Bibliography

Bibliography

URLs are valid as of the publication date of this document.

[1]	B. Cancilla, "Return of the Browser Wars," August 2004. [Online]. Available: http://www.ibmsystemsmag.com/ibmi/trends/whatsnew/Return-of-the-Browser-Wars/. [Accessed 17 May 2017].
[2]	A. Manion, "Vulnerability Note VU#713878 Microsoft Internet Explorer does not properly validate source of redirected frame," CERT/CC, 9 June 2004. [Online]. Available: https://www.kb.cert.org/vuls/id/713878. [Accessed 17 May 2017].
[3]	Oxford Living Dictionaries (English), "process," [Online]. Available: https://en.oxforddictionaries.com/definition/process. [Accessed 17 May 2017].
[4]	Kissel, Richard (Editor), "NISTIR 7298 Revision 2 Glossary of Key Information Security Terms," U.S. Department of Commerce, 2013.
[5]	R. Caralli, J. H. Allen and D. W. White, CERT Resilience Management Model: A Maturity Model for Managing Operational Resilience, Addison-Wesley Professional, 2010.
[6]	A. Shostack, Threat modeling: Designing for Security, John Wiley & Sons, 2014.
[7]	F. Swiderski and W. Snyder, Threat Modeling, Microsoft Press, 2004.
[8]	R. C. Seacord, The CERT C Secure Coding Standard, Pearson Education, 2008.
[9]	F. Long, D. Mohindra, R. C. Seacord and D. a. S. D. Sutherland, The CERT Oracle Secure Coding Standard for Java, Addison-Wesley Professional, 2011.
[10]	G. McGraw, Software Security: Building Security In, Addison-Wesley Professional, 2006.
[11]	G. Peterson, P. Hope and S. Lavenhar, "Architectural Risk Analysis," 2 July 2013. [Online]. Available: https://www.us-cert.gov/bsi/articles/best-practices/architectural-risk-analysis/architectural-risk-analysis. [Accessed 23 May 2017].
[12]	J. Ryoo, R. Kazman and P. Anand, "Architectural Analysis for Security," *IEEE Security & Privacy,* vol. 13, no. 6, pp. 52-59, 2015.
[13]	A. Householder, "Like Nailing Jelly to the Wall: Difficulties in Defining "Zero-Day Exploit," CERT, 7 July 2015. [Online]. Available: https://insights.sei.cmu.edu/cert/2015/07/like-nailing-jelly-to-the-wall-difficulties-in-defining-zero-day-exploit.html. [Accessed 23 May 2017].
[14]	MITRE, "Common Vulnerabilities and Exposures," [Online]. Available: https://cve.mitre.org/. [Accessed 16 May 2017].
[15]	CERT/CC, "Vulnerability Notes Database," [Online]. Available: https://www.kb.cert.org/vuls. [Accessed 16 May 2017].
[16]	SecurityFocus, "Vulnerabilities," [Online]. Available: http://www.securityfocus.com/bid. [Accessed 23 May 2017].
[17]	ISO/IEC, "ISO/IEC 29147:2014 Information technology—Security techniques—Vulnerability disclosure," 2014.
[18]	S. Christey and C. Wysopal, "Responsible Vulnerability Disclosure Process draft-christey-wysopal-vuln-disclosure-00.txt," February 2002. [Online]. Available: https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00. [Accessed 17 May 2017].
[19]	MSRC Ecosystem Strategy Team, "Coordinated Vulnerability Disclosure: Bringing Balance to the Force," 22 July 2010. [Online]. Available: https://blogs.technet.microsoft.com/ecostrat/2010/07/22/coordinated-vulnerability-disclosure-bringing-balance-to-the-force/. [Accessed 23 May 2017].
[20]	Microsoft Security Response Center, "Coordinated Vulnerability Disclosure," Microsoft, [Online]. Available: https://technet.microsoft.com/en-us/security/dn467923.aspx. [Accessed 23 May 2017].

