Secure Systems Architecture

Design Document

# Group 1

Austin Mundy

Ying Chan

Mathew van Beek

Nova Noor

Shota Kameyama

# Table of Contents

[Table of Contents 2](#_Toc104232528)

[List of Figures 2](#_Toc104232529)

[List of Tables 2](#_Toc104232530)

[Introduction 3](#_Toc104232531)

[List of Vulnerabilities 3](#_Toc104232532)

[System Architecture 4](#_Toc104232533)

[Attack-Defence (AD) Tree 5](#_Toc104232534)

[Physical and Network Access 5](#_Toc104232535)

[IoT Controller 7](#_Toc104232536)

[IoT Client 8](#_Toc104232537)

[The Rationale of Domain Quantification 8](#_Toc104232538)

[Mitigation 9](#_Toc104232539)

[Appendix 11](#_Toc104232540)

[Appendix A: IoT Controller AD Tree analysis using “Difficulty for the Proponent” 11](#_Toc104232541)

[Appendix B: Other Potential Considerations 12](#_Toc104232542)

[References 13](#_Toc104232543)

## List of Figures

[Figure 1: System Architecture of the Smart Lock 5](#_Toc104232400)

[Figure 2: AD Tree Network (Probability of Success domain) 6](#_Toc104232401)

[Figure 3: AD Tree IoT Controller (Probability of Success domain) 7](#_Toc104232402)

[Figure 4: List of top 10 vulnerability types (Feng et al., 2019) 7](#_Toc104232403)

[Figure 5: AD Tree IoT Client: Smart Door 8](#_Toc104232404)

[Figure 6: AD Tree Network (Difficulty for the Proponent) 11](#_Toc104232405)

[Figure 7: AD Tree IoT Controller (Difficulty for the Proponent) 12](#_Toc104232406)

## List of Tables

[Table 1: List of Vulnerabilities 4](#_Toc104232427)

[Table 2: CVSS and Probability scoring on Attack / Vulnerability 9](#_Toc104232428)

[Table 3: Mitigations against vulnerabilities 10](#_Toc104232429)

# 

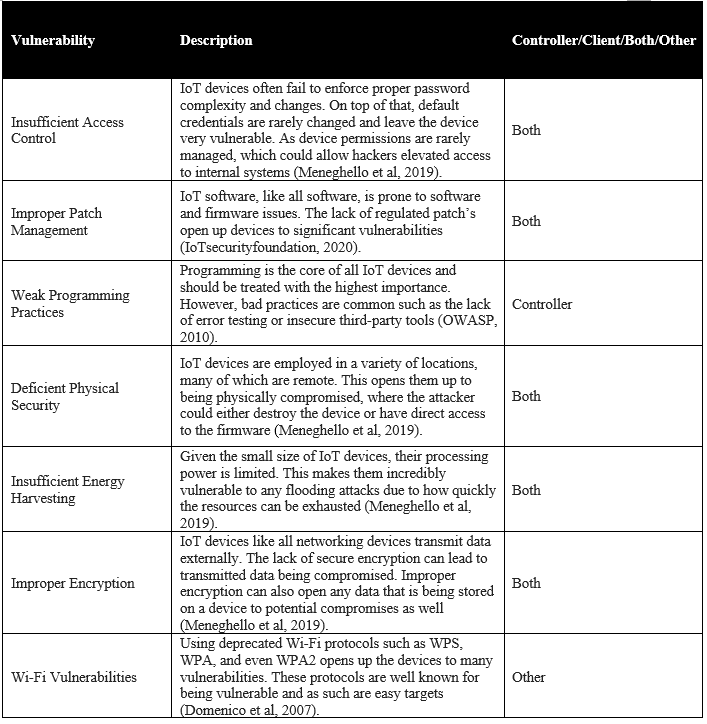
# Introduction

The Internet of Things (IoT) concept embraces the smart home that automates and controls ubiquitous home systems. Smart home devices are proliferating; Pavelić et al. (2018) projected sales from $40 million in 2012 to $26 billion in 2019. Garner (2018) predicted that 25 billion IoT devices would connect to the Internet by 2021. Experts have demonstrated that almost 98% of IoT traffic data is plaintext, disclosing personal and confidential data on the network (Krishna et al., 2021).

# List of Vulnerabilities

Like many networking devices, IoT devices are vulnerable to many cyber threats. The inherent size and lack of power in IoT devices make them particularly difficult to secure. Table 1 lists the known IoT vulnerabilities with references. These vulnerabilities need different mitigation techniques to secure systems.

Table 1: List of Vulnerabilities



# System Architecture

Figure 1 illustrates the system architecture of the smart home using a mobile app and a smart lock to open/close the door lock.

