Security Threats and Issues in Automation IoT

Pal Varga, Sandor Plosz, Gabor Soos
Dept. of Telecommunications and Media Informatics
Budapest University of Technology and Economics
2 Magyar Tudósok krt., Budapest, Hungary, H-1117
Email: pvarga@tmit.bme.hu, plosz@tmit.bme.hu, gsoos@tmit.bme.hu

Csaba Hegedus
AITIA International Inc.
Telecommunication Division
Budapest, Hungary
Email: hegeduscs@aitia.ai

***Abstract*—Solving security concerns are one of the main challenges for the Internet of Things. There are different issues to be solved within the physically connected part of the IoT and in the networking domain, and another set of issues exist for the data-processing back-end, not to mention the presentation/configuration layer, where direct human interaction brings in further threats.**

Automation IoT applications have special real-time requirements, they are expected to have high level of reliability, and often operate in safety-critical environment. These requirements justify extreme security and safety measures.

This paper discusses the security threats that can appear in the different layers of an IoT architecture, especially in the automation domain. The mitigation practices of the various security issues are also discussed, bearing in mind that the solutions can bring quite different measures for the physical equipment in the field, for the communication infrastructure, or for the data processing applications.

I. Introduction

INFORMATION and communication technologies are thoroughly used in many areas around us. The evolution of technology drives increasing automation in numerous fields. Tasks which have been performed by humans are getting replaced by computers. This trend is being consolidated around different goals such as heterogeneity, interoperability, distributed processing and security.

The Internet of Things (IoT) concept targets interconnection of low-cost devices through Wireless Sensor Networks. This concept is adapted by Cyber-Physical Systems (CPS), driving industrial (automation) systems towards Cyber-Physical Production Systems (CPPS), which is a pillar of the so called 4th industrial revolution [1]. CPSS connects industrial systems and the CPS with manufacturing optimization and automation capabilities [2]. By using CPPS, Industry 4.0 targets autonomous operation, mass product customization, collaborative manufacturing and end-to-end digital integration [3].

IoT is a concept to interconnect simple, low power devices, such as sensors and actuators (called things) based on Internet technologies. IoT expresses both the required, adapted technologies, and the resulting network of hundreds of thousands of devices. IoT is not a technology itself, it is defined as a concept to expand Internet technologies to Wireless Sensor Networks (WSN). A wireless sensor network is the interconnection of low-power devices using wireless protocols such as ZigBee, IEEE 802.15.4, WirelessHART, ISA100.11, IETF 6LoW-PAN, IEEE 802.15.3, Wibree.

This heterogeneity of IoT rises a lot of security concerns such as how to keep privacy and maintain trust and confidentiality [4]. The difficulty does not only come from the interoperability issue, but also the processing demand of security solutions. As the technologies got cheaper, simple devices with limited processing power get also connected to each other and to the IT cloud [5].

There is a huge emphasis on security, availability in particular in automation IoT. Nevertheless, automation IoT uses processing- and power constrained devices, and there is a narrow margin for security tasks. The tradeoff between security, performance and cost has to be evaluated. There is a demand for light-weight and autonomic security solutions which later constitutes in self-mitigation capabilities [6].

This paper discusses security issues for the automation IoT area. The paper is organized to follow the "layers" of IoT systems: Sensors and Actuators, Gateway and Network, Data Processing, and finally, Application. These (or other) layers are not yet standardized, and depending on the application area some of them are presented in a common group, others are split into several (sub)layers. Our contribution in this paper is to analyse the security issues of automation IoT in a layered approach, and to present and elaborate on possible mitigation solutions.

II. Security of Automation IoT

Abomhara and Kien [7] provides a taxonomy for IoT and security related terms in that context. It reflects to the vulnerabilities which arise from the nature of Machine-to-Machine (M2M) communications which is thoroughly used in automation IoT. M2M works without human supervision, vulnerabilities can be exploited more easily therefore it has to be robust and failure-proof. This contradicts to the fact that in automation scenarios there are often power and processing-constrained devices – like sensor nodes – used, which have limited security capabilities.