[21]	M. Souppaya and K. Scarfone, "NIST Special Publication 800-40 Revision 3 Guide to Enterprise Patch Management Technologies," U.S. Department of Commerce, 2013.
[22]	A. Arora, A. Nandkumar and R. Telang, "Does information security attack frequency increase with vulnerability disclosure? An empirical analysis," *Information Systems Frontiers,* vol. 8, no. 5, pp. 350-362, 2006.
[23]	FIRST, "Forum for Incident Response and Security Teams," [Online]. Available: https://www.first.org/. [Accessed 17 May 2017].
[24]	FIRST, "Vulnerability Coordination SIG," [Online]. Available: https://www.first.org/global/sigs/vulnerability-coordination. [Accessed 17 May 2017].
[25]	National Telecommunications and Information Administration, "Multistakeholder Process: Cybersecurity Vulnerabilities," 15 December 2016. [Online]. Available: https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities. [Accessed 17 May 2017].
[26]	Harm Reduction Coalition, "Principles of Harm Reduction," [Online]. Available: http://harmreduction.org/about-us/principles-of-harm-reduction/. [Accessed 23 May 2017].
[27]	Harm Reduction Coalition, "What is harm reduction?" [Online]. Available: https://www.hri.global/what-is-harm-reduction. [Accessed 23 May 2017].
[28]	A. Householder, "Systemic Vulnerabilities: An Allegorical Tale of SteampunkVulnerability to Aero-Physical Threats," August 2015. [Online]. Available: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=442528. [Accessed 17 May 2017].
[29]	I Am The Cavalry, "5 Motivations of Security Researchers," [Online]. Available: https://www.iamthecavalry.org/motivations/. [Accessed 17 May 2017].
[30]	NTIA Awareness and Adoption Working Group, "Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group," 15 December 2016. [Online]. Available: https://www.ntia.doc.gov/files/ntia/publications /2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf. [Accessed 6 June 2017].
[31]	FIRST, "Ethics SIG," [Online]. Available: https://www.first.org/global/sigs/ethics. [Accessed 17 May 2017].
[32]	Association for Computing Machinery, "ACM Code of Ethics and Professional Conduct," 16 October 1992. [Online]. Available: https://www.acm.org /about-acm/acm-code-of-ethics-and-professional-conduct. [Accessed 17 May 2017].
[33]	USENIX, "System Administrators' Code of Ethics," 30 September 2003. [Online]. Available: https://www.usenix.org/system-administrators-code-ethics. [Accessed 17 May 2017].
[34]	American Press Institute, "What is the purpose of journalism?" [Online]. Available: https://www.americanpressinstitute.org/journalism-essentials /what-is-journalism/purpose-journalism/. [Accessed 17 May 2017].
[35]	Society of Professional Journalists, "SPJ Code of Ethics," 6 September 2014. [Online]. Available: https://www.spj.org/ethicscode.asp. [Accessed 17 May 2017].
[36]	A. Ozment and S. E. Schechter, "Milk or wine: Does software security improve with age?" in *USENIX Security*, 2006.
[37]	K. Matsudaira, "Bad Software Architecture Is a People Problem," *Communications of the ACM,* vol. 59, no. 9, pp. 42-43, September 2016.
[38]	J. M. Wing, "A Symbiotic Relationship Between Formal Methods and Security," in *Proceedings of the Conference on Computer Security, Dependability and Assurance: From Needs to Solutions*, 1998.
[39]	E. Bobukh, "Equation of a Fuzzing Curve — Part 1/2," 18 December 2014. [Online]. Available: https://blogs.msdn.microsoft.com/eugene_bobukh /2014/12/18/equation-of-a-fuzzing-curve-part-12/. [Accessed 23 May 2017].
