Sensor networks

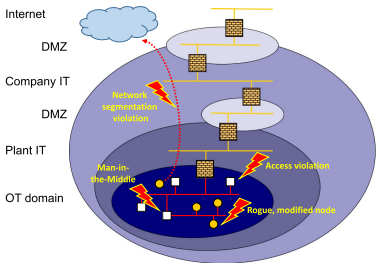
IoT-Enabled Sensors in Automation Systems and Their Security Challenges

Thilo Sauter[1,2*] and Albert Treytl[2**]

[1]*Institute of Computer Technology, TU Wien, 1040 Vienna, Austria*
[2]*Department for Integrated Sensor Systems, University of Continuing Education Krems, 2700 Wiener Neustadt, Austria*
[*]*Fellow, IEEE*
[**]*Member, IEEE*

Manuscript received 10 September 2023; accepted 4 October 2023. Date of publication 13 November 2023; date of current version 27 November 2023.

Abstract—Today, Internet of Things (IoT)-based sensor devices are ubiquitous. Being cost effective and easy to deploy, they are also considered for many applications outside their original domain, which was consumer electronics. Factory and process automation, smart buildings and homes, and, in general, Industry 4.0 are application fields in which the use of IoT technology is gaining popularity, often in addition to existing, classical communication architectures on the operational technology level. IoT devices, however, typically have a different philosophy for communication and data exchange, which makes them easy to use but poses security challenges by bypassing established security architectures, such as the classical defense-in-depth concept defined, for instance, in the IEC 62443 standard. This letter highlights today's security needs and concepts in industrial environments. Furthermore, it looks at possible new attack surfaces opened by IoT-based applications and shows ways how to bridge the security gap.



Index Terms—Sensor networks, defense in depth, Industry 4.0, Internet of Things (IoT), IT/OT integration, operational technology (OT), security.

I. INTRODUCTION

During the last decade at least, the Internet of Things (IoT) paradigm has changed the way smart devices are being designed, deployed, and used all over the globe. Actual numbers reported in commercial forecasts vary, but they typically predict several tens of billion IoT devices by the year 2025. The term "IoT" itself emerged more than 20 years ago, and the general concept is only loosely defined. The common understanding is that devices in the IoT make use of a ubiquitous communication infrastructure based on the Internet protocol that allows them to exchange data anytime and anywhere. Typically, this communication is wireless [1], using WiFi, LoRaWAN, and, of course, mobile communication and the future nbIoT of 5G [2].

In today's practice, the IoT concept evolved into having a strong focus on the mostly private end customer. This is supported by the goals of providing ease of use, which demands simple connectivity and deployment. Therefore, we find IoT devices mostly in the domain of consumer electronics, such as entertainment, wearables, or household devices [3]. Generally, the prefix "smart" has become synonymous for IoT capabilities: smart TVs, smart watches, or smart appliances are distinguished from their conventional or "dumb" counterparts by having an Internet connection. Yet, this smartness also entails new security risks, as the Mirai botnet [4] showed, where (IoT) devices have been hijacked by exploiting default passwords and misused as a platform for large-scale distributed denial of services attacks.

A typical characteristic of smart or IoT devices is that they provide connectivity to a mobile app or web interface that allows remote access, control, and potentially also maintenance. From a user perspective, it eases using the device in a standalone configuration in any arbitrary application environment. From a vendor perspective, it increases also customer retention, which is another desired effect as it ties the user to the vendor's product ecosystem. Practically speaking, a device adopting the IoT concept is often only useable with a connection to some kind of server controlled by the device vendor.

Although mainly designed for the consumer market, simple deployment and low prices also make them interesting for other application domains, such as Industrial IoT (IIoT), which adapts the IoT concept to the needs of industrial operational technology (OT) [5], [6], [7]. Such applications often relate to IoT-enabled sensors or cameras used for plant and machine monitoring. Wearable sensors are becoming attractive for safety-related supervision of workers in hazardous areas [8]. In smart farming, IoT devices are used to monitor environmental conditions and to control, e.g., irrigation systems accordingly. Finally, IoT concepts also play a role in smart renewable energy systems, particularly in controlling end user components, such as PV systems, battery storages, or electric vehicle chargers.

Convenient as IoT devices may be also in industrial and automation settings, and they are at odds with traditional system architectures [9], [10]. In particular, the ad-hoc fashion in which such devices often exchange data with back-end servers of the device vendors is not compatible with the usual hierarchical, strictly controlled structure of industrial OT systems [11]. This poses a security problem because it bypasses established security concepts, such as the defense-in-depth approach. The aim of this letter is to look at the specific security challenges arising from the use of IoT-enabled sensors in industrial settings.

