On the Security of Internet of Things Devices

Torlakov I.

***Abstract*—In this paper, a review is made about the technological development in Internet of Things (IoT) security over the past decade, emphasizing critical aspects such as authentication, encryption methods, and vulnerability mitigation techniques. The rapid development and widespread adoption of Internet of Things (IoT) devices have significantly increased security challenges, presenting unique vulnerabilities and threats. It outlines practical security considerations relevant to software developers and engineers, highlighting best practices and current trends in secure IoT application design. The study also briefly addresses open challenges and identifies promising future directions to guide further technological improvements in IoT security.**

***Keywords*—Internet of Things, IoT Security, Vulnerabilities, Authentication, Encryption**

I. Introduction

Over the past decade, the Internet of Things (IoT) has become one of the fastest growing and most widely deployed technology areas. IoT devices are finding applications in a growing number of areas, including smart homes, industrial automation, healthcare, intelligent transportation, agriculture and many more. The rapid expansion of IoT technologies has led to increased functionality, convenience and efficiency, but has also posed serious information security challenges [1],[2]. The diversity of IoT devices, their massive usage, limited hardware resources and the heterogeneity of communication protocols make the security of these systems a particularly complex task. This leads to the emergence of specific vulnerabilities that differ significantly from traditional information technology systems and require new approaches to protection [3]. Real-world incidents such as the large-scale DDoS attack , like the Mirai botnet attack in 2016, which exploited vulnerable IoT devices, highlight the need for a comprehensive and systematic approach to the security of these devices. The main IoT security challenges can be divided into several areas: authentication, encryption and vulnerability mitigation mechanisms. Over the last ten years, much research has focused on improving and developing new technologies and standards in these areas. However, there is a lack of a systematic and detailed overview that integrates the accumulated knowledge and experience into a clear framework that is easily applicable to engineers and researchers working in the field.

The purpose of this paper is to review and analyze the major technological developments in IoT device security over the past decade. The publication examines existing vulnerabilities in detail, presents authentication and encryption technologies, analyzes current security approaches and derives recommendations for good engineering practices. The publication will benefit researchers and engineers seeking to understand the current state of the field and implement the most effective solutions available.

II. Overview of existing vulnerabilities and threats

Over the past decade, IoT device security has established itself as one of the most active areas in information security. The diversity of devices, standards and communication technologies determines a wide range of potential vulnerabilities and threats. This section discusses and classifies the key categories of IoT device vulnerabilities, as well as sample incidents and attacks that have gained attention in the past years. Vulnerabilities in IoT systems can be broadly classified into three main categories according to the layer at which they occur: hardware, software and network vulnerabilities [4].

Hardware vulnerabilities are limited resources, e.g. small memory size, weak processors, etc., which make it difficult to use efficient encryption and authentication algorithms. Physical access to devices and the ability to extract cryptographic keys and sensitive information (e.g. through side-channel attacks). Vulnerabilities are seen in the sensors and components used that can be exploited for unauthorized access or data manipulation.

Software vulnerabilities are in operating systems and firmware, e.g. insufficient security updates, lack of automatic update systems. Insufficient security testing in application development leading to frequent exploits such as buffer overflow, code injections and Application Programming Interface (API) exploits. Another vulnerability is the weak implementation of authentication mechanisms and cryptographic protocols, allowing authentication to be compromised.

Network vulnerabilities include unprotected network protocols, like MQTT, CoAP, which can be easily exploited by various man-in-the-middle (MITM) attacks. Improperly configured network components, namely firewalls and gateways, allowing unauthorized access by a foreign user. Identity management issues and insufficient segmentation of networks running IoT devices.

The main reasons for the vulnerabilities described include insufficient security design, with IoT devices often being developed with a focus on cost, functionality and speed to market, leading to compromises in security measures. The lack of universal and mandatory standards makes it difficult to enforce effective security practices. Limited user and developer awareness and training and insufficient attention to IoT product security during development and use.

Numerous high-profile incidents involving the exploitation of vulnerable IoT devices have been observed in recent years. For the purpose of this study, let us examine the most renowned entities that have significantly influenced the IoT ecosystem.

The Mirai botnet, which was active in 2016, has become a benchmark for the danger of compromised IoT devices. The malware, which uses factory-set or weak passwords for authentication, managed to infect over half a million

devices, carrying out a massive DDoS attack on critical Internet services [5].

