Design Document

Secure Software Architecture

Group 2:

Adrian Boscu

Gurkan Huray

Haroun Fujah

Muhammad Nasim Akbary

Michael Geiger

Zihaad Khan

Table of Contents

INTRODUCTION **3**

VULNERABILITIES **4**

AD TREES **5**

Client – AD Tree **5**

Controller – AD Tree **10**

DISCUSSION **13**

Method **13**

Client Device **14**

Controller Hub **14**

MITIGATIONS **15**

REFERENCES **17**

APPENDICES **20**

INTRODUCTION

A smart home can be defined as “a residence equipped with a communications network, linking sensors, domestic appliances and devices, that can be remotely monitored, accessed or controlled” by a user (Balta-Ozkan et al., 2014:66). Figure 1 below was extracted from Bugeja (2021) and represents a smart home architecture. Smart (IoT) devices are connected via Wi-Fi provided by the gateway. A user can access these devices via a smart phone or web-based interface. These solutions are commonly enabled by cloud providers.

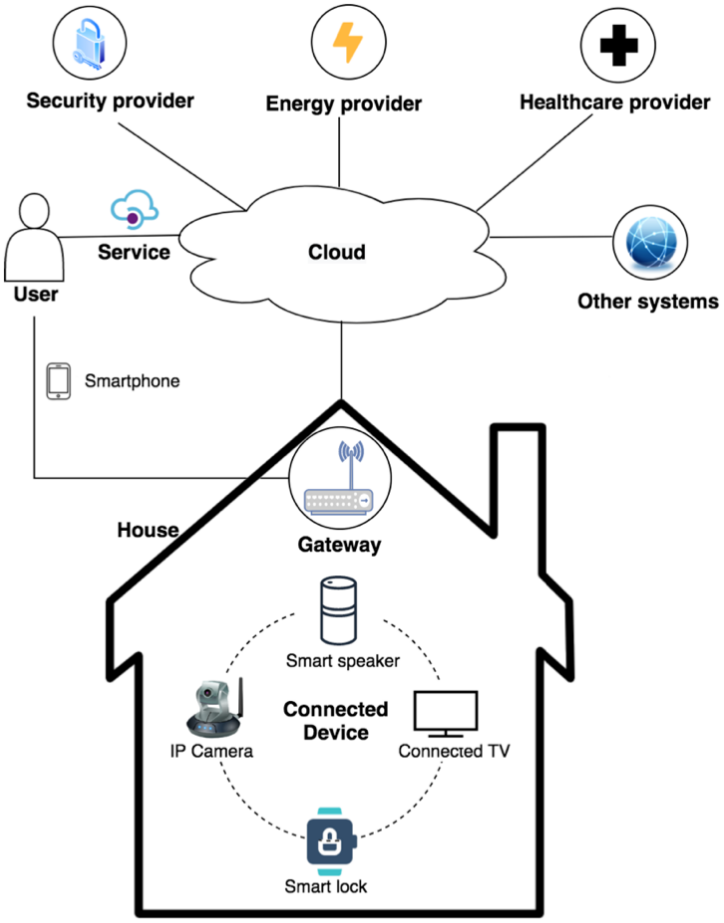

Figure 1: Smart connected home architecture

While smart homes provide great benefits, they can be susceptible to various vulnerabilities as listed in the section below.

VULNERABILITIES

Various vulnerabilities have been identified as listed in Table 2 of the Appendices. The top 9 vulnerabilities (not in order of precedence) are summarised in Figure 2 below:

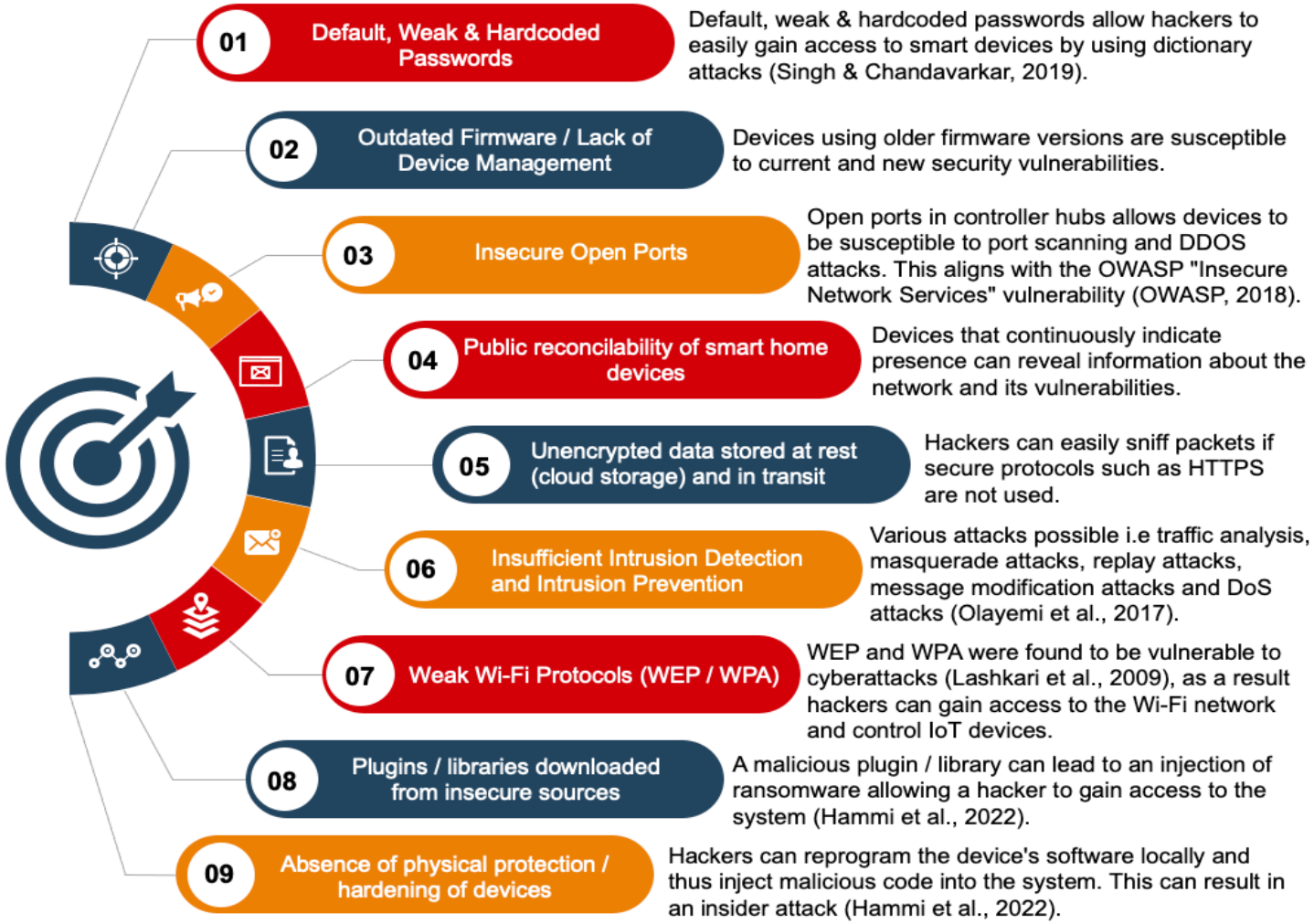

Figure 2: IoT Client & Controller Vulnerabilities

AD TREES

Client – AD Tree

The AD (Attack Defence) Trees for the Client and Controller Hubs are represented in Figures 3-10 below.

