12 References

[1] K. L. Lueth. “The State of IoT 2020: 12 Billion IoT Connections, Surpassing Non-IoT.” IoT Analytics. Nov. 19, 2020. https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/ (accessed: Apr. 27, 2021).

[2] “Global Drone Service Market Report 2019: Market is Expected to Grow from USD 4.4 Billion in 2018 to USD 63.6 Billion by 2025, at a CAGR of 55.9%.” Insider Inc. Apr. 29, 2019. https://markets.businessinsider.com/news/stocks/global-drone-service-market-report-2019-market-is-expected-to-grow-from-usd-4-4-billion-in-2018-to-usd-63-6-billion-by-2025-at-a-cagr-of-55-9-1028147695 (accessed: Apr. 27, 2021).

[3] “How Can Drones Be Hacked? The updated list of vulnerable drones & attack tools | by Sander Walters | Medium” Medium. Aug. 19, 2019. https://medium.com/@swalters/how-can-drones-be-hacked-the-updated-list-of-vulnerable-drones-attack-tools-dd2e006d6809 (accessed: May 18, 2021).

[4] E. Vattapparamban, I. Guvenc, A. I. Yurekli, K. Akkaya, and S. Uluagac, “Drones for smart cities: Issues in cybersecurity, privacy, and public safety.” *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2016, doi: 10.1109/iwcmc.2016.7577060. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7577060.

[5] B. Rao, A. G. Gopi, and R. Maione, “The societal impact of commercial drones.” *Technology in Society*, vol. 45, pp. 83-90, May 2016, doi: 10.1016/j.techsoc.2016.02.009. [Online]. Available: https://www.researchgate.net/publication/298427201_The_societal_impact_of_commercial_drones.

[6] “The compact and resistant drone with a 4K HDR camera - Parrot ANAFI.” Parrot Drone SAS. 2020. https://www.parrot.com/us/drones/anafi (accessed: May 23, 2021).

[7] Goodrich, Michael, & Tamassia, Roberto. (2013). Introduction to Computer Security (Pearson custom library). Harlow: Pearson Education UK.

[8] G. Vasconcelos, G. Carrijo, R. Miani, J. Souza, and V. Guizilini, “The Impact of DoS Attacks on the AR.Drone 2.0.” *2016 XIII Latin American Robotics Symposium and IV Brazilian Robotics Symposium (LARS/SBR)*, Dec. 2016, doi: 10.1109/lars-sbr.2016.28. [Online]. Available: https://www.researchgate.net/publication/313177418_The_Impact_of_DoS_Attacks_on_the_ARDrone_20.

[9] A. Schaad and D. Binder, “ML-Supported Identification and Prioritization of Threats in the OVVL Threat Modelling Tool.” *Data and Applications Security and Privacy XXXIV*, pp. 274-285, Jun. 18, 2020, doi: 10.1007/978-3-030-49669-2_16. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-49669-2_16.

[10] J. Simonjan, S. Taurer, and B. Dieber, “A Generalized Threat Model for Visual Sensor Networks.” *Sensors*, vol. 20, no. 13, p. 3629, Jun. 28, 2020, doi: 10.3390/s20133629. [Online]. Available: https://www.mdpi.com/1424-8220/20/13/3629.

[11] Hussain, Shafiq et al. “Threat Modelling Methodologies: a Survey”. In: Sci. Int.(Lahore) 26.4 (2014), pp. 1607–1609.

[12] E. Dahlman and K. Lagrelius, “A Game of Drones : Cyber Security in UAVs,” 2019.

[13] “How Can Drones Be Hacked? The updated list of vulnerable drones & attack tools.” https://medium.com/@swalters/how-can-drones-be-hacked-the-updated-list-ofvulnerable-drones-attack-tools-dd2e006d6809 (accessed: May 23, 2021).

[14] N. Rodday. Hacking a Professional Drone. (Aug. 17, 2016). Accessed: Jun. 01, 2021. [Online Video]. Available: https://www.youtube.com/watch?v=JRVb-xE1zTI.