II. TRADITIONAL SECURITY VIEWPOINT

Security in automation systems, independent of the actual application domain, usually follows a multilayer structure oriented along the traditional automation pyramid [12]. This defense-in-depth strategy

Corresponding author: Thilo Sauter (e-mail: thilo.sauter@tuwien.ac.at)
Associate Editor: A. K. Roy.
Digital Object Identifier 10.1109/LSENS.2023.3332404

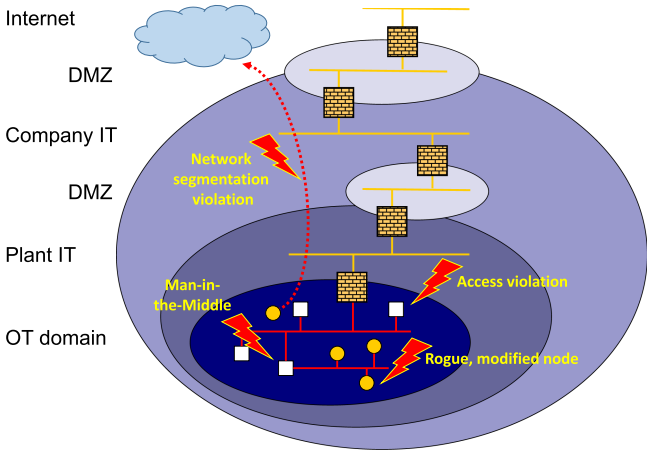


Fig. 1. Classical defense-in-depth concept following the structure of the automation pyramid with distinct zones and access control points at the interconnections [11] including possible attack vectors (in red).

was proposed already at the beginning of the 2000s and has become the gold standard for security architectures [11]. It acknowledges the fact that OT systems typically have little or no built-in security mostly for performance and real-time reasons and the lack of communication or computing resources on the OT devices. The established solution is to divide the system into zones that may use limited security inside, but rigorously control the access from the outside, e.g., by using firewalls. The higher layers of model shown in Fig. 1 relate to IT systems, either on the plant or on the company level. They use typical IT security, whereas the inner domain is reserved for the field level and its OT technologies.

In more recent years, this fundamental concept has been refined for instance in the Purdue model. This model typically adds a demilitarized zone (DMZ) at the top, which is a classical approach to handling company IT systems (such as web servers) that must be reachable from the outside world, but should still be shielded from the core IT. The Purdue model is also the basis for the IEC 62443 standard that defines security concepts and models for industrial automation and control systems [13]. It consists of following two essential elements:

1) *Zones* are groups of assets that share the same security requirements. Such assets can be network nodes, devices, or communication systems. Zones have clearly defined borders and can also have subzones.
2) *Conduits* are connections between zones. They are used to implement security measures for access control, resistance against attacks, and protection of integrity and confidentiality. Conduits must not cross multiple zones and only interconnect servers of two adjacent zones. Segregation can be implemented, e.g., by firewalls or DMZ servers.

According to the standard, the segmentation of an industrial system into appropriate zones and conduits should be based on a thorough risk assessment resulting in a set of recommendations for an adequate security policy. Notably, the process of risk identification, evaluation, and mitigation should be repeated regularly, as well as the segmentation adapted if needed.

III. SECURITY CHALLENGES OF IOT-ENABLED SENSORS

Today's industrial systems adopt many trends from the IT world to increase functionality, in particular for deploying and managing assets, and to become more cost effective by using commercial off-the-shelf (COTS) components and widespread concepts [14]. Hence, security problems with IoT devices are not different from existing basic security problems in classical industrial systems, given as follows.

SP 1: Outdated software and lacking security updates, including application vulnerabilities, allowing attackers to install own code.
SP 2: Lack of encryption by using unencrypted or unsafe protocols, such as MD5 for compatibility reasons.
SP 3: Missing vendor security posture resulting in inadequate handling of security issues, security updates, or limitations of use.
SP 4: Poor user interaction making it difficult to configure the devices securely, resulting in unsecure (default) settings.
SP 5: Insufficient physical security where attackers have physical access to a device.

Nevertheless, additional security risks arise with the use of IoT-enabled devices. They are especially relevant for sensors being the most stripped-down IoT devices.

