Challenges of IoT Security

Lena Boeckmann

HAW Hamburg, Germany
lena.boeckmann@haw-hamburg.de

Abstract. The Internet of Things is getting more relevant in many areas and aspects of our lives, which leads to a constantly growing number of devices worldwide. This growth comes with a heightened threat potential and increasing numbers of IoT related cyber security attacks. Not only user privacy and sensitive enterprise data are at risk, but also health and safety, when connected devices are used in the industry, public infrastructure and medical treatments. The size, heterogenity and constraints of the IoT require the development of new approaches to security, including specialized software and hardware design, communication protocols, regulations and standardizations. This work analyzes recent publications and reports to summarize the challenges of securing IoT systems and how IoT security has developed recently.

Keywords: IoT · IoT Security · Cyber Security · Embedded Systems.

1 Introduction

Table 1: Classes of constrained devices [21]

Class	Data Size	Code Size
0	$< 10KiB$	$< 100KiB$
1	$\sim 10KiB$	$\sim 100KiB$
2	$\sim 50KiB$	$\sim 250KiB$

The internet of things (IoT) consists of physical objects, which are extended by embedded electronics, sensors, processor capabilities and software, that communicate and exchange data with other devices and systems over the internet. There are many application areas for the IoT. Smart devices are being used to protect workers in harsh environments, regulate production processes in industrial plants, or monitor the health of patients. Connected devices increasingly find their ways into people's personal lives in the shape of smart household devices (e.g. vacuum cleaners, smart heating systems, alarm systems), fitness trackers and much more. Also public infrastructure relies on the IoT, connecting smart meters in buildings, tracking waste disposal of whole neighbourhoods

and regulating traffic. Their numbers keep growing, with an expected amount of over 50 billion by 2025 [24]. Each device connected to the internet is a potential attack point [25], so along with the number of devices, the attack surface is also growing.

The IoT is very heterogeneous, consisting of many different types of devices. They offer a broad range of capabilities and most are highly constrained in the amount of available memory, processing capabilities and battery. In general they are divided into several classes, shown in Table 1. Class 0 devices are the most constrained, often highly specialized and do not run an operating system [23]. They don't have the capabilities to run a network stack and need an intermediate node to communicate over the internet. Class 1 and 2 devices are less constrained and less specialized [23]. Thus they can run larger applications and IoT-specific operating systems. They can complete more complex tasks and communicate over the internet by utilizing lightweight, optimized wireless protocols.

The increase in device numbers, their heterogenity and their constraints come with new challenges and require new approaches to the security of IoT systems [19,22,25]. The following sections summarize the individual challenges, the recent development of IoT related cyber attacks as well as legal and political approaches to the problems.

2 Security Challenges

2.1 Low-Cost Production

Often the devices that are part of the IoT perform entirely unrelated functions, with connectivity only being an additional feature (e.g. household devices). This means that the main business of manufacturers lies often in a different sector and often they are unexperienced in the IT sector. Manufacturers seek to reduce time-to-market and to lower the cost of production, often at the expense of security functionality [29]. Radio transmission, communication and cryptogaphy to secure said communication require a lot of resources, which is why the IoT needs optimized, lightweight communication protocols and crypto operations.

Especially cryptography is a challenge, since the operations require much energy, processing time and memory. Asymmetric crypto, which is often used for authentication and verification, operates on large keys, which need to be stored in sufficiently large memory. Increasingly IoT platforms offer cryptographic co-processors to offload the main CPU when performing crypto operations, some of which also offer secure key storage. Those are much faster and more efficient than software implementations [26]. Highly constrained devices can also be extended by external crypto processors, called *secure elements*, which offer a range of operations in hardware as well as protected key storage. IoT OSes are already adapting to integrate the plethora of different crypto implementations at system level [20].

To save money, manufacturers often use open source software and generic hardware, which are often overprovisioned and not optimized for their use case.

