Secure System Architecture: Design Document

Introduction

The Internet of Things (IoT) architecture has facilitated the growth of smart home technology, with home appliances controlled by several wireless devices that store and transmit data through the Internet. However, this technology also opens the door to several security and privacy issues (Touqeer et al, 2021). The goal of this document is to identify and evaluate potential vulnerabilities of a smart home control system using an Attack-Defence Tree (AD-Tree).

Potential Vulnerabilities

- **Data and Identity Theft:** smart devices collect large quantities of sensitive personal information which could be exploited for identity theft if leaked.
- **Breach of Device or Infrastructure:** an adversary may gain control of a client device or main infrastructure (controller, database) through the use of an exploit or backdoor. This could lead to further attack vectors such as accessing the data at rest or limiting access.
- **Denial of Service (DoS):** the smart home may be targeted in a distributed (DDoS) or permanent (PDoS) denial of service attack. Within a PDoS attack, the hardware could be irreversibly damaged, whereas, within a DDoS attack, the system could be made inaccessible for the duration of the attack.
- **Man-in-the-Middle:** an adversary may capture the traffic between the controller and client device and thus gain access to data-in-transit.

Sources: Heartfield et al (2018), Mahbub (2020), Rambus (N.D.)

Attack-Defence Tree

An AD-Tree that models the security vulnerabilities of both the smart device clients and the controller hub has been designed. AD-Trees build upon the foundation of traditional attack trees, with the improvement of including possible countermeasures of a defender (Kordy et al, 2013).

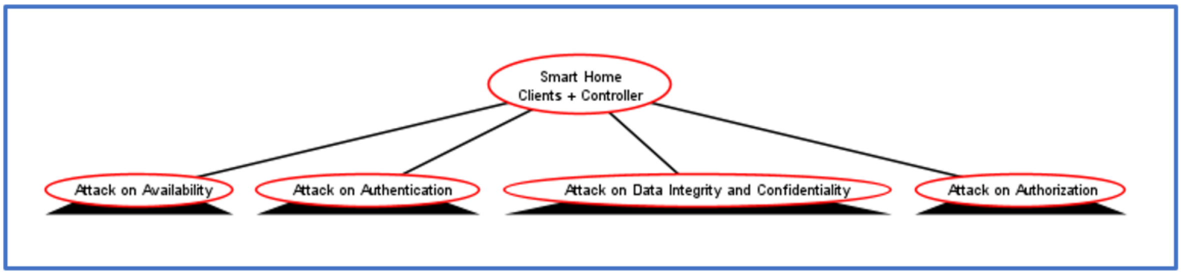

Figure 1: Main AD Tree Vulnerability Nodes

Figure 1 depicts the main vulnerability nodes that are broken down further in figures 2 to 4.

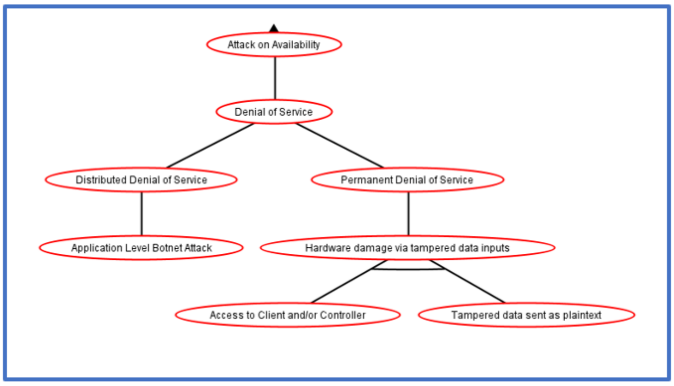
Attack on Availability
Denial of Service
Distributed Denial of Service
Permanent Denial of Service
Application Level Botnet Attack
Hardware damage via tampered data inputs
Access to Client and/or Controller
Tampered data sent as plaintext