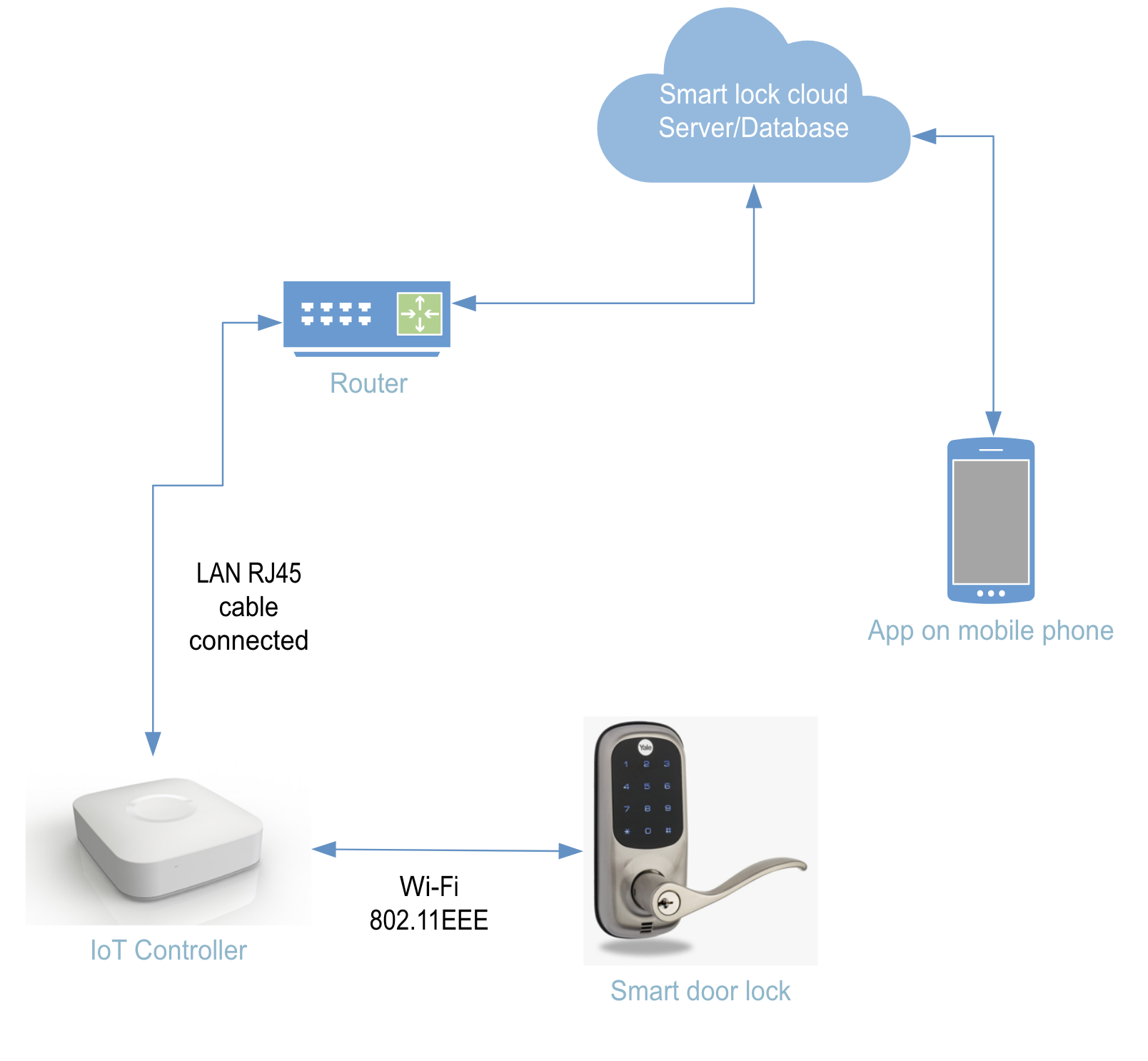


Figure 1: System Architecture of the Smart Lock

# Attack-Defence (AD) Tree

## Physical and Network Access

There are three approaches to attacking IoT devices: physical access, home network access, and Internet access. Figure 2 is an AD tree that illustrates the approaches and mitigations to data theft with the “Probability of Success” domain.

