow, Field, Object-sensitive and Lifecycle-aware Taint Analysis for Android Apps. In Proc. PLDI, 2014. To appear.

[FT 2008] Function Table Class FunctionTable, Field detail, public static FuncLoader m_functions, 2008.

[Gafter 2006] Neal Grafter, Neal Gafter's blog, 2006.

[Gamma 1995] Erich Gamma, Richard Helm, Ralph Johnson, and John M. Vlissides, *Design Patterns: Elements of Reusable Object-Oriented Software*, Addison-Wesley Professional, Boston, 1995.

[Garfinkel 1996] Simson Garfinkel and Gene Spafford, *Practical UNIX & Internet Security*, 2nd ed., O'Reilly, Sebastopol, CA, 1996.

[Garms 2001] Jess Garms and Daniel Somerfield, *Professional Java Security*, Wrox Press, Chicago, 2001.

[GNU 2013] GNU Coding Standards, Section 5.3, "Clean Use of C Constructs," Richard Stallman and other GNU Project volunteers, 2013

[Goetz 2002] Brian Goetz, Java Theory and Practice: Don't Let the "this" Reference Escape during Construction, IBM developerWorks (Java technology), 2002.

[Goetz 2004a] Brian Goetz, Java Theory and Practice: Garbage Collection and Performance, IBM developerWorks (Java technology), 2004.

[Goetz 2004b] Brian Goetz, Java Theory and Practice: The Exceptions Debate: To Check, or Not to Check?, IBM developerWorks (Java technology), 2004.

[Goetz 2004c] Brian Goetz, Java Theory and Practice: Going Atomic, IBM developerWorks (Java technology), 2004.

[Goetz 2005a] Brian Goetz, Java Theory and Practice: Be a Good (Event) Listener, Guidelines for Writing and Supporting Event Listeners, IBM developerWorks (Java technology), 2005.

[Goetz 2005b] Brian Goetz, Java Theory and Practice: Plugging Memory Leaks with Weak References, IBM developerWorks (Java technology), 2005.

[Goetz 2006a] Brian Goetz, Tim Peierls, Joshua Bloch, Joseph Bowbeer, David Holmes, and Doug Lea, *Java Concurrency in Practice*, Addison-Wesley Professional, Boston, 2006.

[Goetz 2006b] Brian Goetz, Java Theory and Practice: Good Housekeeping Practices, IBM developerWorks (Java technology), 2006.

[Goetz 2007] Brian Goetz, Java Theory and Practice: Managing Volatility, Guidelines for Using Volatile Variables, IBM developerWorks (Java technology), 2006.

[Goldberg 1991] David Goldberg, What Every Computer Scientist Should Know about Floating-Point Arithmetic, Sun Microsystems, March 1991.

[Gong 2003] Li Gong, Gary Ellison, and Mary Dageforde, *Inside Java 2 Platform Security: Architecture, API Design, and Implementation*, 2nd ed., Prentice Hall, Boston, 2003.

[Goodliffe 2014] Pete Goodliffe, *Code Craft: The Practice of Writing Excellent Code*, No Starch Press, San Francisco, 2007

[Grand 2002] Mark Grand, *Patterns in Java*, Volume 1, 2nd ed., Wiley, New York, 2002.

[Gray 1985] Jim Gray, Tandem TR 85.7 WHY DO COMPUTERS STOP AND WHAT CAN BE DONE ABOUT IT?, 1985.

[Greanier 2000] Todd Greanier, Discover the Secrets of the Java Serialization API, Sun Developer Network (SDN), 2000.

[Green 2008] Roedy Green, Canadian Mind Products Java & Internet Glossary, 2008.

[Grigg 2006] Jeffery Grigg, Reflection On Inner Classes, 2006.

[Grosso 2001] William Grosso, Java RMI, O'Reilly, Sebastopol, CA, 2001.

