Introduction

This design document provides an overview on the vulnerabilities and its mitigations applicable to the devices in a smart home, specifically, those relevant to smart locks and its centralised controller hub.

Vulnerability Assessment

Threats applicable to smart locks (e.g., Yale, Wyze) and controller hubs (e.g., Amazon Echo, Google Nest) have been identified (see Table 1) by performing qualitative review of academic papers and other materials. The most commonly mentioned vulnerabilities have been included.

|  |  |
| --- | --- |
| **Device type** | **Vulnerabilities** |
| **Smart locks** | Passcode compromise via replay attacks (Rose et al, 2016). |
| Device spoofing used to allow commands from a “trusted source” (Rose et al, 2016). |
| Password compromise via weak encryption algorithms (Gilchrist, 2017). |
| Bluetooth Low Energy (BLE) devices are vulnerable to malicious control and information leakage (Wang, et. al., 2020). |
| Zero-day password reset vulnerabilities (Wang, et. al., 2018). |
| Data from locks can be skimmed, read, and saved (Hassani, 2020). |
| Access keys can be cracked (Hassani, 2020). |
| **Controller hub** | Data (passwords and tokens) remain in flash memory despite factory reset (Giese & Noubir, 2021). |
| User partition data and configuration details are not encrypted (Giese & Noubir, 2021). |
| No or weak voice recognition/authentication (AlOtaibi & Lombardi, 2021). |
| Hubs use more energy and emit more packets in noisy environments; the packets, if decrypted, could reveal sensitive information (AlOtaibi & Lombardi, 2021). |
| Encrypted data flow between the hub and the data centre used by AI to identify users (Barceló-Armada et al, 2022). |
| DDoS attacks such as syn-flood (Overstreet et al, 2019). |
| ‘Always on’ feature allows for conversations to be recorded and shared with third parties (Chung et al, 2017). |
| DHCP starvation attacks can disconnect hubs and all connected devices from the network (Brinson et al, 2021). |
| DNS hijacking attacks can take the whole smart home network down (Brinson et al, 2021). |
| Hub could be physically compromised and resold to an unsuspecting buyer (Wiggins, 2022). |

Table 1: Smart lock and controller hub vulnerabilities.

Vulnerability Analysis

To conduct a quantitative assessment of the vulnerabilities and potential attacks, the attribute domain “Minimal skill level needed for the proponent” (MSL) is used. The benefit of this domain is that it allows for pruning of the ADtree based on the risk tolerance of the average smart home user, who may be worried about stopping moderately skilled criminals, but may not be worried about foiling nation states.

This report uses MSL values adapted from the work of Thomas (2022) where 1 refers to a single low skilled attacker and 6 is a state actor with the highest level of funding, resources, and technical capabilities (Figure 1). Skill levels are assigned to vulnerabilities based on their overall difficulty of execution (Thomas, 2022).



Figure 1: MSL values and its metrics.

Research by Haney et al. (2020) suggests that most smart home users have a high security and privacy risk tolerance. This report accordingly prunes all ADtree leaves with an MSL of 4 or above.

Diagram

Description automatically generated

Figure 2: Controller hub vulnerabilities tree, its countermeasures and minimal skill required.

Diagram

Description automatically generated

Figure 3: Smart lock vulnerabilities tree, its countermeasures and minimal skill required.

Vulnerability Mitigations

To address the vulnerabilities with scores of 4 and below it is suggested to implement the countermeasures (Giese & Noubir, 2021; Brinson et al, 2021; Gordon et al, 2021; Tipton & Krause, 2007; Swatek, 2022; Estrin, 2018; Ciancoso et. al., 2017; Kheshaifaty & Gutub, 2020) presented in Figures 1 and 2.

Conclusion

Intelligent home device technology has recently improved and has been widely adapted worldwide. However, smart homes can pose huge potential risks. Through the use of attack-defence trees, this report illustrates which of these risks are most worrisome for smart home users and how to mitigate those risks.

References

Abrams, M. & Weiss, J. (2008) Malicious Control System Cyber Security Attack Case Study– Maroochy Water Services, Australia. *MITRE* 1(1): 1-16.

AlOtaibi, N. & Lombardi, F. (2021) Privacy and Security Evaluation of Amazon Echo Voice Assistant. [online] IEEE Xplore.