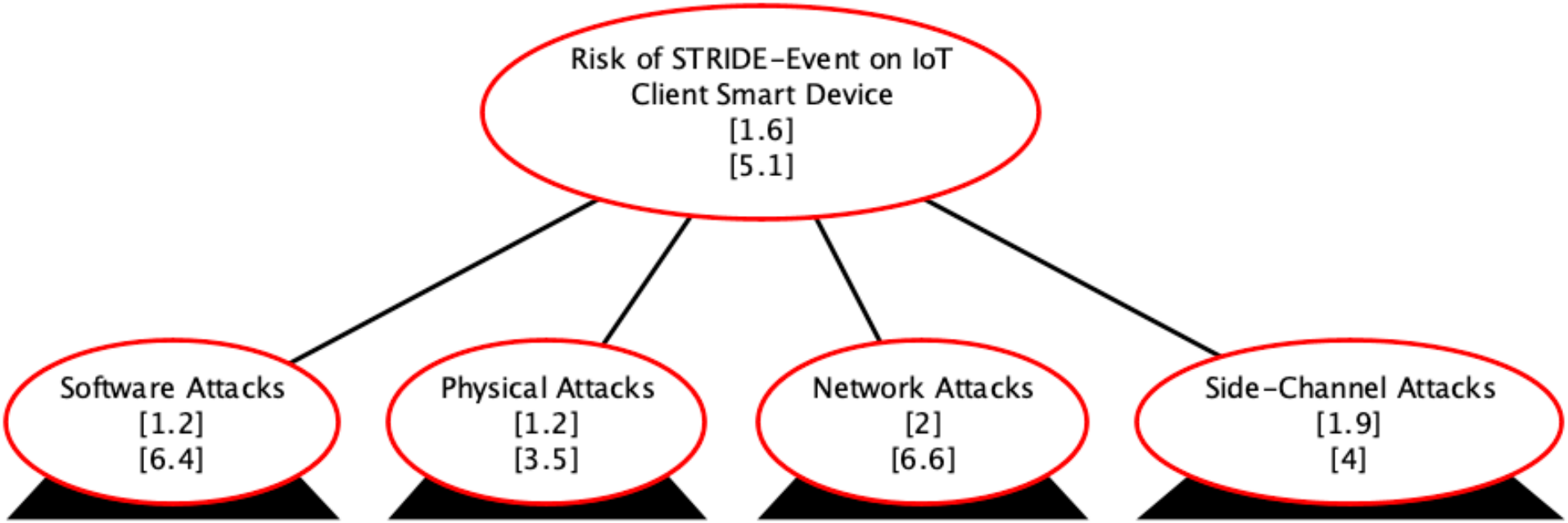

Figure 3: Client Device - Threat Overview

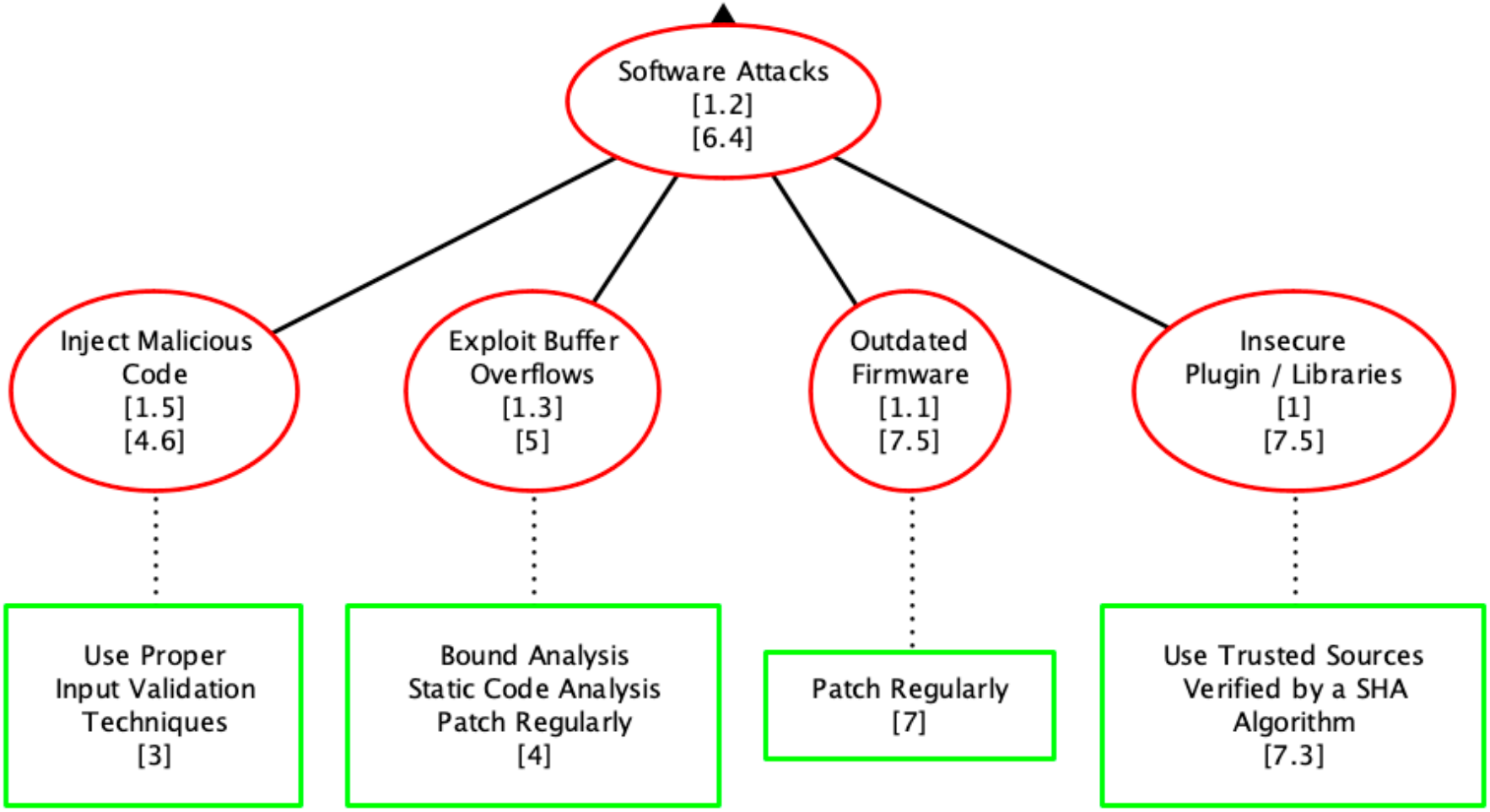

Figure 4: Client Device Software Attacks - ADTree

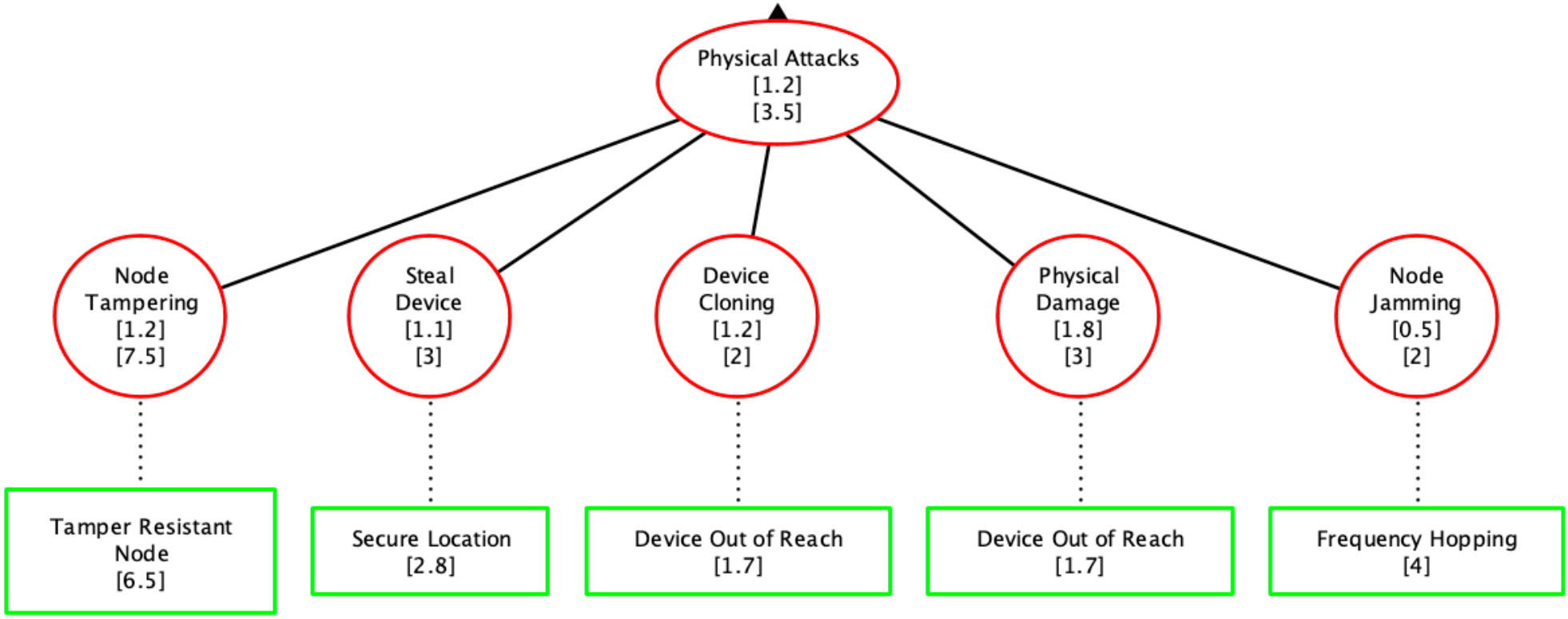

Figure 5: Client Device Physical Attacks - ADTree

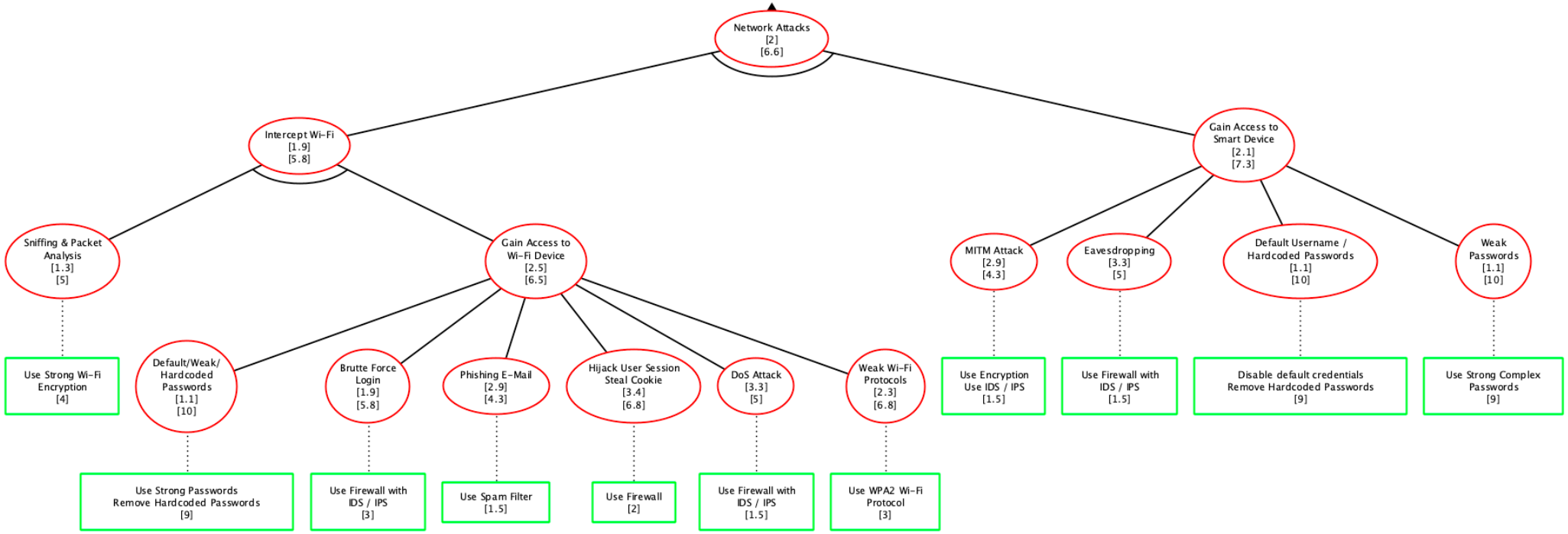

Figure 6: Client Device Network Attacks - ADTree

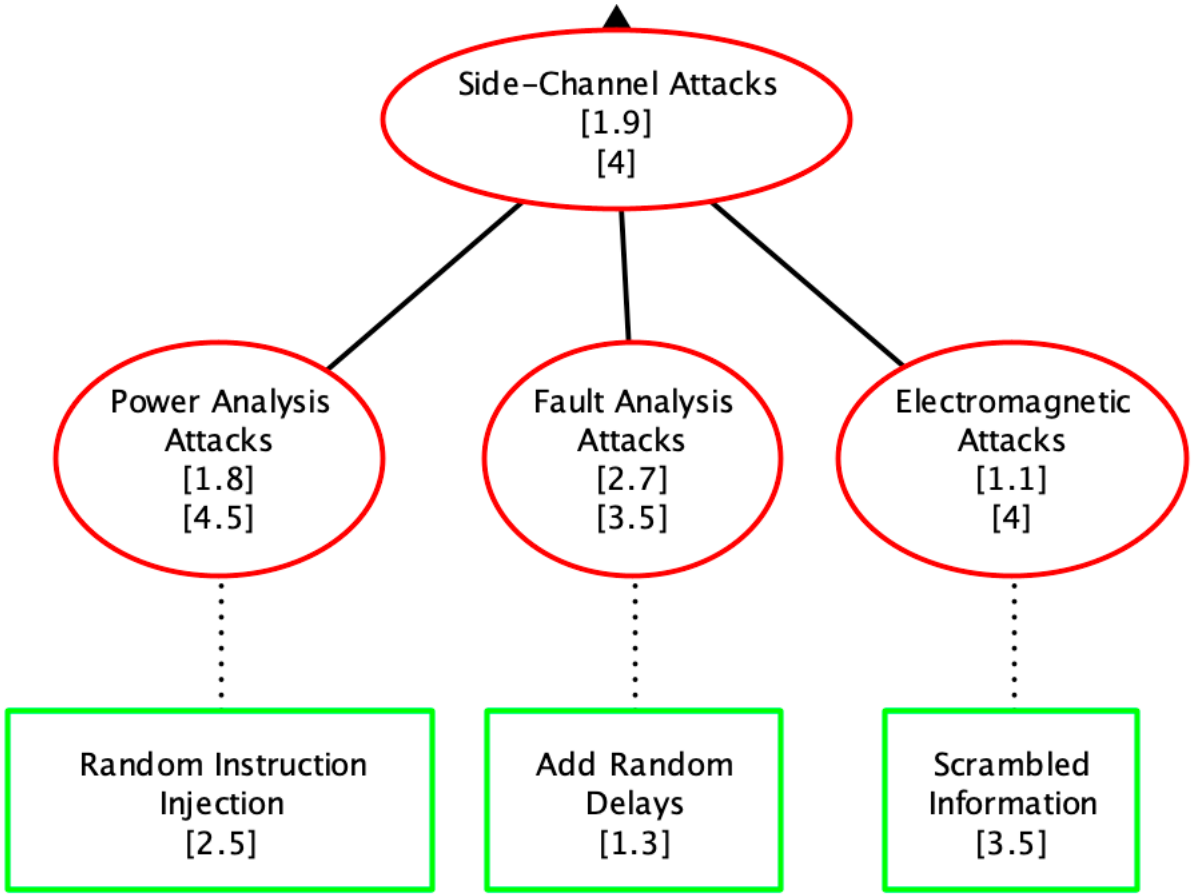

Figure 7: Client Device Side-Channel Attacks - ADTree

Controller – AD Tree

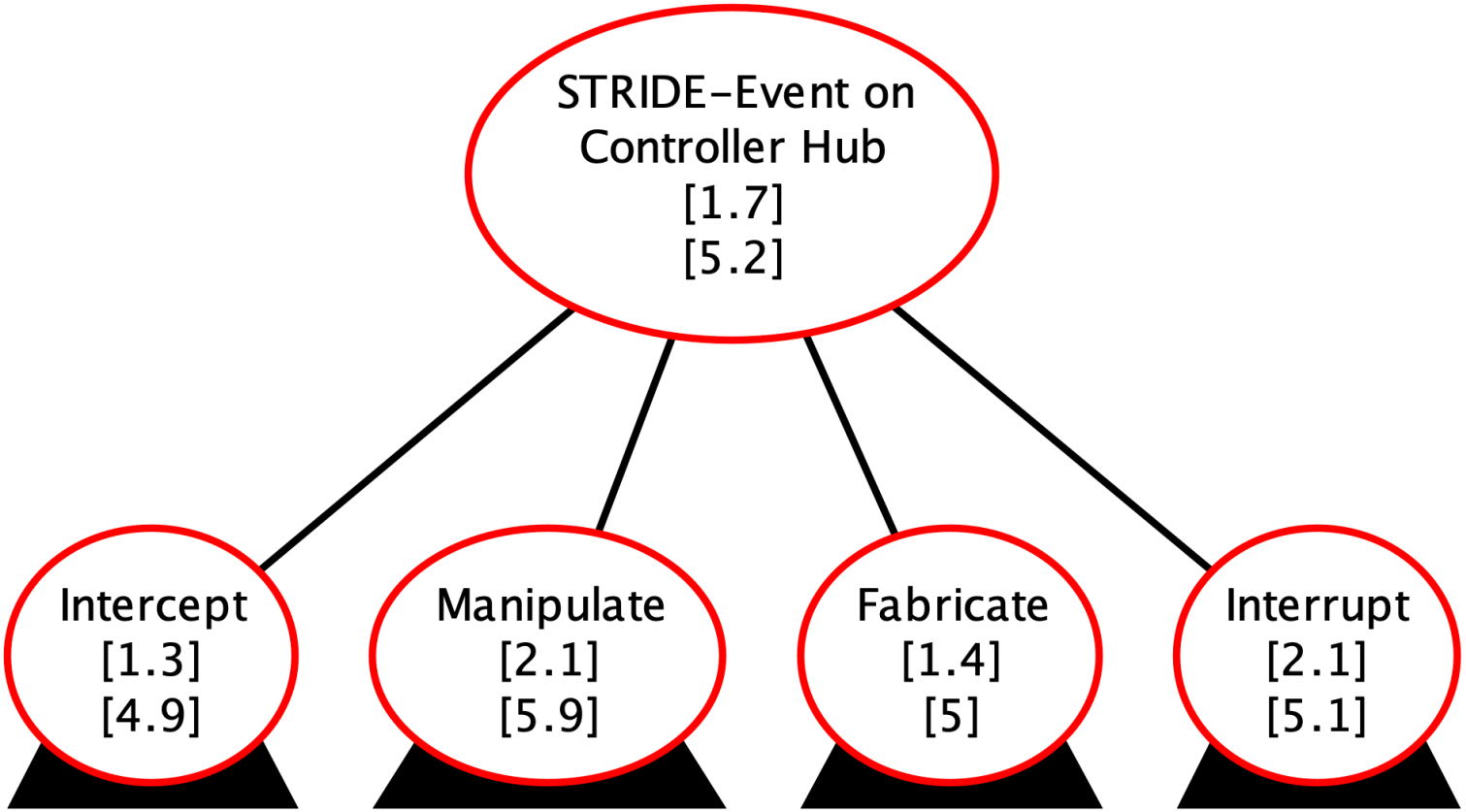

Figure 8: Controller Hub Threat Overview

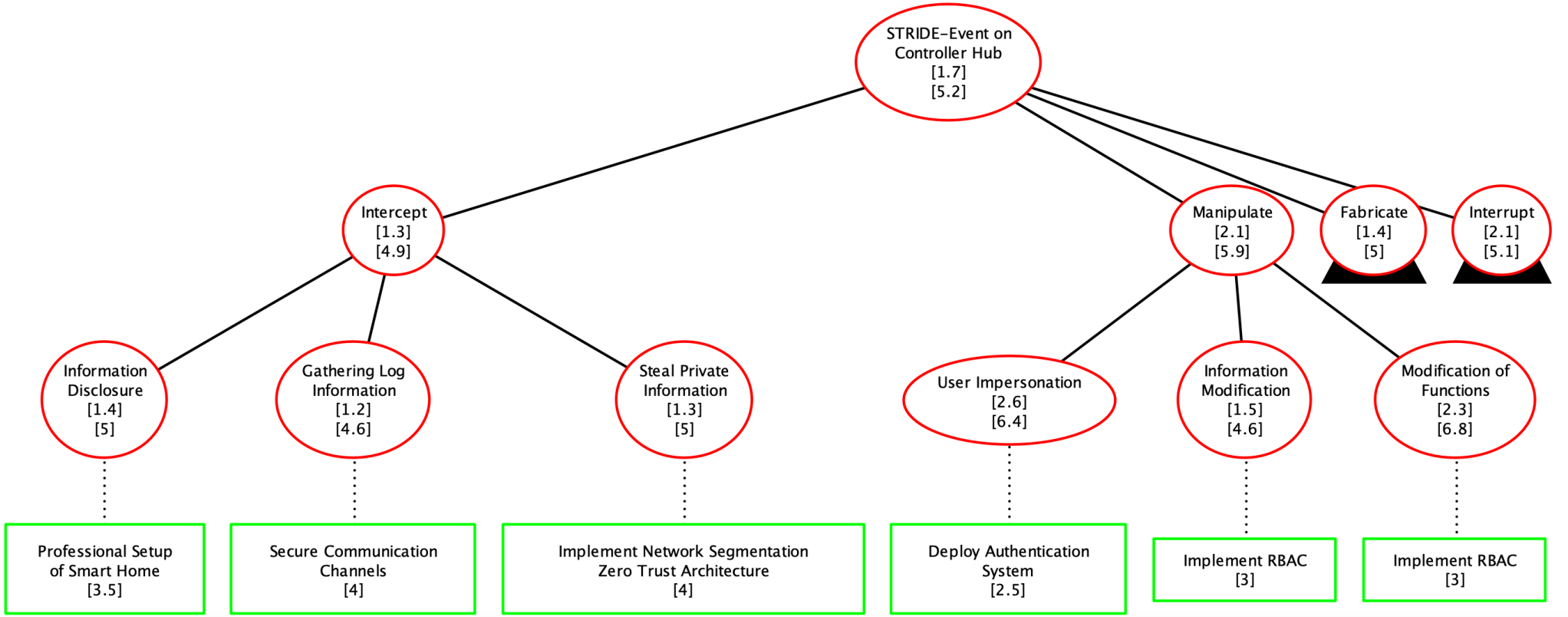

Figure 9: Controller Hub - Intercept & Manipulate

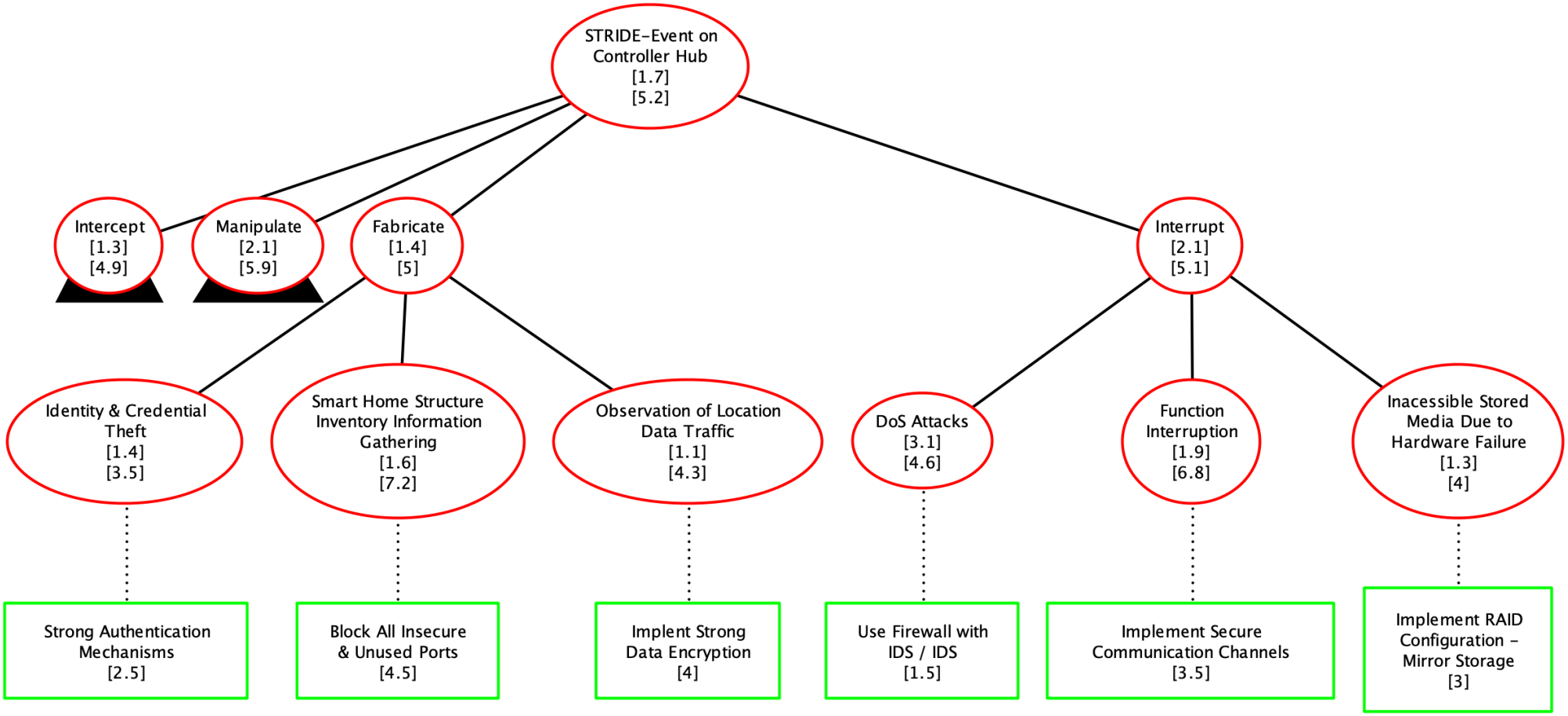

Figure 10: Controller Hub - Fabricate & Interrupt

DISCUSSION

