References

REFERENCES

[1]. Baloh, P., & Trkman, P. (2003*). Influence of internet and information technology on work and human resource management.* Informing Science, 6, 497-499.

[2]. The Internet and business performance, retrieved 16:06, August 11, 2013, URL http://www.oecd.org/sti/business-forums.

[3]. Impacts of IT on Individuals, Organizations, and Society, April 19 2005, http://higheredbcs.wiley.com/legacy/college/turban/0471787124/ch17/ch17.pdf

[4]. Lipson, H. F. (2002). *Tracking and tracing cyber-attacks: Technical challenges and global policy issues* (No. CMU/SEI-2002-SR-009). Carnegie-mellon univ pittsburgh pa software engineering inst.

[5]. Eichin, M. W., & Rochlis, J. A. (1989, May). *With microscope and tweezers: An analysis of the internet virus of November 1988*. In Security and Privacy, 1989. Proceedings, 1989 IEEE Symposium on (pp. 326-343). IEEE.

[6]. Internet. (2013, June 21). In *Wikipedia, The Free Encyclopaedia*. Retrieved 13:15, December 3, 2013, *URL http://en.wikipedia.org/w/index.php?title=Internet&oldid=595060701*.

[7]. Fang, Z. (2002). *E-government in digital era: concept, practice, and development.* International journal of the Computer, the Internet and management, 10(2), 1-22.

[8]. UNCTAD (2011). *Measuring the Impacts of Information and Communication Technology for Development.* Current Studies on Science, Technology and Innovation. Nº 3. Geneva: UNCTAD. Retrieved May 03, 2011 URL http://www.unctad.org/en/docs/dtlstict2011d1_en.pdf.

[9]. Melville, N., Kraemer, K., & Gurbaxani, V. (2004). *Review: Information technology and organizational performance: An integrative model of IT business value.* MIS quarterly, *28(2), 283-322.*

[10]. Brynjolfsson, E., & Hitt, L. M. (2000). *Beyond computation: Information technology, organizational transformation and business performance.* The Journal of Economic Perspectives, 23-48.

[11]. Alshboul, A. (2010). *Information Systems Security Measures and Countermeasures: Protecting Organizational Assets from Malicious Attacks.* Communications of the IBIMA.

[12]. Sanou, B. (2013). *The World in 2013: ICT Facts and Figures*. International Telecommunications Union.

[13]. GAO. (2013). *CYBERSECURITY: National Strategy, Roles, and Responsibilities need to be Better Defined and More Effectively Implemented.* United States Government Accountability Office.

[14]. Centre, C. C. (2003). *CERT/CC Statistics 1988-2003*. Retrieved 10:03, December 28, 2014,URL http://www.cert.org/stats.

[15]. Kern, C., Kesavan, A., & Daswani, N. (2007). *Foundations of security: what every programmer needs to know*. Apress.

[16]. Stuxnet. (2013). In Wikipedia, the Free Encyclopaedia. Retrieved 14:56, August 18, 2013, URL http://en.wikipedia.org/wiki/Stuxnet.

[17]. Mölsä, J. (2005). *Mitigating denial of service attacks: A tutorial.* Journal of computer security, 13(6), 807-837.

[18]. Zargar, S. T., Joshi, J., & Tipper, D. (2013). *A survey of Defense mechanisms against distributed denial of service (DDoS) flooding attacks*. Communications Surveys & Tutorials, IEEE, 15(4), 2046-2069.

[19]. Douligeris, C., & Mitrokotsa, A. (2004). *DDoS attacks and Defense mechanisms: classification and state-of-the-art.* Computer Networks, 44(5), 643-666.

[20]. J. Mirkovic et al., (2005) *Internet Denial of Service: Attack and Defense Mechanisms*, Prentice Hall.

[21]. Intel Security (Mcafee). (2014). Industry Experts Speak Out: The Network Performance and Security Trade-Off. Retrieved February 9,2015, URL http://www.mcafee.com/in/resources/reports/rp-whats-next-network-performance-security-trade-off.pdf

[22]. Garber, L. (2000). *Denial-of-service attacks rip the Internet*. Computer, 33(4), 12-17.

[23]. Anstee, D., Escobar, J., Chui, C.F., Sockrider, G. (2015, January 27). *10th Annual Worldwide Infrastructure Security Report.* Arbor Networks Inc.