Figure 2: Attack on Availability

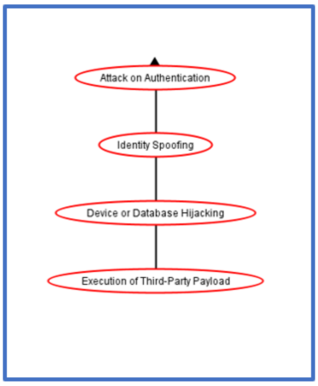
Attack on Authentication
Identity Spoofing
Device or Database Hijacking
Execution of Third-Party Payload

Figure 3: Attack on Authentication

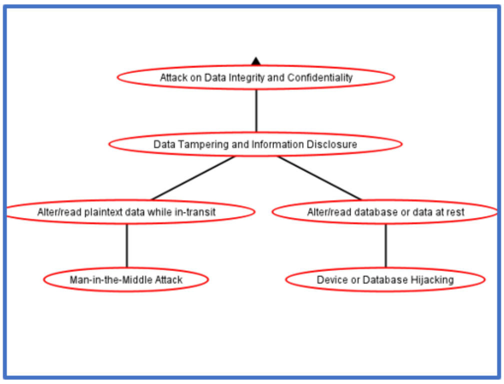
Attack on Data Integrity and Confidentiality
Data Tampering and Information Disclosure
Alter/read plaintext data while in-transit
Alter/read database or data at rest
Man-in-the-Middle Attack
Device or Database Hijacking

Figure 4: Attack on Data Integrity and Confidentiality

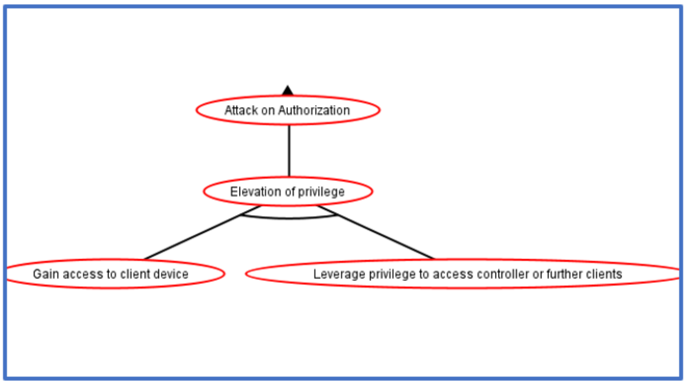
Attack on Authorization
Elevation of privilege
Gain access to client device
Leverage privilege to access controller or further clients

Figure 5: Attack on Authorization

Qualitative Evaluation

Considering the attack execution, technical difficulty level impacts the security vulnerability of the Smart Home, here we evaluate the technical capabilities or/and social skills required for the attacker to succeed in an attack (Byres et al, 2004; Abdulla et al, 2010; Tanu and Arreymbi, 2010; Bagnato et al, 2012).

Technical difficulty levels:

Low: Little technical capabilities and social skills are required to succeed in the attack, thus leading to high-security vulnerability.

Medium: Average cyber hacking skills needed.

High: Demands professionals with advanced hacking skills

Domain selection

”The difficulty for the proponent” (L, M, H) domain is established with the slightest difficulty rank for the proponent, on the set of linearly ordered L < M < H.
Therefore, *low skill requirements lead to low difficulty = High-security vulnerability.*

After applying countermeasures, the tool assumes the most vigorous defender for all opponent nodes in this specific attribute domain and thus assigns it ”∞” (Kordy & Schweitzer, 2015). Hence, after a countermeasure covers most vulnerabilities, ”∞” value carries over to the parent nodes, overriding all security vulnerabilities.