[15] A. Guzman and A. Gupta, *IoT Penetration Testing Cookbook*. Packt Publishing Ltd, 2017.

[16] "NSE Lab: Home." Division of Network and Systems Engineering | KTH. https://nse.digital/ (accessed: May 23, 2021).

[17] R. Lukawiecki. "Threat Modeling for Secure Web Application Development." SlideToDoc. 2003. https://slidetodoc.com/threat-modeling-for-secure-web-application-development-rafal/ (accessed: May 21, 2021).

[18] "Thesis Report - NSE Lab." Division of Network and Systems Engineering | KTH. https://nse.digital/pages/thesis_guidelines/thesis_report.html (accessed: May 23, 2021).

[19] K. Tay. "Wi-Fi de-authentication attacks and how you can prevent them using 802.11w or WPA3 | by Keith Tay | Medium." Medium. Nov. 11, 2020. https://x4bx54.medium.com/use-802-11w-or-wpa3-to-prevent-de-authentication-attacks-in-your-wi-fi-network-4ce63ab20033 (accessed: May 23, 2021).

[20] N. Darchis. "802.11 frames : A starter guide to learn wireless sniffer traces - Cisco Community" Cisco Systems Inc. Nov. 18, 2020. https://community.cisco.com/t5/wireless-mobility-documents/802-11-frames-a-starter-guide-to-learn-wireless-sniffer-traces/ta-p/3110019 (accessed: May 23, 2021).

[21] "Aircrack-ng.org." Aircrack-ng. 2021. https://www.aircrack-ng.org/ (accessed: May 23, 2021).

[22] D. Bombal. Cracking WiFi WPA2 Handshake - YouTube. (Feb. 02, 2021). Accessed: May 23, 2021. [Online Video]. Available: https://www.youtube.com/watch?v=WfYxrLaqlN8.

[23] "LOIC download | SourceForge.net." SourceForge - Slashdot Media. Aug. 17, 2020. https://sourceforge.net/projects/loic/ (accessed: May 23, 2021).

[24] "What is the low orbit ion cannon (LOIC)? | Cloudflare." Cloudflare, Inc. 2021. https://www.cloudflare.com/learning/ddos/ddos-attack-tools/low-orbit-ion-cannon-loic/ (accessed: May 23, 2021).

[25] Computerphile. Slow Loris Attack - Computerphile - YouTube. (Nov. 09, 2016). Accessed: May 23, 2021. [Online Video]. Available: https://www.youtube.com/watch?v=XiFkyR35v2Y.

[26] "Tool 76: Synflood." Syracuse University. https://web.ecs.syr.edu/~wedu/Teaching/cis758/netw522/netwox-doc_html/tools/76.html (accessed: May 23, 2021).

[27] S. Sanfilippo. "Hping - Active Network Security Tool." hping. 2006. http://www.hping.org/ (accessed: May 23, 2021).

[28] I. Muscat. "Mitigate Slow HTTP GET/POST Vulnerabilities in the Apache HTTP Server | Acunetix." Acunetix - Invicti. Jun. 06, 2019. https://www.acunetix.com/blog/articles/slow-http-dos-attacks-mitigate-apache-http-server/ (accessed: May 23, 2021).

[29] "What Is a Distributed Denial of Service (DDoS) Attack? | NETSCOUT." NETSCOUT. https://www.netscout.com/what-is-ddos (accessed: May 24, 2021).

[30] W. M. Eddy, "SYN Cookie Defense," in *Encyclopedia of Cryptography and Security*, Springer US, 2011, pp. 1271-1273.

[31] "What is a SYN flood attack and how to prevent it? | NETSCOUT." NETSCOUT. https://www.netscout.com/what-is-ddos/syn-flood-attacks (accessed: May 24, 2021).

[32] "What Is the Internet of Things (IoT)? - Oracle." Oracle. https://www.oracle.com/internet-of-things/what-is-iot/ (accessed: May 26, 2021).