[24]. 19,000 French websites hit by DDoS. (2015, January 13). Retrieved from http://www.net-security.org/secworld.php?id=17832

[25]. Vijay. (2015, January 11). Extra torrent is under the DDoS attack by hackers right now. Retrieved from http://www.techworm.net/2015/01/extratorrent-down-hackers-launch-ddos-attack.html

[26]. Eden, A. (2014, December 2). Incident Report - DDoS Attack. Retrieved from http://blog.dnsimple.com/2014/12/incident-report-ddos/

[27]. Colon, M. (2014, December 2). Lizard Squad takes credit for DDoS attack on Xbox Live. Retrieved from http://www.scmagazine.com/lizard-squad-takes-credit-for-ddos-attack-on-xbox-live/article/386123

[28]. Tung, L. (2014, December 8). Sony PlayStation back online after attackers claim credit for outage. Retrieved from http://www.zdnet.com/article/sony-playstation-back-online-after-attackers-claim-credit-for-outage

[29]. Tung, L. (2014, December 11). DDoS of unprecedented scale 'stops Sweden working'. The target? A gaming site. Retrieved from http://www.zdnet.com/article/ddos-of-unprecedented-scale-stops-sweden-working-the-target-a-gaming-site/

[30]. Sweden's Telia attack linked to Pirate Bay. (2014, December 12). Retrieved from http://www.thelocal.se/20141212/telia-hit-again-in-new-hacking-attack

[31]. Bogart, N. (2014, November 25). Hacker claiming ties to Anonymous targets Toronto, Ottawa Police with DDoS attack. Retrieved from http://globalnews.ca/news/1689115/hacker-claiming-ties-to-anonymous-targets-toronto-ottawa-police-with-ddos-attack/

[32]. Anonymous alongside victims against police violence that has struck again. (2014, November 22). Retrieved from http://anon-news.blogspot.in/2014/11/anonymouspoliziapenitenziaria.html

[33]. Elise, A. (2014, November 24). EA's Online Service Allegedly Brought Down By Hacker Group Lizard Squad. Retrieved from http://www.ibtimes.com/eas-online-service-allegedly-brought-down-hacker-group-lizard-squad-1728726

[34]. Waqas. (2014, October 26). Anonymous Shuts Down Top Israeli Govt Sites Against Killing Of 14-Yr-Old Kid. Retrieved from http://www.hackread.com/anonymous-hackers-orwah-hammad-israel-idf/

[35]. "Anonymous Pakistan" takes down government sites, leak bank records. (2014, September 1). Retrieved from http://www.dawn.com/news/1129212

[36]. LLascu, L. (2014, Aug 25). Key Israeli Websites Hacked by Anonymous. Retrieved from http://news.softpedia.com/news/Key-Israeli-Websites-Hacked-By-Anonymous-456302.shtml

[37]. Waqas. (2014, August 2). Anonymous hackers take down Mossad website against Gaza attacks. Retrieved from http://www.hackread.com/anonymous-hackers-mossad-website/

[38]. Parnell, B.A. (2014, Jun 11). Evernote taken out by DDoS attack. Retrieved from http://www.theregister.co.uk/2014/06/11/evernote_dos_attack/

[39]. Leyden, J. (2014, May 9). Point DNS blitzed by mystery DDoS assault. Retrieved from http://www.theregister.co.uk/2014/05/09/point_dns_ddos/

[40]. Vatu, G. (2014, Mar 21). GitHub Falls Victim of Another DDOS Attack. Retrieved from http://news.softpedia.com/news/GitHub-Falls-Victim-of-Another-DDOS-Attack-433465.shtml

[41]. Kovacs, E. (2014, Mar 14). GitHub Provides Details on DDOS Attack That Made Services Unreachable for 2 Hours. Retrieved from http://news.softpedia.com/news/GitHub-Provides-Details-on-DDOS-Attack-That-Made-Services-Unreachable-for-2-Hours-432245.shtml

[42]. Gallagher, S. (2014, Feb 11). Biggest DDoS ever aimed at Cloudflare's content delivery network. Retrieved from http://arstechnica.com/security/2014/02/biggest-ddos-ever-aimed-at-cloudflares-content-delivery-network/

[43]. Flitter, E., Miedema, D. (2014, Feb 11). Bitcoin hit by denial of service attacks as regulators prepare clampdown. Retrieved from http://www.reuters.com/article/2014/02/12/us-usa-bitcoin-idUSBREA1A20X20140212