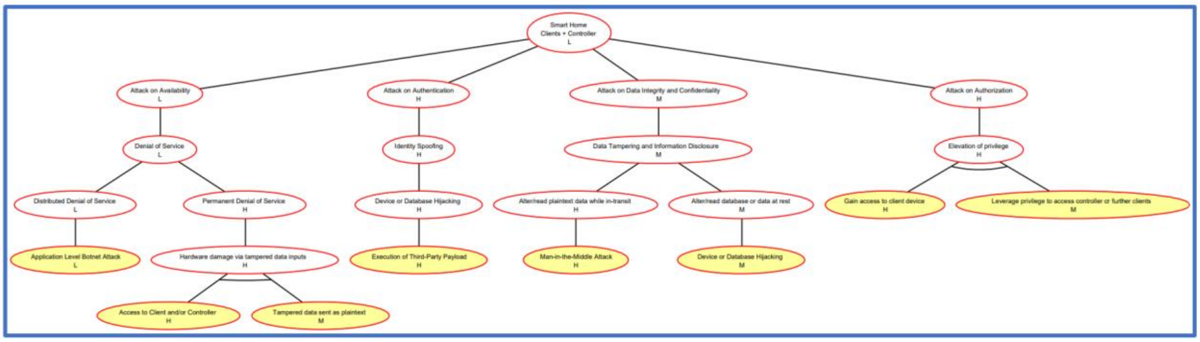
Smart Home
Clients + Controller
L
Attack on Availability
L
Denial of Service
L
Distributed Denial of Service
L
Application Level Botnet Attack
L
Permanent Denial of Service
H
Hardware damage via tampered data inputs
H
Access to Client and/or Controller
H
Tampered data sent as plaintext
M
Attack on Authentication
H
Identity Spoofing
H
Device or Database Hijacking
H
Execution of Third-Party Payload
H
Attack on Data Integrity and Confidentiality
M
Data Tampering and Information Disclosure
M
Alter/read plaintext data while in-transit
H
Man-in-the-Middle Attack
H
Alter/read database or data at rest
M
Device or Database Hijacking
M
Attack on Authorization
H
Elevation of privilege
H
Gain access to client device
H
Leverage privilege to access controller or further clients
M

Figure 5: Level of Difficulty in Attacking the Smart Home

Research initiatives like Bodei et al (2018) are currently working towards the design of a framework to allow quantitative evaluation of IoT security vulnerabilities.

Mitigation

The presented vulnerability analysis compels protecting the connected devices by a comprehensive IoT security solution. As stated by Komnios et al. (2014), a comprehensive security solution must ensure the security requirements of the CIA triad. Based on this premise, our AD-Tree analysis identifies the mitigations and recommended security measures for smart home systems.

To ensure Confidentiality and Privacy, proposed measures include the implementation of two-way authentication using cryptographic algorithms with symmetric or asymmetric keys and the requirement of authenticating devices before receiving and transmitting data.

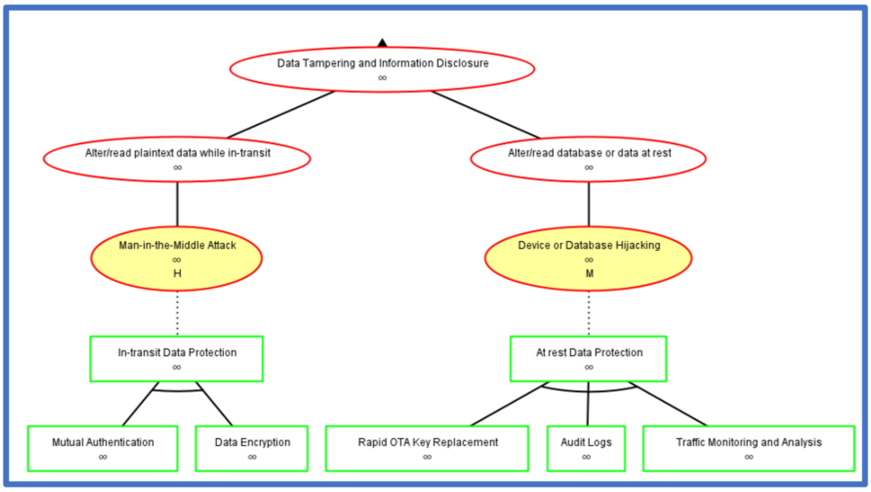
Data Tampering and Information Disclosure
∞
Alter/read plaintext data while in-transit
∞
Alter/read database or data at rest
∞
Man-in-the-Middle Attack
∞
H
Device or Database Hijacking
∞
M
In-transit Data Protection
∞
At rest Data Protection
∞
Mutual Authentication
∞
Data Encryption
∞
Rapid OTA Key Replacement
∞
Audit Logs
∞
Traffic Monitoring and Analysis
∞

