

Rec. AA. References

- [Apache 2014] [Apache Tika: A Content Analysis Toolkit](#). The Apache Software Foundation (2014).
- [API 2006] [Java Platform, Standard Edition 6 API Specification](#), Oracle (2006).
- [API 2011] [Java Platform, Standard Edition 7 API Specification](#), Oracle (2011).
- [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., Boston: Addison-Wesley (2006).
- [Black 2004] Black, Paul E., 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 (2004).
- [Bloch 2001] Bloch, Joshua. *Effective Java: Programming Language Guide*. Boston: Addison-Wesley (2001).
- [Bloch 2005] Bloch, Joshua, and Neal Gafter. *Java Puzzlers: Traps, Pitfalls, and Corner Cases*. Upper Saddle River, NJ: Addison-Wesley (2005).
- [Bloch 2008] Bloch, Joshua. *Effective Java*, 2nd ed. Upper Saddle River, NJ: Addison-Wesley (2008).
- [Campioni 1996] Campione, Mary, and Kathy Walrath. *The Java Tutorial: Object-Oriented Programming for the Internet*. Reading, MA: Addison-Wesley (1996).
- [Chan 1999] Chan, Patrick, Rosanna Lee, and Douglas Kramer. *The Java Class Libraries: Supplement for the Java 2 Platform, v1.2*, 2nd ed., vol. 1. Upper Saddle River, NJ: Prentice Hall (1999).
- [Cohen 1981] Cohen, D. [On Holy Wars and a Plea for Peace](#), *IEEE Computer*, 14(10):48–54 (1981).
- [Conventions 2009] [Code Conventions for the Java Programming Language](#). Oracle (2009).
- [Coomes 2007] Coomes, John, Peter Kessler, and Tony Printezis. [Garbage Collection-Friendly Programming](#). Java SE Garbage Collection Group, Sun Microsystems, JavaOne Conference (2007).
- [Core Java 2004] Horstmann, Cay S., and Gary Cornell. *Core Java™ 2, Vol. 1: Fundamentals*, 7th ed. Upper Saddle River, NJ: Prentice Hall PTR (2004).
- [Coverity 2007] *Coverity Prevent User's Manual (3.3.0)*. [Coverity](#) (2007).
- [Daconta 2003] Daconta, Michael C., Kevin T. Smith, Donald Avondolio, and W. Clay Richardson. *More Java Pitfalls: 50 New Time-Saving Solutions and Workarounds*. Indianapolis, IN: Wiley (2003).
- [Davis 2008] Davis, Mark, and Ken Whistler (Ed.). [Unicode Standard Annex #15: Unicode Normalization Forms](#) (2008).
- [Dennis 1966] Dennis, Jack B., and Earl C. Van Horn. 1966. Programming Semantics for Multiprogrammed Computations. *Communications of the ACM*, 9(3):143–155 (1966). doi: 10.1145/365230.365252.
- [Dougherty 2009] Dougherty, Chad, Kirk Sayre, Robert C. Seacord, David Svoboda, and Kazuya Togashi. [Secure Design Patterns](#). CMU/SEI-2009-TR-010 (2009).
- [ESA 2005] ESA (European Space Agency). [Java Coding Standards](#). Prepared by ESA Board for Software Standardisation and Control (BSSC) (2005).
- [FindBugs 2008] [FindBugs Bug Descriptions](#) (2008/2011).
- [Flanagan 2005] Flanagan, David. *Java in a Nutshell*, 5th ed. Sebastopol, CA: O'Reilly Media (2005).

