1. Introduction

The rapid development of the Internet of Things (IoT) has produced an ever-increasing number of networked devices that are used in almost all areas of life (Pedhadiya et al., 2019). However, this rapidly growing number of IoT devices has also brought with it increased complexity and heterogeneity of the communication standards used (Augusto-Gonzalez et al., 2019). As a result, many of these standards are vulnerable to security threats, as well as interoperability and scalability issues (Touqeer et al., 2021).

IoT devices in the field of smart homes have the primary purpose of making everyday life easier for users. Smart devices such as smart electric shutters or heaters can also increase energy efficiency, and smart door locks and surveillance cameras can contribute to the security of the residents of a smart home. However, malicious access and intervention in such IoT devices can also result in serious dangers. For example, users have already been falsely warned of the impact of a ballistic missile via their smart home device (Hollister, 2019). In another case, smart home residents heard voices from a camera implemented on the network and the hacker took control of the smart thermostat, increasing the indoor temperature to 32°C (Maher, 2019).

Spoofing attacks can be used to spy on victims, which not only compromises their right to privacy, but also information about the behaviour and routines of the victims can be collected, which could be misused for burglaries, social engineering attacks or extortion (Allhoff & Henschke, 2018). Denial of service attacks can render devices inoperable, so that functions of the smart home fail and physical damage can occur. However, the protection provided by IoT security devices can also be significantly impaired. Man-in-the-middle attacks can not only be misused for espionage. With replay attacks, devices connected to the smart home network can be controlled remotely, which not only impairs their functions, but can also be used against the legitimate user. These examples represent only a few practical consequences resulting from the theory of possible threats to smart homes.

One promising attempt to address these challenges is the Matter communications standard, formerly known as Project CHIP, developed by leading technology companies and industry partners (CSA, N.D.a).

1.1 Ethical considerations in IoT

Malicious manipulation of IoT devices can cause them to stop working or malfunction, resulting in device function failure or being used for malicious actions that can result in both financial and physical damage to devices or even people. The psychological component of a successful attack on the smart home should also not be underestimated. Many people perceive their own home as a safe and private place. The psychological consequences of a hacking attack on the victim's home can be the same as those associated with a physical burglary (Brantly, 2017). These include the feeling of insecurity in one's own home, powerlessness and helplessness, a permanent feeling of anxiety, stress and sleep disorders (Wollinger et al., 2014).

In addition to the individual dangers that exist as a consequence of a hacking attack on IoT devices in the smart home network, threats on a macroscopic level must also be taken into account. According to Statista (2022), there were 8.6 billion IoT devices in 2019 and 13.14 billion in 2022 in use. This large number of Internet-enabled devices can pose an enormous risk potential if they are not adequately secured, as they can be misused for Distributed Denial of Service (DDoS) attacks. The consequences of such attacks can be the collapse of parts of the Internet. The fact that these devices pose a serious threat was shown by the Mirai botnet, which blocked access to over 1200 websites for almost a day in 2016 as a result of a DDoS attack using corrupted IoT devices (Zhang et al., 2020). It is important to note that this attack involved *only* 100,000 malicious endpoints (Woolf, 2016).

Manufacturers of IoT devices therefore have a responsibility towards users and society as a whole to adequately protect these devices from malicious manipulation. However, it must be taken into account that security applications in IoT devices are in some cases more difficult to integrate than in conventional Internet-enabled devices, since IoT devices are limited in their technology. A restricted size, limited performance capacities and the need for a low power consumption mean that conventional protective measures cannot always be implemented (Hameed & Alomary, 2019). It should also be noted that the economics of manufacturing IoT devices contribute to the vulnerability of these devices. A key goal of many companies in the manufacture of IoT devices is to develop cost-effective devices. However, the development and implementation of security features is associated with a cost factor that is often neglected (Holz, 2022). Also, in many cases, IoT devices are used for long periods of time without being replaced. Without appropriate updates, these devices may not be protected against newly discovered vulnerabilities (Chantzis et al., 2021).

Matter has been proposed as a mitigation against these threats by standardising the communication standard and the associated regulations. Standardisation is intended to reduce cost factors in the development of security components and strengthen long-term resilience (CSA, N.D.a). With these promises, Matter is therefore responsible for coordinating sufficient security standards among the manufacturers and for protecting end users and society from threats arising by Matter devices.

1.2 Research question and validation approach

This scientific work focuses on the central question of whether the Matter communication standard is able to overcome the vulnerabilities of Bluetooth sniffing, de-authentication attacks, as well as replay attacks. The aim is to examine how Matter is structured, to what extent common security features have been taken into account by the standards used and are operating under Matter, and what the resilience of Matter networks is in relation to hacking attacks.

To carry out the tests within the scope of this project, networks of Matter-capable devices were created on the basis of the publicly available reference implementations and the experiments were executed on them. Test networks were created based on the respective communication standard and the experiments were also carried out on them to compare Matter to the standards used by Matter. This should on the one hand confirm the basic functioning of the hacking attacks and on the other hand create a basis for comparison to validate results and to compare Matter with other standards.