The IoT world is wide in terms of application areas, and deep in terms of their small or large complexity. Requirements against IoT systems also differ in the application area. For automation IoT, the following requirements [8] determine the system architecture and somehow the interworking of systems within the IoT domain:

- interoperability between devices and systems;
- scalability;

- real time performance;
- security;
- engineering simplicity.

Automation is advancing also within the industrial sector. Industrial systems have distinct, more strict security requirements than IT systems. These requirements can be described with the well-known CIA objectives: confidentiality, integrity and availability. There is a difference between IT and Industrial IT on how these objectives are prioritized [9]. This has drawn a lot of research interest in the topic of Industry 4.0 and IoT automation systems [10].

Industry 4.0 is an interworking of several technologies – like IoT –, it is known for its heterogeneity. Hence there is a need to define the way how these technologies are to be integrated, e.g. a reference architecture is desired. There are several initiatives to date. In Germany, the working group for Industry 4.0 is developing a Reference Architecture Model for Industry 4.0 (RAMI 4.0), a three dimensional layered model [11]. The Industrial Internet Consortium (IIC) is developing the Industrial Internet Reference Architecture (IIRA), building on Industrial Internet Systems (IIS) specified in four levels of "viewpoints" [12]. While RAMI 4.0 targets mainly industry automation, IIRA aims to bring IoT into a wider target area, including energy, healthcare, and transportation. Many similarities exist between these two architecture concepts [13].

Security is a major concern in CPSS, especially when it comes to modernizing industrial systems driven by interconnected ICT components. Although current reference architecture models do not deal with security in sufficient detail, it is desired to incorporate security aspects in a reference architecture model. In [14], the possibility to establish a security viewpoint in RAMI 4.0 was investigated. In order to be able to integrate security through the hierarchical axis we must have an overview of the threats that arise in the automation scenario. Therefore in this work we present a layered overview of security threats in industrial IoT and possible mitigations.

III. Layered Approach for IoT systems

Although generally there is no standardized, generally agreed layered structure for IoT systems, the upcoming reference architecture models for Industry 4.0 are layered. This supports our view that such structure is beneficial when describing security threats. Fig. 1 presents the four layered architecture our threat analysis is built upon.

As mentioned in the previous chapter, similar, layered architectures are suggested by various vendors and research groups. Nevertheless, these are not pure technical architectures, since they usually mix in business views and processes, as well. Furthermore, the access (or aggregation) network and the transport network are sometimes suggested to be in different layers, simply because they utilize different networking technologies. In this current paper we suggest the four layered, simple and yet clear architecture, because the security threat types are clearly different for these layers.

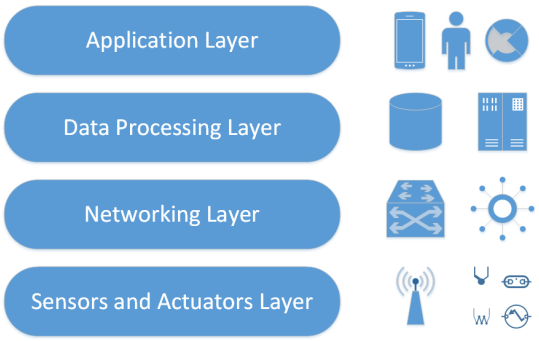

Fig. 1. The architectural layers of IoT systems

The lowest layer in Fig. 1 is denoted as "Sensors and Actuators" as these are the physical building blocks of automation IoT systems. The layer above it is called "Networking", and it covers all communication issues from between the 2-6 layers of the ISO-OSI model; including all sorts of network topologies, aggregation and transport types. The "Data Processing" layer covers all methods, technologies and equipment that helps extracting meaningful information from the collected data. The "Application" layer includes the highest level of logic behind the whole IoT architecture, the ultimate control mechanisms – together with the configuration of the system-of-system, and the presentation of its status.

IV. Security Issues of the Sensors and Actuators Layer

The IoT Sensors and Actuators layer is vulnerable from direct physical access through the following types of attacks: physical tampering of the end devices and the communication link and denial of service (DoS) attack.