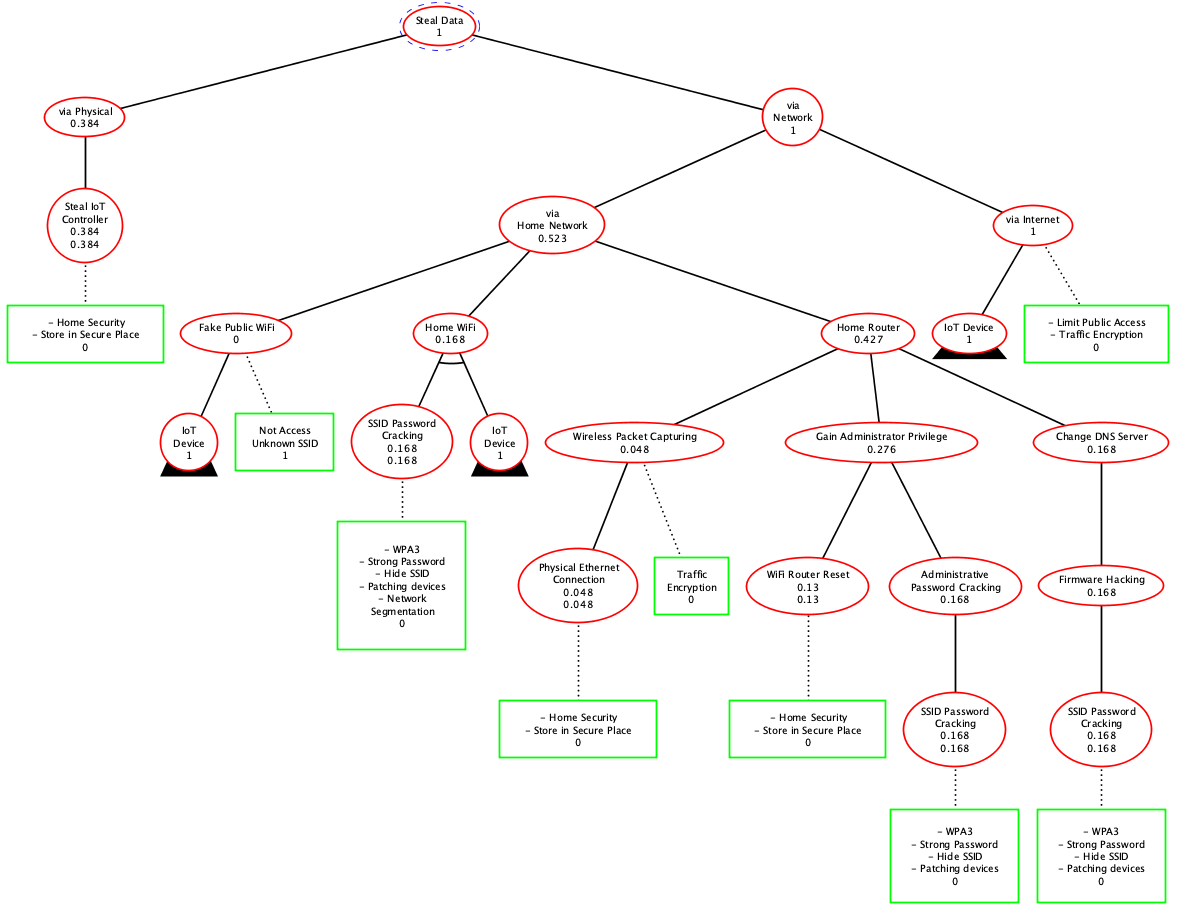


Figure 2: AD Tree Network (Probability of Success domain)

Physically accessing the IoT device to steal requires identifying the target's address and intruding house. Hence, it is more likely to have this attack from an acquaintance.

Gao et al. (2021) detected attacks at 3.92% of the WiFi access points they examined, assuming that the attack rate would be higher if they could find more advanced algorithms to detect attacks. When a target lives nearby, it is relatively easy to hack a wireless network.

Saidi et al. (2020) proved that it could identify millions of IoT devices connected to the Internet, including IP addresses, domain, and port destinations, within minutes. Hence, it is easy to detect IoT devices unless a target stops exposure to the Internet.

## IoT Controller

Figure 3 illustrates the IoT controller vulnerabilities, a subset of the AD tree in Figure 2. As most IoT devices have default ID and password, once URLs and IPs are detected, it is easy to crack the IoT controllers.