If unused features and services are not disabled before deployment, they may expose open ports and increase the system's attack surface [30]. Knowing which services are needed and which should be disabled, requires extensive knowledge of developers, who often lack expertise in security and IoT-related topics [19,28]. Lack of experience also leads to insecure programming practices [30], which are enhanced by the common use of C and C++ language in implementations, which are known to have many exploitable vulnerabilities [19].

Additionally the frequent use of and dependencies on open source software (OSS) can help spread vulnerabilities, a recent example being the Log4j vulnerability [13]. Log4j is an OSS library for logging and is being used as a part of larger software systems worldwide. The vulnerability allowed attackers to steal data, break into systems and spread malware.

2.2 Heterogentity in Hardware and Interfaces

As mentioned before, devices differ widely in capabilities and constraints and there is no clear definition of what an IoT device is. It is therefore difficult to define common hardware and software standards that work for all devices. More complex applications and secure communication protocols may not work in highly constrained environments. If a system consists of many specialized devices, that perform different tasks, it is a challenge to manage and update them in an efficient way. IoT specific OSes can help with this, but may also not work on very small devices [19].

This heterogenity makes it difficult find universal solutions for all devices. The scale of the IoT and its attack surface make complete security impossible and there will always be a tradeoff between security and performance [22]. Security assessment frameworks and standards could help developers build systems, that are more secure, but even though many frameworks and standards exist in the IT security sphere in general, none of them address all the requirements and challenges of developing secure IoT systems [22].

Interfaces to interact with IoT systems also differ from the familiar keyboard and monitor use and may vary depending on the device and manufacturer. Non-standard interfaces for configuration and device interaction might be smart phone apps, cloud management services or voice control. If a system consists of various devices with different interfaces, it becomes hard to manage. Also each new interface broadens the attack surface. Therefore they need individual protection measures that are adapted to their functionality. For example, when interacting with a device through voice control, voice inputs must be checked to make sure only authorized users gain access [19].

2.3 Deployment "In the Wild" and Cyberphysical Interaction

IoT devices interact with their environment through sensors and actuators. Sensors measure environmental states of temperature, humidity, light, etc. This data then needs to be analyzed, which happends either on a more capable IoT device close to the sensor (Fog computing) or on a remote server with large storage and

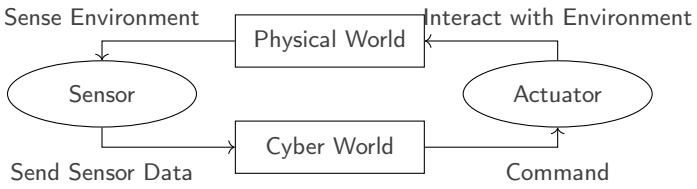

Fig. 1: Schema of a cyberphysical system

processing capabilities (Cloud computing). The latter requires secure data transmission over the internet. Depending on the sensor data, a system may trigger actuators, which can then modify the environment, e.g. by changing the room temperature. An attack on such a cyberphysical system (as shown in Figure 1) allows direct impact on the real world, possibly resulting in real-life damage or even endangering lives. For example, if an attacker can access a sensor, they might be able to manipulate the measured values and use it to impact system behaviour.

In addition to that, devices are often deployed "in the wild" and left unattended. This makes them vulnerable to physical attacks, leading to the exposure of cryptographic keys and other sensitive data.

Sensors of IoT systems record data about their environments and users, such as fitness data, information about the location, the use of water and power, etc. [19, 28]. Especially in the medical sector they monitor and analyze sensitive medical data of patients.

Data-linking from several sources may allow bad actors to draw conclusions about the private life of device owners (such as when they are at home or what their house looks like) or enterprise information. Therefore data must be encrypted during transmission and stored securely, while devices need tamper protection and must be physically secured from unauthorized access. To prevent data theft, only a limited amount of data and information should be stored on individual devices [19].