[40]	E. Bobukh, "Equation of a Fuzzing Curve — Part 2/2," 6 January 2015. [Online]. Available: https://blogs.msdn.microsoft.com/eugene_bobukh/2015 /01/06/equation-of-a-fuzzing-curve-part-22/. [Accessed 23 May 2017].

[41]	H. W. Rittel and M. M. Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences,* vol. 4, no. 1973, pp. 155-169, June 1973.
[42]	BBC, "Xbox password flaw exposed by five-year-old boy," 4 April 2014. [Online]. Available: http://www.bbc.com/news/technology-26879185. [Accessed 16 May 2017].
[43]	Microsoft, "What is the Security Development Lifecycle?" [Online]. Available: https://www.microsoft.com/en-us/sdl/. [Accessed 16 May 2017].
[44]	BSIMM, "BSIMM Framework," [Online]. Available: https://www.bsimm.com/framework/. [Accessed 16 May 2017].
[45]	ISO/IEC, "ISO/IEC 30111:2013 Information technology—Security techniques—Vulnerability handling processes," 2013.
[46]	Microsoft, "Microsoft Security Response Center," [Online]. Available: https://technet.microsoft.com/en-us/security/dn440717.aspx. [Accessed 23 May 2017].
[47]	Cisco Systems, "Security Vulnerability Policy," [Online]. Available: https://www.cisco.com/c/en/us/about/security-center/security-vulnerability-policy.html. [Accessed 23 May 2017].
[48]	FIRST, "FIRST Teams," [Online]. Available: https://www.first.org/members/teams. [Accessed 16 May 2017].
[49]	CERT Division, "CSIRT Frequently Asked Questions (FAQ)," Software Engineering Institute, [Online]. Available: https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm? [Accessed 16 May 2017].
[50]	CERT Division, "Incident Management: Resources for National CSIRTs," Software Engineering Institute, [Online]. Available: https://www.cert.org/incident-management/national-csirts/index.cfm. [Accessed 16 May 2017].
[51]	CERT, "List of National CSIRTs," [Online]. Available: https://www.cert.org/incident-management/national-csirts/national-csirts.cfm. [Accessed 23 May 2017].
[52]	BugCrowd, "BugCrowd," [Online]. Available: https://bugcrowd.com/. [Accessed 23 May 2017].
[53]	HackerOne, "HackerOne," [Online]. Available: https://www.hackerone.com. [Accessed 23 May 2017].
[54]	SynAck, "SynAck," [Online]. Available: https://www.synack.com. [Accessed 23 May 2017].
[55]	Cobalt Labs Inc., "Cobalt," [Online]. Available: https://cobalt.io/. [Accessed 23 May 2017].
[56]	CERT, "Vulnerability Analysis," [Online]. Available: https://www.cert.org/vulnerability-analysis/. [Accessed 23 May 2017].
[57]	National Cyber Security Centre Netherlands, "NCSC-NL," [Online]. Available: https://www.ncsc.nl/english. [Accessed 23 May 2017].
[58]	NCSC-FI, "Finnish Communications Regulatory Authority / National Cyber Security Centre Finland," [Online]. Available: https://www.viestintavirasto.fi/en/cybersecurity.html.
[59]	JPCERT/CC, "Japan Computer Emergency Response Team Coordination Center," [Online]. Available: https://www.jpcert.or.jp/english/. [Accessed 16 May 2017].
[60]	U.S. Department of Homeland Security, "Information Sharing and Analysis Organizations (ISAOs)," [Online]. Available: https://www.dhs.gov/isao. [Accessed 23 May 2017].

[61]	National Council of ISACs, "National Council of ISACs," [Online]. Available: https://www.nationalisacs.org/. [Accessed 23 May 2017].
[62]	W. Dormann, "Supporting the Android Ecosystem," 19 October 2015. [Online]. Available: https://insights.sei.cmu.edu/cert/2015/10/supporting-the-android-ecosystem.html. [Accessed 23 May 2017].