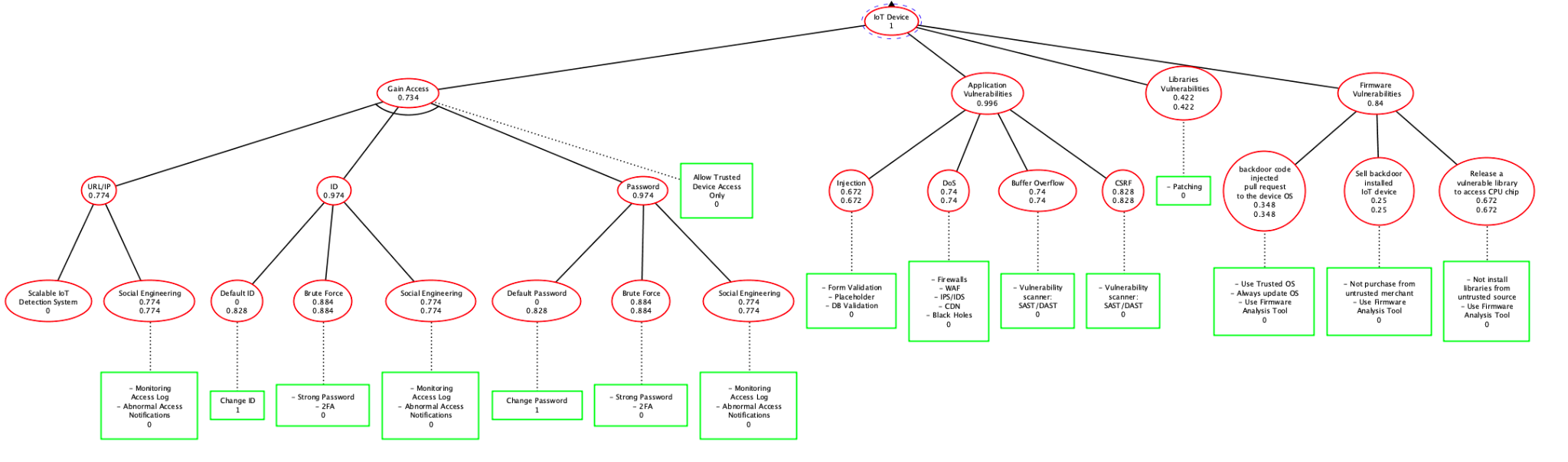


Figure 3: AD Tree IoT Controller (Probability of Success domain)

Examining applications, libraries, and firmware are important to protect from adversaries. Feng et al. (2019) detected 12286 vulnerabilities on IoT devices. The AD tree includes vulnerabilities from the top 10 vulnerabilities in Figure 4.

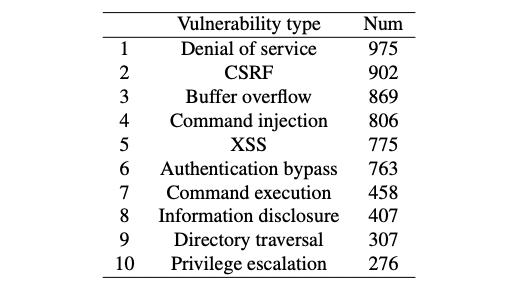


Figure 4: List of top 10 vulnerability types (Feng et al., 2019)

Xie et al. (2017) detected that 2.14 % of the available IoT firmware image has at least one vulnerability. They also found 9,271 issues found in 185 firmware images.

## IoT Client

Figure 5 shows an AD tree for a smart door, showing threats to enter through the door. In the figure, a smart door lock is a lock that attaches to an existing door and is connected via a smartphone connection, either Bluetooth or WiFi (Wilson et al., 2015).