2.4 Configuration and Updates

End-users of IoT products prefer easy-to-use devices, that are easy to configure and deploy and can be "set and forgotten" [19]. Often they are unaware of the security issues and fail to implement basic security measures, like changing default passwords [28]. After configuring and setup, they may not realize that their device is set up in an insecure way, as long as it operates as expected. If they learn that a device also works without secure configuration, they may also neglegt the configuration of other devices in the future. New standards are needed to make sure the devices cannot not be set up and used in an insecure way (e.g. secure default passwords, secure default configuration parameters).

Often, multiple vulnerabilities are exposed over the years after a device has been deployed. Insecure devices allow attackers to infiltrate networks or infect

those devices with malware to integrate them into botnets used for Distributed Denial of Service (DDoS)attacks [18]. To prevent this, frequent software and firmware updates are required to patch those vulnerabilities [30]. Since end-users are not reliable to regularly check for updates and manually install them [19,28], we need different approaches. Automatic or manufacturer-controlled updates are an option, but may not always be available, due to unstable or infrequent internet connection or device constraints. In that case, device owners must be notified, so they can take care of updates themselves. Transferring update management to a third-party might be a solution in case devices outlive their manufacturers, though it may be difficult to provide third-party software on devices that only run minimal firmware without an operating system [19]. Also many active devices, especially older ones, have never been equipped with an update mechanism and remain vulnerable [34].

Additionally, the update process itself may be a vulnerability. Software updates can be hijacked and compromised, to inject malware into a system [32,34], thus requiring secure, trustworthy update mechanisms through authentication and verification and the possibility to revert corrupt updates [19].

2.5 Authorization and Access Control

Numerous IoT devices are shipped with insecure default passwords, which need to be changed during installation. Unchanged credentials make devices vulnerable to unauthorized access, data theft and malware injection. Infected devices can be integrated into botnets, which, in turn, can be utilized to launch DDoS attacks on companies, public services or private systems [18,30], rendering them unusable and unaccessible.

When integrated into a larger system, devices may have specific access rights and permissions within a system, possibly providing unauthorized users with access to services and mechanisms they should not have [17]. Other than traditional IT systems, where user access and permissions can be controlled easily, IoT devices often belong to the environment they are deployed in rather than to single users or user groups [19]. This makes it difficult for a system to differentiate between authorized and unauthorized users, especially on constrained things, which lack authorization mechanisms.

Smart homes, for example, may support various numbers of access levels, ranging from only one user level (treating all users the same) up to four, with the highest being admin and the lowest being "notification-only" [27]. Some platforms also support guest accounts, either limiting access to certain devices or providing limited access to all devices. Often, access must be explicitly granted and later revoked by the device owner. This requires some kind of interface between the smart system and the user, like a hub device and can not be applied to individual "things" [27]. Also it is cumbersome to authenticate for each system access, especially in systems that are used frequently. Authentication gets even more tedious, when smart home devices come from multiple different vendors with individual hubs, that are not compatible with each other or use different types of access controls [19].

When providing access to users, it may have to be revoked later by an administrator, which, again, requires a distinction between different user levels (admin and regular user). An alternate solution are time-limited access tokens, which require good configuration [19].

3 Recent Developments

3.1 Increased Attacks

Even though a lot of research exists about the challenges of IoT security, the number of IoT related cyber attacks is on the rise. In the first half of the year 2021, 1.5 billion IoT attacks have been registered, which is an increase of more than 100% in only six months. The main goals of these attacks were data theft and building botnets for crypto mining and DDoS attacks [9, 10].

Cost reduction and fast production are still the main focus in manufacturing IoT devices, while security features are often omitted. Also, new types of attacks are developed, e.g. Software Attacks Targeting Hardware Vulnerabilities (SATHV), which allow the exploitation of hardware vulnerabilites without physical access to devices [31]. This is made possible through debug features introduced in some new architectures.