A. Tampering

Tampering is an action when an attacker performs physical modifications on the device or on the communication link. This physical layer provides a great attack surface.

Hardware elements can be accessed, identity stolen or replaced, which can violate confidentiality, availability and integrity objectives. One way to avoid this is to use tamper-resistant packaging [15]. However, this may be too expensive considering cheap low-power sensors or consumer devices which are the main drivers of IoT.

Tampering the communication link can be in the form of disconnecting or changing the physical link which is a case of Denial-of-Service attack or altering the transmitted data which is a case of a Man-in-the-Middle attack.

B. Denial of Service

In most cases IoT devices communicate through radio access technologies in the physical layer. The wireless link is very susceptible to the Denial of Service (DoS) attacks, which may take their form in signal distortion or jamming. DoS attacks may compromise system availability. While spread-spectrum techniques can be used against wireless jamming,

there is no general solution to avoid DoS attacks. Even existing approaches require a great deal of processing, which resource-constrained devices of IoT does not have [16]. Possible solutions need to monitor and interpret traffic but these work on higher layers [17].

C. Sensors as Security Treats

On the other side of the coin, IoT sensors are considered a great security threat, since – if tampered – they can be the source nodes for Distributed Denial of Service (DDoS) attacks.

Their management access is considered vulnerable, due to careless deployment practices of weak authentication pairs. The potentially great number of devices with easy-to-break username/password pairs may provide an enormous attack surface. If tampered, these devices may be used for flood-type DDoS attacks. Such attacks neither require high computation capacity nor high network throughput from any device (e.g. 1 byte payload is enough). It is the sum of these packets sent towards the targeted infrastructure that leads to their DoS.

V. Security Issues of the Networking Layer

In case of automation IoT, where real-time information transport is key, networking attacks can be especially harmful. The IoT networking layer suffers all sorts of security threats that are known within the computer networks community. Although there are specialized attacks for

- Wireless Sensor Networks (WSN),
- the aggregation network (often referred to as Gateway or Link layer), and
- the transport network between aggregation points and the cloud and its applications,

in this section we treat them in a common way, since they pose threat to data transport. The following subsections briefly summarize those networking threats and attacks that may have a significant impact on IoT systems.

A. Denial of Service attacks

1) Exhaustion: Networking resources, such as buffers, computation capacity and throughput can be exhausted by targeted attack of the given resource, i.e. of a given node.

2) Collision: Purposefully created collision can be considered a jamming-type attack, since it usually targets the wireless part of information transfer, especially its data link layer. Although the attackers do not jam the full signal, they decrease the goodput of the network, or even make communication impossible.

3) Unfairness: Data Link layer attacks often aim to corrupt the fairness mechanisms of WSNs. Their method includes exhausting of targeted WSN resources, or collision. These methods then lead to weak Denial of Service; although its effect magnifies through the number of nodes involved.

4) Spoofed routing information: While payload information of packets are usually encrypted in the channel, routing and other header information are not. The information carried within routing protocol – in our case: IP – is often the main target of spoofing. Attackers may spoof, alter, or replay IP addresses or transport protocol information (UDP, TCP ports, etc.) to disrupt traffic in the network. The result may be routing loops, extended (or shortened) routes, fake error messages, and many more.

5) Selective forwarding: In multi-hop networks, a malicious or tampered node may alter the traffic by dropping some messages, of selectively forwarding others. The information that reaches its destination is not complete, hence in a way, corrupted.

6) Sinkhole attack: In these type of attacks, some nodes or destinations are made more attractive to traffic (e.g by tampered routing management information) that other, normal nodes. When reaching the sinkhole node, the messages may get dropped (selective forwarding), forwarded with changed content, or altered in other ways.

7) Wormhole attack: A wormhole is maliciously prepared, low latency link, over which the attacker can replay messages. In a wormhole attack, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point.

8) Sybil attack: The Sybil type of attackers use nodes or devices with multiple identities. These generate traffic that seems many-source, or even distributed. This method corrupt fairness resource usage, redundancy, or voting concepts originally present in the infrastructure.

