Secure Systems Architecture Design Document

Introduction

The Smart Home consists of many networked IOT devices. Each of these nodes, once acquired, can be utilized to further escalate the attack. These devices are afflicted by various kinds of weakness, which are the result of poor coding practices, misconfiguration due to human error and in some cases due to the usage of inherently insecure third party libraries just to name a few: -

Device	**Device Group**
Smart TV	Client Device
Smart Assistant	Client Device
Smart Appliance(s)	Application Controller Device
Smart wearable	Client Device
Smart Phone	Client Device
Laptop/PC/MAC	Client Device
Wireless Router	Wireless Controller Device
Wireless Repeater	Wireless Controller Device
Network File Share (NFS)	Application Controller Device

These classifications are described by device groups as mentioned in the table above and are depicted in the individual Attack and Defence Tree in the figures below.

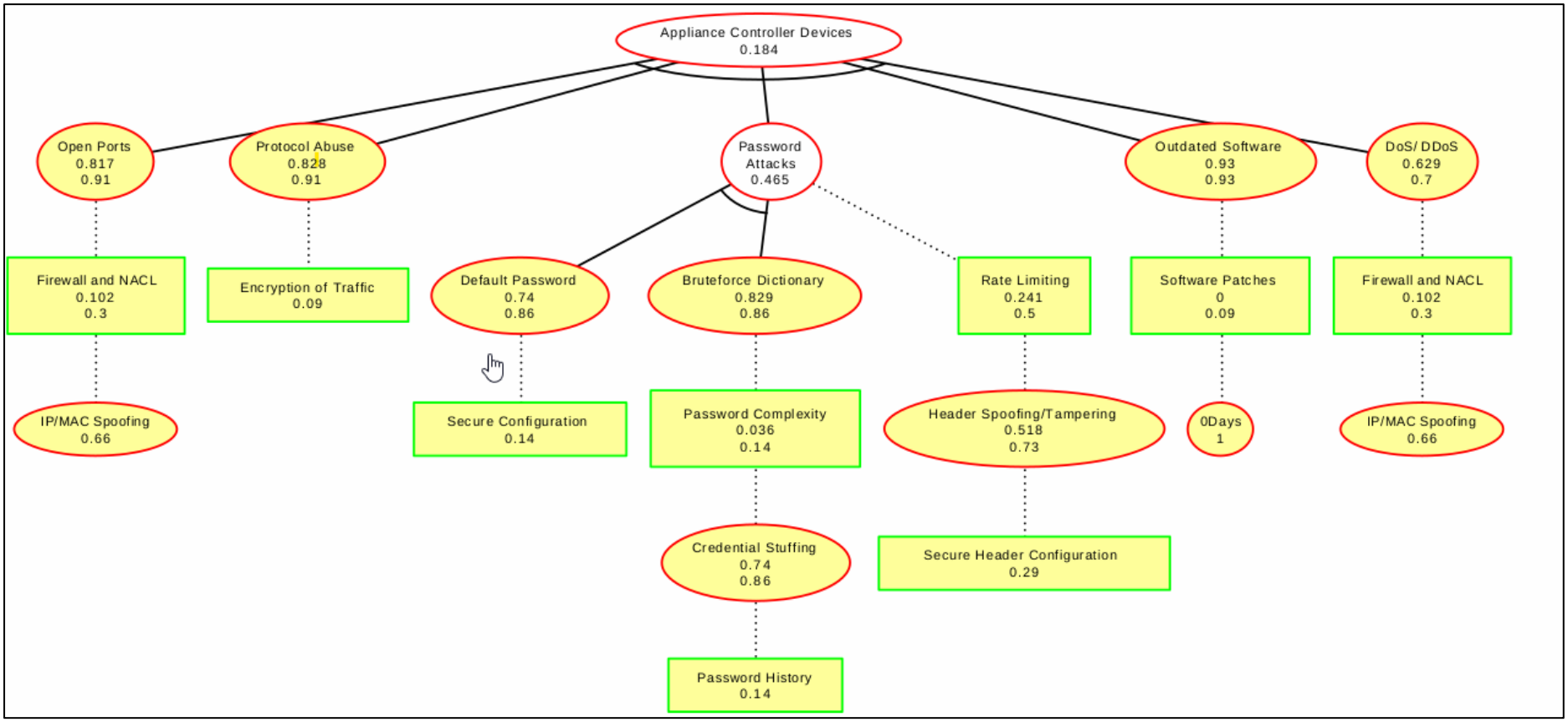

