## **Contents**

[**Contents** 1](#_Toc112700352)

[**Introduction** 2](#_Toc112700353)

[**Threats** 3](#_Toc112700354)

[**ADTree** 6](#_Toc112700355)

[**Mitigations** 7](#_Toc112700356)

[**References** 9](#_Toc112700357)

[**Appendix** 12](#_Toc112700358)

## **Introduction**

The Internet of Things (IoT) is a relatively new architecture model enabling data transfer and provisioning of services over networks. It allows users to turn everyday devices into smart devices capable of collecting data and automating activities, assisted by a growing number of interconnected nodes.

The ever-changing threat landscape and the growing number of sophisticated cyberattacks require novel ways to define and quantify threats to keep systems secure and out of malicious actors’ reach (Kordy et. al., 2014).

Resultantly, an IoT network for a smart home, shown in Figure 1, comprising a coordinator, smart video doorbell, smart energy meter, connected by LoRa and MQTT has been proposed with its application, network, and physical threats modelled using an Attack-Defence Tree (ADTree).

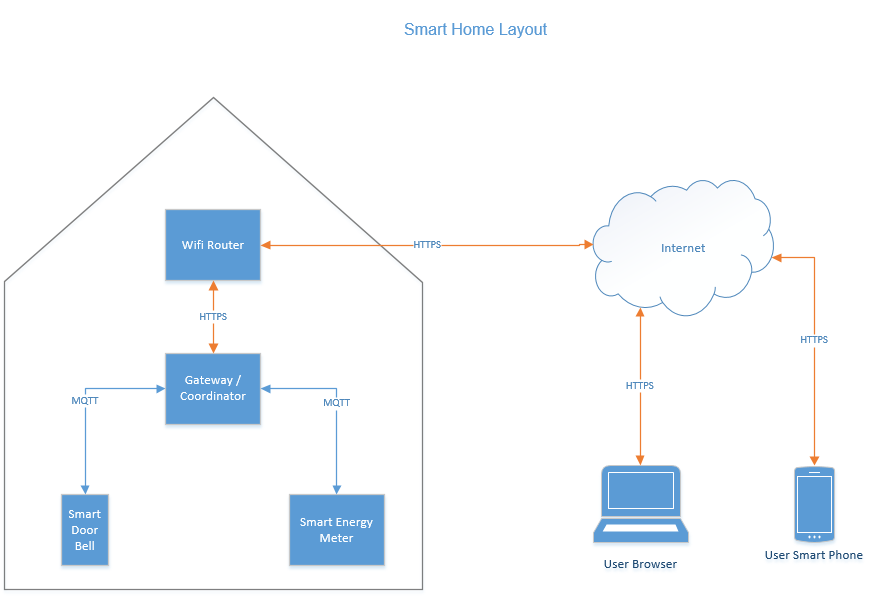


Figure 1: Smart Home Layout

## **Threats**

|  |  |
| --- | --- |
| **Application Threats** | **Description** |
| SQL Injection | Web application vulnerability allowing attackers to manipulate databases through queries (PortSwigger, 2019) |
| Cross Site Scripting (XSS) | Malicious scripts injected into web forms giving unauthorised access to sensitive files such as session cookies, allowing session hijacking (KirstenS, 2020) |
| Broken Authentication | Exploits credentials allowing privileged account access (OWASP, 2017) |
| Privilege Escalation | Programming errors could allow attackers unauthorised access to applications and privileged resources (OWASP, 2020) |