IoT devices can be classified into various domains in which multiple vulnerabilities exist. The vulnerability scoring for this exercise was performed using the Common Vulnerability Scoring System (CVSS). The qualitative severity rating scale used is described in Table 1 below:

Table 1: CVSS Rating Scale (Santos, 2019)

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

A similar method was used by Risvi et al. (2019) where CVSS scores for various domains (healthcare, commerce and home-automation) were determined. The 'probability of success' domain was selected for both Client and Controller devices using the ADTree tool. This method was selected as it provided the ability to estimate mitigation values as well as calculate average ratings for the various attack areas.

Method

The following method was used to determine all the values represented in the ADTree. Figure 1 below represents an example of a sub tree for Weak Passwords. The CVSS rating for this vulnerability was found to be 10 (CVE Details, 2022). The mitigation value was estimated to be 9 as strong passwords (upper case, lower case, mixture of numbers and special characters) are to be used. The rating after mitigation was taken

to be 1.1 (10/9 = 1.1). By using the above method, all values represented in the ADTree were determined.

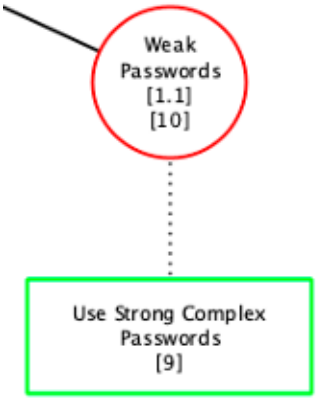

Figure 11: Subtree Example

Client Device

An average risk score for each attack area i.e. Software, Physical, Network and Side-Channel was calculated. It was found that Network Attacks produced the highest rating with a CVSS score of **5.1** without mitigations and **1.6** with mitigations. This falls in the 'Low' rating category as per Table 1 above. Su et al. (2022) further validates that network attacks are amongst the majority of attacks seen in IoT devices.

Controller Hub

An average risk score for each attack area i.e. Intercept, Manipulate, Fabricate and Interrupt was calculated. It was found that the 'Manipulate' and 'Interrupt' trees produced the highest ratings i.e. **5.9** and **5.2** without mitigations respectively. After applying the mitigation criteria, these values dropped to **2.1** for both attack areas which falls in the 'Low' rating category.

MITIGATIONS

Figure 12 below represents mitigation actions for the various vulnerabilities identified.