Figure 1: AD Tree for Application Controller Devices found in a Smart Home

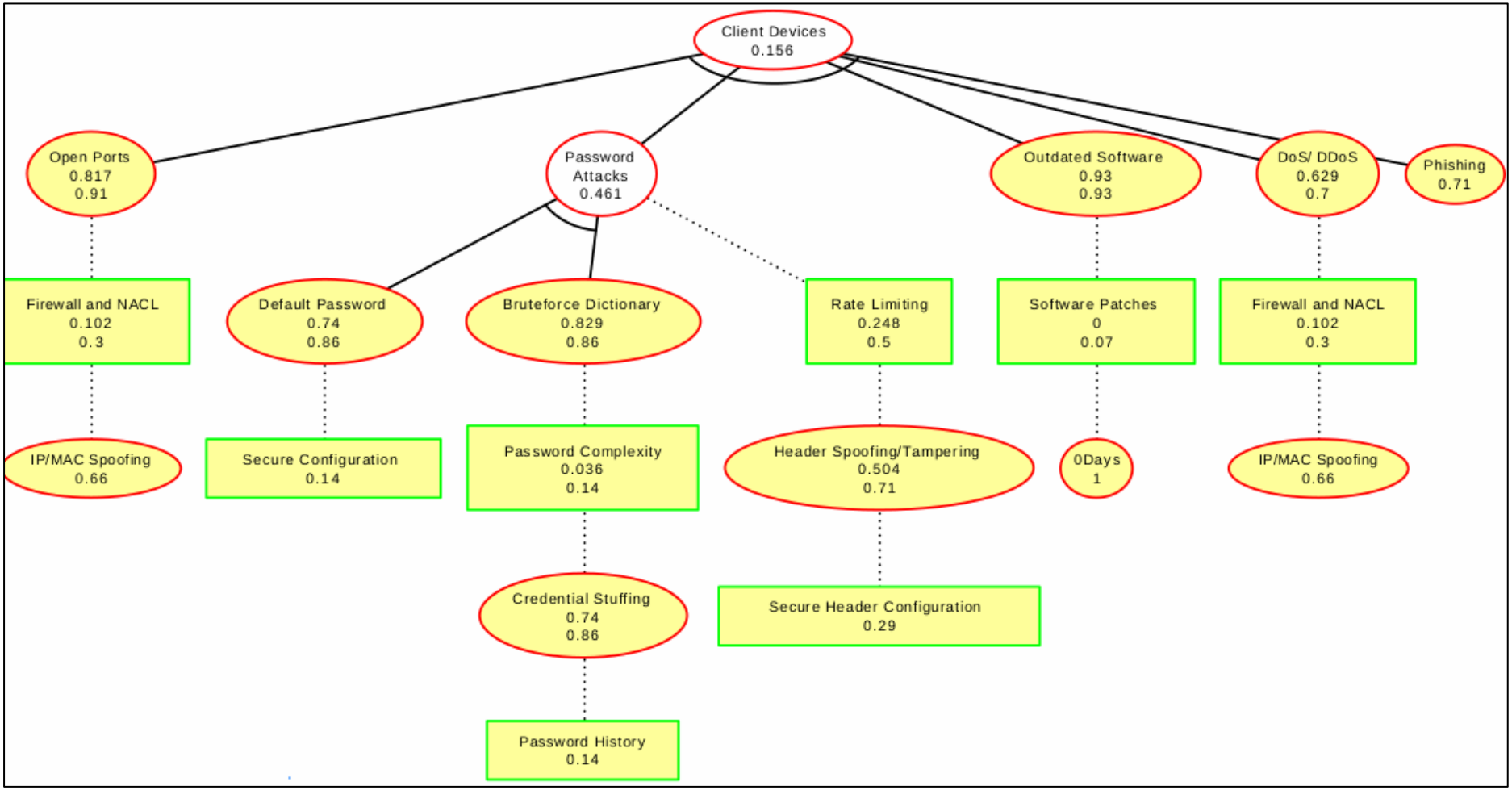

Figure 2: AD Tree for Client Devices found in a Smart Home

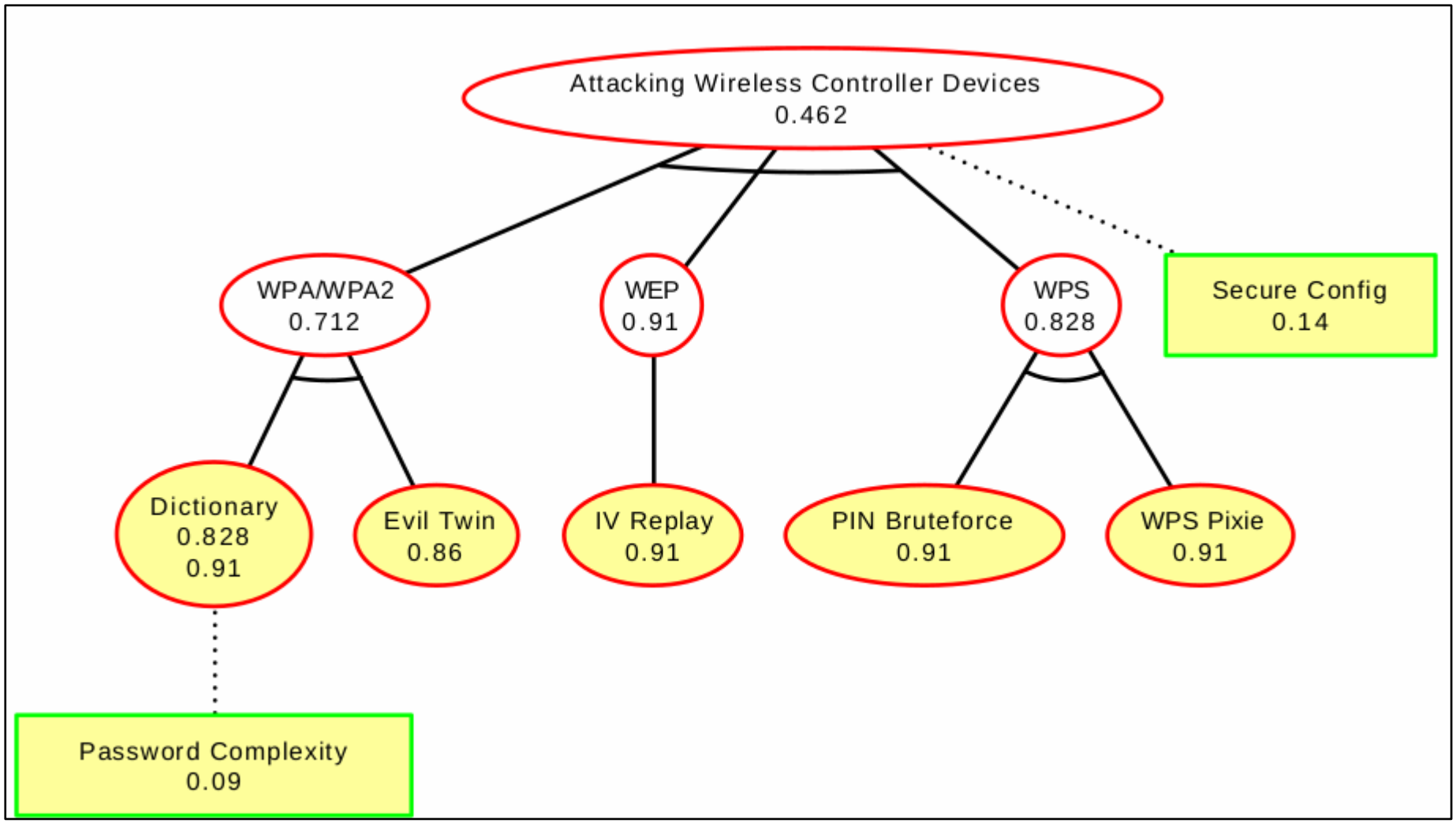

Figure 3 AD Tree for Wireless Controller Devices found in a Smart Home

The above attack trees were enhanced with CVSS 3.1 risk scoring and the probability of success for the attacks were based of on the CVSS score. All the above attack trees have their CVSS 3.1 metrics highlighted below in the tables 1,2, and 3.