[44]. Gaming sites and servers. (2013, Dec 30). Retrieved from http://in.ign.com/news/56090/hacker-group-derp-takes-down-multiple-online-gamin

[45]. Greenberg, A. (2013, Nov 18). Battlefield 4 PC servers experience DDoS attack. Retrieved from http://www.scmagazine.com/battlefield-4-pc-servers-experience-ddos-attack/article/321506/

[46]. Greenberg, A. (2013, Nov 27). Anonymous DDoS attack snowballs, affects several Microsoft services. Retrieved from http://www.scmagazine.com/anonymous-ddos-attack-snowballs-affects-several-microsoft-services/article/322945/

[47]. Network solutions and important DNS registrar is hit by a DDoS attack. (2013, Jun 19). Retrieved from https://www.networksolutions.com/blog/2013/06/important-update-for-network-solutions-customers-experiencing-website-issues/

[48]. Passeri, P. (2013, July 1). 1-15 June 2013 Cyber Attacks Timeline. 48 Retrieved from http://hackmageddon.com/2013/07/01/1-15-june-2013-cyber-attacks-timeline/

[49]. Passeri, P. (2013, June 3). 15-31 May 2013 Cyber Attacks Timeline. Retrieved from http://hackmageddon.com/2013/06/03/15-31-may-2013-cyber-attacks-timeline/

[50]. Passeri, P. (2013, May 5). 16-30 April 2013 Cyber Attacks Timeline. Retrieved from http://hackmageddon.com/2013/05/05/16-30-april-2013-cyber-attacks-timeline/

[51]. Passeri, P. (2013, May 1). 1-15 April 2013 Cyber Attacks Timeline. Retrieved from http://hackmageddon.com/2013/05/01/1-15-april-2013-cyber-attacks-timeline/

[52]. Kovacs, E. (2013, Apr 24). VideoLAN's Downloads Section Hit by DDOS Attack. Retrieved from http://news.softpedia.com/news/VideoLAN-s-Downloads-Section-Hit-by-DDOS-Attack-4-24-2013-348040.shtml

[53]. Passeri, P. (2012, Nov 2). October 2012 Cyber Attacks Timeline. Retrieved from http://hackmageddon.com/2012/11/02/october-2012-cyber-attacks-timeline/

[54]. Sites of Attorney General of Australia. (2012, Sept 22). Retrieved from http://www.cyberwarnews.info/2012/09/22/australian-attorney-general-websites-attacked-for-opfreeassange/

[55]. Kumar, M. (2012, May 20). Anonymous hater takes credit for Pirate Bay and Wikileaks DDos Attack. Retrieved from http://thehackernews.com/2012/05/anonymous-hater-takes-credit-for-pirate.html

[56]. Passeri, P. (2012, May 3). April 2012 Cyber Attacks Timeline (Part II). Retrieved from http://hackmageddon.com/2012/05/03/april-cyber-attacks-timeline-part-ii/

[57]. Sherwood, H. (2011, November 1). Palestinians hit by cyber-attack following success at Unesco. Retrieved from http://www.guardian.co.uk/world/2011/nov/01/palestinians-hit-cyber-attack-unesco

[58]. Passeri, P. (2011, Aug 2). July 2011 Cyber Attacks Timeline. Retrieved from http://hackmageddon.com/2011/08/02/july-2011-cyber-attacks-timeline/

[59]. Passeri, P. (2011, June 28). 2011 Cyber Attacks (and Cyber Costs) Timeline (Updated). Retrieved from http://hackmageddon.com/2011/06/28/2011-cyber-attacks-and-cyber-costs-timeline-updated/

[60]. Arora, K., Kumar, K., & Sachdeva, M. (2011). *Impact analysis of recent DDoS attacks*. International Journal on Computer Science and Engineering, *3*(2), 877-883.

[61]. Hapeman, E. R., Zeuch, W. R., Crandall, J. A., Carioti, S. M., Barclay, S. D., & Underkoffler, C. (2001). *Telecom Glossary 2000*–American National Standard T1. 523-2001.

[62]. Gollmann, D. (2011). *Computer security*. 3rd edition, John Wiley & Sons,

[63]. Schneier, B. (2011). *Secrets and lies: digital security in a networked world*. John Wiley & Sons.

[64]. Mölsä, J. (2006). *Mitigating denial of service attacks in computer networks*. Helsinki University of Technology.