1.3 Structure of the project

This thesis comprises the following structure. In chapter 2 a literature review of the most important advantages and disadvantages as well as the dominant vulnerabilities of common IoT communication standards in use is carried out. Chapter 3 covers the Matter communication standard, its goals and principles, as well as the structure and security aspects relating to the standard. In chapter 4 the methodology of the project is discussed and then in chapter 5 the procedure of the experiments and their results are presented. Finally, in Chapter 6, a discussion of the test results obtained and the associated conclusions took place.

References

Allhoff, F. & Henschke, A. (2018) The internet of things: Foundational ethical issues. *Internet of Things* 1 55-66. Available from: https://www.sciencedirect.com/science/article/pii/S2542660518300532 [Accessed 03 April 2023].

Augusto-Gonzalez, J., Collen, A., Evangelatos, S., Anagnosopoulos, M., Spathaoulas, G., Giannoutakis, K. M., Votis, K., Tzovaras, D., Genge, B., Gelenbe, E. & Nijdam, N.A. (2019) 'From Internet of Threats to Internet of Things: A Cyber Security Architecture for Smart Homes', *International Workshop on Computer Aided Modeling and Design of Communcation Links and Networks*. Limassol, Cyprus, 11-13 September. IEEE. 1-6. Available from: https://ieeexplore.ieee.org/abstract/document/8858493 [Accessed 01 September 2023].

Brantly, A. F. (2017) The violence of hacking: state violence and cyberspace. *The Cyber Defense Review* 2(1): 73-92. Available from: https://www.jstor.org/stable/26267402 [Accessed 04 April 2023].

Chantzis, F., Stais, I., Calderon, P., Deirmentzoglou, E. & Woods, B. (2021) *Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things*. No Starch Press. Available from: https://learning.oreilly.com/library/view/practical-iot-hacking/9781098128876/c02.xhtml#h1-500907c02-0002 [Accessed 23 March 2023].

CSA (N.D.a) The Foundation for Connected Thing. Available from: https://csa-iot.org/all-solutions/matter/ [Accessed 16 March 2023].

Hameed, A. & Alomary, A. (2019) 'Security issues in IoT: A survey', *International conference on innovation and intelligence for informatics, computing, and technologies*. Sakhier, Bahrain, 22-23 September. IEEE. 1-5. Available from: https://ieeexplore.ieee.org/abstract/document/8910320 [Accessed 31 July 2023].

Hollister, S. (January 23, 2019) No, Nest Cams are not being hacked to issue fake nuclar bomb threats. *The Verge*. Available from: https://www.theverge.com/2019/1/22/18193721/nest-cam-hack-north-korea-ballistic-missile-nuclear-threat-debunk [Accessed 03 April 2023].

Holz, T. (2022) Why is the Internet of Things So Hard to Secure? *Keyfactor*. Available from: https://www.keyfactor.com/blog/why-is-the-internet-of-things-so-hard-to-secure/ [Accessed 04 April 2023].

Maher, J. (September 23, 2019) Hacker Takes Over Couple's Smart Home, Plays Vulgar Music And Raises Temperature to 90 Degrees. *Newsweek*. Available from: https://www.newsweek.com/google-nest-hack-milwaukee-1460806 [Accessed 03 April 2023].

Pedhadiya, M. K., Jha, R. K. & Bhatt, H. G. (2019) Device to device communication: A survey. *Journal of Network and Computer Applications* 129(1): 71-89. Available from:

https://www.sciencedirect.com/science/article/pii/S1084804518303345 [Accessed 01 September 2023].

Statista (2022) Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030. Available from: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ [Accessed 04 April 2023].

Touqeer, H., Zaman, S., Amin, R., Hussain, M., Al-Turjman, F. & Bilal, M. (2021) Smart home security: challenges, issues and solutions at different IoT layers. *The Journal of Supercomputing* 77(12): 1453-14089. Available from: https://link.springer.com/article/10.1007/s11227-021-03825-1 [Accessed 02 September 2023].

Wollinger, G. R., Dreißigacker, A., Blauert, K., Bartsch, T. & Baier, D. (2014) Wohnungseinbruch: Tat und Folgen. Kriminologische Forschungsinstitut Niedersachsen e.V. Available from: https://kfn.de/wp-content/uploads/Forschungsberichte/FB_124.pdf [Accessed 04 April 2023].

Woolf, N. (October 26, 2016) DDoS attack that disrupted internet was largest of its kind in history, experts say. *The Guardian*. Available from: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet [Accessed 04 April 2023].

Zhang, X., Upton, O., Beebe, N. L. & Choo, K. K. R. (2020) Iot botnet forensics: A comprehensive digital forensic case study on mirai botnet servers. *Forensic Science International: Digital Investigation 32*: 300926. Available from: https://www.sciencedirect.com/science/article/pii/S2666281720300214 [Accessed 04 April 2023].