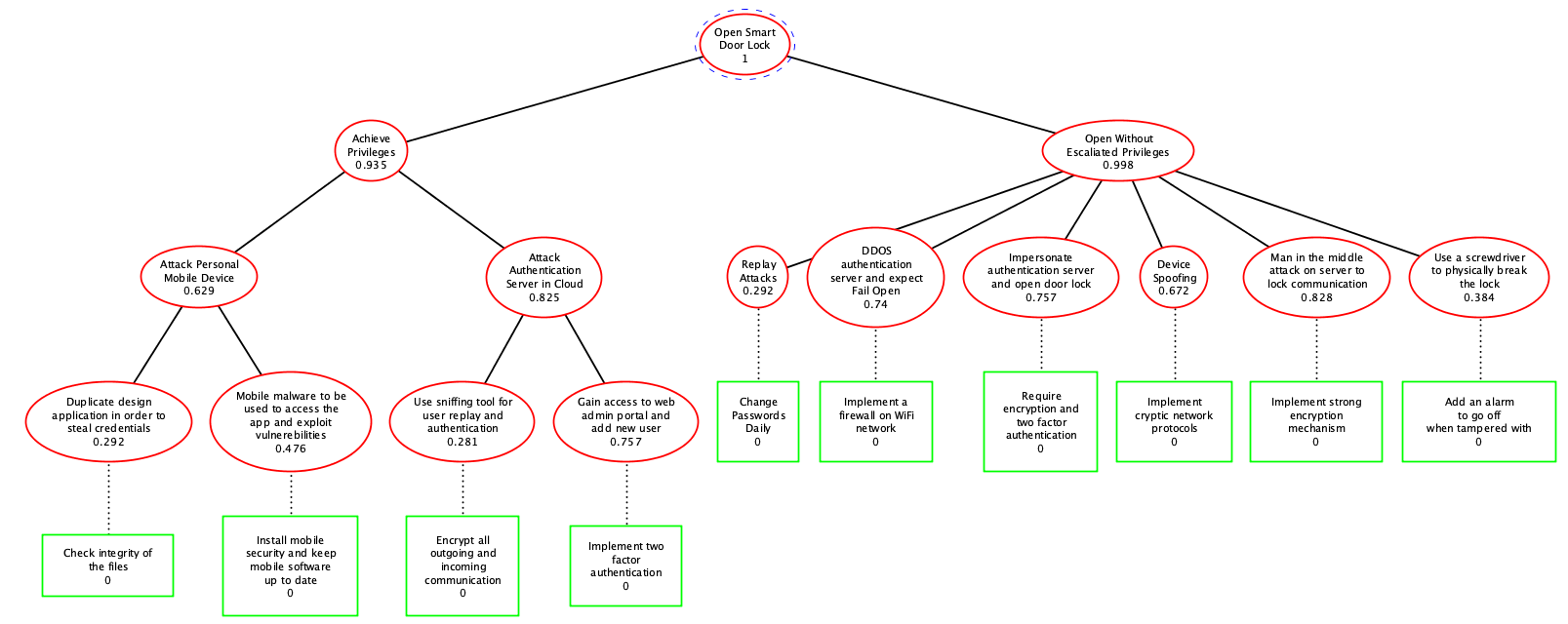


Figure 5: AD Tree IoT Client: Smart Door

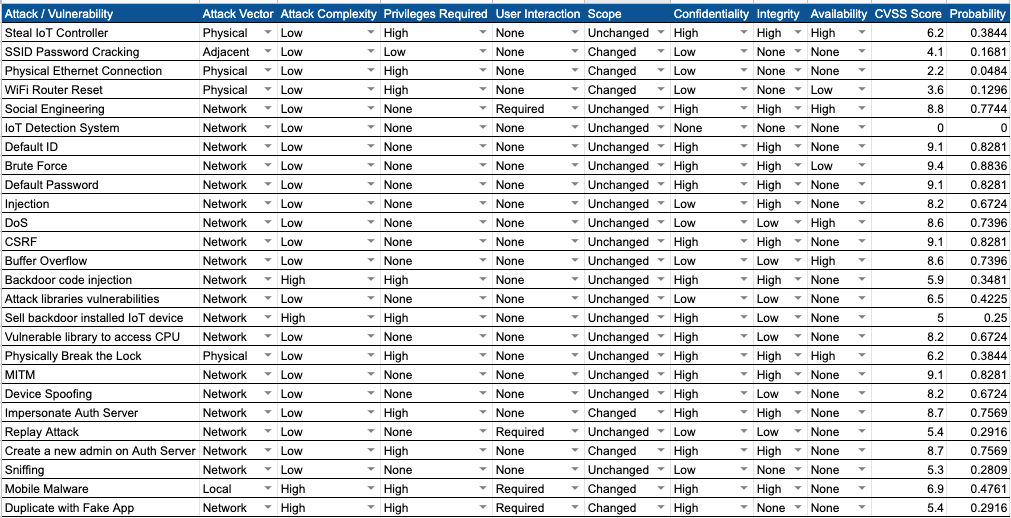
## The Rationale of Domain Quantification

Lippmann et al. (2012) devised a calculation formula for converting CVSS scores to probability using the following formula (Wollaber & Trepagnier, 2016):

.

Table 2 illustrates how the team evaluated each vulnerability and attack using CVSS metrics and converted the CVSS score into the probability of compromise using the formula above.

Table 2: CVSS and Probability scoring on Attack / Vulnerability

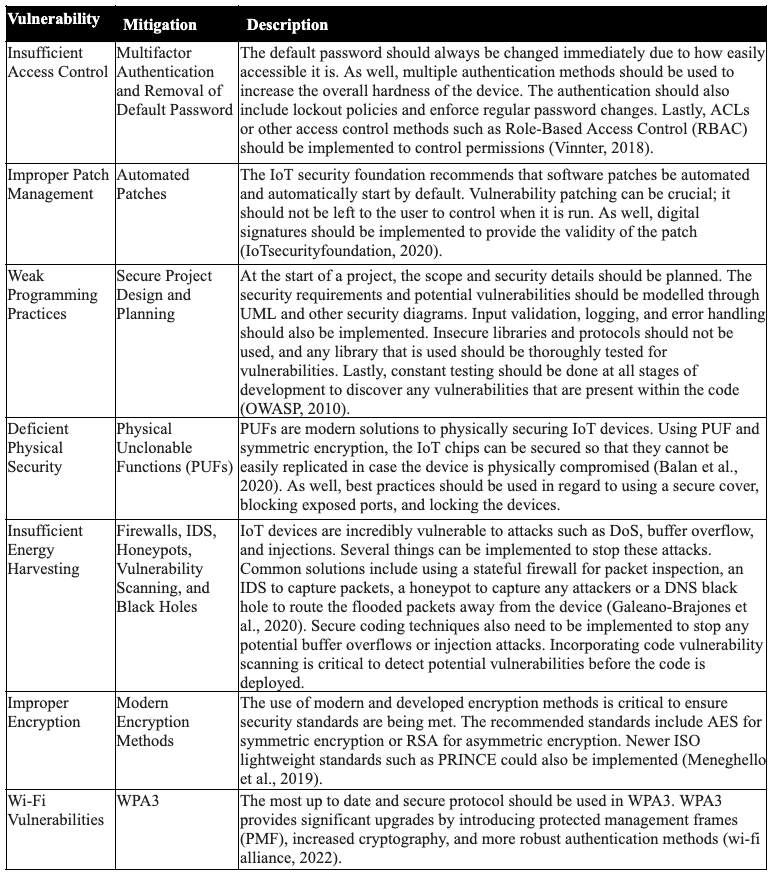


Against countermeasures, the team rated 1 if the vulnerability is entirely resolved by the countermeasures and 0 on the remaining.