[65]. Matthew A. Bishop. (2002). *the Art and Science of Computer Security*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA.

[66]. Whitman, M., & Mattord, H. (2011). *Principles of information security*. Cengage Learning.

[67]. United States National Computer Security Center . (1987, 31 July). *Trusted Network Interpretation of the TCSEC ("The Red Book")*. US Department of Defence, NCSC-TG-005, Library No. S228,526, Version 1. retrieved on 10.05.2012 from http://csrc.nist.gov/publications/secpubs/rainbow/tg005.txt

[68]. White, G. B., Fisch, E. A., & Pooch, U. W. (1995*). Computer system and network security* (Vol. 7). CRC press.

[69]. Pesante, L. (2008). *Introduction to information security*. Carnegie Mellon University. Retrieved March, 10, 2013.

[70]. Avizienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). *Basic concepts and taxonomy of dependable and secure computing.* Dependable and Secure Computing, IEEE Transactions on, 1(1), 11-33.

[71]. CERT Coordination Center. (Oct. 1997). *Denial of service attacks*, [Online]. Available: http://www.cert.org/tech tips/denial of service.html, [accessed Jan. 20, 2012].

[72]. D. Plonka. (Aug. 2003). *Flawed routers flood University of Wisconsin Internet time server,* University of Wisconsin, Tech. Rep. [Online]. Available: http://www.cs.wisc.edu/˜plonka/netgear-sntp/, [accessed Jun. 19, 2012].

[73]. Moore, D., Shannon, C., Brown, D. J., Voelker, G. M., & Savage, S. (2006). *Inferring internet denial-of-service activity*. ACM Transactions on Computer Systems (TOCS), 24(2), 115-139.

[74]. Highland, H. J. (1988). *The BRAIN virus: fact and fantasy*. Computers & Security, 7(4), 367-370.

[75]. Parker, D. B. (1991). *Restating the foundation of information security*. Computer Audit Update, 1991(10), 2-15.

[76]. Khazanchi, D., & Martin, A. P. (2008). *Information Availability*. Handbook of Research on Information Security and Assurance, IGI Global.

[77]. Mitnick, K., Simon, W. (2002). *The Art of Deception: Controlling the Human Element of Security.* John Wiley and Sons.

[78]. Mirkovic, J., & Reiher, P. (2004). *A Taxonomy of DDoS attack and DDoS defense mechanisms.* ACM SIGCOMM Computer Communication Review, 34(2), 39-53.

[79]. Guttman, B., & Roback, E. (1995). *An introduction to computer security: the NIST handbook*. DIANE Publishing.

[80]. Whitman, M. E. (2003). *Enemy at the gate: threats to information security.* Communications of the ACM, 46(8), 91-95.

[81]. Hosmer, H. H. (1996, September). *Availability policies in an adversarial environment*. In Proceedings of the 1996 workshop on new security paradigms (pp. 105-117). ACM.

[82]. Information Security. (Oct, 31 2001). Wikipedia, the free encyclopaedia. Retrieved Feb 2012, from: http://en.wikipedia.org/wiki/Information_security

[83]. Andress, J. (2014). *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. Syngress.

[84]. Chivers, H. (2004*). Security and systems engineering*. Report-university of York department of computer science ycs.

[85]. Latham, D. C. (1986, Dec). *Department of Defense trusted computer system evaluation criteria*. Department of Defense.

[86]. DARPA. (2008, Nov). Wikipedia, the Free Encyclopaedia. Retrieved, Dec, 2013, URL http://en.wikipedia.org/wiki/DARPA

[87]. Gligor, V. D. (1986, February). *On denial-of-service in computer networks*. In Proceedings of the Second International Conference on Data Engineering (pp. 608-617). IEEE Computer Society.

[88]. *Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonized Criteria.* (1991). Luxembourg: Office for Official Publications of the European Communities, 1991 ISBN 92-826-3004-8, Catalogue number: CD-71-91-502-EN-C © ECSC-EEC-EAEC, Brussels • Luxembourg.

[89]. *National Information Systems Security (InfoSec) Glossary*. (2000, Sept). National Security Telecommunications and Information Systems Security Committee. National Security Agency US.

[90]. Pfleeger, C. P. (1997). *Security in Computing.* Second edition, Prentice-Hall 0-13-185794.

