References

[1] A. Georgiadou., S. Mouzakitis., and D. Askounis., "Working from home during covid-19 crisis: a cyber security culture assessment survey," *Security Journal*, Feb. 2021, https://doi-org.focus.lib.kth.se/10.1057/s41284-021-00286-2.

[2] W. Xiong. and R. Lagerström., "Threat modeling – a systematic literature review," *Computers & Security*, vol. 84, pp. 53–69, 2019, https://doi.org/10.1016/j.cose.2019.03.010.

[3] M. Ekstedt, S. Hacks, R. Lagerström, P. Mukherjee, and Z. Afzal, "Yet another cybersecurity risk assessment framework," 2021, submitted manuscript.

[4] R. Lagerström. (2020) EP2790 lecture slides. (Accessed: 2021-05-17). [Online]. Available: https://docs.google.com/presentation/d/1GjNnT3seDnL-1YFuBiDwrObrjkVrLfLlRMD9kiKkIGk/edit#slide=id.p1

[5] C. N. D. Viktor, Lesyk. Mauro, "A survey of man in the middle attacks," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 2027 – 2051, 2016, dOI 10.1109/COMST.2016.2548426.

[6] B. A. Z. D. . M. G. Harel, "A wrinkle in time: a case study in dns poisoning," *International Journal of Information Security*, May 2020, https://doi-org.focus.lib.kth.se/10.1007/s10207-020-00502-x.

[7] S. W. B. D. Keromytis, "Sqlrand: Preventing sql injection attacks," in *eds) Applied Cryptography and Network Security. ACNS 2004. Lecture Notes in Computer Science*. Springer, Berlin, Heidelberg, 2004, vol. 3089, https://doi-org.focus.lib.kth.se/10.1007/978-3-540-24852-1$_2$1.

[8] Loxdal *et al.*, "Why phishing works on smartphones: A preliminary study," in *Proceedings of the 54th Hawaii International Conference on System Sciences 2021*, http://hdl.handle.net/10125/71484.

[9] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *Journal of Information Security and Applications*, vol. 22, pp. 113–122, 2015, https://doi.org/10.1016/j.jisa.2014.09.005.

[10] K. Simon and J. C. Bradfield., "A general definition of malware," *Journal in Computer Virology*, vol. 6, pp. 105–114, Sep. 2009, https://doi-org.focus.lib.kth.se/10.1007/s11416-009-0137-1.

[11] P. Johnson, R. Lagerström, and M. Ekstedt, "A meta language for threat modeling and attack simulations," in *Proceedings of the 13th International Conference on Availability, Reliability and Security*. ACM. doi: 10.1145/3230833.3232799. ISBN 978-1-4503-6448-5 pp. 1–8. [Online]. Available: https://dl.acm.org/doi/10.1145/3230833.3232799

[12] M. Ekstedt, P. Johnson, R. Lagerström, D. Gorton, J. Nydrén, and K. Shahzad, "Securi CAD by foreseeti: A CAD tool for enterprise cyber security management," in *2015 IEEE 19th International Enterprise Distributed Object Computing Workshop*. doi: 10.1109/EDOCW.2015.40 pp. 152–155, ISSN: 2325-6605.

[13] S. Katsikeas, P. Johnson, S. Hacks, and R. Lagerström, "Probabilistic modeling and simulation of vehicular cyber attacks: An application of the meta attack language:," in *Proceedings of the 5th International Conference on Information Systems Security and Privacy*. SciTePress - Science and Technology Publications. doi: 10.5220/0007247901750182 pp. 175–182.

[14] S. Hacks, S. Katsikeas, E. Ling, R. Lagerström, and M. Ekstedt, "powerLang: a probabilistic attack simulation language for the power domain," *Energy Informatics*, p. 30, Nov. 2020, https://doi.org/10.1186/s42162-020-00134-4.

[15] W. Xiong., E. Legrand., O. Åberg., and R. Lagerström., "Cyber security threat modeling based on the MITRE enterprise ATT&CK matrix," *Journal of Software Systems and Modeling*, 2021, (forthcoming).

[16] P. Johnson, A. Vernotte, M. Ekstedt, and R. Lagerström, "pwnPr3d: An attack-graph-driven probabilistic threat-modeling approach," in *2016 11th International Conference on Availability, Reliability and Security (ARES)*. doi: 10.1109/ARES.2016.77

[17] N. Friman, "Security analysis of smart buildings," Bachelor's Thesis, Royal Institute of Technology, KTH:s publikationsdatabas DiVA, 2020.

[18] L. Wessman and N. Wessman, "Threat modeling of large scale computer systems: Implementing and evaluating threat modeling at company x," Bachelor's Thesis, Royal Institute of Technology, KTH:s publikationsdatabas DiVA, 2020.

[19] C. Weigelt, "A process for threat modeling of large-scale computer systems: A case study," Bachelor's Thesis, Royal Institute of Technology, KTH:s publikationsdatabas DiVA, 2020.

[20] R. S. Murch, W. K. So, W. G. Buchholz, S. Raman, and J. Peccoud, "Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy," *Frontiers in Bioengineering and Biotechnology*, vol. 6, 4 2018, https://doi.org/10.3389/fbioe.2018.00039.

[21] A. Almulhem, "Threat modeling for electronic health record systems," *Journal of Medical Systems*, vol. 36, no. 5, pp. 2921–2926, 2012, https://doi.org/10.1007/s10916-011-9770-6.

[22] S. Alshehri, S. Mishra, and R. Raj, "Insider threat mitigation and access control in healthcare systems," in *2016 IEEE International Conference on Healthcare Informatics (ICHI)*. Chicago, IL, USA: IEEE, 10 2016, DOI: 10.1109/ICHI.2016.11.

[23] K. Fowler, *Data Breach Preparation and Response: Breaches are Certain, Impact is Not*. Syngress Publishin, 2016, ch. 1, pp. 1–26, https://doi.org/10.1016/C2014-0-04209-8.

Appendix A

Abuse cases

Table A.1: Abuse case 1 - Damaging instrument, hardware

Abuse Case 1	Damaging instrument, hardware
Target asset	Instrument
Attack surface	Instrument hardware
Accessibility to attack surface	Physical access to instrument
Window of opportunity	Any time
Resources	physically brute force
Contact Frequency	365
Perceived deterrence	Medium
Perceived ease of attack	Low, the attacker does not need any special knowledge to damage the instrument
Perceived benefit of success	Low, repair time for instrument
Probability of Action	0,90%
Threat Event Frequency (CF * PoA)	3, 285
Loss Event	Lab equipment failure (9,10)
CIA impact breach	Availability
Threat agent	Rogue employee, Criminal organisation
Effort Spent (low / mid / high)	Criminal Organisation: 1 / 3 / 7 Rogue employee: 5 / 10 / 15