# Mitigation

This paper described IoT related threats and vulnerabilities, resulting in a 100% Probability of Success in the AD Tree, which requires proper mitigation techniques. Table 3 suggests how each threat can be mitigated.

Table 3: Mitigations against vulnerabilities



# Appendix

## Appendix A: IoT Controller AD Tree analysis using “Difficulty for the Proponent”

Figure 6 is an attack-defence (AD) tree that illustrates the approaches and mitigations to data theft with the “difficulty for the proponent” domain. Physically accessing the IoT device or power suspension requires identifying the address of the target and intruding house, which require much effort, rating high difficulty. When a target is living nearby, it is relatively easy to hack a wireless network, which leads to a rating low difficulty in Home Network hacking. Saidi et al. (2020) proved that it can identify millions of IoT devices connected to the Internet, including IP addresses, domain, and port destinations, within minutes. Hence, it is easy to detect IoT devices unless a target stops exposure to the Internet.

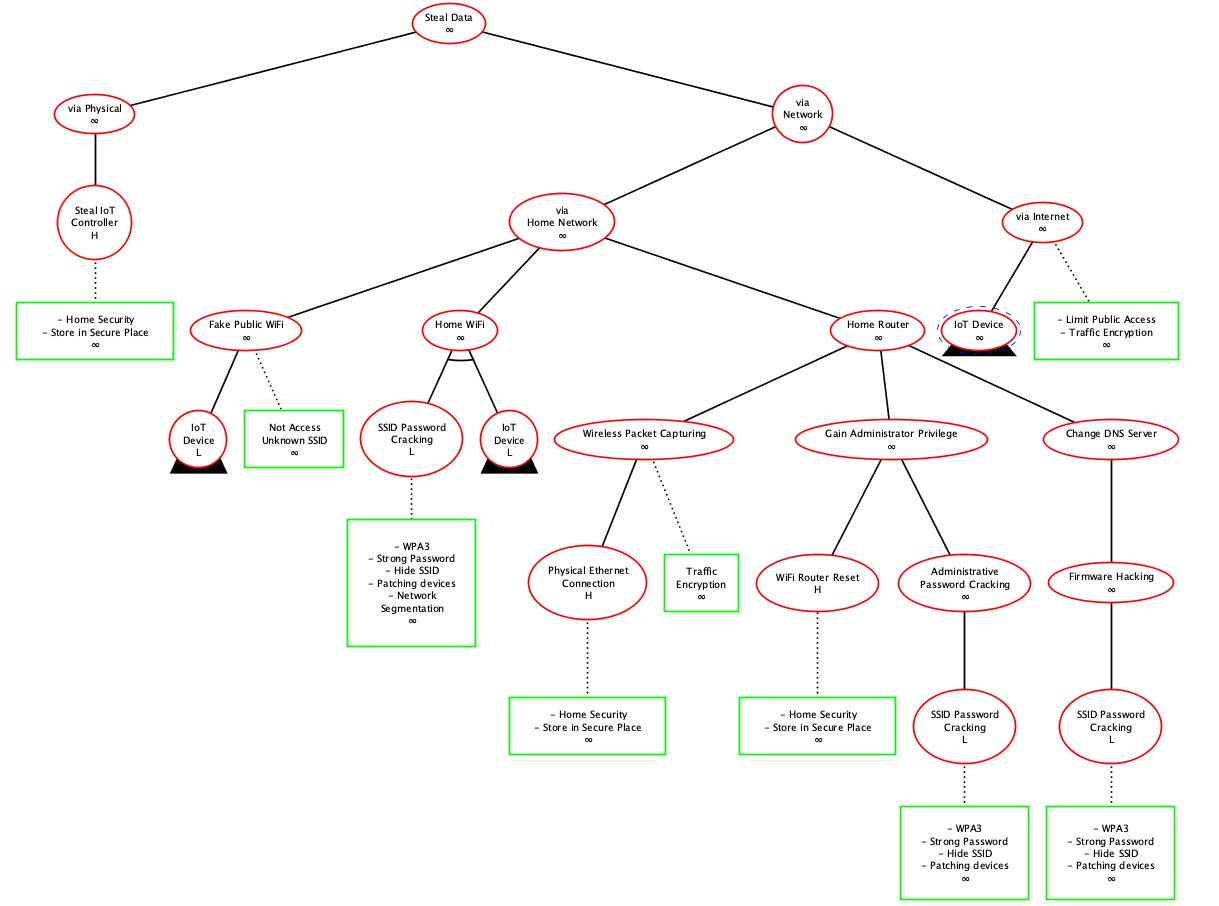


Figure 6: AD Tree Network (Difficulty for the Proponent)

Figure 7 illustrates the AD tree pertaining to the vulnerabilities of the IoT controller. As most IoT devices have default ID and password, once URL and IP are detected using Saidi et al.’s (2020) detection system, it is easy to crack the IoT controller. Against application vulnerabilities, Feng et al. (2019) detected 12286 vulnerabilities on IoT devices, including 975 Denial of Service (DoS) vulnerabilities, 869 buffer overflow vulnerabilities, and 806 injection vulnerabilities, considering it relatively easy to attack the device. Libraries and firmware vulnerabilities require additional effort to contribute by adding a backdoor to the libraries and firmware; hence difficulty ratings are high.