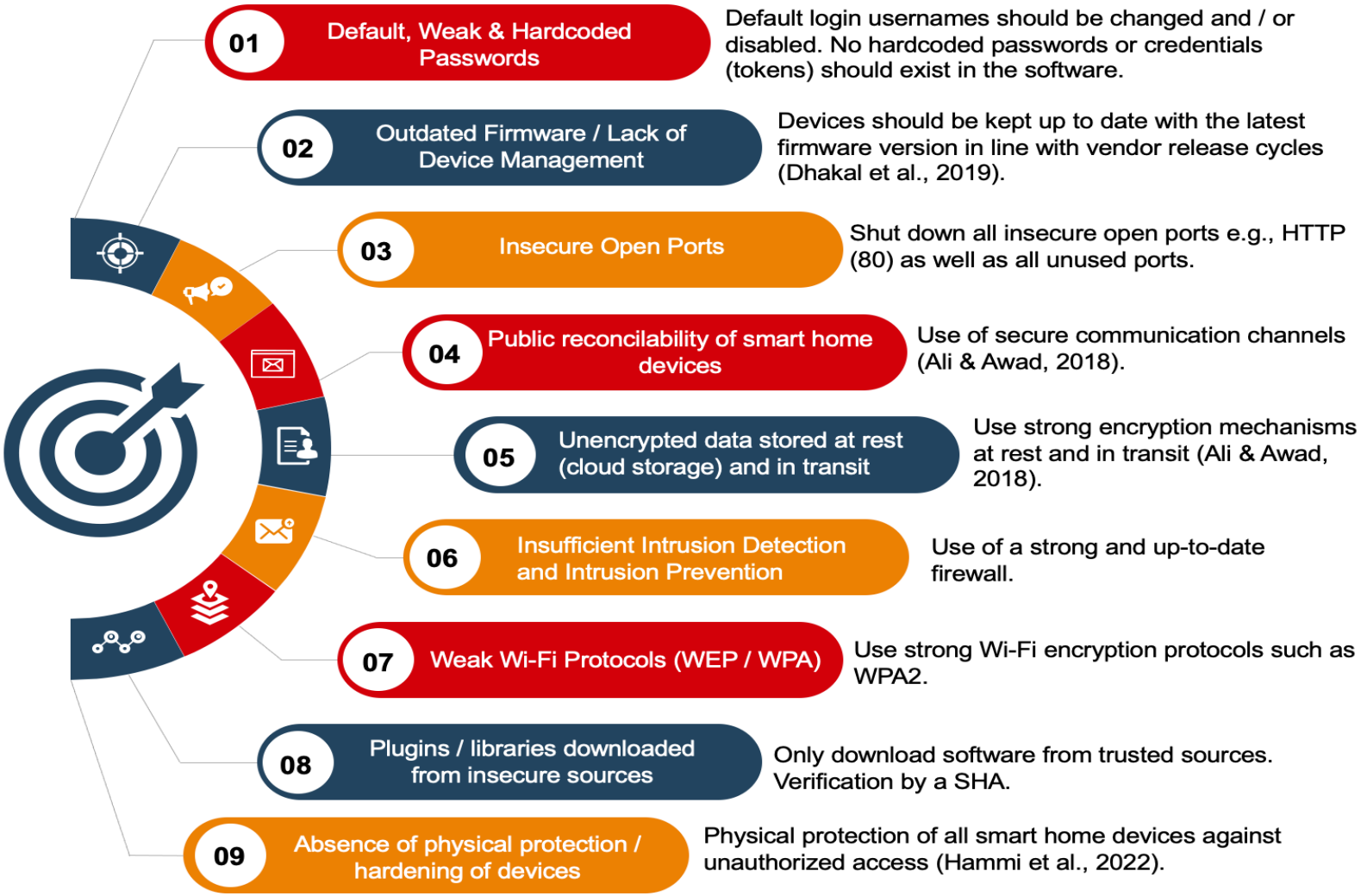

Figure 12: Mitigation Actions

While performing the above exercise, some limitations were also discovered. These are as follows (Haritha and Lavanya, 2017):

- Enabling encryption on IoT devices require significant CPU speeds, this may not be possible as IoT devices are battery powered.
- Memory restriction may also pose a problem to implement security measures, IoT devices usually have low memory assigned.
- Most IoT devices use lightweight operating systems and cannot be patched or update libraries.

REFERENCES

Ali, B. & Awad, A. I. (2018) Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes. *Sensors*. 18 (3): 817. Available from: https://www.mdpi.com/1424-8220/18/3/817 [Accessed 20 May 2022].

Ali, K. & Askar, S. (2021) Security Issues and Vulnerability of IoT Devices. *International Journal of Science and Business.* 5(3): 101-115. Available from: https://ijsab.com/wp-content/uploads/690.pdf [Accessed 12 May 2022].

Balta-Ozkan, N., Boteler, B., & Amerighi, O. (2014) European smart home market development: Public views on technical and economic aspects across the United Kingdom, German and Italy. *Energy Research & Social Science*. 3: 65–77. Available from: https://www.sciencedirect.com/science/article/abs/pii/S2214629614000851 [Accessed 21 May 2022].

Bugeja, J. (2021) On Privacy and Security in Smart Connected Homes. Available from: https://www.um.edu.mt/library/oar/handle/123456789/76297 [Accessed 14 May 2022].

Chang, S. & Nam, K. S. (2019) Spatial Design Direction of Smart Home in IoT Paradigm. *2nd World Symposium on Communication Engineering (WSCE).* 74-77. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9041130 [Accessed 19 May 2022].

Chang, Z. (2019) IoT Device Security: Locking Out Risks and Threats to Smart Homes. *Trend Micro Research*. Available from: https://documents.trendmicro.com/assets/white_papers/IoT-Device-Security.pdf [Accessed 18 May 2022].

CVE Details (2022) Vulnerability Details: CVE-2022-1039. Available from: https://www.cvedetails.com/cve/CVE-2022-1039/ [Accessed 22 May 2022].

Dhakal, S., Jaafar, F. & Zavarsky, P. (2019) Private Blockchain Network for IoT Device Firmware Integrity Verification and Update. *IEEE 19th International Symposium on High Assurance Systems Engineering (HASE).* 164-170. Available from: https://ieeexplore.ieee.org/abstract/document/8673027 [Accessed 20 May 2022].

Divatia, A. (2019) The Fact and Fiction of Homomorphic Encryption. *Dark Reading*. Available from: https://www.darkreading.com/attacks-breaches/the-fact-and-fiction-of-homomorphic-encryption [Accessed 21 May 2022].

Hammi, B., Zeadally, S., Khatoun, R. & Nebhen, J. (2022) Survey on smart homes: Vulnerabilities, risks, and countermeasures. *Computers & Security*. 117: 102677. Available from: https://www.sciencedirect.com/science/article/pii/S016740482200075X [Accessed 18 May 2022].