9) Flooding: Network flooding and their possible mitigation has a wide literature, because of their complexity and their impacts of our systems' life. Nowadays DDoS flooding attacks are the most disturbing ones; the authors of [18] provide a comprehensive survey of their algorithms and defence mechanisms.

10) Node Replication: An attacker can copy the identity of a node and create another (virtual) node with the same identity. Then it can send false data in its name through random routes to disrupt the network.

B. Man-in-the-Middle attacks

Man-in-the-Middle attack is when an attacker gains access to the information sent between nodes and can used it for his advantage. To avoid the risk of this attack, data encryption needs to be applied. The following three attacks belong to this category:

1) Eavesdropping: Eavesdropping is an action when an attacker can gain access to a communication channel. It is a passive attack unless the attacker slightly alters the received packets and sends it back to either participant. This method is called replay attack, a very common subtype of spoofing.

2) Routing attack: Since usually the routing information is not encrypted an attacker may change the routing information thereby creating routing loops which significantly deteriorates quality of service.

3) Replay attack: An attacker my capture a signed packet, and even if it cannot decrypt it, it may gain the trust of the destined entity by re-sending the packet at a later time. Replay attacks can be circumvented by using message sequence numbers and message authentication code (MAC).

C. Security Counter-measures for the Networking Layer

The above mentioned attacks can be eliminated by proper network-security counter-measures. Defence methods include active firewalls that filter the traffic, passive monitoring (probing) to raise alarms, traffic admission control through authentication, and bi-directional link authentication.

IoT sensors are very often simple, low-power end devices. Due to the limited functionality of IoT sensors, security processing, such as encryption get handled in hardware. It is also the best to implement encryption at the lowest layer possible, since the payload of a protocol layer can only be encrypted in the protocol layer below [19]. There is a need for lightweight, processing-friendly and cheap solutions, such as [20] where a low-layer, lightweight encryption method is presented for authenticating RFID tags in IoT.

Encryption however is not always enough against eavesdropping. Without authorization, trust cannot be established between communicating parties. Authorization, however, is a complex task since it requires key management with asymmetric encryption, which is processing-demanding. This practically means that in many cases there is no key management or the simple devices cannot implement it. [21] presents a method for generating symmetric (session) key directly from the wireless channel.

In automation IoT there is a further issue, when complex legacy systems are integrated into the IoT infrastructure. In such cases a middleware is introduced to translate the legacy interfaces and provide security [5]. However, in industrial Systems there is a huge emphasis also on safety. In [22] we elaborated on the safety and security analysis of such an industrial automation system.

VI. Security Issues of the Data Processing Layer

In the centralized IoT the aggregation and processing of data is performed on the data processing layer – usually within the cloud. This layer is susceptible for exhaustion type-of attacks from the end-nodes, malwares embedded in the incoming data [6].

Some of the weaknesses of distributed data centres are also present. The defence mechanisms against these attacks can be found among data-centre security solutions. These include physical security measures, usage of top-notch firewalls, and other security best practices of critical IT infrastructures [23]. The authors list common threats and vulnerabilities that appear in the cloud infrastructure. These include the following:

- Logon Abuse,
- Inappropriate System Use,
- Eavesdropping,
- Network Intrusion,
- Denial-of-Service (DoS) Attacks,
- Session Hijacking Attacks,
- Fragmentation Attacks, as well as
- Cloud Access Control and Database Integrity Issues.

A. Cloud Service Provider Risks

The following risks are specific to the data processing layer, and the potential attackers can exploit the vulnerabilities of Cloud Service Providers. [23]

- Back-Door - getting control of the infrastructure from asynchronous external connections, such as modems.
- All network-level risks, that are targeting the cloud infrastructure – which has its own Data Center Network.
- Social Engineering - the ultimate hack, when the attacker uses social skills to obtain information such as passwords or PIN numbers to be used against information systems. Dumpster diving is a sub-category: when trashed data is not sanitized, and important information (e.g. password lists, internal documentation, etc.) is searched, found, and applied for attacks.
- Password Guessing - a risk that exists at all layers of the IoT architecture; although the cloud infrastructure has a large attack surface.

