Cyber-Security and Its Future Challenges

Gagandeep SINGH
Department of Computer Science and Engineering, GNA University, Phagwara, Punjab, India
gagandeep.singh@gnaunidersity.edu.in

Vikrant SHARMA
Department of Electronics and Communication Engineering, GNA University, Phagwara, Punjab, India
vikrant.sharma@gnauniversity.edu.in

Abstract

This paper pertains to the existing challenges of cybersecurity, along with its threats in the future. On the other hand, the internet is expanding every day, and attackers see it as an opportunity to exploit people over the internet. In the future, this can lead to severe consequences in the coming time. This review paper reflects the challenges faced in cybersecurity and the terrible consequences of cyber threats in the future.

Index terms: cyber-attack, Industry 4.0, IoT, network vulnerabilities, bots, DDoS, virus, worms, malwares, ransomware

References:

[1]. R. Von Solms and J. Van Niekerk, "From information security to cyber security," Comput. Secur., vol. 38, pp. 97–102, 2013, doi: 10.1016/j.cose.2013.04.004.
[2]. I. B. M. X. I. Response and I. Services, "X-Force Threat," 2020.
[3]. N. McCarthy, "Where Cyberbullying Is Most Prevalent," Statistica, 2018. https://www.statista.com/chart/15926/the-share-of-parents-who-say-their-child-has-experienced-cyberbullying/ (accessed Jun. 23, 2020).
[4]. J. Kim, "Cyber-security in govern- ment : reducing the risk," Comput. Fraud Secur. Bull., vol. 2017, no. 7, pp. 8–11, 2017, doi: 10.1016/S1361-3723(17)30059-3.
[5]. R. Nagpal, "Evolution of Cyber Crimes," Asian Sch. Cyber Laws, p. 2, 2008, [Online]. Available: http://www.cyberlawdb.com/docs/ebooks/cc.pdf.
[6]. R. Bidgoli, Hossein; Azarmsa, "Computer Security: New Managerial Concern For The 1980s And.pdf." Journal of Systems Management; Cleveland Vol. 40, Iss. 10, 1989.

[7]. A. Avaibbiliv, B. Integriv, D. Gruber, and G. Watt, "E-mail Bombs and Countermeasures: Cyber attacks on availability and brand integrity," Ieee Netw., pp. 10–17, 1998.

[8]. F. Cohen, "Simulating Cyber Attacks, Defences, and Consequences Modeling, Simulation, and Data Limitations in Information Protection," Comput. Secur., vol. 18, pp. 479–518, 1999.

[9]. B. C. Ervural and B. Ervural, "Overview of Cyber Security in the Industry 4.0 Era," pp. 267–284, 2018, doi: 10.1007/978-3-319-57870-5_16.

[10]. J. R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," Secur. Stud., vol. 22, no. 3, pp. 365–404, 2013, doi: 10.1080/09636412.2013.816122.

[11]. R. Jenkins, "Is stuxnet physical? does it matter?," J. Mil. Ethics, vol. 12, no. 1, pp. 68–79, 2013, doi: 10.1080/15027570.2013.782640.

[12]. R. Arora and A. Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms," Int. J. Eng. Res. Appl., vol. 3, no. 4, pp. 1922–1926, 2013.

[13]. C. Cachin and M. Schunter, "A cloud you can trust," IEEE Spectr., vol. 48, no. 12, 2011, doi: 10.1109/MSPEC.2011.6085778.

[14]. D. GOODIN, "NoTrade group exposes 100,000 passwords for Google, Apple engineers Title," 2012. https://arstechnica.com/information-technology/2012/09/ieee-trade-group-exposes-100000-password-for-google-apple-engineers/ (accessed May 01, 2020).

[15]. C. Bronk and E. Tikk-Ringas, "The Cyber Attack on Saudi Aramco," Survival (Lond)., vol. 55, no. 2, pp. 81–96, 2013, doi: 10.1080/00396338.2013.784468.