|  |  |
| --- | --- |
| **Network Threats** | **Description** |
| Session Hijack | Exploits web session control mechanisms. Gives unauthorised webserver access using compromised session tokens (OWASP, 2020) |
| Man in the Middle | Attacker positioned between two communicating parties manipulates passing data, compromising integrity and confidentiality (NIST, N.D.) |
| Wireless Key Compromise | Wireless key obtained and used for unauthorised resource access |
| Eavesdropping | Hackers intercept unencrypted data transmitted between two devices (Fortinet, N.D.) |
| Resource Exhaustion | Exploits vulnerabilities, compromising service availability and rendering legitimate service unavailable (Antunes et al., 2008) |
| Port Scanning | Used to discover open services or weak entry points in networks and systems (Fortinet, N.D.) |
| Malicious Code Download | Downloading harmful programs to exploit system vulnerabilities (Kaspersky, 2019) |
| Connections from unknown devices | Connections of unsolicited devices, leaving the IoT network compromised |

|  |  |
| --- | --- |
| **Physical Threat** | **Description** |
| Access and Compromise of Devices. | Physical breach, damage or theft of devices |

## **ADTree**

ADTrees describe clearly and simply how attackers can abuse a system, while also showing defensive measures to mitigate them in the same graphical representation (Kordy et al., 2010). Figure 2 describes an ADTree based on the smart home network, which is magnified in the Appendix.

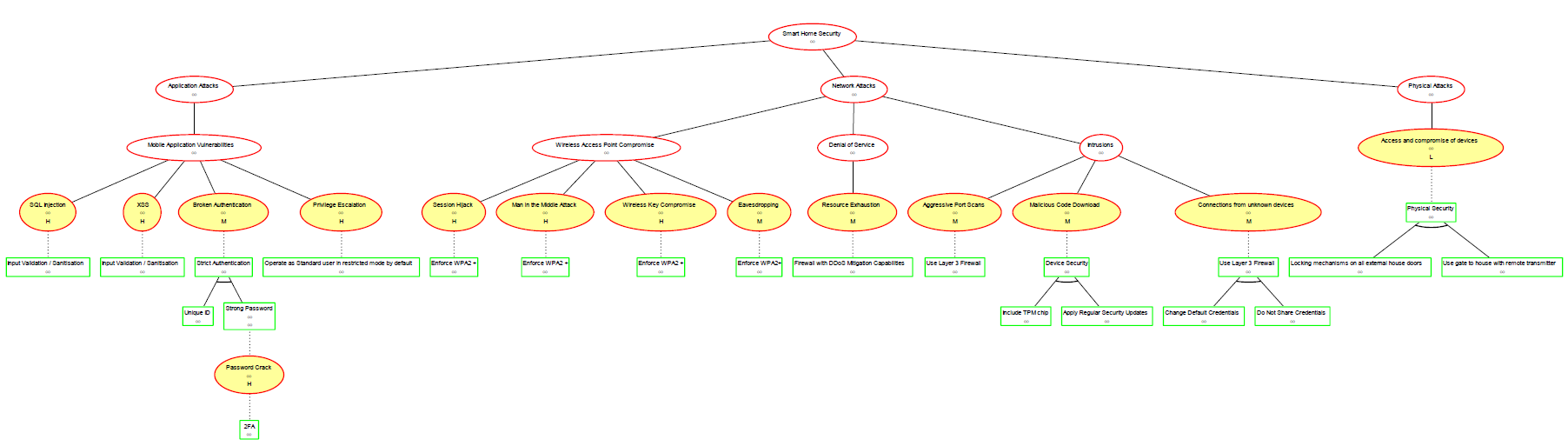


Figure 2: Attack-Defence Tree for Smart Home Security created using ADTool (Université Du Luxembourg, N.D.)

**Domain**

Domain attributes quantify system threats. Because direct threats to the Smart Home system are not financially motivated, the domain “Difficulty for the Proponent (L, M, H)” has been selected. This demonstrates the minimal difficulty level for the proponent, based on the assumption that adversary actions are already in effect (Kordy & Schweitzer, 2015), and clearly shows the most vulnerable areas of the system which need further protection. Delaying an attacker provides no benefit to the homeowner, so time-based domains are also unsuitable.