For enhanced risk scoring, we also looked into the temporal scoring metrics; which showcased reduce risks overtime as the risk and it's countermeasures mature overtime.

Application Controller Devices													
Threat	Attack Vector (AV)	Attack Complexity (AC)	Privileges Required (PR)	User Interaction (UI)	Scope (S)	Confidentiality (C)	Integrity (I)	Availability (A)	CVSS 3.1 Score	Exploit Code Maturity	Remediation Level	Report Confidence	CVSS 3.1 Score
0 Day	Network	Low	None	None	Changed	High	High	High	10	Not Defined	Not Defined	Not Defined	10
Outdated Software	Network	Low	None	None	Changed	High	High	High	10	Functional	Offcial Fix	Confirmed	9.3
Open Ports	Network	Low	None	None	Unchanged	High	High	High	9.8	Functional	Offcial Fix	Confirmed	9.1
Default Password	Network	Low	None	None	Unchanged	High	High	Low	9.1	Functional	Work Around	Confirmed	8.6
Brute Force	Network	Low	None	None	Unchanged	High	High	Low	9.1	Functional	Work Around	Confirmed	8.6
Credential Stuffing	Network	Low	None	None	Unchanged	High	High	Low	9.1	Functional	Work Around	Confirmed	8.6
Protocol Abuse	Network	Low	Low	None	Unchanged	High	High	High	8.8	Functional	Offcial Fix	Confirmed	8.2
Header Spoofing	Network	High	None	None	Unchanged	High	High	Low	7.7	Functional	Offcial Fix	Confirmed	7.1
DoS/DDoS	Network	Low	None	None	Unchanged	None	None	High	7.5	Functional	Offcial Fix	Confirmed	7
IP/MAC Spoofing	Network	High	Low	None	Unchanged	High	High	Low	7.1	Functional	Offcial Fix	Confirmed	6.6

Table 1: Application Controller Devices – CVSS Base and Temporal Scoring.

Wireless Devices													
Threat	Attack Vector (AV)	Attack Complexity (AC)	Privileges Required (PR)	User Interaction (UI)	Scope (S)	Confidentiality (C)	Integrity (I)	Availability (A)	CVSS 3.1 Score	Exploit Code Maturity	Remediation Level	Report Confidence	CVSS 3.1 Score
Dictionary	Network	Low	None	None	Unchanged	High	High	High	9.8	Functional	Offcial Fix	Confirmed	9.1
IV Replay	Network	Low	None	None	Unchanged	High	High	High	9.8	Functional	Offcial Fix	Confirmed	9.1
PIN Bruteforce	Network	Low	None	None	Unchanged	High	High	High	9.8	Functional	Offcial Fix	Confirmed	9.1
WPS Pixie	Network	Low	None	None	Unchanged	High	High	High	9.8	Functional	Offcial Fix	Confirmed	9.1
Brute Force	Network	Low	None	None	Unchanged	High	High	High	9.8	Functional	Offcial Fix	Confirmed	9.1
Evil Twin	Network	Low	None	Required	Unchanged	High	High	High	8.8	Functional	Offcial Fix	Confirmed	8.6

Table 2: Wireless Devices – CVSS Base and Temporal Scoring.