B. Exhaustion

Exhaustion or flooding is used by an attacker to interrupt data processing of the IoT infrastructure. Since this is a higher layer attack and due to the distributed nature of IoT this attack does not have high risk. Also within the cloud it is much easier to implement protective measures against it [6].

C. Malware

Malware can be easily embedded in the data of IoT devices which can reach the cloud and the data centres when an end device gets compromised. Therefore it is not sufficient to have strong firewalls on the cloud edge but also implement protective measures before data processing. Beside providing malware listings, the authors of [24] present a classification system to detect malwares.

D. Operational weaknesses of cloud computing

There are known operational weaknesses of cloud computing that are mostly due to improper conduct processes. The threats can be organized into two subtypes: those related to virtualization, and those related to cloud computing architectures and their operation.

1) Virtualization threats: The following threats are related to virtualization, and its operational practice:

- communication blind spots of the virtual machines (VMs),
- inter-VM attacks and hypervisor compromises,
- mixed trust level VMs (i.e. dynamic or careless changes in VM groupings can introduce less trusted or secured VM into the group),
- Instant-On gaps (i.e. VMs take over tasks instantly; often missing out security measures),
- resource contention (i.e. periodic updates happening at the same time for many VMs) [25].

2) Threats originated from cloud computing weaknesses: Furthermore, regarding the cloud computing practices, the following threats – that are originated from operational weaknesses – are well known:

- cloning and rapid resource pooling (i.e. time constraints gave birth to careless cloning practices that can lead to mixed trust level VMs in the resource pool),
- motility of data (i.e. dynamic copying of data to achieve optimized resource usage can leave un-sanitized data in later unsecured areas),
- elastic perimeter of accessing devices (i.e. accessing from less secure terminals or networks is not completely restricted),
- unencrypted data,
- shared multi-tenant environments of the public cloud [25].

VII. Security Issues of the Application Layer

A. Threats and Issues with the Client Application

The Application layer suffers the threats that any IT client with a Human-Machine Interface (HMI) does.

The most common threats of this area are connected to Web client security measures. The machine that has access to the IoT system configurations is usually a http-connectable device, which makes it vulnerable to attacks over the Web. Malware can sneak into the otherwise closed IoT system through security holes of the client. A further, connected issue is that the attacker can have access to the local client HW, possibly taking over its control – together with the control of the applications running over that. Such attackers often remain hidden (non-intrusive), while their malware application keeps eavesdropping and continuously reporting about the IoT system status, its usage, or even its authentication information to the attacker. Malware detection and anti-virus solutions are recommended to filter such applications.

Furthermore, the client application status, its operating system status or its hardware status should not be tied to the status of other parts of the IoT system, at all. Its status (active, sleeping, failed, etc.) should not have any negative effect of the data processing layer, the networking layer, or the layer of sensors and actuators. An unfortunate practical example is when the screen saver going active in the application would halt the system under configuration.

B. Issues with the Communication Channel of the Client Application

Tampering with configuration data is possible when the attackers get control over the configuration interface – as discussed above –, or they are able to sniff into the communication channel.

The application that allows remote configuration of the IoT system – including its sensors and actuators – normally has VPN (Virtual Private Network) access to the systems that it configures. VPNs usually have some security measures associated with, such as

- Confidentiality through data encryption throughout the channel;
- Integrity of information content through detecting tampering of messages;
- although it lacks supporting the third security objective, Availability – which may open possibilities for various attacks, including DDoS.

C. Issues with System Integrity of the Client Application

System integrity is a key property of reliably working IoT systems. Losing the integrity of the system easily leads to safety risks and security threats. System should not fail during high activity stress or abnormal process situations, network or computer failures, multiple alarms, executing previously unexecuted error path code or system recovery code, or incorrectly executed commands. This requires careful and complex testing.