- [Fortify 2014] Fortify Software Security Research Group with Gary McGraw. [A Taxonomy of Coding Errors That Affect Security](#) (see Java/JSP) (2008/2014).
- [GNU 2013] [GNU Coding Standards, §5.3, "Clean Use of C Constructs."](#) Richard Stallman and other GNU Project volunteers (2013).
- [Goetz 2004] Goetz, Brian. [Java Theory and Practice: Garbage Collection and Performance: Hints, Tips, and Myths about Writing Garbage Collection-Friendly Classes](#). IBM developerWorks (2004).
- [Goetz 2006] Goetz, Brian, Tim Peierls, Joshua Bloch, Joseph Bowbeer, David Holmes, and Doug Lea. *Java Concurrency in Practice*. Boston: Addison-Wesley Professional (2006).
- [Goetz 2007] Goetz, Brian. [Java Theory and Practice: Managing Volatility: Guidelines for Using Volatile Variables](#). IBM developerWorks (2007).
- [Gong 2003] Gong, Li, Gary Ellison, and Mary Dageforde. *Inside Java 2 Platform Security: Architecture, API Design, and Implementation*, 2nd ed. Boston: Addison-Wesley (2003).
- [Goodliffe 2007] Pete Goodliffe. *Code Craft: The Practice of Writing Excellent Code*. San Francisco: No Starch Press (2007).
- [Grand 2002] Grand, Mark. *Patterns in Java, Vol. 1: A Catalog of Reusable Design Patterns Illustrated with UML*, 2nd ed. Indianapolis, IN: Wiley (2002).
- [Grubb 2003] Penny Grubb, and Armstrong A. Takang. *Software Maintenance Concepts and Practice*, 2nd ed. River Edge, NJ: World Scientific (2003).
- [Guillardoy 2012] Guillardoy, Esteban. [Java 0-day Analysis \(CVE-2012-4681\)](#) (2012).
- [Hatton 1995] Hatton, Les. *Safer C: Developing Software for High-Integrity and Safety-Critical Systems*. New York: McGraw-Hill (1995).
- [Havelund 2009] Havelund, Klaus, and Al Niessner. [JPL Coding Standard, Version 1.1](#) (2009)
- [Hawtin 2006] Hawtin, Thomas. [\[drlvm\]\[kernel_classes\] ThreadLocal Vulnerability](#). MarkMail (2006).
- [Hirondelle 2013] Hirondelle Systems. [Passwords Never Clear in Text](#) (2013).
- [ISO/IEC 9126-1:2001] *Software Engineering—Product Quality—Part 1, Quality Model* (ISO/IEC 9126-1:2001). Geneva, Switzerland: International Organization for Standardization (2001).
- [ISO/IEC 24765:2010] *Systems and Software Engineering—Vocabulary* (ISO/IEC 24765:2010). Geneva, Switzerland: International Organization for Standardization (2010).
- [JLS 2013] Gosling, James, Bill Joy, Guy Steele, Gilad Bracha, and Alex Buckley. *Java Language Specification: Java SE 7 Edition*. Oracle America (2013).
- [Jovanovic 2006] Jovanovic, Nenad, Christopher Kruegel, and Engin Kirda. [Pixy: A Static Analysis Tool for Detecting Web Application Vulnerabilities \(Short Paper\)](#). In *Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P'06)*, pp. 258–263, May 21–24, Oakland, CA (2006).
- [JPL 2006] Arnold, Ken, James Gosling, and David Holmes. *The Java™ Programming Language*, 4th ed. Reading, MA: Addison-Wesley Professional (2006).
- [JVMSpec 1999] [The Java Virtual Machine Specification](#). Sun Microsystems (1999).
- [JVMSpec 2013] [The Java Virtual Machine Specification: Java SE 7 Edition](#). Oracle America (2013).
- [Kabanov 2009] Kabanov, Jevgeni. [The Ultimate Java Puzzler](#) (2009).
- [Kalinovsky 2004] Kalinovsky, Alex. *Covert Java: Techniques for Decompiling, Patching, and Reverse Engineering*. Indianapolis: SAMS (2004).

- [Knoernschild 2002] Knoernschild, Kirk. *Java™ Design: Objects, UML, and Process*. Boston: Addison-Wesley Professional (2002).
- [Lea 2000] Lea, Doug. *Concurrent Programming in Java: Design Principles and Patterns*, 2nd ed. Boston: Addison-Wesley (2000).
- [Lo 2005] Lo, Chia-Tien Dan, Witawas Srisa-an, and J. Morris Chang. [Security Issues in Garbage Collection](#). *STSC Crosstalk*, (2005, October).
- [Long 2012] Long, Fred, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland, and David Svoboda. *The CERT Oracle Secure Coding Standard for Java*, SEI Series in Software Engineering. Boston: Addison-Wesley (2012).
- [Manion 2013] Manion, Art. [Anatomy of Java Exploits](#), CERT/CC Blog (January 15, 2013).
- [Martin 1996] Martin, Robert C. [Granularity](#). *The C++ Report* 8(10):57–62 (1996).
- [McGraw 1999] McGraw, Gary, and Edward W. Felten. *Securing Java: Getting Down to Business with Mobile Code*, 2nd ed. New York: Wiley (1999).
- [Mettler 2010] 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] Miller, Alex. [Java™ Platform Concurrency Gotchas](#). JavaOne Conference (2009).
- [Netzer 1992] Netzer, Robert H. B., and Barton P. Miller. [What Are Race Conditions? Some Issues and Formalization](#). *ACM Letters on Programming Languages and Systems* 1(1):74–88 (1992).
- [Oaks 2001] Oaks, Scott. *Java Security*. Sebastopol, CA: O'Reilly (2001).
- [Oracle 2008] [Permissions in the Java™ SE 6 Development Kit \(JDK\)](#). Oracle (2008).
- [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.servelet.http](#), Oracle 2011.
- [Oracle 2011d] [Permissions in the Java™ SE 6 Development Kit \(JDK\)](#), Oracle, 2011.
- [Oracle 2012a] [API for Privileged Blocks](#). Oracle (1993/2012).
- [Oracle 2012b] ["Reading ASCII Passwords from an InputStream Example," Java Cryptography Architecture \(JCA\) Reference Guide](#). Oracle (2012).
- [Oracle 2012c] [Java Platform Standard Edition 7 Documentation](#). Oracle (2012).
- [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.