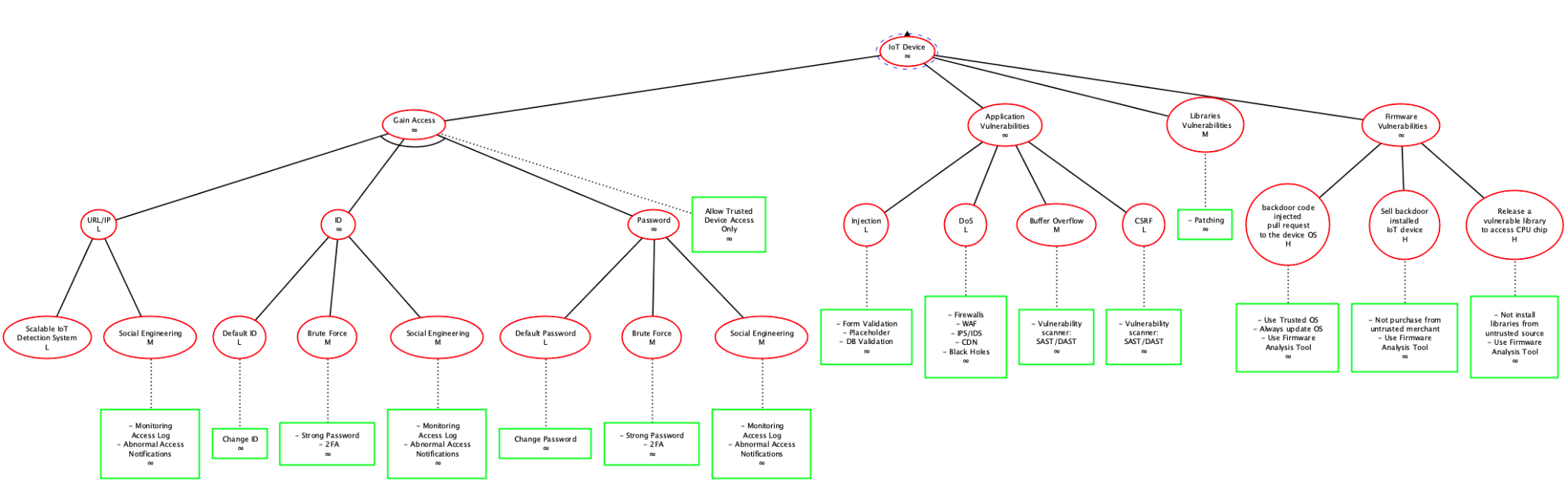


Figure 7: AD Tree IoT Controller (Difficulty for the Proponent)

However, as the constraints of the Luxembourg AD Tree software do not allow us to add values to the countermeasures, the parent instances automatically change to an infinite value.

## Appendix B: Other Potential Considerations

IoT devices support different communication protocols such as WiFi (IEEE 802.11), Bluetooth (IEEE 802.15), BLE, infrared, RFID and ZigBee (IEEE 802.15.4). Pallavi & Narayanan (2019) alerted that the BLE protocol is, especially BLE 4.0 and 4.1, vulnerable to MITM attack so the integrity and confidentiality of data are at risk. ZigBee defines a suite of IEEE 802.15.4 based protocols that enable communications with low-power devices over short distances. Efforts have been made in enhancing ZigBee security with some of the current efforts, however, an insecure implementation of cryptography for exchanging data between devices is a well-known vulnerability (Asonye et al., 2020). Although the AD tree focused on Wi-Fi (IEEE 802.11) protocol, as most IoT devices support multiple communication protocols, it is recommended to consider other vulnerabilities on different communication channels.