Figure 6: Data Tampering and Disclosure Mitigations

To ensure Integrity, Authenticity and Non-Repudiation, features such as encrypted communication and secure boot have been identified. Encrypted communication protects data in transit and ensures that only devices with the decryption key can access the data. Secure boot uses code signatures to prevent the execution of malicious code.

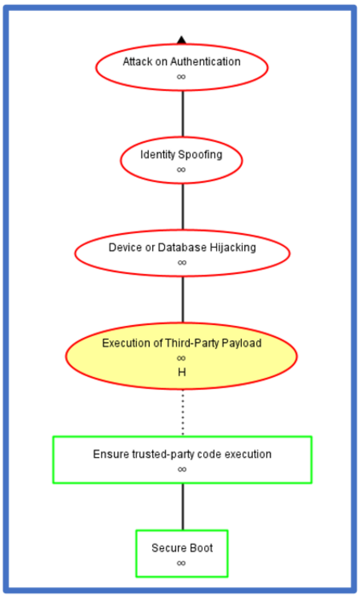
Attack on Authentication
∞
Identity Spoofing
∞
Device or Database Hijacking
∞
Execution of Third-Party Payload
∞
H
Ensure trusted-party code execution
∞
Secure Boot
∞

Figure 7: Spoofing Mitigations

Finally, to ensure Availability and prevent eventual DoS attacks, data monitoring and analysis tools can be used to detect possible security violations or threats.

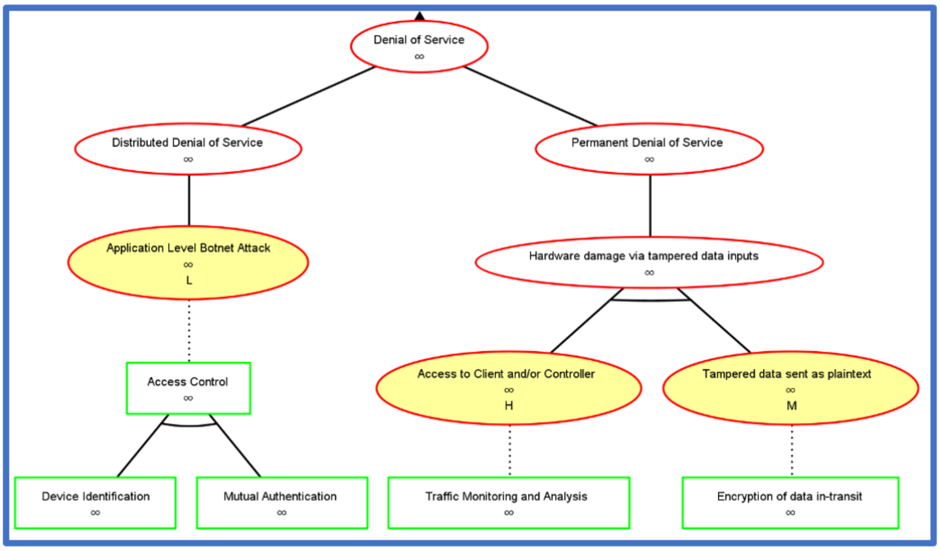
Denial of Service
∞
Distributed Denial of Service
∞
Permanent Denial of Service
∞
Application Level Botnet Attack
∞
L
Hardware damage via tampered data inputs
∞
Access Control
∞
Access to Client and/or Controller
∞
H
Tampered data sent as plaintext
∞
M
Device Identification
∞
Mutual Authentication
∞
Traffic Monitoring and Analysis
∞
Encryption of data in-transit
∞

Figure 8: Denial of Service Mitigations

To further analyse the effectiveness of these measures our future work will consist of implementing suggested mitigation measures as a proof of concept.