SP 6—Incorrect access control: Proper fine-granular authentication and authorization are missing or insufficiently enforced by resource-limited devices. Common problems are unchanged default passwords. In addition, most IoT sensors only have the ability to support one single account or privilege level, thus reducing security to a single secret and lacking diversification of access control.
SP 7—Overly large attack surface due to the need for interoperability: Especially sensors are expected to connect with a plethora of systems. The simpler they connect or the more protocols they support, the more entry points an attacker has. Open ports and services not required for actual operation are common flaws when using COTS components unthinkingly.
SP 8—Intrusion ignorance: Flat hierarchies in typical IoT installations as well as simple mechanisms for adding new nodes make it hard to monitor typical network traffic, power usage, or similar indicators used in intrusion detection systems (IDS). Hence, compromised devices are not discovered quickly, since they often keep functioning normally from the user's viewpoint.

On the OT level, IoT contradicts the traditional paradigm, since access is often wireless and flat in contrast to hierarchical wired systems. Breaches of traditional security concepts can occur in two principal ways: 1) IoT devices on the OT level requiring a direct connection to and accessibility from a server in the Internet, as shown in Fig. 1, bypass all firewalls outside-in and often also circumvent deep-packet inspection when using a proprietary protocol or a default channel such as http. 2) Alternatively, the devices can actively open a parallel communication channel that also bypasses security measures inside-out, e.g., by establishing a tunnel or providing a completely independent, for instance mobile connection. Hence, an access path is set up that cannot be controlled.

IV. SECURITY MEASURES FOR IOT DEVICES

Security challenges for IoT sensors and devices result in the following common attack scenarios:

1) breach of the legitimate access (SP 3,4) and confidentiality of data (SP 1,2,6);
2) man-in-the-middle attacks;
3) network segmentation violation attacks (SP 6,7,8);
4) insertion of rogue nodes or modification of node functionality (SP 5,6,8).

These attack scenarios are sketched in Fig. 1. Countermeasures will be discussed by means of examples in the following sections.

A. IoT Network Segmentation

In process automation, inexpensive IoT devices, such as webcams, could be used to monitor parts of the plant, not for access control purposes, but to get additional information about the plant status outside the existing SCADA system. Another application of the IoT concept are third-party devices and services for machine condition monitoring or for temporary installation during maintenance works [15]. Common to these applications is that they are outside the actual OT and provide additional, mostly monitoring functionality.

Network segmentation by virtual LANs, separate networks, or connection via a DMZ is a technique for easy and immediately deployable countermeasures in existing installations. Within the scope of a recent research project, we had to install additional equipment in a petrochemical plant for measurement data acquisition. Although this was a long-term measurement campaign that would have justified integration into the company IT/OT infrastructure, the operator preferred us to establish a separate mobile connection for data transfer. This seems paradoxical at first but is a policy we also heard from other, predominantly large companies: Any third-party devices used for engineering, commissioning, or maintenance must not be connected to the company network for security reasons.

Also, if IoT devices should be integrated into the plant network infrastructure, network segmentation is a first step to establish a perimeter within a defense-in-depth approach. To increase security, device authentication using MAC addresses or better cryptographically protected protocols, such as https, is required. Deep-packet inspection and IDS can further monitor traffic and identify malicious or unknown nodes. Important for this concept is a proper white-listing strategy clearly defining allowed devices. Yet, network segmentation can only be a first step, since hijacked devices still can enter the network.

Even if network segmentation is employed, it can also be circumvented by typical installations. For example, the elements of a modern PV system for both private and industrial users are typically connected to the in-house IT network. In addition to services provided in the local network, such as Modbus-TCP, Telnet, or a basic web server, they also connect to a server of the vendor to upload operational data, such as measurement values and status information. In the investigated installation, the system also establishes a tunnel through the firewall that can be used for software and even firmware updates of the system without the owner being aware of it. It uses port 80 usually used for surfing the Internet, since this port is open in many firewalls and also not blocked by Internet providers. This channel is a potential bypass of network segmentation and allows full access to the local network, since it terminates behind the firewall.

B. Device and API Hardening

Security measures need to be implemented at all levels: hardware, firm/software, and network connection. First, the device hardware has to be designed in a secure way reducing possible manipulation. Security modules, such as Infineon's SLM 76 or ISO/IEC 11889 Trusted Platform Module, offer a secure base to store credentials and API tokens, provide advanced cryptographic functions, and be the base for further security measures. Sensitive data may be stored on a device only encrypted. Second, code signing and secure boot processes can prevent the installation of unauthorized firm or software. This is especially important for, but not limited to, devices to which the attacker has physical access, such as in building and home automation.