Haritha, A. & Lavanya, A. (2017) Internet of Things: Security Issues. *International Journal of Engineering Science Invention*. 6(11): 45-52. Available from: http://www.ijesi.org/papers/Vol(6)11/Version-2/G0611024552.pdf [Accessed 21 May 2022].

Kerman, A., Borchert, O., Rose, S., Division, Eileen, & Tan, A. (2020) Implementing a zero-trust architecture. National Institute of Standards and Technology. Available from: https://www.nccoe.nist.gov/sites/default/files/legacy-files/zta-project-description-final.pdf [Accessed 22 May 2022].

Lashkari, A. H., Danesh, M. M. S., & Samadi, B. (2009) A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). *2nd IEEE international conference on computer science and information technology*. 48-52. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5234856 [Accessed 23 May 2022].

Monaswarnalakshmi, S. & Sai Aravindhan, C. (2018) Multifactor Authentication in IoT devices for ensuring secure cloud storage in smart banking. *International Research Journal of Engineering and Technology*. 5(3): 1307-1311. Available from: https://www.irjet.net/archives/V5/i3/IRJET-V5I3296.pdf [Accessed 21 May 2022].

Neil, I. (2018) *CompTIA Security+ Certification Guide: Master IT security essentials and exam topics for CompTIA Security+ SY0-501 certification*. *Packt Publishing Ltd.* Available from: https://scholar.google.com/scholar?hl=de&as_sdt=0%2C5&q=Neil%2C+I.%2C+%282018%29.+CompTIA+Security+%2B+Certification+Guide.+Birmingham%2C+United+Kingdom%3A+Packt+Publishing&btnG [Accessed 19 May 2022].

Olayemi, O., Antii, V., Keijo, H. & Pekka, T. (2017) Security issues in smart homes and mobile health system: threat analysis, possible countermeasures and lessons learned. *International Journal on Information Technologies and Security*. 9(1): 31-52. Available from: https://erepo.uef.fi/handle/123456789/5124 [Accessed: 17 May 2022].

OWASP (2018) OWASP Internet of Things Top 10. Available from: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf [Accessed 19 May 2022].

Rizvi, S., McIntyre, N. & Ryoo, J. (2019) Computing security scores for IoT device vulnerabilities. *International Conference on Software Security and Assurance (ICSSA).* 52-59. Available from: https://ieeexplore.ieee.org/abstract/document/9307685 [Accessed 19 May 2022].

Rose, S., Borchert, O., Mitchell, S. & Connelly, S. (2020) Zero Trust Architecture. *National Institute of Standards and Technology*. Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf [Accessed 20 May 2022].

Singh Verma, R. & Chandavarkar, B. R. (2019) Hard-coded Credentials and Web Service in IoT: Issues and Challenges. *International Journal of Computational Intelligence & IoT*. 2(3): 565-570. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3358283 [Accessed 21 May 2022].