The following year at St. Jude Medical, a vulnerability was identified in medical IoT devices (pacemakers) that allowed potential unauthorized access and even modification of the devices' modes of operation, endangering patients' lives [6].

In the same year, BrickerBot software attacked IoT devices whose passwords were weak or factory passwords, using an older version of SSH and Telnet for a brute force attack. Once it gained access, it deleted firmware and configuration files, rendering the devices unusable. This type of attack is known as Permanent Denial-of-Service (PDoS). BrickerBot has affected millions of devices worldwide [7].

Reaper, also known as IoT Troop, is a botnet that exploits vulnerabilities in the software of IoT devices instead of relying solely on weak passwords like Mirai. It has infected over a million networks using exploits for various vulnerabilities in popular IoT devices [8].

The VPNFilter malware affected over 500,000 routers and IoT devices, allowing attackers to collect data, reroute traffic, and even block the device in the subsequent year of 2018 [9].

Next year Mozi, which is a peer-to-peer (P2P) botnet that uses a BitTorrent-like network to infect IoT devices such as routers and digital video recorders (DVRs). It exploits weak Telnet passwords and multiple unpatched vulnerabilities in IoT devices. Mozi has been used to conduct DDoS attacks, extract data, and execute commands or load malware [10].

In 2020, Ripple20 vulnerabilities manifested, which is a series of critical vulnerabilities identified in a popular TCP/IP library used by millions of IoT devices. The vulnerabilities allow remote code execution and compromise of the networks in which the devices are plugged [11].

These incidences and numerous others unequivocally illustrate the necessity for a comprehensive methodology to secure IoT devices and infrastructures. The main reasons for the vulnerabilities described include insufficient security design, with IoT devices often being developed with a focus on cost, functionality and speed to market, leading to compromises in security measures. The lack of universal and mandatory standards makes it difficult to enforce effective security practices. Limited user and developer awareness and training and insufficient attention to IoT product security during development and use.

III. Using the Template

To address the identified vulnerabilities and threats, various methods and technologies have been developed over the last decade to provide information security in IoT devices. Some of the most significant protection measures in the field are authentication, encryption and vulnerability mitigation.

A. Authentication

Authentication is a key element of IoT security, ensuring that the device is communicating with legitimate and trusted systems and users. The most common and easy to implement method, which is however vulnerable to weak passwords and poor key management, is Pre-Shared Keys, (PSK) [12]. Examples of improvements include automatically generated and rotary keys that are subject to brute-force attacks. Authentication through digital certificates uses cryptographic certificates, which are difficult to forge and provide a strong basis for trust. The approach requires a centralized public key infrastructure (PKI), which can be challenging for resource-constrained IoT devices [13]. Such examples are X.509, SSL/TLS.

Another approach is to use unique biometrics, such as fingerprints, voice, facial recognition, which increases the level of security, but increases the computational requirements and has potential privacy issues [14]. Two-factor authentication (2FA) is the combination of two different methods, e.g., a password plus a temporary token, which significantly improves security and reduces the risk of unauthorized access [15]. The most commonly used example is a temporary token that is generated on a device that is managed by the IoT administrator on the network.

B. Encryption

Encryption of communications ensures confidentiality and protection against eavesdropping and data manipulation. The main methods used include symmetric and asymmetric algorithms, cryptographic protocols.

Advanced Encryption Standard (AES) is widely used due to efficiency and relatively low hardware requirements. It was developed by the National Institute of Standards and Technology (NIST) in 2001 and works as a block cipher. AES-128 and AES-256 are among the most popular solutions for IoT applications, providing good security with appropriate key management [16].

Another mechanism is the use of asymmetric algorithms such as Rivest–Shamir–Adleman (RSA) proposed in 1977 and Elliptic-curve cryptography(ECC) presented in 1985. RSA is widely used but for IoT devices ECC is becoming preferred due to smaller key sizes and lower computational requirements suitable for resource constrained devices [17].

The use of cryptographic protocols, such as Transport Layer Security/Secure Sockets Layer (TLS/SSL), Datagram Transport Layer Security (DTLS), Message Queuing Telemetry Transport (MQTT) with TLS, and others, is a way to deal with device security. TLS and DTLS have been enforced as standard solutions for securing communication between IoT devices and cloud or edge systems. MQTT with TLS is also used to secure IoT real-time communications [18].