Client Devices													
Threat	Attack Vector (AV)	Attack Complexity (AC)	Privileges Required (PR)	User Interaction (UI)	Scope (S)	Confidentiality (C)	Integrity (I)	Availability (A)	CVSS 3.1 Score	Exploit Code Maturity	Remediation Level	Report Confidence	CVSS 3.1 Score
0 Day	Network	Low	None	None	Changed	High	High	High	10	Not Defined	Not Defined	Not Defined	10
Outdated Software	Network	Low	None	None	Changed	High	High	High	10	Functional	Offcial Fix	Confirmed	9.3
Open Ports	Network	Low	None	None	Unchanged	High	High	High	9.8	Functional	Offcial Fix	Confirmed	9.1
Default Password	Network	Low	None	None	Unchanged	High	High	Low	9.1	Functional	Work Around	Confirmed	8.6
Brute Force	Network	Low	None	None	Unchanged	High	High	Low	9.1	Functional	Work Around	Confirmed	8.6
Credential Stuffing	Network	Low	None	None	Unchanged	High	High	Low	9.1	Functional	Work Around	Confirmed	8.6
Phishing	Network	High	None	Required	Unchanged	High	High	High	7.5	Unproven	Unavailable	Reasonable	7.3
Header Spoofing	Network	High	None	None	Unchanged	High	High	Low	7.7	Functional	Offcial Fix	Confirmed	7.1
DoS/DDoS	Network	Low	None	None	Unchanged	None	None	High	7.5	Functional	Offcial Fix	Confirmed	7
IP/MAC Spoofing	Network	High	Low	None	Unchanged	High	High	Low	7.1	Functional	Offcial Fix	Confirmed	6.6

Table 3: Client Devices – CVSS Base and Temporal Scoring.

The details of vulnerabilities listed within devices are showcased below: -

Wireless Controller Devices

Types: WPA/WPA2/WPE/WPS

Vulnerabilities: Dictionary, Evil Twin and IV Replay are potentially viable attacks.

Mitigation:

These can be mitigated with a combination of password complexity, upgraded WPA3 standard, and secure device configuration (Hammi, 2022).

Application Controller Devices

Types: Android, Apple: Amazon Alexa, Google Assistant or Apple's Siri

Vulnerabilities: Denial of Service, Man in the Middle, Skill Squatting, Vulnerable Software.

Mitigation:

Up-to-date firmware, utilizing a VPN for entire network, skill-name scanners and sanitizers (Yıldırım, 2019).

These are remedied with updated software, encryption of traffic and securing the device behind a firewall (Michéle, 2014).

Client Devices

Types: Android, IOS, Window/Mac OS, Linux,

Vulnerabilities: Outdated Software, Default password, Brute force, Phishing, IP and MAC spoofing

Mitigation:

Up-to-date firmware, utilizing a VPN for the entire network, skill-name scanners and sanitizers (Yıldırım, 2019).

These are remedied with updated software, encryption of traffic and securing the device behind a firewall (Michéle, 2014).

These can be mitigated with a combination of password complexity and secure device configuration (Hammi, 2022)

Research from case studies (Echeverría et al., 2021) and government (CISA, 2020) recommendations were also performed to ensure that the majority of mitigation actions have been captured. Please see figure 4