[33] J. Clark. "What is the Internet of Things (IoT)?" IBM Business Operations Blog. Nov. 17, 2016. https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/ (accessed: May 26, 2021).

[34] S. Weisman. "What Is a DDoS Attack? Distributed Denial-of-Service Attack Explained | Norton" NortonLifeLock Inc. Jul. 26, 2020. https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html (accessed: May 26, 2021).

[35] "What Is a distributed denial-of-service (DDoS) attack? | Cloudflare" Cloudflare, Inc. 2021. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ (accessed: May 26, 2021).

[36] D. Balaban. “The History and Evolution of DDoS Attacks - Experfy Insights” Experfy Inc. May. 11, 2021. https://resources.experfy.com/bigdata-cloud/history-evolution-of-ddos-attacks/ (accessed: May 26, 2021).

[37] J. Valente and A. A. Cardenas, “Understanding Security Threats in Consumer Drones Through the Lens of the Discovery Quadcopter Family.” *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, Nov. 2017, doi: 10.1145/3139937.3139943. [Online]. Available: https://www.researchgate.net/publication/320793517_Understanding_Security_Threats_in_Consumer_Drones_Through_the_Lens_of_the_Discovery_Quadcopter_Family.

[38] S. Kamkar. “SkyJack: autonomous drone hacking - Samy Kamkar.” SkyJack. Dec. 13, 2013. http://www.samy.pl/skyjack/ (accessed: May 27, 2021).

[39] W. Hennigan. “Experts Say Drones Pose a National Security Threat — and We ..” TIME. May 31, 2018. https://time.com/5295586/drones-threat/ (accessed: May 27, 2021).

[40] F. Lambert. “Tesla car hacked using drone; a patch has already been released ..” Electrek. May 13, 2021. https://electrek.co/2021/05/13/tesla-car-hacked-using-drone-patch/ (accessed: May 27, 2021).

[41] E. Deligne, “ARDrone corruption.” *Journal in Computer Virology*, vol. 8, no. 1, pp. 15-27, Dec. 29, 2011, doi: 10.1007/s11416-011-0158-4. [Online]. Available: https://link.springer.com/article/10.1007/s11416-011-0158-4.

[42] F. Lakew Yihunie, A. K. Singh, and S. Bhatia, “Assessing and Exploiting Security Vulnerabilities of Unmanned Aerial Vehicles.” *Smart Systems and IoT: Innovations in Computing*, pp. 701-710, Oct. 27, 2019, doi: 10.1007/978-981-13-8406-6_66. [Online]. Available: https://link.springer.com/chapter/10.1007%2F978-981-13-8406-6_66.

[43] “What Is The Difference Between White Hat, Grey Hat, and Black Hat ..” SEWORKS. Sep. 27, 2017. https://blog.se.works/what-is-the-difference-between-white-hat-grey-hat-and-black-hat-hackers/ (accessed: May 28, 2021).

[44] “Responsible disclosure - NSE Lab.” Division of Network and Systems Engineering | KTH. https://nse.digital/pages/thesis_guidelines/responsible_disclosure.html (accessed: May 28, 2021).

Appendix A

	Rating	**High (3)**	**Medium (2)**	**Low (1)**
D	Damage potential	Can subvert all security controls and get full trust to take over the whole IoT ecosystem.	Could leak sensitive information.	Could leak sensitive information.
R	Reproducibility	The attack is always reproducible.	The attack can be reproduced only within a timed window or specific condition.	It's very difficult to reproduce the attack, even with specific information about the vulnerability.
E	Exploitability	A novice attacker could execute the exploit.	A skilled attacker could make the attack repeatedly.	Allows a skilled attacker with in-depth knowledge to perform the attack.
A	Affected users	All users, default configurations, all devices.	Affects some users, some devices, and custom configurations.	Affects a small percentage of users and/or devices through an obscure feature.
D	Discoverability	Attack explanation can be easily found in a publication.	Affects a seldom-used feature where an attacker would need to be very creative to discover a malicious use for it.	Is obscure and unlikely an attacker would discover a way to exploit the bug.