# References

1. Asonye, E.A., Anwuna, I. & Musa, S.M. (2020) ‘Securing ZigBee IoT Network Against HULK Distributed Denial of Service Attack’, *2020 IEEE 17th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*. Charlotte, NC, USA, 14-16 December. IEEE: 156-162. DOI: 10.1109/HONET50430.2020.9322808.
2. Balan, A., Balan, T., Cirstea, M. & Sandu, F. (2020) A PUF based cryptographic security solution for IoT systems on chip. *EURASIP Journal on Wireless Communications and Networking* 1(231): 1-22. DOI: https://doi.org/10.1186/s13638-020-01839-6
3. Domenico Aime, M., Calandriello, G. & Lioy, A. (2007) Dependability in Wireless Networks: Can We Rely on WiFI? *Journal of IEEE Security & Privacy* 5(1): 23-29. Available from:<https://ieeexplore.ieee.org/document/4085590> [Accessed 14 May 2022].
4. Feng, X., Liao, X., Wang, X., Wang, H., Li, Q., Yang, K., Zhu, H. & Sun, L. (2019) 'Understanding and securing device vulnerabilities through automated bug report analysis', *SEC'19: Proceedings of the 28th USENIX Conference on Security Symposium*. Santa Clara, California, 14-16 August. USENIX Association.
5. Galeano-Brajones, J., Carmona--Murillo, J., Valenzuela-Valdes, J. & Luna-Valero, F. (2020) Detection and Mitigation of DoS and DDoS Attacks in IoT-Based Stateful SDN: An Experimental Approach. *Sensors* 20(3): 816. DOI: https://doi.org/10.3390/s20030816
6. Gao, D., Lin, H., Li, Z., Qian, F., Chen, Q. A., Qian, Z., Liu, W., Gong, L. & Liu, Y. (2021) ‘A nationwide census on wifi security threats: prevalence, riskiness, and the economics’, *MobiCom ‘21 Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*. New Orleans Louisiana, United States, 25-29 October. New York: Association for Computing Machinery. 242-255.
7. Gartner (2018) Gartner Identifies Top 10 Strategic IoT Technologies and Trends. Available from: https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends [Accessed 15 May 2022].
8. IoTsecurityfoundation (2020) Consumer IoT Security Quick Guide: Software Updates. Available from: https://www.iotsecurityfoundation.org/wp-content/uploads/2020/08/IoTSF-Updates-QG\_FINAL.pdf [Accessed 14 May 2022].
9. Krishna, R.R., Priyadarshini, A., Jha, A.V., Appasani, B., Srinivasulu, A. & Bizon, N. (2021) State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions. *Sustainability* 13(16):9463. DOI: 10.3390/su13169463
10. Lippmann, R. P., Riordan, J. F., Yu, T. H., & Watson, K. K. (2012) Continuous security metrics for prevalent network threats: introduction and first four metrics. *Massachusetts Inst of Tech Lexington Lincoln Lab*. Available from: <https://apps.dtic.mil/sti/pdfs/AD1098014.pdf> [Accessed 21 May 2022].
11. Pallavi, S. & Narayanan, V.A. (2019) ‘An Overview of Practical Attacks on BLE Based IOT Devices and Their Security’, *2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS).* Coimbatore, India, 15-16 March. IEEE:694-698. DOI: 10.1109/ICACCS.2019.8728448.
12. Pavelić, M., Lončarić, Z., Vuković, M. & M. Kušek (2018) ‘Internet of Things Cyber Security: Smart Door Lock System,’ *2018 International Conference on Smart Systems and Technologies (SST)*. Osijek, Croatia, 10-12 October. IEEE:227-232. DOI: 10.1109/SST.2018.8564647.
13. Meneghello, F., Calore, M., Zucchetto, D., Polese, M. & Zanella, A. (2019) IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices. Available from: https://polese.io/assets/pdf/2019\_menegheelo\_iot.pdf [Accessed 12 May 2022].
14. OWASP (2010) OWASP Secure Coding Practices Quick Reference Guide. Available from: https://owasp.org/www-pdf-archive/OWASP\_SCP\_Quick\_Reference\_Guide\_v2.pdf [Accessed 14 May 2022].
15. Saidi, S. J., Mandalari, A. M., Kolcun, R., Haddadi, H., Dubois, D. J., Choffnes, D., Smaragdakis, G. & Feldmann, A. (2020) ‘A haystack full of needles: Scalable detection of IoT devices in the wild’, *Proceedings of the ACM Internet Measurement Conference*. Virtual Event, the United States, 27-29 October. New York: Association for Computing Machinery. 87-100.
16. Vinnter. (2018) Access Control & IoT Security: Challenges and Opportunities. Available from: https://vinnter.se/access-control-iot-security-challenges-and-opportunities/ [Accessed 13 May 2022].
17. Wi-Fi Alliance (2022) Discover Wi-Fi Security. Available from: https://www.wi-fi.org/discover-wi-fi/security [Accessed 13 May 2022].
18. Wilson, C., Hargreaves, T. & Hauxwell-Baldwin, R. (2015) Smart Homes and Their Users: A Systematic Analysis and Key Challenges. *Personal Ubiquitous Comput*. 19:463-476. DOI: 10.1007/s00779-014-0813-0.
19. Wollaber, A. B., & Trepagnier, P. C. (2016) Exploit Probabilities Conditioned on CVSS Scores. *MIT Lincoln Laboratory Lexington United States*. Available from: <https://apps.dtic.mil/sti/pdfs/AD1098014.pdf> [Accessed 21 May 2022].
20. Xie, W., Jiang, Y., Tang, Y., Ding, N., Gao, Y. (2017) ‘Vulnerability Detection in IoT Firmware: A Survey’, *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS).*14-16 December. IEEE: 769-772. DOI: 10.1109/ICPADS.2017.00104.