## **Mitigations**

|  |  |
| --- | --- |
| **Application Threat Mitigations** | **Description** |
| Layer 7 Firewall with DDoS capability | Firewall accepting traffic on ports but blocking traffic containing known vulnerabilities through deep packet inspection (Nife & Kotulski, 2020). Can detect DoS attacks |
| Input Validation / Sanitisation | Prevents execution of malicious queries designed for unauthorised data access (Levis et al., 2008) |
| Strict Authentication (Unique IDs and Strong Passwords) | Mitigates authentication-based attacks as attackers are less likely to guess user credentials |
| Multi Factor Authentication | Further mitigates unauthorised system access (Mohamed, 2019) |
| Standard User accounts with restricted privileges | Limits the damage extent, if compromised |

|  |  |
| --- | --- |
| **Network Threat Mitigations** | **Description** |
| WPA2 (or greater) Wireless Encryption | Provides data encryption by TKIP which used strong encryption mechanisms (Malgaonkar et al., 2017) |
| In-built TPM chip for IoT devices and coordinator | Supports cryptographic algorithms and secure boot on devices |
| Patch Management | Continuous mitigation of discovered IoT vulnerabilities |
| Credential hygiene (e.g., change default credentials and keeping them secret) | Minimises the chance of credentials being guessed. |

|  |  |
| --- | --- |
| **Physical Threat Mitigations** | **Description** |
| External door locks | Prevents unauthorised access to facilities where IoT equipment is located |
| External walls and gate, if possible | Deters and delays intruders |

## **References**

Antunes, J., Ferreira Neves, N. and Verissimo, P. (2008) ‘Detection and Prediction of Resource-Exhaustion Vulnerabilities’, *2008 19th International Symposium on Software Reliability Engineering (ISSRE).* Seattle 10-14 November. IEEE

Fortinet (N.D.) Eavesdropping. Available from: https://www.fortinet.com/resources/cyberglossary/eavesdropping [Accessed 28 August 2022].

‌

Fortinet. (N.D.) What Is A Port Scan? How To Prevent Port Scan Attacks?. Available from: https://www.fortinet.com/resources/cyberglossary/what-is-port-scan [Accessed 28 August 2022].

Kaspersky. (2019) What is Malicious code?. Available from: https://www.kaspersky.com/resource-center/definitions/malicious-code [Accessed 28 August 2022].

KirstenS. (2020) Cross Site Scripting (XSS). Available from: https://owasp.org/www-community/attacks/xss [Accessed 28 August 2022].

Kordy, B., Mauw, S., Radomirović, S. & Schweitzer, P. (2010) ‘Foundations of Attack–Defense Trees’, *Formal Aspects of Security and Trust - 7th International Workshop, FAST 2010.* Pisa, Italy, 16-17 September, 2010. Berlin: Springer.

Kordy, B., Mauw, S., Radomirović, S. & Schweitzer, P. (2014) Attack-defense trees. *Journal of Logic and* *Computation* 24(1): 55-87. DOI: <https://doi.org/10.1093/logcom/exs029>

Kordy, P. & Schweitzer, P. (2015) The ADTool Manual. Available from: https://satoss.uni.lu/members/piotr/adtool/manual.pdf [Accessed 28 August 2022].

Levis, M., Helfert, M. & Brady, Malcolm. (2008) Website Design Quality and Form Input Validation: An Empirical Study on Irish Corporate Websites. *Journal of Service Science and Management* 1(01): 91-100. DOI: https://doi.org/10.4236/jssm.2008.11009

Malgaonkar, S., Patil, R., Rai, A. & Singh, A. (2017) Research on Wi-Fi Security Protocols. *International Journal of Computer Applications* 164(3): 30-36. DOI: <https://doi.org/10.5120/ijca2017913601>

Mohamed, T. S. (2019) Security of Multifactor Authentication Model to Improve Authentication Systems. *Information and Knowledge Management* 6: DOI: <https://doi.org/10.13140/RG.2.2.18515.53288>

Nife, F. & Kotulski, Z. (2020) Application-Aware Firewall Mechanism for Software Defined Networks. *Journal of Network and Systems Management* 28: 605-626 DOI: https://doi.org/10.1007/s10922-020-09518-z

NIST (N.D.) man-in-the-middle attack (MitM). Available from https://csrc.nist.gov/glossary/term/man\_in\_the\_middle\_attack [Accessed: 29 August 2022].