C. Vulnerability Mitigation

Effective mitigation of vulnerabilities in IoT systems requires a comprehensive approach, including both preventive measures and attack detection and response mechanisms. Automatic firmware and software update and patching systems significantly reduce the risk of exploiting known vulnerabilities. This requires robust authentication and encryption mechanisms for updates [19]. Combining secure connection and update increases the security level of IoT devices. Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS) monitor network traffic and device behavior, detect suspicious activity, and take automatic protection measures [20]. Commonly used solutions are based on machine learning, which increases

the effectiveness in detecting new and unknown threats. IDS detects attacks and malicious actions in the network traffic by comparing it against common signatures and rules. On the other hand IPS Prevents malicious actions by blocking or cutting off network traffic identified as harmful.

Segmentation and network partitioning, in particular isolating IoT devices into separate network segments, reduces the potential harm of compromising a single device. Virtual Local Area Networks (VLAN) and network micro-segmentation are commonly used approaches to limit the spread of attacks [21]. This allows grouping devices based on their function and can simplify network management. Reducing the size of the broadcast domains can improve the network performance which is crucial fo the IoT devices. Limit physical access and hardware protection by using secure hardware like Trusted Platform Module (TPM), protection against physical tampering and tamper-resistant devices, and secure storage of keys and sensitive data [22].

Table 1 provides a summary of security technologies in IoT. These technology approaches form the basis for building secure IoT systems and applications.

TABLE I
SECURITY TECHNOLOGIES IN INTERNET OF THINGS

Domain	Methods and technologies	Application for IoT
Authentication	Passwords, PSK, X.509, biometrics, two-factor authentication	High with appropriate choice of method
Encryption	AES, RSA, ECC, TLS, DTLS, MQTT/TLS	High (AES, ECC, TLS/DTLS)
Vulnerability mitigation	IDS/IPS, automatic updates, VLAN segmentation, TPM hardware	High, but depends on the specific environment

IV. ANALYSIS

Authentication methods are central to IoT security as they ensure that communication only takes place between trusted parties. The choice of approach depends largely on the resources and application domain of the devices. A strength of the password and PSK approach is the simplicity of implementation and low cost. The main disadvantage is the high vulnerability to weak passwords and inappropriate key management. Best practices include the use of automated mechanisms for key generation and periodic change, as well as management through dedicated IoT management platforms [9]. Digital certificates provide a high level of security and reliability, especially for industrial and critical applications. A major drawback is the need to build and maintain a PKI infrastructure, which can be cumbersome and expensive for small devices and small IoT networks. In such cases, ECC certificates are preferable to RSA due to the smaller key size [17]. Biometric and two-factor methods are primarily suitable for devices with sufficient computing resources and for scenarios where security and user identification are critical. Medical devices are such an example. Two-factor authentication significantly improves security but introduces additional complexity that may not be suitable for all application scenarios [15].

Encryption is critical to prevent eavesdropping and data manipulation. However, the selection of an appropriate algorithm depends on the resources and security requirements of the devices. Using AES is universally applicable to most IoT devices due to the balance between security and performance. However, the key problem is symmetric key management - if the keys are compromised, the security of the entire system is compromised [16]. On the other hand, ECC versus RSA provides significantly better performance in terms of efficiency, especially in resource-constrained devices. RSA remains applicable in IoT systems with more computational resources, but in practice ECC is considered more suitable and is preferred in modern IoT implementations [17]. The TLS/DTLS and MQTT protocols with TLS have established themselves as standards for secure communication. DTLS is particularly suitable for IoT applications using the User Datagram Protocol (UDP) protocol where standard TLS is not applicable. A major weakness of these protocols is the additional consumption of resources, namely CPU, memory, energy, which may limit their use in devices with extremely limited resources [18].