[16]. Z. Dehlawi and N. Abokhodair, "Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident," IEEE ISI 2013 - 2013 IEEE Int. Conf. Intell. Secur. Informatics Big Data, Emergent Threat. Decis. Secur. Informatics, pp. 73–75, 2013, doi: 10.1109/ISI.2013.6578789.

[17]. "ICS Joint Security Awareness Report," JSAR-12-241-01B. https://www.us-cert.gov/ics/jsar/JSAR-12-241-01B (accessed May 01, 2020).

[18]. Wikipedia, "2013 Singapore cyberattacks," 2019. https://en.wikipedia.org/wiki/2013_Singapore_cyberattacks#cite_note-1 (accessed May 01, 2020).

[19]. M. Teo, "Lessons Learnt from the Cyber Attacks," Website, Singapore Government Agency, 2014. https://www.psd.gov.sg/challenge/ideas/feature/lessons-learnt-from-the-cyber-attacks (accessed May 02, 2020).

[20]. E. Jager, "Home | Newsfront Tags: Middle East | Iran | hackers | cyberattack | Navy | Marine Corps | NSA Iranian Hackers Penetrated U.S. Navy Marine Corps Internet for Four Months," Feb. 18, 2014. https://www.newsmax.com/Newsfront/Iran-hackers-cyberattack-Navy/2014/02/18/id/553238/ (accessed May 10, 2020).

[21]. M. Connell, "Deterring Iran's Use of Offensive Cyber: A Case Study," no. October, p. 25, 2014.

[22]. S. Haggard and J. R. Lindsay, "North Korea and the Sony hack: Exporting instability through cyberspace," Asia Pacific Issues, no. 117, pp. 1–8, 2015.

[23]. S. Shukla and P. Bhakta, "3.2 million debit cards compromised; SBI, HDFC Bank, ICICI, YES Bank and Axis worst hit," Ecoomic Times. https://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms (accessed May 10, 2020).

[24]. N. Christopher, "The worst cyber attacks of 2016," Economic Times. https://economictimes.indiatimes.com/small-biz/security-tech/security/the-worst-cyber-attacks-of-2016/articleshow/56212448.cms (accessed May 10, 2020).

[25]. S. Iyar, "Security breach: SBI blocks over 6 lakh debit cards," Economic Times. https://economictimes.indiatimes.com/industry/banking/finance/banking/security-breach-sbi-blocks-over-6l-debit-cards/articleshow/54933861.cms (accessed May 10, 2020).

[26]. Wiki, "2016 Indian Banks data breach," Wikipedia. https://en.wikipedia.org/wiki/2016_Indian_Banks_data_breach (accessed May 10, 2020).

[27]. S. Mohurle and M. Patil, "A brief study of Wannacry Threat: Ransomware Attack 2017," Int. J. Adv. Res. Comput. Sci., vol. 8, no. 5, pp. 1938–1940, 2017, doi: http://dx.doi.org/10.26483/ijarcs.v8i5.4021.

[28]. N. Perlorth, M. Scott, and S. Frankel, "Cyberattack Hits Ukraine Then Spreads Internationally," New York Times. https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html (accessed May 11, 2020).

[29]. A. Dekkubger, "Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?," Forbes, 2019. https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/#1e0b22f1567f (accessed May 11, 2020).

[30]. WHO, "WHO reports fivefold increase in cyber attacks, urges vigilance," World Health Organization, 2020. https://www.who.int/news-room/detail/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance (accessed May 11, 2020).

[31]. D. Reed, "Applying the OSI Seven Layer Network Model To Information Security SANS GIAC GSEC Practical Assignment version 1.4b Option One Introduction to the OSI Seven Layer Model," 2003.

