Secure Systems Architecture module: Unit 3 Team Project Design Document

Smart Door Lock

1. Overview of the system and key priorities

- Z-wave Wi-Fi protocol is the most common for smart lock devices (Lynx, N.D.)
- Connected via Hub/Gateway
- No conflict with home Wi-Fi due to different frequencies
- The network is strengthened by Mesh technology when devices are connected
- Low power consumption for energy saving
- Ability to communicate with other smart devices such as lighting
- Offers AES 128 encryption
- Slower than Zigbee
- WebSocket technology supports TCP protocol between Client and Server with low latency (Pavelić et al., 2018)
- Token-based authentication for users communicating between the controlling hub and mobile device

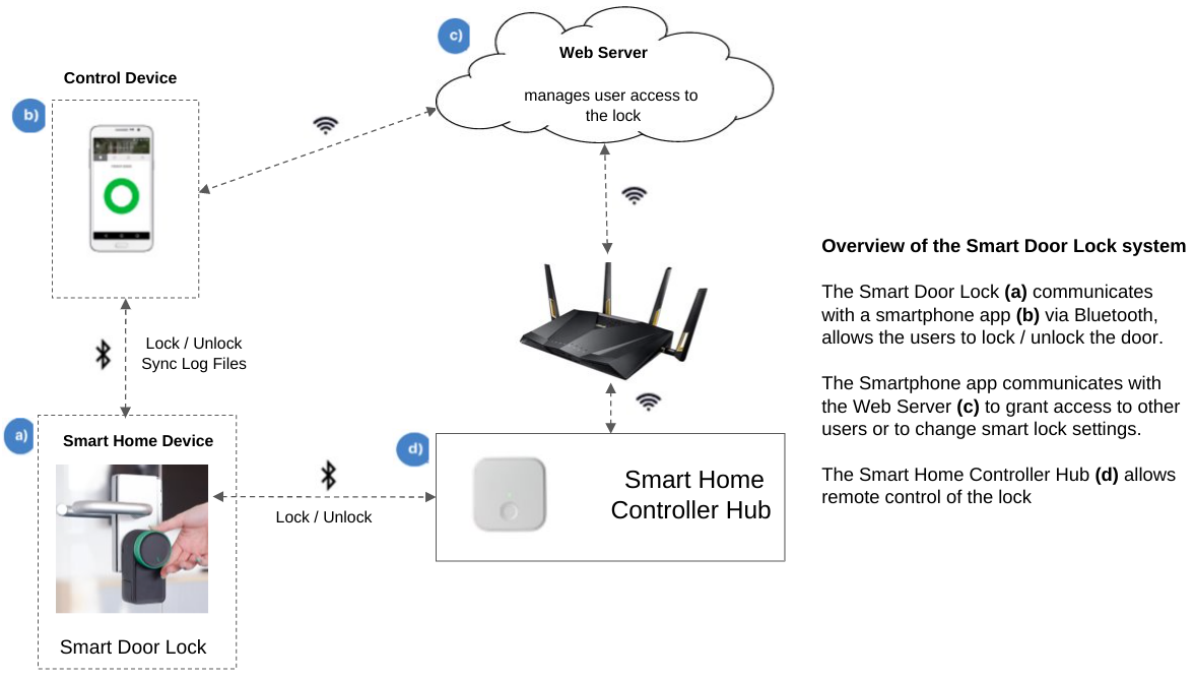

Figure 1: A smart home environment and its main components (Ye et al., 2017)