[Grubb 2003] Penny Grubb and Armstrong A. Takang, *Software Maintenance: Concepts and Practice*, 2nd ed., World Scientific, River Edge, NJ, 2003.

[Guillardoy 2012] Esteban Guillardoy, Java 0Day Analysis (CVE-2012-4681), 2012.

[Gupta 2005] Satish Chandra Gupta and Rajeev Palanki, Java Memory Leaks - Catch Me If You Can, 2005.

[Haack 2006] Christian Haack, Erik Poll, Jan Schafer and Aleksy Schubert, Immutable Objects in Java, 2006.

[Haggar 2000] Peter Haggar, *Practical Java™ Programming Language Guide*, Addison-Wesley Professional, Boston, 2000.

[Halloway 2000] Stuart Halloway, Java Developer Connection Tech Tips, March 28, 2000.

[Halloway 2001] Stuart Halloway, Java Developer Connection Tech Tips, January 30, 2001.

[Harold 1997] Elliotte Rusty Harold, *Java Secrets*, Wiley, New York, 1997.

[Harold 1999] Elliotte Rusty Harold, *Java I/O*, O'Reilly, Sebastopol, CA, 1999.

[Harold 2006] Elliotte Rusty Harold, *Java I/O*, 2nd ed., O'Reilly, Sebastopol, CA, 2006.

[Hatton 1995] Les Hatton, *Safer C: Developing Software for High-Integrity and Safety-Critical Systems*, McGraw-Hill, New York, 1995.

[Hawtin 2008] Thomas Hawtin, Secure Coding Antipatterns: Preventing Attacks and Avoiding Vulnerabilities, Sun Microsystems, Make it Fly 2008, London, 2008.

[Havelund 2009] Klaus Havelund and Al Niessner, JPL Coding Standard, version 1.1, California Institute of Technology, 2009.

[Heffley 2004] J. Heffley and P. Meunier, Can Source Code Auditing Software Identify Common Vulnerabilities and Be Used to Evaluate Software Security? *Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS–04)*, Track 9, Volume 9, IEEE Computer Society, January 2004.

[Henney 2003] Kevlin Henney, Null Object, Something for Nothing, 2003.

[Hewlett-Packard 2015] Hewlett-Packard Development Company, J2EE Bad Practices: Leftover Debug Code [generated from version 2015.1.0.0009 of the Fortify Secure Coding Rulepacks], 2015.

[Hirondelle 2013] Passwords Never Clear in Text, Hirondelle Systems, 2013.

[Hitchens 2002] Ron Hitchens, Java™ NIO, O'Reilly, Sebastopol, CA, 2002.

[Hovemeyer 2007] David Hovemeyer and William Pugh, Finding More Null Pointer Bugs, But Not Too Many, *Proceedings of the 7th ACM SIGPLAN-SIGSOFT workshop on Program Analysis for Software Tools and Engineering*, 2007.

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

[Hughes 2011] Elliott Hughes, JNI Local Reference Changes in ICS, November 2011.

[Hunt 1998] J. Hunt and F. Long, Java's Reliability: An Analysis of Software Defects in Java, *Software IEEE Proceedings*, 1998.

[IEC 60812 2006] *Analysis Techniques for System Reliability — Procedure for Failure Mode and Effects Analysis (FMEA)*, 2nd ed., International Electrotechnical Commission, Geneva, Switzerland, 2006.

[IEEE 754 2006] IEEE, Standard for Binary Floating-Point Arithmetic (IEEE 754-1985), 2006.

[IETF OAuth1.0a] Internet Engineering Task Force (IETF). OAuth core 1.0 revision a. http://oauth.net/core/1.0a/.

[IETF OAuth2.0] Internet Engineering Task Force (IETF). The OAuth 2.0 authorization framework. http://tools.ietf.org/html/rfc6749.

[Intrepidus 2012] Intrepidus Group (Mobile Security), NDK File Permissions Gotcha and Fix , 2012.