[91]. Millen, J. K. (1995). *Denial of service: A perspective In Dependable Computing for Critical Applications 4* (pp. 93-108). Springer Vienna.

[92]. *Trusted Network Interpretation of the TCSEC ("The Red Book")*. (1987, July). US Department of Defence, NCSC-TG-005. retrieved on 10.05.2012 from http://csrc.nist.gov/publications/secpubs/rainbow/tg005.txt

[93]. Needham, R. M. (1994). *Denial of service: an example*. Communications of the ACM, 37(11), 42-46.

[94]. Jonsson, E. (1998, January). *An integrated framework for security and dependability.* In Proceedings of the 1998 workshop on new security paradigms (pp. 22-29). ACM.

[95]. Jon Haugsand. (2004, April) *.A model of information availability*.

[96]. Vargas, E., & BluePrints, S. (2000). *High availability fundamentals*. Sun Blueprints series.

[97]. Engelmann, C., Scott, S. L., Leangsuksun, C. B., & He, X. B. (2006). *Symmetric active/active high availability for high-performance computing system services.* Journal of Computers, 1(8), 43-54.

[98]. Sarkar, S. (2013). *Modeling and Measurement of Availability of IT Assets in Enterprise Information System* (Doctoral dissertation, Jadavpur University Kolkata).

[99]. Tryfonas, T., Gritzalis, D., & Kokolakis, S. (2000). *A qualitative approach to information availability.* In *Information Security for Global Information Infrastructures* (pp. 37-47). Springer US.

[100]. Engelmann, C., Scott, S. L., Leangsuksun, C. B., & He, X. B. (2006). *Symmetric active/active high availability for high-performance computing system services.* JCP.

[101]. Resnick, R. I. (1996). *A modern taxonomy of high availability,* Technical report, Interlog.

[102]. Wood, A. (1995). *Predicting client/server availability*. Computer, 28(4), 41-48, DOI: 10.1109/2.375176, ISSN: 0018-9162.

[103]. Marcus, E., & Stern, H. (2003). *Blueprints for high availability*. John Wiley & Sons.

[104]. Siponen, M. T., & Oinas-Kukkonen, H. (2007). *A review of information security issues and respective research contributions*. ACM Sigmis Database, 38(1), 60-80.

[105]. Sandhu, R. S., & Samarati, P. (1994). *Access control: principle and practice.* Communications Magazine, IEEE, 32(9), 40-48.

[106]. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). *Role-based access control models.* Computer, 29(2), 38-47.

[107]. Lampson, B. W. (1974). *Protection*. ACM SIGOPS Operating Systems Review, 8(1), 18-24.

[108]. Brown, A., Johnston, S., & Kelly, K. (2002). *Using service-oriented architecture and component-based development to build web service applications.* Rational Software Corporation, 6.

[109]. Grechanik, M., Perry, D. E., & Batory, D. (2006, February). A security mechanism for component-based systems. In *Commercial-off-the-Shelf (COTS)-Based Software Systems, 2006.* Fifth International Conference on(pp. 10-pp). IEEE.

[110]. Sockstress. (2014, January 26). In Wikipedia, The Free Encyclopaedia. Retrieved 13:58, February 14, 2016, from https://en.wikipedia.org/w/index.php?title=Sockstress&oldid=592455393

[111]. Avizienis, A., Laprie, J. C., & Randell, B. (2012). *Fundamental concepts of dependability.Computers & Operations Research*, Elsevier.

[112]. Li, B. (2003, September). *Managing dependencies in component-based systems based on matrix model.* In Proc. Of Net. Object. Days (Vol. 2003, pp. 22-25).

[113]. Rosen, K. H., (2007). *Discrete mathematics and its applications* (Vol. 6). ACM,10 , 12.

[114]. D. P. Gilliam, T. L. Wolfe, J. S. Sherif, and M. Bishop. ―*Software security checklist for the software life cycle*. In Proceedings of the Twelfth IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'03), 2003.

[115]. Deswarte, Y., & Powell, D. (2006). *Internet security: an intrusion-tolerance approach.* Proceedings of the IEEE, 94(2), 432-441.

[116]. Verissimo, P., Correia, M., Neves, N. F., & Sousa, P. (2009). *Intrusion-resilient middleware design and validation*. Information Assurance, Security and Privacy Services, 4, 615-678.