2. Use Case and Sequence Diagram of Smart Door Lock

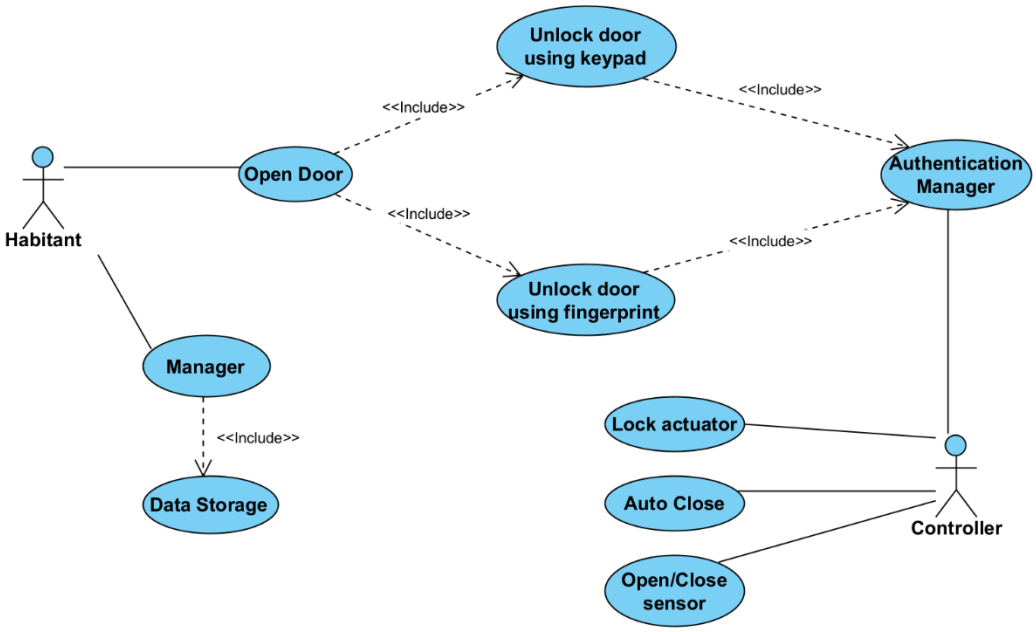

Figure 2: Use case diagram of a smart door lock system

- The use case shows the common features of a smart door lock and how they may be utilised.
- It also shows a variable feature fingerprint scanner as an alternative for a keypad.