[ISO/IEC 11889-1:2009] ISO/IEC. *Information Technology—Trusted Platform Module—Part 1: Overview* (ISO/IEC 11889-1:2009). Geneva, Switzerland: ISO, 2009.

[ISO/IEC TR 24772:2010] ISO/IEC TR 24772. *Information Technology — Programming Languages — Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use*, October 2010.

[ISO/IEC TR 24772:2013] ISO/IEC TR 24772:2013. *Information Technology—Programming Languages—Guidance to Avoiding Vulnerabilities in Programming Languages through Language Selection and Use*. Geneva, Switzerland: International Organization for Standardization, March 2013.

[J2SE 2000] Java™ 2 SDK, Standard Edition Documentation, Sun Microsystems, J2SE Documentation version 1.3, Sun Microsystems, 2000.

[J2SE 2011] Java™ SE 7 Documentation, J2SE Documentation version 1.7, Oracle Corporation, 2011.

[JarSpec 2008] J2SE Documentation version 1.5, Jar File Specification, Sun Microsystems, 2000.

[Java 2006] Java - The Java Application Launcher, Sun Microsystems, 2006.

[Java2NS 1999] Marco Pistoia, Duane F. Reller, Deepak Gupta, Milind Nagnur, and Ashok K. Ramani, *Java 2 Network Security*, Prentice Hall, Upper Saddle River, NJ, 1999.

[JavaGenerics 2004] Oracle, Generics, Sun Microsystems, 2004.

[JavaThreads 1999] Scott Oaks and Henry Wong, *Java Threads*, 2nd ed., O'Reilly, Sebastopol, CA, 1999.

[JavaThreads 2004] Scott Oaks and Henry Wong, *Java Threads*, 3rd ed., O'Reilly, Sebastopol, CA, 2004.

[Java Tutorials] The Java Tutorials, Sun Microsystems, 1995, 2015.

[JCF 2014] The Java Collections Framework, Oracle, 2014.

[JDK Bug 2015] JDK Bug System, Oracle, 2015.

[JDK7 2008] Java™ Platform, Standard Edition 7 documentation, Sun Microsystems, December 2008.

[JLS 2005] James Gosling, Bill Joy, Guy Steele, and Gilad Bracha, *The Java Language Specification*, 3rd ed., Prentice Hall, Upper Saddle River, NJ, 2005.

[JLS 2015] James Gosling, Bill Joy, Guy Steele, Gilad Bracha, and Alex Buckley, *The Java® Language Specification*, Java SE 8 Edition, 2015.

[JMX 2006] Monitoring and Management for the Java Platform, Sun Microsystems, 2006.

[JMXG 2006] Java SE Monitoring and Management Guide, Sun Microsystems, 2006.

[JNI 2006] Java Native Interface, Sun Microsystems, 2006.

[JNISpec 2014] Java Native Interface Specification, Oracle, 2014.

[JNI Tips] Java Tips, Android Training.

[Jovanovic 2006] Nenad Jovanovic, Christopher Kruegel, and Engin Kirda, Pixy: A Static Analysis Tool for Detecting Web Application Vulnerabilities (Short Paper), *Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P'06)*, pp. 258–263, May 21–24, 2006.

[JPDA 2004] Java Platform Debugger Architecture (JPDA), Sun Microsystems, 2004.

[JPL 2006] Ken Arnold, James Gosling, and David Holmes, *The Java™ Programming Language*, 4th ed., Addison-Wesley Professional, Boston, 2006.

[JSR-133 2004] JSR-133: Java™ Memory Model and Thread Specification, 2004.

[JSSEC 2013] Android Secure Design and Coding Guidebook, (in Japanese),Japan Smartphone Security Association, 2013.

[JSSEC 2014] Android Application Secure Design / Secure Coding Guidebook, Japan Smartphone Security Association, 2014.

[JVMTI 2006] Java Virtual Machine Tool Interface (JVM TI), Sun Microsystems, 2006.