[63]	U.S. Food & Drug Administration, "Medical Device Reporting (MDR)," [Online]. Available: https://www.fda.gov/medicaldevices/safety/reportaproblem/. [Accessed 23 May 2017].
[64]	National Highway Traffic Safety Administration, "File a Vehicle Safety Complaint," [Online]. Available: https://www-odi.nhtsa.dot.gov/VehicleComplaint/. [Accessed 23 May 2017].
[65]	Federal Aviation Administration, "Report Safety Issues," [Online]. Available: https://www.faa.gov/aircraft/safety/report/. [Accessed 23 May 2017].
[66]	NASA Office of the Chief Engineer, "NASA Lessons Learned," NASA Lessons Learned Steering Committee (LLSC), [Online]. Available: https://www.nasa.gov/offices/oce/functions/lessons/index.html. [Accessed 16 May 2017].
[67]	European Commission, "Dual Use Controls: Commission proposes to modernise and strengthen controls on exports of dual-use items," 28 September 2016. [Online]. Available: http://europa.eu/rapid/press-release_IP-16-3190_en.htm. [Accessed 23 May 2017].
[68]	FIRST, "Vulnerability Database Catalog," FIRST VRDX SIG, 17 March 2016. [Online]. Available: https://www.first.org/global/sigs/vrdx/vdb-catalog. [Accessed 16 May 2017].
[69]	J. T. Chambers and J. W. Thompson, "National Infrastructure Advisory Council Vulnerability Disclosure Framework Final Report and Recommendations by the Council," 13 January 2004. [Online]. Available: https://www.dhs.gov/xlibrary/assets/vdwgreport.pdf. [Accessed 17 May 2017].
[70]	J. C. Knight, "Safety critical systems: challenges and directions," in *ICSE '02 Proceedings of the 24th International Conference on Software Engineering*, Orlando, 2002.
[71]	U.S. Department of Health & Human Services, "Health Information Privacy," [Online]. Available: https://www.hhs.gov/hipaa/. [Accessed 23 May 2017].
[72]	U.S. Department of Education, "Family Educational Rights and Privacy Act (FERPA)," [Online]. Available: https://ed.gov/policy/gen/guid/fpco/ferpa/index.html. [Accessed 23 May 2017].
[73]	Federal Trade Commission, "Children's Online Privacy Protection Rule ("COPPA")," [Online]. Available: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule. [Accessed 23 May 2017].
[74]	PCI Security Standards Council, "PCI Security," [Online]. Available: https://www.pcisecuritystandards.org/pci_security/. [Accessed 23 May 2017].
[75]	Electronic Frontier Foundation, "Coders' Rights Project Vulnerability Reporting FAQ," [Online]. Available: https://www.eff.org/issues/coders/vulnerability-reporting-faq. [Accessed 17 May 2017].
[76]	K. Price, "Writing a bug report - Attack Scenario and Impact are key!" 2 August 2015. [Online]. Available: https://forum.bugcrowd.com/t/writing-a-bug-report-attack-scenario-and-impact-are-key/640. [Accessed 17 May 2017].
[77]	MITRE, "Common Weakness Enumeration (CWE)," [Online]. Available: https://cwe.mitre.org/. [Accessed 17 May 2017].
[78]	MITRE, "Common Attack Pattern Enumeration and Classification," [Online]. Available: https://capec.mitre.org/. [Accessed 17 May 2017].
[79]	CERT/CC, "Vulnerability Reporting Form," [Online]. Available: https://vulcoord.cert.org/VulReport/. [Accessed 17 May 2017].
[80]	FIRST, "Common Vulnerability Scoring System," [Online]. Available: https://www.first.org/cvss. [Accessed 17 May 2017].

[81]	MITRE, "Common Weakness Scoring System (CWSS) version 1.0.1," 5 September 2014. [Online]. Available: https://cwe.mitre.org/cwss/cwss_v1.0.1.html. [Accessed 17 May 2017].