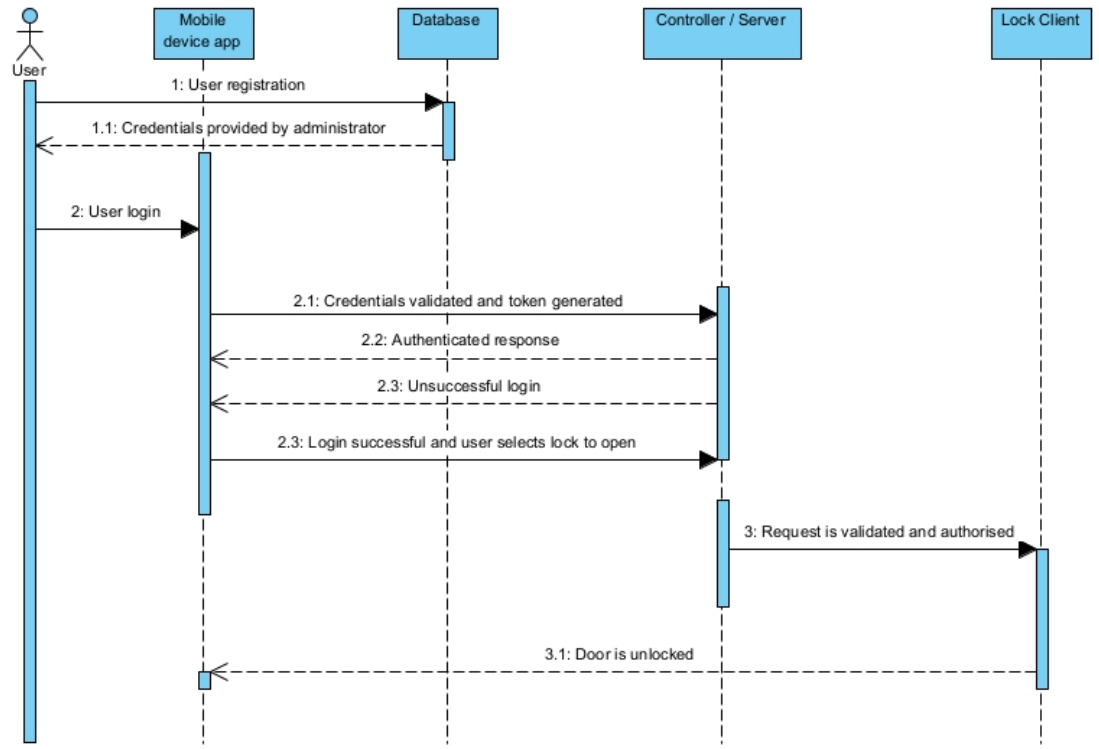

Figure 3: Sequence diagram of the user process of unlocking a door

- The sequence diagram requires implementing an effective risk management policy whereby administrators manage access privileges to mitigate unauthorised use (Pradeep Kumar et al., 2021).
- Coates et al. (2010) suggest that this system architecture requires vigilance. Furthermore, unnecessary communication ports should be closed, system patches updated, strict access controls considered (Coates et al., 2010).
- Authorised users can access secured resources such as door opening. The server can monitor resource usage over time which is helpful for energy saving.
- Distributed in the system are lock clients listening for commands from the controller/server unit. This follows the separation of concerns principle (De Win et al., 2002). This practice offers more significant challenges in development however can facilitate better usability (Castellanos Ardila and Gallina, 2020).

3. Potential Vulnerabilities

- Content spoofing

The attacker's ability to modify the server's content. According to OWASP, such attacks work alongside social engineering attacks; in our case, we refer to phishing attacks (Smith et al., 2021).

- Cryptography Failures

Insecure protocols such as HTTP, SMTP or FTP and unsecured algorithms make the system vulnerable to attacks (OWASP, 2021). Encrypted communication is one way to protect the integrity of the data.

- Snooping Bluetooth packages

Bluetooth Low-Energy (BLE) devices are prone to malicious control and information leakage (Wang et al., 2020).

- Reverse engineering

Applications are exposed due to insecure coding and programming. Running a source code analysis by a malicious actor raises the possibility of such attacks (OWASP, 2016).

- Obtain Admin privileges

Security misconfigurations are a potential threat. Keeping the default username and password is a common vulnerability (OWASP, 2021).

4. **Attack-Defence Tree**

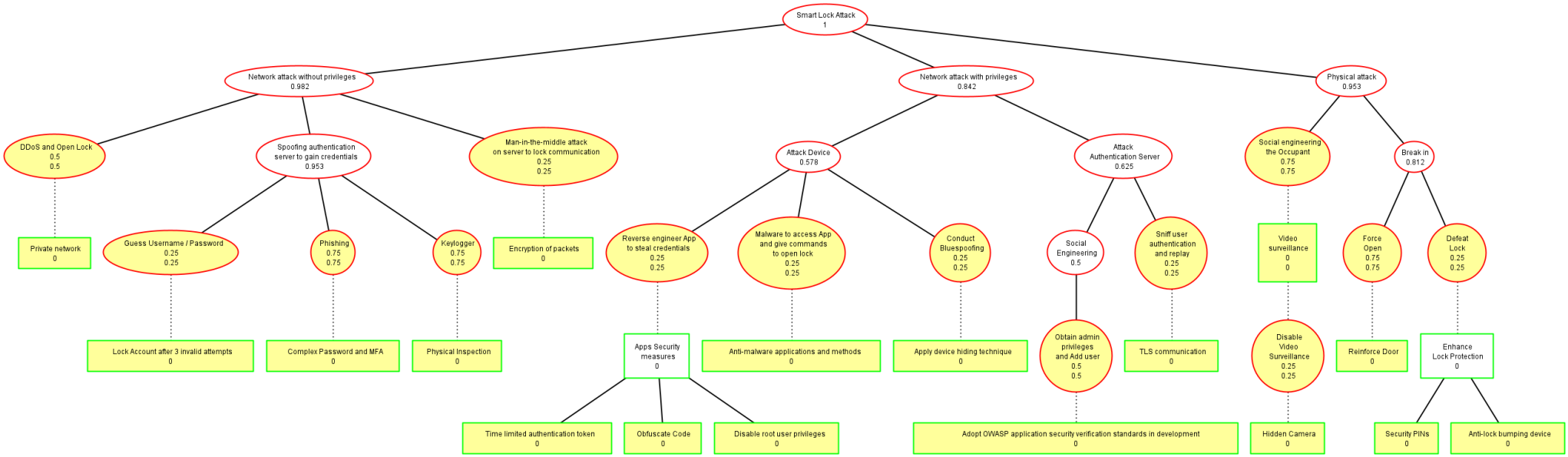

Figure 4: Attack-Defence Tree on Smart Door Lock

The "probability of success" domain is employed due to the assets at stake. The attributes of time, cost and expertise all relate to the probability of success. Even a low probability of success could have a disastrous impact and outcome for the end user (Fila and Wideł, 2019).