[117]. Raj, S. B. E., & Varghese, G. (2011, March). *Analysis of intrusion-tolerant architectures for Web Servers.* In Emerging Trends in Electrical and Computer Technology (ICETECT), 2011 International Conference on (pp. 998-1003). IEEE.

[118]. Wen-ling, P., Li-Na, W., Huan-guo, Z., & Wei, C. (2005). *Building intrusion tolerant software system.* Wuhan University Journal of Natural Sciences, 10(1), 47-50.

[119]. Wylie, J. J., Bigrigg, M. W., Strunk, J. D., Ganger, G. R., Kiliccote, H., & Khosla, P. K. (2000). *Survivable information storage systems*. Computer, 33(8), 61-68.

[120]. W. Jansen, *Directions in security metrics research*‖, U.S. National Institute of Standards and Technology, NISTIR 7564, Apr. 2009.

[121]. Neto, A. A., & Vieira, M. (2009, October). *Untrustworthiness: A trust-based security metric.* In Risks and Security of Internet and Systems (CRiSIS), 2009 Fourth International Conference on (pp. 123-126). IEEE.

[122]. Cheng, Y., Deng, J., Li, J., DeLoach, S. A., Singhal, A., & Ou, X. (2014). *Metrics of Security.* In Cyber Defense and Situational Awareness (pp. 263-295). Springer International Publishing.

[123]. Qadir, S. and Quadri, S.M.K. (2016) *Information Availability: An Insight into the Most Important Attribute of Information Security*. Journal of Information Security, 7, 185-194. http://dx.doi.org/10.4236/jis.2016.73014.

[124]. Laprie, J. C. (1995, June). *Dependable computing: Concepts, limits, challenges*. In Special Issue of the 25th International Symposium On Fault-Tolerant Computing (pp. 42-54).

[125]. Mir, I. A., & Quadri, S. M. K. (2012). Analysis and evaluating security of component-based software development: A security metrics framework. International Journal of Computer Network and Information Security, 4(11), 21.

[126]. García, C. (2016). *Reputation management of an Open Source Software system based on the trustworthiness of its contributions*.

[127]. Blom, M. (2006). *Empirical Evaluations of Semantic Aspects in Software Development.*

[128]. Bugnion, E., Devine, S., Rosenblum, M., Sugerman, J., & Wang, E. Y. (2012). *Bringing virtualization to the x86 architecture with the original vmware workstation*. ACM Transactions on Computer Systems (TOCS), 30(4), 12.

[129]. Lyon, G. F. (2009). *Nmap network scanning: The official Nmap project guide to network discovery and security scanning*. Insecure.

[130]. Mirkovic, J., Fahmy, S., Reiher, P., Thomas, R., Hussain, A., Schwab, S., & Ko, C. (2006, June). *Measuring impact of DoS attacks.* In Proceedings of the DETER community workshop on cyber security experimentation.

[131]. Siege (software). (2016, May 26). In Wikipedia, the Free Encyclopaedia. Retrieved 09:26, February 20, 2017, from https://en.wikipedia.org/w/index.php?title=Siege_(software)&oldid=722155219

[132]. Botnet. (2017, February 23). In Wikipedia, the Free Encyclopaedia. Retrieved 18:07, February 27, 2017, from https://en.wikipedia.org/w/index.php?title=Botnet&oldid=766992978

[133]. Command and control (malware). (2017, January 14). In Wikipedia, the Free Encyclopaedia. Retrieved 18:08, February 27, 2017, from https://en.wikipedia.org/w/index.php?title=Command_and_control_(malware)&oldid=759947676

[134]. Dark web. (2017, February 26). In Wikipedia, The Free Encyclopedia. Retrieved 17:39, February 28, 2017, from https://en.wikipedia.org/w/index.php?title=Dark_web&oldid=767565229

[135]. Ianelli, N., & Hackworth, A. (2005). *Botnets as a vehicle for online crime.* Forensic Computer Science ijofcs, 19.

[136]. MessageLabs, (2006) "*2005 annual security report*," MessageLabs Ltd., Tech. Rep.

[137]. Rautiainen, Sami; et al. (September 2002). "*F-Secure Virus Descriptions: Slappe*r". Retrieved 2016-03-08.

[138]. Mirkovic, J., & Reiher, P. (2005). *D-WARD: a source-end defense against flooding denial-of-service attacks.* IEEE transactions on Dependable and Secure Computing, 2(3), 216-232.