Reference List

Abdulla, P.A., Cederberg, J. & Kaati, L. (2010) Analyzing the Security in the GSM Radio Network using Attack Jungles. Available from: http://user.it.uu.se/~parosh/publications/papers/isola10.pdf [Accessed 9 February 2022].

Bagnato, A., Kordy, B., Meland, P. H. & Schweitzer, P. (2012). Attribute decoration of attack--defense trees. *International Journal of Secure Software Engineering (IJSSE)* 3: 1-35. Available from: https://www.researchgate.net/publication/231049180_Attribute_decoration_of_attack--defense_trees [Accessed 9 February 2022].

Bodei, C., Chessa, S., & Galletta, L. (2019). Measuring security in IoT communications. *Theoretical Computer Science*, 764:100-124. Available from: http://dx.doi.org/10.1016/j.tcs.2018.12.002 [Accessed 13 February 2022]

Byres, E.J., Franz, M. & Miller, D. (2004) The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems. Available from: https://www.researchgate.net/publication/228952316_The_use_of_attack_trees_in_assessing_vulnerabilities_in_SCADA_systems [Accessed 9 February 2022].

Heartfield, R., Loukas, G., Budimir, S., Bezemskij, A., Fontaine, J.R.J., Filippoupolitis, A. & Roesch, E. (2018). A Taxonomy of Cyber-Physical Threats and Impact in The Smart Home. *Computers & Security* 78: 398–428. Available from: https://doi.org/10.1016/j.cose.2018.07.011 [Accessed 10 February 2022].

Kordy, B., Kordy, P., Mauw, S. and Schweitzer, P. (2013*) ADTool: Security Analysis with Attack–Defense Trees*. Berlin: Springer. DOI: https://0-doi-org.serlib0.essex.ac.uk/10.1007/978-3-642-40196-1_15 [Accessed 10 February 2022].

Kordy, P. & Schweizer, P. (2015) ADTool Manual. Available from: https://satoss.uni.lu/members/piotr/adtool/manual.pdf [Accessed 9 February 2022].

Komninos, N., Philippou, E. & Pitsillides, A. (2014) Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures. *IEEE Communications Surveys & Tutorials* 16(4): 1933-1954. Available from: https://doi.org/10.1109/COMST.2014.2320093 [Accessed 12 February 2022].

Mahbub, M. (2020). Progressive Researches on IoT Security: An Exhaustive Analysis from the Perspective of Protocols, Vulnerabilities, and Preemptive Architectonics. *Journal of Network and Computer Applications* 168: 102761. Available from: https://doi.org/10.1016/j.jnca.2020.102761 [Accessed 10 February 2022].

Rambus (N.D.) Smart Home: Threats and Countermeasures. Available from: https://www.rambus.com/iot/smart-home/?fbclid=IwAR3h9kddLxVSgtHQjyXArJY-BbA-dlYTSO4bXbJPOZBN4d4lW3vvWtQFumo [Accessed 10 February 2022].

Tanu, E. & Arreymbi, J. (2010) An examination of the security implications of the supervisory control and data acquisition (SCADA) system in a mobile networked environment: An augmented vulnerability tree approach. Available from: https://repository.uel.ac.uk/download/96962e6e9e1b6da88d37e65f1b4066288ec56cd24fdfaceaa92fd4073c973c05/407484/Tanu%2C%20E%20%282010%29%20AC%26T%20228.pdf [Accessed 9 February 2022].

Touqeer, H., Zaman, S., Amin, R. et al. (2021) Smart home security: challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing* 77: 14053–14089. Available from: https://doi.org/10.1007/s11227-021-03825-1 [Accessed 5 February 2022].