Examples of vulnerabilities that were exploited are insecure communication protocols like telnet [10], hard-coded keys and passwords, elevation of privilege and credentials that were stored unencrypted [16].

This shows that vendors fall short of fixing known issues and still introduce new vulnerabilities when developing new products.

3.2 Enterprise Security

The number of non-business related IoT devices in enterprise networks is growing, including things like smart lightbulbs, heart rate monitors, coffee machines, etc. [8]. At the same time many organisations do not have adequate security protocols for IoT devices. In a survey, only half of the queried IT experts stated that they connect IoT devices to a separate network from the rest of the company and only 26% isolated devices even further by segmenting them into security zones [8]. According to the survey, many of them are aware of the problems, though. Their main concerns are attacks on the industrial IoT (IIoT), which is growing due to manufacturing environments undergoing the process of digital transformation, and DDoS attacks, which have increased by $\sim 30\%$ between 2020 and 2021 [8,15]. Increasingly, DDoS attacks come with demands for ransom payments [15].

Impact of COVID-19 and Remote Work

Enterprise networks have become more vulnerable during the COVID-19 pandemic, due to an increase in remote work [8, 10, 12, 33]. The transition from physical to virtual space was sudden and and companies were unprepared. Reasons for the increased vulnerability were the extensive use of communication and

Table 2: Examples of IoT Regulations worldwide

Country	Year	Name	Mandatory
Australia	2019	Voluntary Code of Practice [1, 7]	No
Singapore	2020	IoT Cyber Security Guide [4]	No
US	2020	IoT Cybersecurity Improvement Act [5]	Yes
California	2020	The California IoT cybersecurity law [3]	Yes
EU/UK	2019	The EU Cybersecurity Act [2]	Yes

video conference tools, the increased uptime of IoT devices in people's homes [10] and the use of private devices for work in private networks [33]. Since most people lack knowledge of cyber security measures, most don't properly secure their private networks and connect their work devices to the same network as their smart devices and entertainment systems [12]. The latter makes it possible for attackers to infiltrate an insecure device and then laterally move on to other devices in the same network or access sensitive enterprise data on unsecured work devices. Additionally, increased stress during the pandemic resulted in failures to follow security protocols correctly [33].

To enable their employees to work remotely, companies increased their cloud presence and virtualization, using standardized systems for more efficiency and cost-reduction. While standardization is generally good, this can lead to the spread of bugs in widely used software, like the Log4j vulnerability mentioned above or the *Ripple20* vulnerabilities, which were part of a TCP/IP stack commonly used in IoT software [6]. Ripple20 consists of 19 individual vulnerabilities, including multiple remote code execution vulnerabilities.

3.3 Political and Legal Approaches

Many of the vulnerabilities in IoT devices, like insecure credentials, lack of encryption, overpriviledged users, etc. could be easily prevented if manufacturers invested more in security instead of cheap and timely production [17]. To enforce more security, multiple countries have developed regulations that require manufacturers to protect connected devices and private data of their users to varying extent. Table 2 shows a selection of regulations that have been made in the past years. Regulations in Australia and Singapore are only guidelines and compliance is voluntary. The Australian government queried companies one year after publishing the code of practice and found that manufacurers "found it difficult to implement". It is now considering further action [7].

Regulations in the US, UK and the EU are laws and thus mandatory. The US Cybersecurity Improvement Act avoids to directly regulate private manufacturers in order to not slow down innovation. Instead it requires the federal government to only buy products, which comply with the guidelines, hoping that the potential loss of profit encourages producers to invest more in security measures [11].

The Californian law regulates manufacturers, but remains quite vague, e.g. requiring them to fit devices with "reasonable security features" without specifying them any further [11].

In addition to IoT security laws, countries all over the world have enacted data protection laws to protect their citizen's private data. Some examples of countries are the EU and UK, California [11] and a number of African states such as Rwanda, South Africa, Kenya and more [14].