[32]. Supriyanto, I. H. Hasbullah, R. K. Murugesan, and S. Ramadass, "Survey of internet protocol version 6 link local communication security vulnerability and mitigation methods," IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India), vol. 30, no. 1, pp. 64–71, 2013, doi: 10.4103/0256-4602.107341.

[33]. P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," J. Electr. Comput. Eng., vol. 2017, 2017, doi: 10.1155/2017/9324035.

[34]. H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: A review," Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012, vol. 3, pp. 648–651, 2012, doi: 10.1109/ICCSEE.2012.373.

[35]. I. Ali, S. Sabir, and Z. Ullah, "Internet of Things Security, Device Authentication and Access Control: A Review," vol. 14, no. 8, pp. 456–466, 2019, [Online]. Available: http://arxiv.org/abs/1901.07309.

[36]. S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: Challenges, solutions and future directions," Proc. Annu. Hawaii Int. Conf. Syst. Sci., vol. 2016-March, pp. 5772–5781, 2016, doi: 10.1109/HICSS.2016.714.

[37]. L. Liu, O. De Vel, Q. L. Han, J. Zhang, and Y. Xiang, "Detecting and Preventing Cyber Insider Threats: A Survey," IEEE Commun. Surv. Tutorials, vol. 20, no. 2, pp. 1397–1418, 2018, doi: 10.1109/COMST.2018.2800740.

[38]. G. Silowash, T. J. Shimeall, D. Cappelli, A. Moore, L. Flynn, and R. Trzeciak, "Common Sense Guide to Mitigating Threats," CERT Progr., vol. 4th Ed., no. December, pp. 1–144, 2012.

[39]. M. Ben Salem and S. J. Stolfo, "Decoy document deployment for effective masquerade attack detection," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6739 LNCS, pp. 35–54, 2011, doi: 10.1007/978-3-642-22424-9_3.

[40]. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Surveying port scans and their detection methodologies," Comput. J., vol. 54, no. 10, pp. 1565–1581, 2011, doi: 10.1093/comjnl/bxr035.

[41]. S. Jajodia, S. Noel, and B. O'Berry, "Topological Analysis of Network Attack Vulnerability," Manag. Cyber Threat., pp. 247–266, 2005, doi: 10.1007/0-387-24230-9_9.

[42]. J. Bau, E. Bursztein, D. Gupta, and J. Mitchell, "State of the art: Automated black-box web application vulnerability testing," Proc. - IEEE Symp. Secur. Priv., pp. 332–345, 2010, doi: 10.1109/SP.2010.27.

[43]. J. Fonseca, M. Vieira, and H. Madeira, "Testing and comparing web vulnerability scanning tools for SQL injection and XSS attacks," Proc. - 13th Pacific Rim Int. Symp. Dependable Comput. PRDC 2007, pp. 365–372, 2007, doi: 10.1109/PRDC.2007.63.

[44]. C. Hadnagy, Social engineering: The art of human hacking, vol. 53, no. 9. 2019.

[45]. K. Chiang and L. Lloyd, "A case study of the rustock rootkit and spam bot," HotBots'07 Proc. first Conf. First Work. Hot Top. Underst. Botnets, p. 10, 2007, [Online]. Available: http://dl.acm.org/citation.cfm?id=1323128.1323138.

[46]. M. Sikorski and A. Honig, Practical malware analysis: the hands-on guide to dissecting malicious software. no starch press. 2012.

[47]. N. Falliere, L. O. Murchu, and E. Chien, "W32. Stuxnet Dossier, Symantec Security Response, Version 1.4, February 2011," Symantec Secur. Response, vol. 4, no. February, pp. 1–69, 2011, doi: Sept. 20, 2015.

[48]. N. Nissim, A. Cohen, C. Glezer, and Y. Elovici, "Detection of malicious PDF files and directions for enhancements: A state-of-the art survey," Comput. Secur., vol. 48, pp. 246–266, 2015, doi: 10.1016/j.cose.2014.10.014.