Third, APIs need to be hardened, which often comes down to enforcing very simple principles: All unused ports, protocols, or services need to be deactivated, and messages have to be properly verified beyond mere access control. Also, none-used or reserved bits and length values need to be checked. This way, attacks, such as usage of buffer overflows, can be prevented. Although practically not always possible, an IoT device should only possess one point to request or store data or services, respectively, limiting the attack surface and allowing more comprehensive security review. Finally, device authentication and authorization need to be implemented in a fine granular way. Role-based access and public key infrastructures are best practices for network authentication and access control [16].

Reducing the attack surface is the first step toward securing a system, since each connection or service provides a new set of opportunities for an attacker to discover and exploit vulnerabilities. In particular, dedicated development access and services, such as Telnet, SSH, or a debug terminal interface, should be deactivated for secure operation. Security modules are the second major step. Many microcontrollers today include such security modules that are still to be used in practice. eSIMs [17] are another good solution transforming a removable and, therefore, exchangeable SIM card into an integral part of a printed circuit board (PCB) that is hard to remove and, thus, provides a protected identity. When using 5G as communication, this is also no extra effort.

C. Privacy and Confidentiality Enforcement

Although IIoT is mainly about machine-to-machine communication, privacy and confidentiality are also important for automation systems. In certain areas, such as building and home automation or healthcare, the need is obvious and well anticipated by the general public demanding a responsible processing of data [18]. That paper also revealed that users further demand better support and information from vendors on the use of their data.

In industrial automation, problems are similar but focused on process data rather than on personal data. Threats are on the one hand tampering or hijacking of data, e.g., by man-in-the-middle attacks, requiring proper encryption and integrity protection. On the other hand, also transfer of vital production knowledge to competitors is an issue. While direct espionage exists, companies are also concerned about a kind of "unintended" transfer. In recent talks with the paper and cardboard industry, we noticed that sensor and monitoring data have been kept highly confidential, even if the manufacturer of the machines could optimize machine operation by accessing these data. Although this might only optimize a small part of the machine, the customer feared that the knowledge gained by the manufacturer could give competitors additional advantages. Similarly, small and per se unimportant data can be aggregated in so-called mosaic attacks to gain a picture of an organization or retrieve critical process know how.

D. IoT Platforms

While today's IoT implementations are rather closed data silos and closed ecosystems, the trend is going toward dedicated IoT platforms that provide the infrastructure and relieve the operator from the lifecycle management [19]. Platforms, such as Ditto (Bosch), Siemens' Mindsphere IoT, or Amazon's AWS IoT, provide IoT infrastructures and platforms as a service (IaaS, PaaS), easing the deployment, operation, and decommissioning of IoT devices. From the security point of view, standardized security mechanisms and automated processes for updates, key exchange, and authentication increase the security level. Yet, if a security exploit is found, the impact is widespread, since all IoT devices only communicate with the platform.

Another aspect is that the platform also breaks the end-to-end security of the transmitted data. Typically, the security protocol is changed at points, such as edge devices, data concentrators, or database

servers, such as the LoRaWAN application server, establishing a new secure connection for the application access. To provide full end-to-end security in such systems, additional security measures, such as a watermark integrated in the sensor data, can counter this interruption of the security chain (e.g., [20] and [21]).

V. CONCLUSION

While the security of traditional industrial systems can be addressed by the proven defense-in-depth approach according to IEC 62443, the introduction of IoT devices on the OT level brings new challenges for establishing proper security architectures. This applies in particular to mixed scenarios comprising a heterogeneous combination of IoT devices and traditional automation systems. Here, and in particular when the IoT devices lack adequate native security features, proper network segmentation is the first and immediate security strategy to be taken.

An aspect not specifically addressed in this letter is hardware Trojans, i.e., malicious functionalities introduced in devices during the design or manufacturing process. These Trojans are primarily a threat to the device vendors and their business models. From the user and system perspective adopted in this article, a threat introduced by a hardware Trojan does not differ from the threats discussed above.

Looking more into the future, a combination of dedicated IoT security and the traditional layered approach will be needed. On the IoT side, this will comprise a bundle of measures such as device authentication, elaborate access control, secure code deployment, and automated security management. How such genuine IoT security mechanisms can be best integrated with traditional defense-in-depth will still be a topic of further research.

ACKNOWLEDGMENT

This work was supported in part the County of Lower Austria through Dataskop and Smart Communities project and in part by the TU Wien and TUV Austria through a joint project #SafeSecLab. The authors acknowledge TU Wien Bibliothek for financial support through its Open Access Funding Programme.

REFERENCES

[1] S. Mumtaz, A. Alsohaily, Z. Pang, A. Rayes, K. F. Tsang, and J. Rodriguez, "Massive Internet of Things for industrial applications: Addressing wireless IIoT connectivity challenges and ecosystem fragmentation," *IEEE Ind. Electron. Mag.*, vol. 11, no. 1, pp. 28–33, Mar. 2017.