- [OWASP 2005] OWASP (Open Web Application Security Project). [A Guide to Building Secure Web Applications and Web Services](#) (2005).
- [OWASP 2008] OWASP. [Open Web Application Security Project homepage](#) (2008).
- [OWASP 2009] OWASP. [Session Fixation in Java](#) (2009).
- [OWASP 2011] OWASP. [Cross-site Scripting \(XSS\)](#) (2011).
- [OWASP 2012] OWASP. ["Why Add Salt?" Hashing Java](#) (2012).
- [OWASP 2013] OWASP. [OWASP Guide Project](#) (2011).
- [Paar 2010] Paar, Christof, and Jan Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*. New York: Springer (2009). (Companion website contains online cryptography course that covers hash functions.)
- [Pistoia 2004] Pistoia, Marco, Nataraj Nagaratnam, Larry Koved, and Anthony Nadalin. *Enterprise Java Security: Building Secure J2EE Applications*. Boston: Addison-Wesley (2004).
- [Policy 2010] [Default Policy Implementation and Policy File Syntax](#), Document revision 1.6, Oracle (2010).
- [Reddy 2000] Reddy, Achut. [Java Coding Style Guide](#). (2000).
- [Rogue 2000] Vermeulen, Allan, Scott W. Ambler, Greg Bumgardner, and Eldon Metz. *The Elements of Java Style*. New York: Cambridge University Press (2000).
- [SCG 2010] [Secure Coding Guidelines for the Java Programming Language, version 4.0](#). Oracle (2010).
- [Seacord 2009] Seacord, Robert C. *The CERT C Secure Coding Standard*. Boston: Addison-Wesley (2009).
- [Seacord 2012] Seacord, Robert, Will Dormann, James McCurley, Philip Miller, Robert Stoddard, David Svoboda, and Jefferson Welch. *Source Code Analysis Laboratory (SCALe)* (CMU/SEI-2012-TN-013). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2012. <http://www.sei.cmu.edu/library/abstracts/reports/12tn013.cfm>.
- [Seacord 2013] Seacord, Robert C. *Secure Coding in C and C++*, 2nd ed. Boston: Addison-Wesley (2013). See <http://www.cert.org/books/secure-coding> for news and errata.
- [SecuritySpec 2010] [Java Security Architecture](#). Oracle (2010).
- [Sen 2007] Sen, Robi. [Avoid the Dangers of XPath Injection](#). IBM developerWorks (2007).
- [Sethi 2009] Sethi, Amit. [Proper Use of Java's SecureRandom](#). Digital Justice League Blog (2009).
- [Steinberg 2008] Steinberg, Daniel H. Using the Varargs Language Feature. Java Developer Connection Tech Tips (2008).
- [Sterbenz 2006] Sterbenz, Andreas, and Charlie Lai. [Secure Coding Antipatterns: Avoiding Vulnerabilities](#). JavaOne Conference (2006).
- [Sun 2006] [Java™ Platform, Standard Edition 6 Documentation](#). Oracle (2006).
- [Sutherland 2010] Sutherland, Dean F., and William L. Scherlis. [Composable Thread Coloring](#). In *Proceedings of the 15th ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming*. New York: ACM (2010).
- [Tools 2011] [JDK Tools and Utilities Specification](#). Oracle (2011).
- [Tutorials 2013] [The Java Tutorials](#). Oracle (2013).

[Unicode 2009] The Unicode Consortium. The Unicode Standard, Version 5.2.0, defined by [The Unicode Standard, Version 5.2](#). Mountain View, CA: The Unicode Consortium (2009).

[Unicode 2013] The Unicode Consortium. The Unicode Standard, Version 6.2.0, defined by [Unicode 6.2.0](#). Mountain View, CA: The Unicode Consortium (2013).

[Vermeulen 2000] Vermeulen, Allan, Scott W. Ambler, Greg Bumgardner, and Eldon Metz. *The Elements of Java Style*. New York: Cambridge University Press (2000).

[Viega 2005] Viega, John. [CLASP Reference Guide, Volume 1.1](#). Secure Software (2005).

[W3C 2003] [The World Wide Web Security FAQ](#). World Wide Web Consortium (W3C) (2003).

[Ware 2008] Ware, Michael S. [Writing Secure Java Code: A Taxonomy of Heuristics and an Evaluation of Static Analysis Tools](#) (thesis). James Madison University (2008).

[White 2003] White, Tom. [Memoization in Java Using Dynamic Proxy Classes](#). O'Reilly onJava.com (2003).

[Zadegan 2009] Zadegan, Bryant. [A Lesson on Infinite Loops](#) (2009).