4 Conclusion

In this work I analyze a number of resources researching common IoT security challenges and vulnerabilities and summarize their findings. I describe recent developments and which challenges still exist or may have worsened. I also describe the impact of the COVID-19 pandemic on enterprise security and user privacy.

Many of the sources propose solutions and describe what measures are needed to improve security, but there seems to be a descrepancy between what is known and what the industry and manufactuerers actually implement. Even though the security challenges of the IoT are well researched and have been known for many years, there is still a lack of sufficient security measures in the sector. The vulnerabilities found in hardware, firmware and software increase steadily and the number of IoT related cyber attacks grows with the number of devices deployed in the world. Especially during the COVID-19 pandemic and the rise in remote work it has become clear, that IoT devices still pose a security challenge.

Research, reports and security analysis from the past two years reveal that many attacks could be prevented by implementing basic security measures, better standardization and IoT specific assessment frameworks. A big problem are the reduction of production cost and time. Manufacturers avoid spending money on security of hardware and software. To reduce time-to-market, quick solutions are preferred over secure ones. This leads to the use of insecure or overprovisioned open source software, which introduces bugs and vulnerabilities.

Countries and governments have realized the economic potential of the IoT, as well as the threat potential, and have begun to enact regulations and standards to encourage or force manufacturers to invest more in security and data protection. Often those regulations are vague or merely guidelines, with compliance being only voluntary. Further advancements could be made if governments were more strict and specific. Many countries have recognized the need for data protection and enact according regulations, which is an advancement. But regulation and standardization still provide room for improvement.

References

1. Australia releases draft iot cybersecurity code of practice. `https://www.zdnet.com/article/australia-releases-draft-iot-cybersecurity-code-of-practice/` (2019), retrieved 2022-07-23

2. Iot cybersecurity improvement act of 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN (2019), retrieved 2022-07-23
3. The california iot cybersecurity law. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327 (2020), retrieved 2022-07-23
4. Iot cyber security guide. https://www.imda.gov.sg/news-and-events/Media-Room/Media-Releases/2020/IMDA-Launches-IoT-Cyber-Security-Guide-to-Help-Enterprise-Users-and-\Vendors-Secure-IoT-Systems (2020), retrieved 2022-07-23
5. Iot cybersecurity improvement act of 2020. https://www.congress.gov/bill/116th-congress/house-bill/1668 (2020), retrieved 2022-07-23
6. Overview ripple20. https://www.jsof-tech.com/disclosures/ripple20/ (2020), retrieved 2022-07-23
7. Voluntary code of practice. https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/code-of-practice (2020), retrieved 2022-07-23
8. The connected enterprise: Iot security report 202. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/research/connected-enterprise-iot-security-report-2021 (2021), retrieved 2022-06-01
9. Iot attacks skyrocket, doubling in 6 months. https://threatpost.com/iot-attacks-doubling (September 2021), retrieved 2022-06-01
10. Iot cyberattacks escalate in 2021, according to kaspersky. https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky (2021), retrieved 2022-06-01
11. Iot regulations. https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations (2021), retrieved 2022-06-01
12. Iot security in the covid-19 pandemic. https://blog.isa.org/iot-security-in-the-covid-19-pandemic (2021), retrieved 2022-06-01
13. Log4j vulnerability - what everyone needs to know. https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know (2021), retrieved 2022-07-23
14. Tech regulation in africa: Recently enacted data protection laws. https://www.insidetechmedia.com/2021/12/13/tech-regulation-in-africa-recently-enacted-data-protection-laws/ (2021), retrieved 2022-07-23
15. Ddos attacks that come combined with extortion demands are on the rise. https://www.zdnet.com/article/ddos-attacks-that-come-combined-with-extortion-demands-are-on-the-rise/ (2022), retrieved 2022-07-23
16. A look back at the top 12 iot exploits of 2021. https://finitestate.io/blog/top-12-iot-exploits-of-2021-p1 (2022), retrieved 2022-07-23
17. Abdul Sattar, K., Al-Omary, A.: A survey: security issues in iot environment and iot architecture. In: 3rd Smart Cities Symposium (SCS 2020) (2020)
18. Antonakakis, et al.: Understanding the mirai botnet. In: 26th USENIX Security Symposium (USENIX Security 17) (2017)