Su, J., He, S., & Wu, Y. (2022) Features selection and prediction for IoT attacks. *High-Confidence Computing*. 2(2): 100047. Available from: https://www.sciencedirect.com/science/article/pii/S2667295221000374 [Accessed 20 May 2022].

APPENDICES

Table 2: Threats, Rationale & Mitigations

Threats / Vulnerability	Rationale	Mitigations
Client Device		
ZigBee Network - Unencrypted IoT Traffic	Traffic between IoT devices on ZigBee network remains unencrypted. Attackers can sniff/capture packets that have been transmitted (Ali & Askar, 2021).	Encrypt traffic in transit e.g. HTTPS
Default Username / Hardcoded Passwords	Often default usernames are used to login into systems. In addition, hard coded passwords represent one of the main security issues in IoT and smart home systems (Singh & Chandavarkar, 2019).	Default login usernames should be changed and / or disabled. No hardcoded passwords or credentials (tokens) should exist in the software.
Outdated Firmware	Devices using older firmware versions are susceptible to current and new security vulnerabilities.	Devices should be kept up to date with the latest firmware version in line with vendor release cycles. (Dhakal et al., 2019)
Weak Passwords	Default, weak & hardcoded passwords allow hackers to easily gain access to smart devices by using dictionary attacks (Singh & Chandavarkar, 2019).	A stronger IoT device security posture is achieved with the amendment of weak device password settings to avoid unauthorized access of adversaries, by using distinctive passwords (Chang, 2019). The enforcement of password policies which prohibit IoT device users from reusing the same password and a maximum password validity threshold which pinpoints the number of days a password is used before it is changed (Neil, 2018).
Absence of Physical Protection / Hardening of Devices	Hackers can reprogram the device's software locally and thus inject malicious code into the system. This can result in an insider attack (Hammi et al., 2022).	Physical protection of all smart home devices against unauthorised access.
Weak Mobile Phone Protection	Weak protected apps on a mobile phone can lead to a malicious code injection, which can corrupt devices.	Avoid insecure Wi-Fi
Public Reconisability of Smart Home Devices	Devices that continiously indicate presence can reveal information about the network and its vulnerabilities.	Use of secure communication channels.
Lack of Manual Usage Options	Corrupted device or power failure can lead to inability to use important devices.	Doors with keyholes, shutters that can be used manually and such to be able to use basic functions in an emergency.
Permanent Stand-by Mode of Irregularly Used Devices	Firmware can become outdated and devices such as smart TVs, computer cameras or virtual assistant technology devices (Alexa and similar) can be used to spy.	Unplug devices that are rarely used.
Careless behaviour of users	User can open phishing emails that contain malicious software or visit malicious websites which can corrupt the device or the entire system (Hammi et al., 2022).	Educate users about the dangers and proficient use ot the internet.
Unsecure Remote Access	Hackers can login remotely and tamper with the device (Hammi et al., 2022).	Biometric multifactor means of authentication such as fingerprints implemented on smart home IoT devices provide robust user verification capabilities (Ali & Awad, 2018). However, traditional multifactor authentication solutions are frequently overlooked at the design stage of most IoT devices, which makes it an arduous mitigation to implement (Monaswarnalakshmi & Sai-Aravindhan, 2018).
Overprivileged Apps	Hackers can get information through overprivileged apps (Apps requesting more priviliges than needed). The App provider may have insufficient security mechanisms.	Apply least privilege principle.

Controller Hub		
Insecure Open Ports	Open ports in controller hubs allows the device to be susceptible to port scanning and DDOS attacks. This aligns with the OWASP "Insecure Network Services" vulnerability (OWASP, 2018).	Shut down all insecure open ports e.g. HTTP (80) as well as all unused ports.
Weak Passwords	Weak passwords used on applications controlling smart devices are easily guessable.	Always use strong complex passwords
Weak Wi-Fi protocols (WEP / WPA)	WEP and WPA were found to be vulnerable to cyberattacks (Lashkari et al., 2009), as a result hackers are able to gain access to the Wi-Fi network and control IoT devices.	Use strong Wi-Fi encryption protocols such as WPA2
Outdated Firmware / Lack of Device Management	Often firmware versions are not kept up to date as a result newly discovered security vulnerabilities are not mitigated immediately.	Define and maintain a firmware upgrade policy as per vendor release cycles.
Unencrypted data stored at rest (cloud storage) and in transit	Hackers can easily sniff packets if secure protocols such as HTTPS are not used.	Ali & Awad (2018) state that secure communication channels are enforced by utilizing encryption mechanisms. This is achieved with homomorphic encryption whereby the alteration of data into cipher text is utilised as If it was in the original state (Divatia, 2019). However, IoT device vendors must tailor their applications to make homomorphic encryption increasingly viable. This may not be financially feasible for vendor corporations in terms of business scalability (Divatia, 2019).
Insufficient intrusion detection and intrusion prevention	Allows a hacker a variety of attacks such as Eavesdropping attack, traffic analysis, masquerade attacks, replay attacks, message modification attacks, DoS and malicious code injection (Olayemi et al., 2017).	Use of a strong and up-to-date firewalls
Faulty smart home setups	Incorrect smart home settings can lead to the disclosure of information or the corruption of the system.	Professional setup of the smart home controller hub.
Unsecure physical protection of the smart home system	Malicious person can gain access to the controller hub to permanently corrupt the system unoticed.	Physical protection of the controller hub (Hammi et al., 2022). Do not allow stragners access to the controller hub.
Root permissions for smart home system users	A successful attack can lead to the takeover of the entire system.	The implementation of network segmentation for smart home IoT devices averts the compromise of all devices on the home network in an attack scenario (Chang, 2019). This is achieved with the adoption of a zero-trust architecture, whereby unauthorised access of the IoT devices is restricted to users with permission to access the device's resources with least privileges granted solely for the user. Thus, enabling granular access rules whilst maintaining availability of the devices (Rose et al, 2020). However, a shortfall persists in vendor products which support a zero-trust architecture due to the significant financial investment (Kerman et al., 2020).
Too detailed and permanent storage of information	Movement and usage patterns can be evaluated in order to exploit them maliciously (Ali & Awad, 2018).	Periodic erasure of recorded information. Implementation of a honey pot.
Insufficient physical layer protection	Internet cables connetcted to the smart home can be tapped to steal information or tamper with the system.	Physical protection of the internet cable.
Plugins / libraries downloaded from insecure sources	A malicious plugin / libraries can lead to an injection of ransomware allowing a hacker to gain access to the system (Hammi et al., 2022).	Only download software from trusted sources. Verification by a SHA.