[JVMSpec 1999] The Java Virtual Machine Specification, Sun Microsystems, 1999.

[Kabanov 2009] Jevgeni Kabanov, The Ultimate Java Puzzler, February 16th, 2009.

[Kabutz 2001] Heinz M. Kabutz, *The Java Specialists' Newsletter*, 2001.

[Kalinovsky 2004] Alex Kalinovsky, *Covert Java: Techniques for Decompiling, Patching, and Reverse Engineering*, SAMS Publishing, Boston, 2004.

[Klieber 2014] William Klieber, Lori Flynn, Amar Bhosale, Limin Jia, and Lujo Bauer. *Android Taint Flow Analysis for App Sets*, ACM SIGPLAN International Workshop on the State Of the Art in Java Program Analysis, 2014.

[Knoernschild 2001] Kirk Knoernschild, *Java™ Design: Objects, UML, and Process*, Addison-Wesley Professional, Boston, 2001.

[Lai 2008] Charlie Lai, Java Insecurity: Accounting for Subtleties That Can Compromise Code, 2008.

[Langer 2008] Angelica Langer, Practicalities – Programming with Java Generics, 2008.

[Laplante 2005] Phillip A. Laplante, Colin J. Neill, Antipatterns: Identification, Refactoring, and Management, Auerbach Publications, Boca Raton, FL, 2005.

[Lea 2000a] Doug Lea, *Concurrent Programming in Java*, 2nd ed., Addison-Wesley Professional, Boston, 2000.

[Lea 2000b] Doug Lea and William Pugh, Correct and Efficient Synchronization of Java™ Technology based Threads, JavaOne Conference, 2000.

[Lea 2008] Doug Lea, The JSR-133 Cookbook for Compiler Writers, 2008.

[Lee 2009] Sangjin Lee, Mahesh Somani, and Debashis Saha, Robust and Scalable Concurrent Programming: Lessons from the Trenches, JavaOne Conference, 2009.

[Liang 1997] Sheng Liang, *The Java™ Native Interface, Programmer's Guide and Specification*, Addison-Wesley Professional, Reading, MA, 1997.

[Liang 1998] Sheng Liang and Gilad Bracha, Dynamic Class Loading in the Java™ Virtual Machine, *Proceedings of the 13th ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages, and Applications*, 1998.

[Lieberman 1986] Henry Lieberman, Using Prototypical Objects to Implement Shared Behavior in Object-Oriented Systems, *Proceedings on Object-Oriented Programming, Systems, Languages, and Applications*, pp. 214–223 (ISSN 0362-1340), Massachusetts Institute of Technology, 1986.

[Lo 2005] Chia-Tien Dan Lo, Witawas Srisa-an, and J. Morris Chang, Security Issues in Garbage Collection, *STSC Crosstalk*, October 2005.

[Long 2005] Fred Long, Software Vulnerabilities in Java, CMU/SEI-2005-TN-044, Software Engineering Institute, Carnegie Mellon University, 2005.

[Long 2013] Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland, and David Svoboda, *Java Coding Guidelines: 75 Recommendations for Reliable and Secure Programs*, Addison-Wesley Professional, Reading, MA, 2013.

[LSOD 02] Last Stage of Delirium Research Group, *Java and Java Virtual Machine Security*. Poland: Last Stage of Delirium Research Group, 2002.

[Low 1997] Douglas Low, Protecting Java Code via Obfuscation, *Crossroads* Volume 4, Issue 3, 1997.

[MacGregor 1998] Robert MacGregor, Dave Durbin, John Owlett, and Andrew Yeomans, *Java Network Security*, Prentice Hall PTR, Upper Saddle River, NJ, 1998.

[Mahmoud 2002] Qusay H. Mahmoud, Compressing and Decompressing Data Using Java APIs, Oracle, 2002.

[Mak 2002] Ronald Mak, *Java Number Cruncher: The Java Programmer's Guide to Numerical Computing*, Prentice Hall PTR, Upper Saddle River, NJ, 2002.