[2] L. Joris, F. Dupont, P. Laurent, P. Bellier, S. Stoukatch, and J.-M. Redouté, "An autonomous sigfox wireless sensor node for environmental monitoring," *IEEE Sensors Lett.*, vol. 3, no. 7, Jul. 2019, Art. no. 5500604.

[3] H. Thapliyal, "Internet of Things-based consumer electronics: Reviewing existing consumer electronic devices, systems, and platforms and exploring new research paradigms," *IEEE Consum. Electron. Mag.*, vol. 7, no. 1, pp. 66–67, Jan. 2018.

[4] M. Antonakakis et al., "Understanding the Mirai botnet," in *Proc. 26th USENIX Conf. Secur. Symp.*, 2017, pp. 1093–1110.

[5] B. Cheng, J. Zhang, G. P. Hancke, S. Karnouskos, and A. W. Colombo, "Industrial cyberphysical systems: Realizing cloud-based Big Data infrastructures," *IEEE Ind. Electron. Mag.*, vol. 12, no. 1, pp. 25–35, Mar. 2018.

[6] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The Industrial Internet of Things (IIoT): An analysis framework," *Comput. Ind.*, vol. 101, pp. 1–12, Oct. 2018.

[7] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Inform.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[8] S. Misra, C. Roy, T. Sauter, A. Mukherjee, and J. Maiti, "Industrial Internet of Things for safety management applications: A survey," *IEEE Access*, vol. 10, pp. 83415–83439, 2022.

[9] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in Industrial Internet of Things," in *Proc. 52nd Assoc. Comput. Machinery/Eur. Des. Automat. Conf. /IEEE Des. Automat. Conf.*, 2015, pp. 1–6.

[10] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K.-K. R. Choo, "Consumer, commercial, and Industrial IoT (in) security: Attack taxonomy and case studies," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 199–221, Jan. 2022.

[11] A. Treytl, T. Sauter, and C. Schwaiger, "Security measures in automation systems-a practice-oriented approach," in *Proc. IEEE 10th Int. Conf. Emerg. Technol. Factory Automat.*, 2005, pp. 9–855.

[12] J. Jasperneite, T. Sauter, and M. Wollschlaeger, "Why we need automation models: Handling complexity in industry 4.0 and the Internet of Things," *IEEE Ind. Electron. Mag.*, vol. 14, no. 1, pp. 29–40, Mar. 2020.

[13] *Security for Industrial Automation And Control Systems*, IEC Standard IEC 62443, 2020.

[14] M. Radovan and B. Golub, "Trends in IoT security," in *Proc. 40th Int. Conv. Inf. Commun. Technol., Electron. Microelectron.*, 2017, pp. 1302–1308.

[15] E. Ragusa, F. Zonzini, L. De Marchi, and P. Gastaldo, "Vibration monitoring in the compressed domain with energy-efficient sensor networks," *IEEE Sensors Lett.*, vol. 7, no. 8, Aug. 2023, Art. no. 6004604.

[16] S. Dey and A. Hossain, "Session-key establishment and authentication in a smart home network using public key cryptography," *IEEE Sensors Lett.*, vol. 3, no. 4, Apr. 2019, Art. no. 7500204.

[17] S. Colley, "Key IoT security trends for 2023," IoT.Business.News, Dec. 2022. [Online]. Available: https://iotbusinessnews.com/2022/12/21/08703-key-iot-security-trends-for-2023

[18] B. Pospisil, T. Sauter, A. Treytl, E. Huber, and W. Seböck, "Cyber security at home-what really matters to people," in *Proc. IEEE 31st Int. Symp. Ind. Electron.*, 2022, pp. 1208–1213.

[19] A. Griffiths, "Trends and innovations in the Industrial IoT," Embedded Computing, Jun. 2018. [Online]. Available: https://embeddedcomputing.com/technology/iot/trends-and-innovations-in-the-industrial-iot

[20] A. Treytl, A. R. Kondapuram, T. Sauter, and H. Ruotsalainen, "Comprehensive analysis of supply voltage watermarking for protection of sensor systems," in *Proc. IEEE 27th Int. Conf. Emerg. Technol. Factory Automat.*, 2022, pp. 1–8.

[21] L. Vogl, T. Sauter, A. Treytl, and T. Bigler, "Work in progress: Side-channel watermarking for LoRaWAN using robust inter-packet timing: An experimental approach," in *Proc. IEEE 18th Int. Conf. Factory Commun. Syst.*, 2022, pp. 1–4.