[82]	Security Focus, "BugTraq Archive," [Online]. Available: http://www.securityfocus.com/archive/1. [Accessed 23 May 2017].
[83]	Seclists.org, "Full Disclosure Mailing List," [Online]. Available: http://seclists.org/fulldisclosure/. [Accessed 23 May 2017].
[84]	MITRE, "Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA) Rules Version 1.1," 16 September 2016. [Online]. Available: https://cve.mitre.org/cve/cna/CNA_Rules_v1.1.pdf. [Accessed 16 May 2017].
[85]	J. Postel, "Internet Protocol (RFC 760)," 1980.
[86]	N. Brownlee and E. Guttman, "Expectations for Computer Security Incident Response," The Internet Society, 1998.
[87]	S. Shepherd, "Vulnerability Disclosure: How Do We Define Responsible Disclosure?" SANS GIAC SEC Practical Repository, 2003.
[88]	FIRST, "Multi-Party Coordination and Disclosure," [Online]. Available: https://www.first.org/global/sigs/vulnerability-coordination/multiparty. [Accessed 6 June 2017].
[89]	Codenomicon, "The Heartbleed Bug," 29 April 2014. [Online]. Available: http://heartbleed.com/. [Accessed 16 May 2017].
[90]	J. P. Lanza, "Vulnerability Note VU#484891 Microsoft SQL Server 2000 contains stack buffer overflow in SQL Server Resolution Service," 26 July 2002. [Online]. Available: https://www.kb.cert.org/vuls/id/484891. [Accessed 23 May 2017].
[91]	W. Dormann, "Vulnerability Note VU#916896 Oracle Outside In 8.5.2 contains multiple stack buffer overflows," 20 January 2016. [Online]. Available: https://www.kb.cert.org/vuls/id/916896. [Accessed 23 May 2017].
[92]	W. Dormann, "Vulnerability Note VU#582497 Multiple Android applications fail to properly validate SSL certificates," CERT/CC, 3 September 2014. [Online]. Available: https://www.kb.cert.org/vuls/id/582497. [Accessed 16 May 2017].
[93]	W. Dormann, "Android apps that fail to validate SSL," 29 August 2014. [Online]. Available: https://docs.google.com/spreadsheets/d/1t5GXwjw82SyunALVJb2w0zi3FoLRIkfGPc7AMjRF0r4. [Accessed 16 May 2017].
[94]	University of Oulu, "PROTOS Test-Suite: c06-snmpv1," 2002. [Online]. Available: https://www.ee.oulu.fi/research/ouspg/PROTOS_Test-Suite_c06-snmpv1. [Accessed 16 May 2017].
[95]	I. A. Finlay, S. V. Hernan, J. A. Rafail, C. Dougherty, A. D. Householder, M. Lindner and A. Manion, "Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)," CERT/CC, 12 February 2002. [Online]. Available: https://www.cert.org/historical/advisories/CA-2002-03.cfm. [Accessed 16 May 2017].
[96]	I. A. Finlay, "Vulnerability Note VU#854306 Multiple vulnerabilities in SNMPv1 request handling," CERT/CC, 12 February 2002. [Online]. Available: https://www.kb.cert.org/vuls/id/854306. [Accessed 16 May 2017].
[97]	I. A. Finlay, "Vulnerability Note VU#107186 Multiple vulnerabilities in SNMPv1 trap handling," CERT/CC, 12 February 2002. [Online]. Available: https://www.kb.cert.org/vuls/id/107186. [Accessed 16 May 2017].
[98]	B. Stock, G. Pellegrino and C. Rossow, "Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification," in *25th USENIX Security Symposium*, 2016.
[99]	R. M. Axelrod, The Evolution of Cooperation, Revised ed., Basic books, 2006.

[100]	D. R. Grimes, "On the Viability of Conspiratorial Beliefs," *PLOS One,* vol. 11, no. 1, p. e0147905, 26 January 2016.