[Manson 2008] Jeremy Manson, Data-Race-ful Lazy Initialization for Performance [blog], 2008.

[Manson 2004] Jeremy Manson and Brian Goetz, JSR 133 (Java Memory Model) FAQ, 2004.

[Manson 2006] Jeremy Manson and William Pugh, The Java™ Memory Model: The Building Block of Concurrency, JavaOne Conference, 2006.

[Martin 1996] Robert C. Martin, Granularity, 1996.

[Masson 2011] Neil D. Masson, Tip: Secure Your Code against the Finalizer Vulnerability, IBM developerWorks, 2011.

[McCluskey 2001] Glen McCluskey, Java Developer Connection Tech Tips, April 10, 2001.

[McGraw 1999] Gary McGraw and Edward W. Felten, *Securing Java, Getting Down to Business with Mobile Code*, Wiley, New York, 1999.

[McGraw 1998] Gary McGraw and Edward W. Felten, Twelve Rules for Developing More Secure Java Code, JavaWorld.com, 1998.

[Mettler 2010a] Adrian Mettler, David Wagner, and T. Close, Joe-E: A Security-Oriented Subset of Java, 17th Network & Distributed System Security Symposium, 2010.

[Mettler 2010b] Adrian Mettler and David Wagner, Class Properties for Security Review in an Object-Capability Subset of Java, *Proceedings of the 5th ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS '10)*. ACM, Article 7, DOI=10.1145/1814217.1814224, 2010.

[Miller 2009] Alex Miller, Java™ Platform Concurrency Gotchas, JavaOne Conference, 2009.

[MITRE 2011] MITRE Corporation, Common Weakness Enumeration, 2011.

[Mocha 2007] Mocha, the Java Decompiler, 2007.

[Monsch 2006] Jan P. Monsch, Ruining Security with java.util.Random Version 1.0, 2006.

[MSDN 2009] Microsoft Corporation, Using SQL Escape Sequences, 2009.

[Muchow 2001] John W. Muchow, MIDlet Packaging with J2ME, ONJava.com, 2001.

[Müller 2002] Dr. Andreas Müller and Geoffrey Simmons, Exception Handling: Common Problems and Best Practice with Java 1.4, Sun Microsystems GmbH, 2002.

[Naftalin 2006a] Maurice Naftalin and Philip Wadler, *Java Generics and Collections*, O'Reilly, Sebastopol, CA, 2006.

[Naftalin 2006b] Maurice Naftalin and Philip Wadler, Java™ Generics and Collections: Tools for Productivity, JavaOne Conference, 2007.

[Netzer 1992] Robert H. B. Netzer and Barton P. Miller, *What Are Race Conditions? Some Issues and Formalization*, University of Wisconsin, Madison, 1992.

[Neward 2004] Ted Neward, *Effective Enterprise Java*, Addison-Wesley Professional, Boston, 2004.

[Nisewanger 2007] Jeff Nisewanger, Avoiding Antipatterns, JavaOne Conference, 2007.

[Nolan 2004] Godfrey Nolan, *Decompiling Java*, Apress, Berkley, CA, 2004.

[Oaks 2001] Scott Oaks, *Java Security*, O'Reilly, Sebastopol, CA, 2001.

[Octeau 2013] D. Octeau, P. McDaniel, S. Jha, A. Bartel, E. Bodden, J. Klein, and Y. Le Traon. Effective Inter-component communication mapping in Android with Epicc: An essential step towards holistic security analysis. In Proc. USENIX Security, 2013.

[Open Group 2004] The IEEE and The Open Group, The Open Group Base Specifications Issue 6, 2004.

[Oracle 2010a] Java SE 6 HotSpot™ Virtual Machine Garbage Collection Tuning, Oracle, 2010.

[Oracle 2010b] New I/O APIs, Oracle, 2010.