[139]. Ramanauskaite, S., & Cenys, A. (2011). *Taxonomy of DoS attacks and their countermeasures*. Open Computer Science, 1(3), 355-366.

[140]. Akamai. "*Internet of Things and the Rise of 300 Gbps DDoS Attacks*", Threat Advisory, *Akamai FASTER FORDWARD* (2017).

[141]. Rudman, L., & Irwin, B. (2015, August). *Characterization and analysis of NTP amplification based DDoS attacks.* In Information Security for South Africa (ISSA), 2015 (pp. 1-5). IEEE.

[142]. Czyz, J., Kallitsis, M., Gharaibeh, M., Papadopoulos, C., Bailey, M., & Karir, M. (2014, November). *Taming the 800 pound gorilla: The rise and decline of NTP DDoS attacks.* In Proceedings of the 2014 Conference on Internet Measurement Conference (pp. 435-448). ACM.

[143]. Rossow, C. (2014, February). *Amplification Hell: Revisiting Network Protocols for DDoS Abuse*. In NDSS.

[144]. Akamai. "Akamai's [state of the internet] / security", Reports, *Akamai FASTER FORDWARD* (2002-2017).

[145]. Connolly, P. J. (2001). *Security protects bottom line. InfoWorld*, Vol. 23, No. 15, p. 47.

[146]. Eddy, W. M. (2007). *TCP SYN flooding attacks and common mitigations*.

[147]. Killalea, T., "*Recommended Internet Service Provider Security Services and Procedures*", BCP 46, RFC 3013, November 2000.

[148]. Ferguson, P. and D. Senie, "*Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing*", BCP 38, RFC 2827, May 2000.

[149]. Baker, F. and P. Savola, "*Ingress Filtering for Multihomed Networks*", BCP 84, RFC 3704, March 2004.

[150]. Peng, T., Leckie, C., & Ramamohanarao, K. (2003, May). *Protection from distributed denial of service attacks using history-based IP filtering.* In

Communications, 2003. ICC'03. IEEE International Conference on (Vol. 1, pp. 482-486). IEEE.

[151]. Park, K., & Lee, H. (2001, August). *On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets*. In ACM SIGCOMM computer communication review (Vol. 31, No. 4, pp. 15-26). ACM.

[152]. Li, J., Mirkovic, J., Wang, M., Reiher, P., & Zhang, L. (2002, June). *SAVE: Source address validity enforcement protocol.* In INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE (Vol. 3, pp. 1557-1566). IEEE.

[153]. Abliz, M. (2011). *Internet denial of service attacks and defense mechanisms*. University of Pittsburgh, Department of Computer Science, Technical Report, 1-50.

[154]. Wang, H., Jin, C., & Shin, K. G. (2007). *Defense against spoofed IP traffic using hop-count filtering.* IEEE/ACM Transactions on Networking (ToN), 15(1), 40-53.

[155]. Eddy, W. M. (2006). *Defenses against TCP SYN flooding attacks*. The Internet Protocol Journal, 9(4), 2-16.

[156]. Gont, F. (2011). *Reducing the TIME-WAIT state using TCP timestamps*.

[157]. Lemon, J. (2002, February). *Resisting SYN Flood DoS Attacks with a SYN Cache*. In BSDCon (Vol. 2002, pp. 89-97).

[158]. "SYN cookies." [Online]. Retrieved on 10, Januray, 2017. URL: http://cr.yp.to/syncookies.html

[159]. Sun, C., Fan, J., & Liu, B. (2007, August). *A robust scheme to detect SYN flooding attacks.* In Communications and Networking in China, 2007. CHINACOM'07. Second International Conference on (pp. 397-401). IEEE.

[160]. Al-Duwairi, B., & Manimaran, G. (2005, March). *Intentional dropping: a novel scheme for SYN flooding mitigation.* In INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE (Vol. 4, pp. 2820-2824). IEEE.

[161]. Jin, C., Wang, H., & Shin, K. G. (2003, October). *Hop-count filtering: an effective defense against spoofed DDoS traffic*. In Proceedings of the 10th ACM conference on Computer and communications security (pp. 30-41). ACM.

[162]. Wang, X., Li, M., & Li, M. (2009, December). *A scheme of distributed hop-count filtering of traffic*. In Wireless Mobile and Computing (CCWMC 2009), IET International Communication Conference on (pp. 516-521). IET.