19. Bellman, C., van Oorschot, P.C.: Analysis, implications, and challenges of an evolving consumer iot security landscape. In: 2019 17th International Conference on Privacy, Security and Trust (PST). pp. 1–7 (2019). https://doi.org/10.1109/PST47121.2019.8949058
20. Boeckmann, L., Kietzmann, P., Lanzieri, L., Schmidt, T.C., Wählisch, M.: Usable Security for an IoT OS: Integrating the Zoo of Embedded Crypto Components Below a Common API. In: International Conference on Embedded Wireless Systems and Networks (EWSN'22). ACM, New York, USA (October 2022)
21. Bormann, C., Ersue, M., Keränen, A.: Terminology for Constrained-Node Networks. RFC 7228 (2014), https://www.rfc-editor.org/info/rfc7228
22. Dongre, N., Atique, M., Shaik, Z.A., Raut, A.D.: A survey on security issues and secure frameworks in internet of things (iot). In: 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT) (2022)
23. Hahm, O., Baccelli, E., Petersen, H., Tsiftes, N.: Operating systems for low-end devices in the internet of things: A survey. IEEE Internet of Things Journal (12 2015)
24. Hurlburt, G.: The internet of things... of all things. XRDS: Crossroads, The ACM Magazine for Students **22** (Dec 2015)
25. Karie, et al.: A review of security standards and frameworks for iot-based smart environments. IEEE Access **9** (2021)
26. Kietzmann, P., Boeckmann, L., Lanzieri, L., Schmidt, T.C., Wählisch, M.: A Performance Study of Crypto-Hardware in the Low-end IoT. In: International Conference on Embedded Wireless Systems and Networks (EWSN'21). ACM, New York, USA (February 2021)
27. Mare, et al.: Consumer Smart Homes: Where We Are and Where We Need to Go. In: Proceedings of the 20th International Workshop on Mobile Computing Systems and Applications. ACM
28. Meneghello, F., Calore, M., Zucchetto, D., Polese, M., Zanella, A.: Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices. IEEE Internet of Things Journal **6** (2019)
29. Morgner, P., Benenson, Z.: Exploring security economics in IoT standardization efforts. In: Proceedings 2018 Workshop on Decentralized IoT Security and Standards. Internet Society (2018).
30. Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., Ghani, N.: Demystifying iot security: An exhaustive survey on iot vulnerabilities and a first empirical look on internet-scale iot exploitations. IEEE Communications Surveys & Tutorials **21** (2019)
31. Polychronou, N.F., Thevenon, P.H., Puys, M., Beroulle, V.: A Comprehensive Survey of Attacks without Physical Access Targeting Hardware Vulnerabilities in IoT/IIoT Devices, and Their Detection Mechanisms. ACM Transactions on Design Automation of Electronic Systems **27** (Jan 2021)
32. Ronen, E., Shamir, A., Weingarten, A.O., O'Flynn, C.: Iot goes nuclear: Creating a zigbee chain reaction. IEEE Security & Privacy **16**(1), 54–62 (2018).
33. Tawalbeh, L., Muheidat, F., Tawalbeh, M., Quwaider, M., Saldamli, G.: Predicting and preventing cyber attacks during covid-19 time using data analysis and proposed secure iot layered model. In: 2020 Fourth International Conference on Multimedia Computing, Networking and Applications (MCNA) (2020)
34. Zandberg, K., Schleiser, K., Acosta, F., Tschofenig, H., Baccelli, E.: Secure firmware updates for constrained iot devices using open standards: A reality check. IEEE Access **7** (2019)