[Oracle 2011a] Java PKI Programmer's Guide, Oracle, 2011.

[Oracle 2011b] Java Platform™, Standard Edition 6 Documentation, Oracle, 2011.

[Oracle 2011c] Package javax.servelt.http, Oracle 2011.

[Oracle 2011d] Permissions in the Java™ SE 6 Development Kit (JDK), Oracle, 2011.

[Oracle 2013a] API for Privileged Blocks, Oracle, 1993/2013.

[Oracle 2013b] Reading ASCII Passwords from an InputStream Example, *Java Cryptography Architecture (JCA) Reference Guide*, Oracle, 2013.

[Oracle 2013c] Java Platform Standard Edition 7 Documentation, Oracle, 2013.

[Oracle 2013d] Oracle Security Alert for CVE-2013-0422, Oracle, 2013.

[Oracle 2014] Secure Coding Guidelines for Java SE, Version 5.0, Oracle, 2014.

[Oracle 2015] Oracle GlassFish Server Performance Tuning Guide, Tuning the Java Runtime System, Oracle, 2015.

[OWASP 2005] A Guide to Building Secure Web Applications and Web Services, Open Web Application Security Project (OWASP), 2005.

[OWASP 2007] OWASP Top 10 for Java EE, OWASP, 2007.

[OWASP 2009] Double Encoding, OWASP, 2009.

[OWASP 2011] Open Web Application Security Project (OWASP), 2011.

[OWASP 2014a] Preventing LDAP Injection in Java, OWASP, 2014.

[OWASP 2014b] XSS (Cross Site Scripting) Prevention Cheat Sheet, OWASP, 2014.

[PCI 2010] PCI Security Standards Council, Payment Card Industry (PCI) Data Security Standard, Version 2.0, October, 2010.

[Permissions 2008] Permissions in the Java™ SE 6 Development Kit (JDK), Sun Microsystems, 2008.

[Philion 2003] Paul Philion, Beware the Dangers of Generic Exceptions, JavaWorld.com, 2003.

[Phillips 2005] Addison P. Phillips, Are We Counting Bytes Yet?, 27th Internationalization and Unicode Conference, webMethods, 2005.

[Pistoia 2004] Marco Pistoia, Nataraj Nagaratnam, Larry Koved, and Anthony Nadalin, Enterprise *Java Security: Building Secure J2EE Applications*, Addison-Wesley Professional, Boston, 2004.

[Policy 2002] Sun Microsystems, Default Policy Implementation and Policy File Syntax, Document revision 1.6, 2002.

[Pugh 2004] William Pugh, The Java Memory Model (discussions reference), 2004.

[Pugh 2008] William Pugh, Defective Java Code: Turning WTF Code into a Learning Experience, JavaOne Conference, 2008.

[Pugh 2009] William Pugh, Defective Java Code: Mistakes That Matter, JavaOne Conference, 2009.

[Rapid7 2014] Jeroen Frijters and Juan Vazquez, Java AtomicReferenceArray Type Violation Vulnerability, 2014.

[Reasoning 2003] Reasoning Inspection Service Defect Data Tomcat v 1.4.24, November 14, 2003.

[Reflect 2006] Sun Microsystems, Reflection, 2006.

[Rogue 2000] Vermeulen, Ambler, Metz, Misfeldt, Shur, and Thompson, *The Elements of Java Style*, Cambridge University Press, New York, 2000.

[Rotem 2008] Arnon Rotem-Gal-Oz, Fallacies of Distributed Computing Explained, 2008.

[Roubtsov 2003a] Vladimir Roubtsov, Breaking Java Exception-Handling Rules is Easy, JavaWorld.com, 2003.

[Roubtsov 2003b] Vladimir Roubtsov, Into the Mist of Serialization Myths, JavaWorld.com, 2003.

