References

[1] A. Grizhnevich, "IoT architecture: building blocks and how they work," *ScienceSoft*, Oct 2020. [Online]. Available: https://www.scnsoft.com/blog/iot-architecture-in-a-nutshell-and-how-it-works

[2] "Product page: Mi Home Security Camera 360° 1080P," Feb 2021, [Online; accessed 24. Feb. 2021]. [Online]. Available: https://www.mi.com/global/camera-360

[3] "UniFi Protect - Getting started," Feb 2021, [Online; accessed 24. Feb. 2021]. [Online]. Available: https://help.ui.com/hc/en-us/articles/360058454253-UniFi-Protect-Getting-started

[4] "Kasa Spot - User Guide," Feb 2021, [Online; accessed 24. Feb. 2021]. [Online]. Available: https://help.ui.com/hc/en-us/articles/360058454253-UniFi-Protect-Getting-started

[5] A. Guzman and A. Gupta, *IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices*. Packt Publishing Ltd, 2017.

[6] B. Schneier, "Attack trees," 1999.

[7] *Mi Home Security Camera 360° 1080p User Manual*, Xiaomi, Room 001A, Floor 11, Block 1, No. 588 Zixing Road, Minhang District, Shanghai, China, [Online; accessed 1. Mar. 2021]. [Online]. Available: http://go.buy.mi.com/uk/servicecenter/file/Mi_Home_Security_Camera_360%C2%B0_1080p_uk?publicationId=20572&namespaceId=2&binaryId=12128

[8] A. Shostack, *Threat modeling: Designing for security*. John Wiley & Sons, 2014.

[9] "OWASP Internet of Things - Top 10," OWASP, Tech. Rep., dec 2018, [Online; accessed 2. Mar. 2021]. [Online]. Available: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

[10] "OWASP Web - Top 10," OWASP, Tech. Rep., 2017, [Online; accessed 23. Apr. 2021]. [Online]. Available: https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf

[11] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying iot security: an exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2702–2733, 2019.

[12] P. Cerwall, "Ericsson mobility report," Ericsson, Tech. Rep., 2017.

[13] A. B. Brush, B. Lee, R. Mahajan, S. Agarwal, S. Saroiu, and C. Dixon, "Home automation in the wild: challenges and opportunities," in *proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2011, pp. 2115–2124.

[14] N. Kalbo, Y. Mirsky, A. Shabtai, and Y. Elovici, "The security of ip-based video surveillance systems," *Sensors*, vol. 20, no. 17, p. 4806, 2020.

[15] "CVE-2017-11632." Available from MITRE, CVE-ID CVE-2017-11632., Feburary 2018. [Online]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11632

[16] M. Stanislav and T. Beardsley, "Hacking iot: A case study on baby monitor exposures and vulnerabilities," *Rapid7 Report*, 2015.

[17] B. Cusack and Z. Tian, "Evaluating ip surveillance camera vulnerabilities," 2017.

[18] Y. Seralathan, T. T. Oh, S. Jadhav, J. Myers, J. P. Jeong, Y. H. Kim, and J. N. Kim, "Iot security vulnerability: A case study of a web camera," in *2018 20th International Conference on Advanced Communication Technology (ICACT)*. IEEE, 2018, pp. 172–177.

[19] A. Tekeoglu and A. S. Tosun, "Investigating security and privacy of a cloud-based wireless ip camera: Netcam," in *2015 24th International Conference on Computer Communication and Networks (ICCCN)*. IEEE, 2015, pp. 1–6.

[20] P. A. Abdalla and C. Varol, "Testing iot security: The case study of an ip camera," in *2020 8th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE, 2020, pp. 1–5.

[21] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Systematically evaluating security and privacy for consumer iot devices," in *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, 2017, pp. 1–6.

[22] "Course description for degree project in computer science and engineering." [Online]. Available: https://www.kth.se/student/kurser/kurs/DA231X?l=en

[23] S. Cirani, G. Ferrari, M. Picone, and L. Veltri, *Internet of things: architectures, protocols and standards*. John Wiley & Sons, 2018.

[24] "Google Books Ngram Viewer," Feb 2021, [Online; accessed 23. Feb. 2021]. [Online]. Available: https://books.google.com/ngrams/graph?content=internet+of+things&year_start=1950&year_end=2019&corpus=26&smoothing=0&case_insensitive=true#

[25] M. Weiser, "The computer for the 21 st century," *Scientific american*, vol. 265, no. 3, pp. 94–105, 1991.

[26] ——, "Hot topics-ubiquitous computing," *Computer*, vol. 26, no. 10, pp. 71–72, 1993.

[27] F. Wortmann and K. Flüchter, "Internet of things," *Business & Information Systems Engineering*, vol. 57, no. 3, pp. 221–224, 2015.

[28] G. Weidman, *Penetration testing: a hands-on introduction to hacking*. No Starch Press, 2014.

[29] A. Gupta, *The IoT Hacker's Handbook*. Springer, 2019.

[30] M. Berner, "Where's my car? ethical hacking of a smart garage," 2020.

[31] M. Howard and D. LeBlanc, *Writing secure code*. Pearson Education, 2003.

[32] "Threat Modeling | OWASP," Aug 2020, [Online; accessed 16. Apr. 2021]. [Online]. Available: https://owasp.org/www-community/Threat_Modeling

[33] B. W. J.D. Meier, Alex Mackman, "Threat Modeling Web Applications," May 2005, [Online; accessed 16. Apr. 2021]. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648006(v=pandp.10)?redirectedfrom=MSDN

[34] L. Kohnfelder and P. Garg, "The threats to our products," *Microsoft Interface, Microsoft Corporation*, vol. 33, 1999.

[35] B. Russell and D. Van Duren, *Practical Internet of Things Security: Design a security framework for an Internet connected ecosystem*. Packt Publishing Ltd, 2018.

[36] O.-J. Dahl, E. W. Dijkstra, and C. A. R. Hoare, *Structured programming*. Academic Press Ltd., 1972.

[37] L. Osterman, "Threat Modeling Again, STRIDE per Element," Mar 2021, [Online; accessed 1. Mar. 2021]. [Online]. Available: https://docs.microsoft.com/en-us/archive/blogs/larryosterman/threat-modeling-again-stride-per-element

[38] C. Salter, O. S. Saydjari, B. Schneier, and J. Wallner, "Toward a secure system engineering methodolgy," in *Proceedings of the 1998 workshop on New security paradigms*, 1998, pp. 2–10.

[39] "ATT&CK 101," May 2018, [Online; accessed 27. May 2021]. [Online]. Available: https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/attck-101

[40] A. Shostack, "Experiences threat modeling at microsoft." *MODSEC@ MoDELS*, vol. 2008, 2008.

[41] "Appendix N: SDL Security Bug Bar (Sample)," Feb 2021, [Online; accessed 17. Feb. 2021]. [Online]. Available: https://docs.microsoft.com/en-us/previous-versions/windows/desktop/cc307404(v=msdn.10)

[42] "Probability-impact assessment - Praxis Framework," Feb 2021, [Online; accessed 17. Feb. 2021]. [Online]. Available: https://www.praxisframework.org/en/library/probability-impact-assessment

[43] "CVSS v3.1 Specification Document," Jan 2021, [Online; accessed 18. Feb. 2021]. [Online]. Available: https://www.first.org/cvss/specification-document