[101]	Black Hat, "Black Hat," [Online]. Available: https://www.blackhat.com/. [Accessed 23 May 2017].
[102]	DEF CON, "DEF CON," [Online]. Available: https://www.defcon.org/. [Accessed 23 May 2017].
[103]	USENIX, "USENIX Security Conferences," [Online]. Available: https://www.usenix.org/conferences/byname/108. [Accessed 23 May 2017].
[104]	RSA, "RSA Conference," [Online]. Available: https://www.rsaconference.com/. [Accessed 23 May 2017].
[105]	CanSecWest, "CanSecWest Vancouver 2018," [Online]. Available: https://cansecwest.com/. [Accessed 23 May 2017].
[106]	Federal Trade Commission, "ASUSTeK Computer Inc., In the Matter of," 28 July 2016. [Online]. Available: https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter. [Accessed 16 May 2017].
[107]	Federal Trade Commission, "HTC America Inc., In the Matter of," 2 July 2013. [Online]. Available: https://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter. [Accessed 16 May 2017].
[108]	Federal Trade Commission, "Fandango, LLC," 19 August 2014. [Online]. Available: https://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc. [Accessed 16 May 2017].
[109]	A. Askar, "Minecraft Vulnerability Advisory," 16 April 2015. [Online]. Available: http://blog.ammaraskar.com/minecraft-vulnerability-advisory/. [Accessed 23 May 2017].
[110]	A. Ozment, "The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting," in *Workshop on Economics and Information Security*, 2005.
[111]	M. Finifter, D. Akhawe and D. Wagner, "An Empirical Study of Vulnerability Rewards Programs," in *22nd USENIX Security Symposium*, 2013.
[112]	L. Ablon and T. Bogart, "Zero Days, Thousands of Nights," RAND Corporation, 2017.
[113]	T. Herr and B. Schneier, "Taking Stock: Estimating Vulnerability Rediscovery," 7 March 2017. [Online]. Available: https://ssrn.com/abstract=2928758. [Accessed 16 May 2017].
[114]	B. Grubb, "Heartbleed disclosure timeline: who knew what and when," The Sydney Morning Herald, 15 April 2014. [Online]. Available: http://www.smh.com.au/it-pro/security-it/heartbleed-disclosure-timeline-who-knew-what-and-when-20140414-zqurk.html. [Accessed 23 May 2017].
[115]	SerNet, "Badlock Bug," 12 April 2016. [Online]. Available: http://www.badlock.org/. [Accessed 23 May 2017].

[116]	N. Perlroth, "Security Experts Expect 'Shellshock' Software Bug in Bash to Be Significant," 25 September 2014. [Online]. Available: https://www.nytimes.com/2014/09/26/technology/security-experts-expect-shellshock-software-bug-to-be-significant.html. [Accessed 23 May 2017].
[117]	A. Sarwate, "The GHOST Vulnerability," 27 January 2015. [Online]. Available: https://blog.qualys.com/laws-of-vulnerabilities/2015/01/27/the-ghost-vulnerability. [Accessed 23 May 2017].
[118]	A. Watts, C. Huang and L. Chih-chang. Tao: The Watercourse Way, Pantheon, 1975.
[119]	M. Masnick, "For 10 Years Everyone's Been Using 'The Streisand Effect' Without Paying; Now I'm Going To Start Issuing Takedowns," 8 January 2015. [Online]. Available: https://www.techdirt.com/articles/20150107/13292829624/10-years-everyones-been-using-streisand-effect-without-paying-now-im-going-to-start-issuing-takedowns.shtml. [Accessed 23 May 2017].
[120]	R. Devendra, "Key Elements of the Sprint Retrospective," 24 April 2014. [Online]. Available: https://www.scrumalliance.org/community/articles/2014/april/key-elements-of-sprint-retrospective. [Accessed 23 May 2017].