Automatic updating and paging is efficient but requires a high level of automation and security of the update mechanisms. It is critical that all updates are cryptographically protected and authenticated to avoid the risk of submitting false or compromised updates [16]. The use of IDS and IPS is highly effective in detecting attacks and abnormal behavior from the normal. However, these solutions can be limited by high computational resource requirements and frequent false-positive alerts if not set up correctly. The use of machine learning helps to reduce false positives but adds complexity and additional computational requirements [20]. This addition power can be balanced by using a more powerful processor or chip. Segmentation and hardware protection are key approaches to reduce the risk of compromise and limit potential harm. These techniques are highly effective and relatively easy to implement in large infrastructures. However, they require careful planning and appropriate network architecture [21], [22].

Based on the critical analysis presented, good security practices include:

- Use ECC certificates and two-factor authentication for devices with high security requirements;
- AES-128/256 encryption with appropriate key management for most IoT applications;
- Implement automated and cryptographically secure firmware and software update systems;
- Network segmentation via VPNs and IDS/IPS solutions for large and critical IoT networks.

These practices provide effective protection against most known threats and provide a solid foundation for future IoT security development.

Despite significant advances in IoT device security, many important questions and challenges have remained open in recent years that require further attention and research. Key open issues in IoT device security include the scalability of security solutions, their integration, the energy efficiency of devices, security in new models, privacy, and others. With billions of connected devices, ensuring the scalability of authentication, key management and encryption mechanisms remains a major challenge. There is a need for efficient and lightweight protocols that are both secure and applicable in very large IoT ecosystems. The lack of uniform security standards and the diversity of communication protocols and hardware platforms complicate integration and security management. There is a

need to develop standardized and universally applicable security methods that are easy to adapt in different scenarios.

On the other hand, most IoT devices are limited in resources such as memory, processing power, and batteries. Building energy-efficient cryptographic algorithms and security protocols that simultaneously provide a high level of protection remains an important unsolved problem. The growing edge-computing and fog-computing computing paradigms introduce additional complexity and new potential vulnerabilities. Security issues in these models, including trust management and secure communication between edge and cloud components, require further research and development. The increasing proliferation of IoT devices raises serious privacy issues. Innovative solutions are needed to ensure privacy without compromising the functionality and performance of the systems.

Based on the open issues in the IoT devices, the following promising directions for future IoT security developments can be proposed. Continue work on the development and optimization of cryptographic algorithms e.g., lightweight variants of known solutions such as AES-128, that provide a balance between security and resource efficiency. Exploring the application of blockchain for secure and decentralized authentication and trust management in IoT ecosystems. This direction has the potential to solve some of the scalability and centralized management issues. Further develop and deploy artificial intelligence-based IDS and IPS systems to detect and prevent threats more intelligently and with fewer false-positives.

Particularly important is work to reduce computational requirements to make such solutions applicable on limited devices. Development of new materials and technologies enabling physical protection of devices as well as integration of hardware security modules specifically optimized for IoT. Actively participate in the creation of international and industry standards to unify security requirements and methods and facilitate their integration and mass deployment.

In short, future research and development in IoT security should focus on addressing issues related to scalability, energy efficiency, data security, and standardization. Integrating advanced technologies such as blockchain, machine learning, and optimized cryptographic approaches will be critical to achieving sustainable advances in the security of IoT devices and infrastructures.

V. Conclusion

Over the past decade, IoT device security has emerged as a critical area of information security driven by the widespread adoption and diversity of IoT technologies and applications. This publication systematizes the key technological developments and approaches for securing IoT devices, highlighting both their strengths and limitations, and outlines best practices useful for engineers and researchers.

The main classes of vulnerabilities - hardware, software and network - are discussed in detail, as well as real incidents demonstrating the need for a more thorough approach to security. Authentication technologies, including digital certificates and two-factor authentication, encryption methods such as AES and ECC, and vulnerability mitigation mechanisms such as automatic updates and IDS and IPS solutions are analyzed. Critical analysis shows that despite significant progress, many challenges remain for IoT security, such as scalability, standardization and resource efficiency. These open issues form the basis for future research and development, including the creation of lightweight cryptographic algorithms, integration of AI security technologies, and standardization of solutions.

The systematic review presented in this publication provides a solid foundation for future security developments in the IoT field and serves as a starting point for engineers and researchers who wish to deepen their knowledge and put effective solutions into practice. In conclusion, only through an integrated approach combining innovative technology solutions, good engineering practices and standardization can the sustainable security of IoT ecosystems be ensured in the coming years.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.