[163]. Yaar, A., Perrig, A., & Song, D. (2006). StackPi: *New packet marking and filtering mechanisms for DDoS and IP spoofing defense.* IEEE Journal on Selected Areas in Communications, 24(10), 1853-1863.

[164]. Mopari, I. B., Pukale, S. G., & Dhore, M. L. (2008, December). *Detection and defense against DDoS attack with IP spoofing*. In Computing, Communication and Networking, 2008. ICCCn 2008. International Conference on (pp. 1-5). IEEE.

[165]. Wu, Z., & Chen, Z. (2006, October). *A three-layer defense mechanism based on web servers against distributed denial of service attacks*. In Communications and Networking in China, 2006. ChinaCom'06. First International Conference on (pp. 1-5). IEEE.

[166]. Mukaddam, A., Elhajj, I., Kayssi, A., & Chehab, A. (2014, May). *IP spoofing detection using modified hop count*. In Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on (pp. 512-516). IEEE.

[167]. Swain, B. R., & Sahoo, B. (2009, March). *Mitigating DDoS attack and Saving Computational Time using a Probabilistic approach and HCF method*. In Advance Computing Conference, 2009. IACC 2009. IEEE International (pp. 1170-1172). IEEE.

[168]. Chen, Q., Lin, W., Dou, W., & Yu, S. (2011, December). *CBF: a packet filtering method for DDoS attack defense in cloud environment.* In Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on (pp. 427-434). IEEE.

[169]. Cheswick, B., Burch, H., & Branigan, S. (2000, June). *Mapping and visualizing the Internet*. In USENIX Annual Technical Conference, General Track (pp. 1-12).

[170]. Muelder, C., Ma, K. L., & Bartoletti, T. (2005, September). *Interactive visualization for network and port scan detection.* In International Workshop on Recent Advances in Intrusion Detection (pp. 265-283). Springer Berlin Heidelberg.

[171]. Jung, J., Paxson, V., Berger, A. W., & Balakrishnan, H. (2004, May). *Fast portscan detection using sequential hypothesis testing.* In Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on (pp. 211-225). IEEE.

[172]. Wireshark. (2017, January 5). In Wikipedia, the Free Encyclopedia. Retrieved 18:36, January 21, 2017, from https://en.wikipedia.org/w/index.php?title=Wireshark&oldid=768792980

[173]. Schwartz, M. (1987). *Telecommunication networks: protocols, modelling and analysis* (Vol. 7). Reading, MA: Addison-Wesley.

[174]. Bolot, J. C. (1993, October). *End-to-end packet delay and loss behaviour in the Internet.* In ACM SIGCOMM Computer Communication Review (Vol. 23, No. 4, pp. 289-298). ACM.

[175]. M. G., & Karol, M. J. (1988). *Queuing in high-performance packet switching*. IEEE Journal on selected Areas in Communications, *6*(9), 1587-1597.

[176]. Lai, K., & Baker, M. (2000, August). *Measuring link bandwidths using a deterministic model of packet delay*. In ACM SIGCOMM Computer Communication Review (Vol. 30, No. 4, pp. 283-294). ACM.

[177]. Forouzan, A. B. (2002). *TCP/IP protocol suite*. McGraw-Hill, Inc.

[178]. Forouzan, A. B. (2006). *Data communications & networking (sie)*. Tata McGraw-Hill Education.

[179]. Yalagandula, P., Nath, S., Yu, H., Gibbons, P. B., & Seshan, S. (2004, December). *Beyond Availability: Towards a Deeper Understanding of Machine Failure Characteristics in Large Distributed Systems*. In WORLDS.

[180]. Wang, A. J. A. (2005, March). *Information security models and metrics*. In Proceedings of the 43rd annual Southeast regional conference-Volume 2 (pp. 178-184). ACM.

[181]. Lyu, M. R. (1996). *Handbook of software reliability engineering*. Retrieved on 15:11, May 23, 2005. URL http://www.cse.cuhk.edu.hk/~lyu/book/reliability/

[182]. Stearley, J. (2005, June). *Defining and measuring supercomputer Reliability, Availability, and Serviceability (RAS)*. In Proceedings of the Linux clusters institute conference.

[183]. Engelmann, C., Ong, H., & Scott, S. L. (2009). *The case for modular redundancy in large-scale high performance computing systems*. In Proceedings of the IASTED International Conference (Vol. 641, p. 046).