[121]	CERT/CC, "Sending Sensitive Information," [Online]. Available: https://www.cert.org/contact/sensitive-information.cfm. [Accessed 24 May 2017].
[122]	Symantec, "Symantec Desktop Email Encryption," [Online]. Available: https://www.symantec.com/products/information-protection/encryption/desktop-email-encryption. [Accessed 24 May 2017].
[123]	The GnuPG Project, "GNU Privacy Guard," [Online]. Available: https://gnupg.org/. [Accessed 24 May 2017].
[124]	B. Ramsdell and S. Turner, "RFC 5751 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification," January 2010. [Online]. Available: https://tools.ietf.org/html/rfc5751. [Accessed 24 May 2017].
[125]	Internet Security Research Group (ISRG), "Let's Encrypt," [Online]. Available: https://letsencrypt.org/. [Accessed 16 May 2017].
[126]	The Enigmail Project, "Enigmail," [Online]. Available: https://www.enigmail.net/index.php/en/. [Accessed 24 May 2017].
[127]	Gpg4win Initiative, "GNU Privacy Guard for Windows," [Online]. Available: https://www.gpg4win.org/. [Accessed 24 May 2017].
[128]	"KGpg," [Online]. Available: https://utils.kde.org/projects/kgpg/. [Accessed 24 May 2017].
[129]	G. Wassermann, "Reach Out and Mail Someone," 6 August 2015. [Online]. Available: https://insights.sei.cmu.edu/cert/2015/08/reach-out-and-mail-someone.html. [Accessed 24 May 2017].
[130]	"White Source Software," [Online]. Available: https://www.whitesourcesoftware.com/. [Accessed 24 May 2017].
[131]	"Black Duck Software," [Online]. Available: https://www.blackducksoftware.com. [Accessed 24 May 2017].

[132]	"Sonatype," [Online]. Available: https://www.sonatype.com/. [Accessed 24 May 2017].
[133]	"Synopsis," [Online]. Available: https://www.synopsys.com/. [Accessed 24 May 2017].
[134]	"Flexera Software," [Online]. Available: https://www.flexerasoftware.com/. [Accessed 24 May 2017].
[135]	TagVault.org, "SWID Tags," [Online]. Available: http://tagvault.org/swid-tags/. [Accessed 16 May 2017].
[136]	National Institute of Standards and Technology, "Common Platform Enumeration (CPE)," [Online]. Available: https://scap.nist.gov/specifications/cpe/ [Accessed 16 May 2017].
[137]	SPDX Workgroup, "Software Package Data Exchange," [Online]. Available: https://spdx.org/ . [Accessed 16 May 2017].
[138]	CERT, "Dranzer," [Online]. Available: https://vuls.cert.org/confluence/display/tools/Dranzer. [Accessed 24 May 2017].
[139]	CERT, "BFF - Basic Fuzzing Framework," [Online]. Available: https://vuls.cert.org/confluence/display/tools/CERT+BFF+-+Basic+Fuzzing+Framework. [Accessed 24 May 2017].
[140]	FIRST, "TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 1.0," [Online]. Available: https://www.first.org/tlp. [Accessed 16 May 2017].
[141]	B. Rothke, "Building a Security Operations Center (SOC)," 29 Feb 2012. [Online]. Available: https://www.rsaconference.com/events/us12/agenda/sessions/683/building-a-security-operations-center-soc. [Accessed 24 May 2017].
[142]	S. Ragan, "Avoiding burnout: Ten tips for hackers working incident response," 30 April 2014. [Online]. Available: http://www.csoonline.com/article/2149900/infosec-careers/avoiding-burnout-ten-tips-for-hackers-working-incident-response.html. [Accessed 24 May 2017].
[143]	S. C. Sundaramurthy, A. G. Bardas, J. Case, X. Ou, M. Wesch, J. McHugh and S. R. Rajagopalan, "A human capital model for mitigating security analyst burnout," in *Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, July 2015.