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

[Saltzer 1975] J. H. Saltzer and M. D. Schroeder, The Protection of Information in Computer Systems, *Proceedings of the IEEE*, Volume 63, Issue 9, 1975, 1278–1308.
Available at http://web.mit.edu/Saltzer/www/publications/protection/.

[SCG 2009] Sun Microsystems, Secure Coding Guidelines for the Java Programming Language, version 3.0, 2009.

[Schildt 2007] Herb Schildt, *Herb Schildt's Java Programming Cookbook*, McGraw-Hill, New York, 2007.

Schindler, Uwe. The Policeman's Horror: Default Locales, Default Charsets, and Default Timezones, The Generics Policeman Blog, November 2012.

[Schneier 2000] Bruce Schneier, *Secrets and Lies—Digital Security in a Networked World*, Wiley, New York, 2000.

[Schönefeld 2002] Marc Schönefeld, Security Aspects in Java Bytecode Engineering, Blackhat Briefings 2002, Las Vegas, August 2002.

[Schönefeld 2004] Marc Schönefeld, Java Vulnerabilities in Opera 7.54, BUGTRAQ Mailing List (bugtraq@securityfocus.com), November 2004.

[Schwarz 2004] Don Schwarz, Avoiding Checked Exceptions, ONJava 2004.

[Schweisguth 2003] Dave Schweisguth, Java Tip 134: When Catching Exceptions, Don't Cast Your Net Too Wide, Javaworld.com, 2003.

[SDN 2008] Sun Microsystems, SUN Developer Network, 1994–2008.

[Seacord 2005] Robert C. Seacord, *Secure Coding in C and C++*, Addison-Wesley Professional, Boston, 2005.

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

[Seacord 2010] Robert C. Seacord, William Dormann, James McCurley, Philip Miller, Robert Stoddard, David Svoboda, and Jefferson Welch, Source Code Analysis Laboratory (SCALe) for energy delivery systems, CMU/SEI-2010-TR-021, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, December 2010.

[Seacord 2013] Seacord, Robert C. *Secure Coding in C and C++*, 2nd ed. Addison-Wesley, Boston, 2013.

[Seacord 2015] Seacord, Robert C. Secure Coding Rules for Java. Addison-Wesley Professional, Boston, 2013.

[SecArch 2006] Sun Microsystems, Java 2 Platform Security Architecture, 2006.

[Secunia 2008] Secunia ApS, Secunia Advisories, 2008.

[Security 2006] Java Security Guides, Sun Microsystems, 2006.

[SecuritySpec 2008] Sun Microsystems, Java Security Architecture, 2008.

[Sen 2007] Robi Sen, Avoid the Dangers of XPath Injection, IBM developerWorks, 2007.

[Shipilv 2014] Shipilv, Aleksey, Safe Publication and Safe Initialization in Java, December 2014.

[Steel 2005] Christopher Steel, Ramesh Nagappan, and Ray Lai, *Core Security Patterns: Best Practices and Strategies for J2EEâ¢, Web Services, and Identity Management*, Prentice Hall PTR, Upper Saddle River, NJ, 2005.

[Steele 1977] G.L. Steele, Arithmetic Shifting Considered Harmful, *ACM SIGPLAN Notices*, Volume 12, Issue 11 (1977), 61–69.

[Steinberg 2005] Daniel H. Steinberg, Java Developer Connection Tech Tips Using the Varargs Language Feature, January 4, 2005.

[Sterbenz 2006] Andreas Sterbenz and Charlie Lai, Secure Coding Antipatterns: Avoiding Vulnerabilities, Sun Microsystems, JavaOne Conference, 2006.

[Steuck 2002] Gregory Steuck, XXE (Xml eXternal Entity) Attack, 2002.

[Sun 1999] Why Are Thread.stop, Thread.suspend, Thread.resume and Runtime.runFinalizersOnExit Deprecated?, Sun Microsystems, 1999.

[Sun 2002] Reflection, Sun Microsystems, 2002.