Findings:

a. There is a high chance of 0.75 that the smart door lock can be compromised, and out of which, Network attack without privilege and Physical attack have a higher probability of success of 0.464 and 0.35, respectively, over Network attack privilege.
b. With the countermeasures being put in place, the most viable option to break the lock is via spoofing the authentication server, which has the highest probability of success of 0.238

5. **Mitigations**
    a. Adopt OWASP security best practices during application development of the App.
    b. Anti-malware applications and methods to defend against malicious attacks
    c. Network
        i. Network segmentation to prevent DDoS attacks
        ii. Encryption of data packets to prevent Man-in-the-Middle Attack
        iii. TLS/SSL communication between devices
    d. Credential Management
        i. Lock account after 3 invalid login attempts
        ii. Enforce complex password requirement
        iii. Enforce Multi-Factor Attenuation (MFA)
    e. Device Hiding to defend against Bluetooth attack
    f. Physical
        i. Physical check
        ii. CCTV surveillance
        iii. Hidden Camera
        iv. Reinforced Door

6. References

Castellanos Ardila, J. & Gallina, B. 2020. Separation of Concerns in Process Compliance Checking: Divide-and-Conquer.

Coates, G. M., Hopkinson, K. M., Graham, S. R. & Kurkowski, S. H. 2010. A Trust System Architecture for SCADA Network Security. *IEEE Transactions on Power Delivery,* 25**,** 158-169.

De Win, B., Piessens, F., Joosen, W. & Verhanneman, T. On the importance of the separation-of-concerns principle in secure software engineering. Workshop on the Application of Engineering Principles to System Security Design, 2002. Citeseer, 1-10.

Fila, B. & Wideł, W. Efficient Attack-Defense Tree Analysis using Pareto Attribute Domains. 2019 IEEE 32nd Computer Security Foundations Symposium (CSF), 25-28 June 2019 2019. 200-20015.

Lee, J. (2010). A Comparison of Software Product Line Scoping Approaches [Online] Available from: https://www.researchgate.net/publication/220344699_A_Comparison_of_Software_Product_Line_Scoping_Approaches [Accessed 20 August 2022]

Lynx. N.D. Z-wave vs WiFi vs Zigbee vs Matter [Online]. Available: https://www.getlynx.co/z-wave-vs-wifi-vs-zigbee-vs-matter/ [Accessed 21 August 2022].

Mengmei Ye; Nan Jiang; Hao Yang; Qiben Yan (2017), Security analysis of Internet-of-Things: A case study of august smart lock. 10.1109/INFCOMW.2017.8116427

OWASP Foundation, Inc. (2021) OWASP Top 10:2021. Available from: https://owasp.org/Top10/A02_2021-Cryptographic_Failures/ [Accessed 19 August 2022].

OWASP Foundation, Inc. (2016) OWASP. Available from: https://owasp.org/www-project-mobile-top-10/2016-risks/m9-reverse-engineering [Accessed 20 August 2022].

OWASP Foundation, Inc. (2021) OWASP Top 10:2021. Available from: https://owasp.org/Top10/A05_2021-Security_Misconfiguration/ [Accessed 20 August 2022].

Pavelić, M., Lončarić, Z., Vuković, M. & Kušek, M. Internet of Things Cyber Security:Smart Door Lock System. 2018 International Conference on Smart Systems and Technologies (SST), 10-12 Oct. 2018 2018. 227-232.

Pradeep Kumar, K., Pillai, V., Sarath Chandra, K. & Chowdary, C. 2021. Disaster recovery and risk management over private networks using data provenance: Cyber security perspective. *Indian Journal of Science and Technology,* 14**,** 725-737.

Smith, A. Jmanico. Wichers. h3lix, D. Ranjan, R. ADubhlaoich. (2021) OWASP. Available from: https://owasp.org/www-community/attacks/Content_Spoofing [Accessed 19 August 2022].

Wang. J., Feng Hu, Ye Zhou, Yunhao Liu, Hanyi Zhang, Zhe Liu (2020) BlueDoor: breaking the secure information via BLE vulnerability. MobiSys '20: Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services 1(1): 286-298. https://doi.org/10.1145/3386901.3389025.