[144]	A. Householder, "Vulnerability IDs, Fast and Slow," 11 March 2016. [Online]. Available: https://insights.sei.cmu.edu/cert/2016/03/vulnerability-ids-fast-and-slow.html. [Accessed 7 June 2017].
[145]	N. Mercer, "Further simplifying servicing models for Windows 7 and Windows 8.1," 15 August 2016. [Online]. Available: https://blogs.technet.microsoft.com/windowsitpro/2016/08/15/further-simplifying-servicing-model-for-windows-7-and-windows-8-1/. [Accessed 24 May 2017].
[146]	FIRST, "Vulnerability Reporting and Data eXchange SIG (VRDX-SIG)," [Online]. Available: https://www.first.org/global/sigs/vrdx. [Accessed 16 May 2017].
[147]	D. Klinedinst, "Coordinating Vulnerabilities in IoT Devices," 27 January 2016. [Online]. Available: https://insights.sei.cmu.edu/cert/2016/01/coordinating-vulnerabilities-in-iot-devices.html. [Accessed 16 May 2017].

[148]	S. Christey Coley and B. Martin, "Buying Into the Bias: Why Vulnerability Statistics Suck," in *BlackHat*, 2013.
[149]	MITRE, "CVE Abstraction Content Decisions: Rationale and Application," 15 June 2005. [Online]. Available: https://cve.mitre.org/cve/editorial_policies/cd_abstraction.html. [Accessed 24 May 2017].
[150]	National Institute of Standards and Technology, "National Vulnerability Database," [Online]. Available: https://nvd.nist.gov/. [Accessed 16 May 2017].
[151]	CNNVD, "China National Vulnerability Database of Information Security," [Online]. Available: http://www.cnnvd.org.cn/. [Accessed 16 May 2017].
[152]	CNVD, "China National Vulnerability Database," [Online]. Available: http://www.cnvd.org.cn/. [Accessed 16 May 2017].
[153]	D. Kahneman, Thinking, Fast and Slow, Macmillan, 2011.
[154]	V. Driessen, "A successful Git branching model," 5 January 2010. [Online]. Available: http://nvie.com/posts/a-successful-git-branching-model/. [Accessed 16 May 2017].
[155]	H. Booth and K. Scarfone, "Vulnerability Data Model draft-booth-sacm-vuln-model-02," 25 April 2013. [Online]. Available: https://tools.ietf.org/html/draft-booth-sacm-vuln-model-02. [Accessed 16 May 2107].
[156]	A. Householder, "Vulnerability Discovery for Emerging Networked Systems," 20 November 2014. [Online]. Available: https://insights.sei.cmu.edu/cert/2014/11/-vulnerability-discovery-for-emerging-networked-systems.html. [Accessed 16 May 2017].
[157]	D. Geer, "Security of Things," 14 May 2014. [Online]. Available: http://geer.tinho.net/geer.secot.7v14.txt. [Accessed 16 May 2017].
[158]	S. Arbesman, Overcomplicated: Technology at the Limits of Comprehension, Current, 2016.
[159]	A. Householder, "What's Different About Vulnerability Analysis and Discovery in Emerging Networked Systems?" 6 January 2015. [Online]. Available: https://insights.sei.cmu.edu/cert/2015/01/-whats-different-about-vulnerability-analysis-and-discovery-in-emerging-networked-systems.html. [Accessed 16 May 2017].
[160]	JPCERT/CC and IPA, "Japan Vulnerability Notes," [Online]. Available: https://jvn.jp/en/. [Accessed 16 May 2017].
[161]	O. H. Alhazmi, Y. K. Malaiya and I. Ray, "Measuring, analyzing and predicting security vulnerabilities in software systems," *Computers & Security,* vol. 26, no. 3, pp. 219-228, 2007.
[162]	Wikipedia, "Wicked problem," [Online]. Available: https://en.wikipedia.org/wiki/Wicked_problem. [Accessed 5 June 2017].