OWASP. (2017) A2:2017-Broken Authentication. Available from: https://owasp.org/www-project-top-ten/2017/A2\_2017-Broken\_Authentication [Accessed 28 August 2022].

OWASP. (2020) Session hijacking attack. Available from: https://owasp.org/www-community/attacks/Session\_hijacking\_attack [Accessed 28 August 2022].

PortSwigger. (2019) SQL Injection. Available from: https://portswigger.net/web-security/sql-injection [Accessed 28 August 2022].

Université Du Luxembourg. (N.D.) ADTool. Available From: https://satoss.uni.lu/members/piotr/adtool [Accessed 27 August 2022].

## **Appendix**

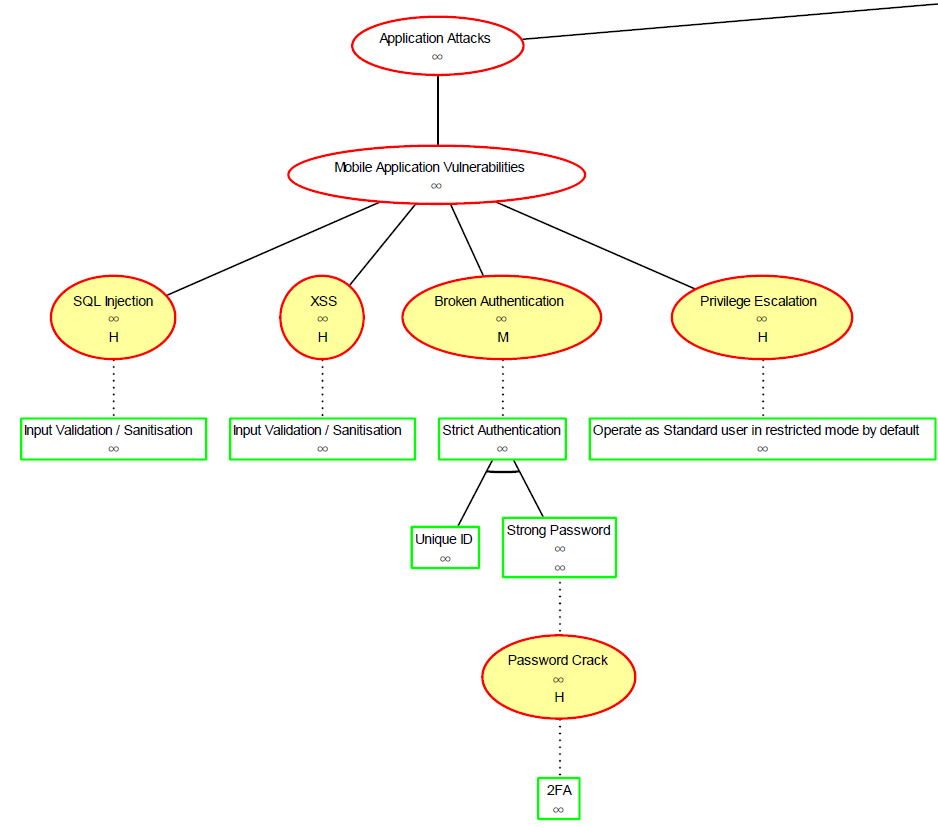


Figure 4: Application Threats

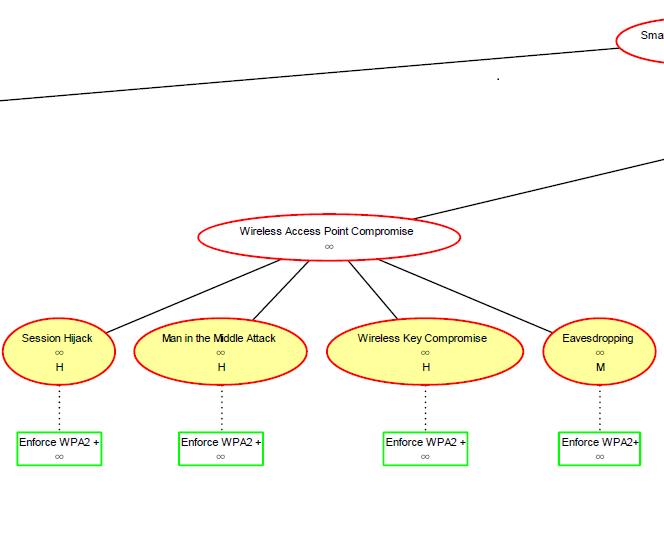


Figure 5: Network Threats (Wireless Access Point Compromise)

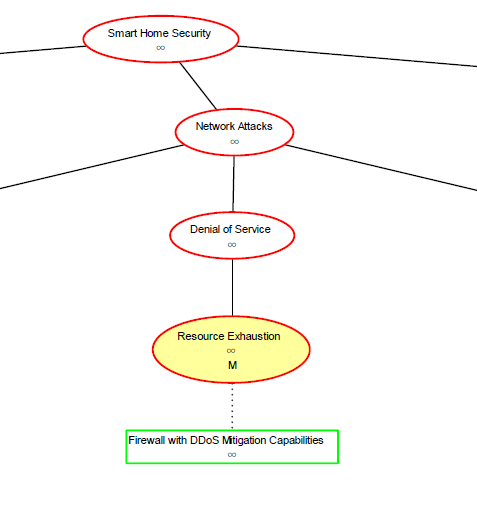


Figure 6: Network Threats (DoS)

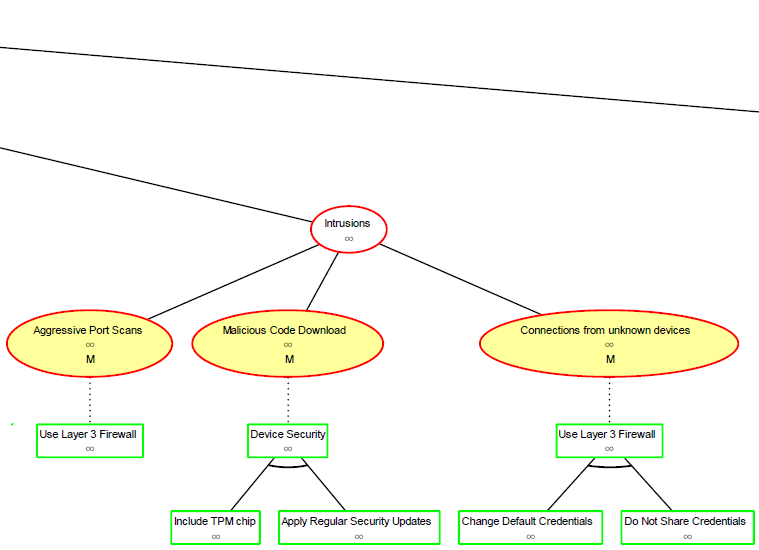


Figure 7: Network Threats (Intrusions)

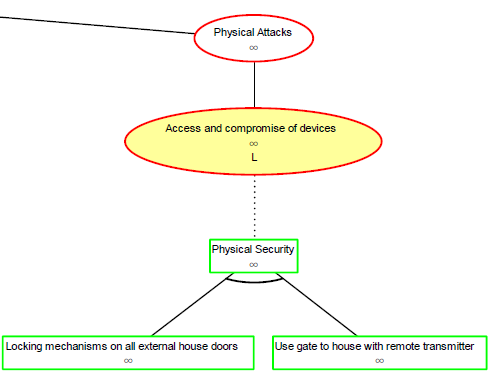


Figure 8: Physical Attacks