[Sun 2003] Sun Microsystems, Sun ONE Application Server 7 Performance Tuning Guide, 2003.

[Sun 2004a] Java Management Extensions (JMX), Sun Microsystems, 2004.

[Sun 2004b] Java Object Serialization Specification, Version 1.5.0, Sun Microsystems, 2004.

[Sun 2004d] JVM Tool Interface, Sun Microsystems, 2004.

[Sun 2006] Java™ Platform, Standard Edition 6 documentation, Sun Microsystems, 2006.

[Sun 2008] Java™ Plug-in and Applet Architecture, Sun Microsystems, 2008.

[Sutherland 2010] Dean F. Sutherland and William L. Scherlis, Composable Thread Coloring, *Proceedings of the 15th ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming*, Association for Computing Machinery, New York, 2010.

[Tanenbaum 2003] Andrew S. Tanenbaum and Maarten Van Steen, *Distributed Systems: Principles and Paradigms*, 2nd ed., Prentice Hall, Upper Saddle River, NJ, 2003.

[Techtalk 2007] Josh Bloch and William Pugh, The PhantomReference Menace. Attack of the Clone. Revenge of the Shift, JavaOne Conference, 2007.

[Tomcat 2009] Apache Software Foundation, Changelog and Security fixes, Tomcat documentation, 2009.

[Unicode 2003] The Unicode Consortium, *The Unicode Standard*, Version 4.0.0, defined by The Unicode Standard, Version 4.0, Addison-Wesley, Reading, MA, 2003.

[Unicode 2007] The Unicode Consortium, *The Unicode Standard*, Version 5.1.0, defined by The Unicode Standard, Version 5.0, Addison-Wesley, Reading, MA, 2007, as amended by Unicode 5.1.0.

[Unicode 2011] The Unicode Consortium, *The Unicode Standard*, Version 6.0.0, The Unicode Consortium, Mountain View, CA, 2011.

[Unicode 2012] The Unicode Consortium. *The Unicode Standard, Unicode 6.2.0*, (Mountain View, CA: The Unicode Consortium, 2012. ISBN 978-1-936213-07-8)

[Urma 2014] Raoul-Gabriel Urma, Tired of Null Pointer Exceptions? Consider Using Java SE 8's Optional!, Oracle, March 2014.

[Venners 1997] Bill Venners, Security and the Class Loader Architecture, Java World.com, 1997.

[Venners 2003] Bill Venners, Failure and Exceptions, A Conversation with James Gosling, Part II, Artima.com, 2003.

[Verify] Verifying App Behavior on the Android Runtime (ART), Android.

[Vermeulen 2000] Allan Vermeulen, Scott W. Ambler, Greg Bumgardner, Eldon Metz, Trevor Misfeldt, Jim Shur, and Patrick Thompson. *The Elements of Java™ Style*. Cambridge University Press, New York, 2000.

[viaForensics 2014] Secure mobile development best practices, viaForensics LLC., 2014.

[W3C 2008] Tim Bray, Jean Paoli, C. M. Sperberg-McQueen, Eve Maler, and François Yergeau, *Extensible Markup Language (XML) 1.0*, 5th ed., W3C Recommendation, 2008.

[W3C 2013] Andrei Popescu, Geolocation API Specification, W3C Recommendation, 2013.

[Ware 2008] Michael S. Ware, *Writing Secure Java Code: A Taxonomy of Heuristics and an Evaluation of Static Analysis Tools*, Masters thesis, James Madison University, Harrisonburg, VA, 2008.

[Weber 2009] Chris Weber, Exploiting Unicode-enabled Software, CanSecWest, March 2009.

[Wheeler 2003] David A. Wheeler, Secure Programming for Linux and Unix HOWTO, 2003.

[White 2003] Tom White, Memoization in Java Using Dynamic Proxy Classes, August 2003.

[Zukowski 2004] John Zukowski, Creating Custom Security Permissions, Java Developer Connection Tech Tips, May 18, 2004.