[49]. N. Provos, D. Mcnamee, P. Mavrommatis, K. Wang, and N. Modadugu, "The Ghost In The Browser Analysis of Web-based Malware," Proc. first Conf. First Work. Hot Top. Underst. Botnets, vol. 462, p. 4, 2007, doi: 10.1038/nature08624.

[50]. L. Xu, Z. Zahan, and S. Xu, "Cross-Layer Detection of Malicious Websites," Proc. third ACM Conf. Data Appl. Secur. Priv., pp. 141–152, 2013.

[51]. G. Silowash and C. King, "Insider threat control: Understanding data loss prevention (DLP) and detection by correlating events from multiple sources," no. January, p. 30, 2013, [Online]. Available: http://repository.cmu.edu/sei/708/.

[52]. M. Ben Salem, S. Hershkop, and S. J. Stolfo, "A Survey of Insider Attack Detection Research," Adv. Inf. Secur., vol. 39, pp. 69–70, 2008, doi: 10.1007/978-0-387-77322-3_5.

[53]. A. F. Emmott, S. Das, T. Dietterich, A. Fern, and W. K. Wong, "Systematic construction of anomaly detection benchmarks from real data," Proc. ACM SIGKDD Work. Outlier Detect. Descr. ODD 2013, pp. 16–21, 2013, doi: 10.1145/2500853.2500858.

[54]. N. Virvilis and D. Gritzalis, "The big four - What we did wrong in advanced persistent threat detection?," Proc. - 2013 Int. Conf. Availability, Reliab. Secur. ARES 2013, pp. 248–254, 2013, doi: 10.1109/ARES.2013.32.

[55]. K. Alieyan, A. Almomani, A. Manasrah, and M. M. Kadhum, "A survey of botnet detection based on DNS," Neural Comput. Appl., vol. 28, no. 7, pp. 1541–1558, 2017, doi: 10.1007/s00521-015-2128-0.

[56]. S. García, M. Grill, J. Stiborek, and A. Zunino, "An empirical comparison of botnet detection methods," Comput. Secur., vol. 45, pp. 100–123, 2014, doi: 10.1016/j.cose.2014.05.011.

[57]. G. Gu, R. Perdisci, J. Zhang, and W. Lee, "BotMiner: Clustering analysis of network traffic for protocol- and structure-independent botnet detection," Proc. 17th USENIX Secur. Symp., pp. 139–154, 2008.

[58]. Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "The Socialbot Network: When bots socialize for fame and money," ACM Int. Conf. Proceeding Ser., pp. 93–102, 2011, doi: 10.1145/2076732.2076746.

[59]. X. Sun, R. Torres, and S. Rao, "DDoS attacks by subverting membership management in P2P systems," 2007 3rd IEEE Work. Secur. Netw. Protoc. NPSec, pp. 13–18, 2007, doi: 10.1109/NPSEC.2007.4371618.

[60]. S. Khan, A. Gani, A. W. A. Wahab, and P. K. Singh, "Feature Selection of Denial-of-Service Attacks Using Entropy and Granular Computing," Arab. J. Sci. Eng., vol. 43, no. 2, pp. 499–508, 2018, doi: 10.1007/s13369-017-2634-8.

[61]. D. Sahoo, C. Liu, and S. C. H. Hoi, "Malicious URL Detection using Machine Learning: A Survey," vol. 1, no. 1, pp. 1–37, 2017, [Online]. Available: http://arxiv.org/abs/1701.07179.

[62]. H. Haddadi and A. Perrig, "Public Review for Fighting Online Click-Fraud Using Bluff Ads a c m s i g c o m m Fighting Online Click-Fraud Using Bluff Ads," vol. 40, no. 2, pp. 21–25, 2010.

[63]. T. Rid and B. Buchanan, "Attributing Cyber Attacks," J. Strateg. Stud., vol. 38, no. January 2015, pp. 4–37, 2015, doi: 10.1080/01402390.2014.977382.