[2] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," IEEE Internet Things J., vol. 6, no. 5, pp. 8182–8201, Oct. 2019, doi: 10.1109/JIOT.2019.2935189.

[3] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," J. Inf. Secur. Appl., vol. 38, pp. 8–27, Feb. 2018, doi: 10.1016/j.jisa.2017.11.002

[4] M. Abomhara and G. M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," J. Cyber Secur. Mobility, vol. 4, no. 1, pp. 65–88, Jan. 2015, doi: 10.13052/jcsm2245-1439.414.

[5] M. Antonakakis et al., "Understanding the Mirai Botnet," in Proc. 26th USENIX Security Symp., Vancouver, BC, Canada, 2017, pp. 1093–1110.

[6] FDA, "Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter," FDA Safety Communication, Jan. 2017. [Online]. Available: https://www.moph.gov.lb/userfiles/files/Medical%20Devices/Medical%20Devices%20Recalls%202017/16-1-2017/St_JudeMedicalimplantablecardiacdevices.pdf.

[7] CISA, "BrickerBot Permanent Denial-of-Service Attack (Update A)," ICS Alert ICS-ALERT-17-102-01A, Cybersecurity & Infrastructure Security Agency, U.S. Dept. of Homeland Security, Apr. 18, 2017. [Online]. Available: https://www.cisa.gov/news-events/ics-alerts/ics-alert-17-102-01a.

[8] B. Schneier, "Reaper Botnet," Schneier on Security blog, Oct. 24, 2017. [Online]. Available: https://www.schneier.com/blog/archives/2017/10/reaper_botnet.html

[9] Cisco Talos, "VPNFilter malware analysis," Cisco Talos Intelligence Group, May 2018. [Online]. Available: https://blog.talosintelligence.com/vpnfilter/.

[10] D. Atch, G. Regev, and R. Bevington, "How to proactively defend against Mozi IoT botnet," Microsoft Security Blog, Aug. 19, 2021. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2021/08/19/how-to-proactively-defend-against-mozi-iot-botnet/

[11] JSOF Research Lab, "Ripple20: Critical vulnerabilities in TCP/IP software library," JSOF, Jun. 2020. [Online]. Available: https://www.jsof-tech.com/ripple20/.

[12] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," Future Gener. Comput. Syst., vol. 89, pp. 110–125, Dec. 2018, doi: 10.1016/j.future.2018.06.027.

[13] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, Internet Engineering Task Force, Aug. 2018. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc8446.

[14] M. Ometov et al., "Multi-Factor Authentication: A Survey," Cryptography, vol. 2, no. 1, p. 1, 2018, doi: 10.3390/cryptography2010001.

[15] Y. Liu et al., "Two-factor authentication schemes for IoT devices: A survey," IEEE Internet Things J., vol. 9, no. 5, pp. 3648–3664, Mar. 2022, doi: 10.1109/JIOT.2021.3106544

[16] NIST, "Advanced Encryption Standard (AES)," FIPS PUB 197, National Institute of Standards and Technology, U.S. Dept. Commerce, Nov. 2001, doi: 10.6028/NIST.FIPS.197

[17] V. S. Miller, "Use of Elliptic Curves in Cryptography," in CRYPTO '85, Berlin, Heidelberg: Springer-Verlag, 1986, pp. 417–426.

[18] A. Banks and R. Gupta, "MQTT Version 3.1.1," OASIS Standard, Oct. 2014. [Online]. Available: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf.

[19] ENISA, "Good Practices for Security of IoT," European Union Agency for Cybersecurity (ENISA), Nov. 2019. [Online]. Available: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1/

[20] A. Shafiq, H. T. Ngu, N. H. Tran, Z. Han, and C. S. Hong, "Machine Learning Methods for Cyber Security Intrusion Detection: Datasets, Techniques, and Challenges," IEEE Commun. Surv. Tutor., vol. 22, no. 3, pp. 1725–1765, Thirdquarter 2020, doi: 10.1109/COMST.2020.2986444.

[21] Cisco, "Segmenting Networks and IoT Devices to Mitigate Risk," Cisco White Paper, San Jose, CA, USA, Jan. 2021.

[22] Trusted Computing Group, "Trusted Platform Module (TPM) Specification," TCG Published Specifications, 2020. [Online]. Available: https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/