Barceló-Armada, R., Castell-Uroz, I. & Barlet-Ros, P. (2022) Amazon Alexa traffic traces. Computer Networks, 205, p.108782.

Brinson, R., Wimmer, H. & Booker, Q. (2021) Security Analysis of the Amazon Echo Dot. Issues in Information Systems, Volume 22, Issue 4, pp. 208-220, 2021.

Chung, H., Iorga, M., Voas, J. & Lee, S. (2017) ‘Alexa, Can I Trust You?’ Computer, [online] 50(9), pp.100–104.

Ciancoso, R., Budhwa, D. & Hayajneh, T. (2017) ‘A Framework for Zero Day Exploit Detection and Containment’ 2017 *IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech.* Orlando, Florida, USA, 6-10 November. New York: IEEE. 663-668.

Estrin, E. (2018) Best practices for using AWS access keys. Available from: <https://www.iucc.ac.il/en/blog/best-practices-for-using-aws-access-keys/> [Accessed 16 August 2022].

Swatek, F. (2022) Device spoofing a sign of serious mobile app security threats.Available from: <https://nethone.com/post/device-spoofing-sign-of-serious-mobile-app-security-threats> [Accessed August 16, 2022].

Giese, D. & Noubir, G. (2021) Amazon echo dot or the reverberating secrets of IoT devices. Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks.

Gilchrist, A. (2017) IoT security issues. De Gruyter, Incorporated, pp.76-80.

Gordon, H., Batula, C., Tushir, B., Dezfouli, B. and Liu, Y. (2021) Securing Smart Homes via Software-Defined Networking and Low-Cost Traffic Classification.

Hassani, R. (2020) Security Evaluation of a Smart System. *KTH Vetenskap Och Konst* (1)1: 1-46. <https://kth.diva-portal.org/smash/get/diva2:1533957/FULLTEXT01.pdf>

Haney, J., Furman, S. & Acar, Y. (2020) Smart Home Security and Privacy Mitigations: Consumer Perceptions, Practices, and Challenges. Available from: <https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=929479> [Accessed 13 Aug. 2022].

Kheshaifaty, N. & Gutub, A. (2020) Preventing Multiple Accessing Attacks via Efficient Integration of Captcha Crypto Hash Functions. *IJCSNS International Journal of Computer Science and Network Security* 20(9): 16-28.

Overstreet, D., Wimmer, H. & Haddad, R. J. (2019) Penetration Testing of the Amazon Echo Digital Voice Assistant Using a Denial-of-Service Attack. 2019 SoutheastCon.

Rose, A. & Ramsey, B. (2016) Picking Bluetooth Low Energy Locks from a Quarter Mile Away. DEF CON 24 Hacking Conference. Available from: <https://media.defcon.org/DEF%20CON%2024/DEF%20CON%2024%20presentations/DEF%20CON%2024%20-%20Rose-Ramsey-Picking-Bluetooth-Low-Energy-Locks-UPDATED.pdf> [Accessed 13 August 2022].

Tipton, H.F. & Krause, M. (2007) Information Security Management Handbook, Sixth edition, CRC Press, pp. 1220.

Thomas, M. A. (2022) Distinguishing Cyberattacks by Difficulty, International Journal of Intelligence and CounterIntelligence, DOI: 10.1080/08850607.2021.2018565. Available from: <https://www-tandfonline-com.uniessexlib.idm.oclc.org/doi/full/10.1080/08850607.2021.2018565> [Accessed 13 August 2022].

Wang, J., Hu, F., Zhou, Y., Liu, Y., Zhang, H. & Liu, Z. (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.

Wang, D., Ming, J., Chen, T., Zhang, X. & Wang, C. (2018) Cracking IoT Device User Authentication via Brute-Force Attack to SMS Authentication Code. *RESEC '18: Proceedings of the First Workshop on Radical and Experiential Security* 1(1): 57-60.

Wiggins, T. (2022). The weird ways your Amazon Echo can be hacked - and how to stop them. [online] The Ambient. Available from: <https://www.the-ambient.com/features/weird-ways-echo-can-be-hacked-how-to-stop-it-231> [Accessed 13 August 2022].