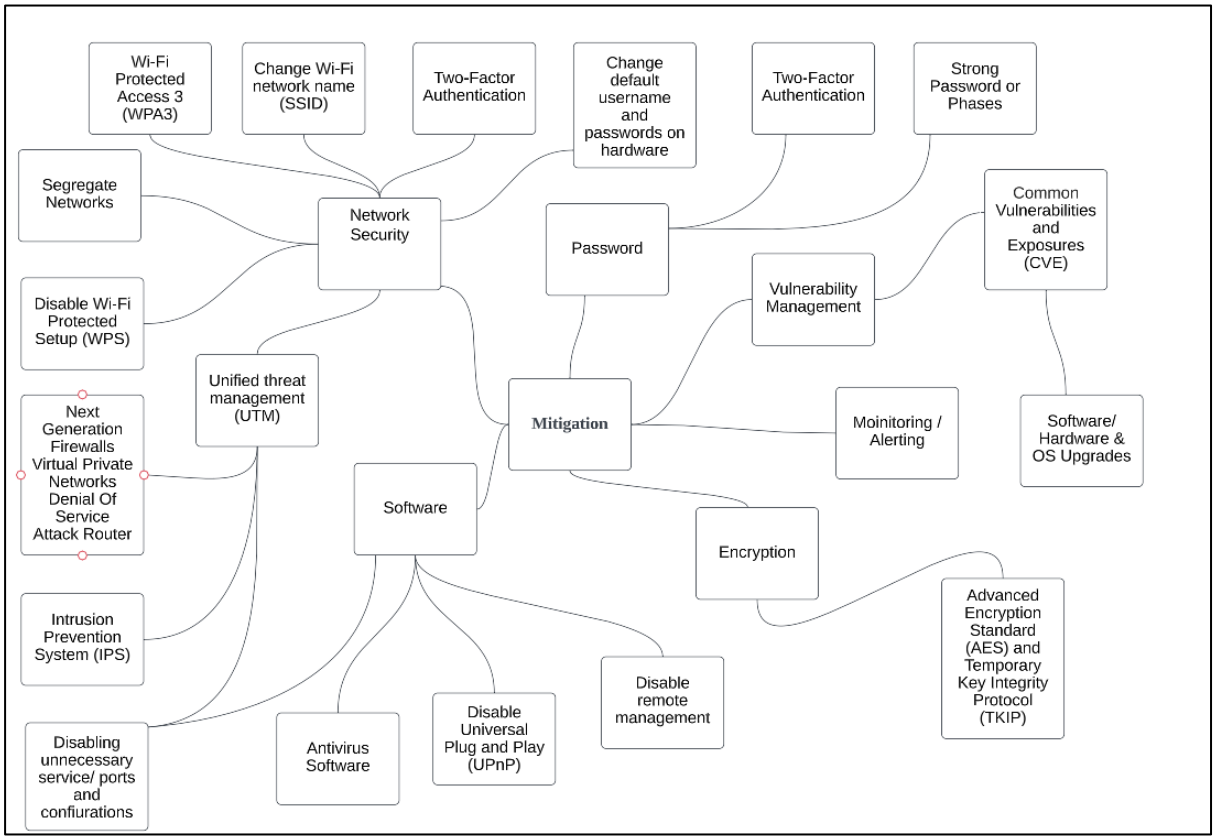

Figure 4 Mitigation Chart

Conclusion

The Smart Home is a perfect playground for both hackers and security professionals.

Each component is an opportunity for both mitigation and threat acceleration.

References

CISA (2020). Home Network Security | CISA. [online] www.cisa.gov. Available at: https://www.cisa.gov/uscert/ncas/tips/ST15-002. [Accessed 11 February 2023]

Costa, L., Barros, J.P. & Tavares, M. (2019) Vulnerabilities in IoT devices for smart home environment. In *Proceedings of the 5th International Conference on Information Systems Security e Privacy, ICISSP 2019.* (Vol. 1 : 615-622). SciTePress.

Echeverría, A., Cevallos, C., Ortiz-Garces, I. and Andrade, R.O. (2021). Cybersecurity Model Based on Hardening for Secure Internet of Things Implementation. Applied Sciences, 11(7), p.3260. doi:https://doi.org/10.3390/app11073260. [Accessed 11 February 2023]

Hammi, B., Zeadally, S., Khatoun, R. & Nebhen, J. (2022) Survey on smart homes: vulnerabilities, risks, and countermeasures. *Computers & Security*, *117*.

Michéle, B. & Karpow, A. (2014) January. Watch and be watched: Compromising all smart tv generations. In *2014 IEEE 11th consumer communications and networking conference* : 351-356. IEEE.

SearchNetworking. (n.d.). Explore 9 essential elements of network security. [online] Available at: https://www.techtarget.com/searchnetworking/tip/Explore-9-essential-elements-of-network-security. [Accessed 11 February 2023]

Sun, J., Li, S., Xu, J. & Huang, J. (2022) The Security War in File Systems: An Empirical Study from A Vulnerability-Centric Perspective.

Yıldırım, İ., Bostancı, E. & Güzel, M.S. (2019, September). Forensic analysis with anti-forensic case studies on Amazon Alexa and Google assistant build-in smart home speakers. In *2019 4th International Conference on Computer Science and Engineering* : 1-3. IEEE.