D. Minor modifications leading to complex issues

Unexpected environmental change together with minor system modifications and configuration changes can have unexpected side effects. As the system of system grows bigger, these side-effects can propagate to bigger problems.

Such effects and propagations can be minimized by thorough validation of the system elements, complex testing, and continuous monitoring of the overall system.

E. Multi-user access and concurrent editing of configuration

Systems should be robust against multi-user access. When many users are able to change the configurations of various parts of the IoT systems, concurrent editing of configuration files, and concurrent execution of configuration changes easily lead to unstable system status. This should be eliminated by careful process planning and design for the multi-user environment.

F. Data Access and Traceability

The earlier discussed data access security measures should be applied in the application layer, as well. Furthermore, traceability of any configuration change and change of system status should be provided by design.

VIII. Conclusion

The Internet of Things, due to its success in the IT world driving its way toward automation and industrial systems. Despite the fact that technologies get reliable to be used for IT applications, the heterogeneity of the usable technologies and consequently the lack of standardized methods for certain use cases opens up a lot of unanswered questions. In industry there is a very narrow margin of accepted risk which may result in security issues not to mention that safety risk may also be involved. IoT in terms of safety and security cannot be called mature because its heterogeneous structure involves a great deal of possible vulnerabilities yet to be fully understood.

In order to operate a secure and safe IoT system, security – and safety – should be applied through the full planning, implementation, deployment and operation cycle:

TABLE I
SECURITY THREATS IN AUTOMATION IOT AND THEIR POSSIBLE MITIGATION

Layer	Threat type	Mitigation
Physical	Tampering	tamper-resistant packaging
	Denial of Service	spread-spectrum techniques
Networking	Denial of Service	active firewalls, passive monitoring (probing), traffic admission control, bi-directional link authentication
	Eavesdropping	encryption, authorization
Data processing	Back door attack	properly configured firewalls on all system entry point
	Social Engineering	educating employees to security awareness
	Exhaustion	traffic monitoring
	Malware	malware detection
Application	Client app.	anti-virus filtering
	Comm. channel	proper authentication, authorization, integrity verification
	Integrity	testing
	Modifications	validation
	Multi-user access	process planning and design
	Data access	Traceability

- selection of technologies, architecture and tools;
- project configuration, programming and verification;
- deployment and commissioning;
- operation and maintenance.

In this paper we have collected the possible threats of automation IoT systems and described them in a layered approach. Table I summarizes our work. We have found that there exist vulnerabilities of wireless sensor network nodes used in IoT which cannot be solved directly, only at higher layers due to the simplicity of these devices. In automation IoT additional requirements may be set even for end device capabilities. Nevertheless, the real risk which may be involved behind these vulnerabilities in the industrial context needs further investigation in the future.

REFERENCES

[1] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. Johnson, "M2M: From mobile to embedded internet," *Communications Magazine, IEEE*, vol. 49, no. 4, pp. 36–43, April 2011.

[2] H. ElMaraghy and L. Monostori, "Variety management in manufacturing cyber-physical production systems: Roots, expectations and r&d challenges," *Procedia CIRP*, vol. 17, pp. 9 – 13, 2014. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2212827114003497

[3] M. Brettel, N. Friederichsen, M. Keller, and M. Rosenberg, "How virtualization, decentralization and network building change the manufacturing landscape: An industry 4.0 perspective," *International Journal of Mechanical, Aerospace, Industrial, Mechatronic and Manufacturing Engineering*, vol. 8, no. 1, pp. 37 – 44, 2014. [Online]. Available: http://waset.org/Publications?p=85

[4] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266 – 2279, 2013, towards a Science of Cyber SecuritySecurity and Identity Architecture for the Future Internet. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128613000054

[5] S. Sicaria, A. Rizzardia, L. A. Griecob, and A. Coen-porisinia, "Security, privacy and trust in internet of things: The road ahead," *Computer Networks*, pp. 146–164, 2015.

[6] Q. M. Ashraf and M. H. Habaebi, "Autonomic schemes for threat mitigation in internet of things," *J. Netw. Comput. Appl.*, vol. 49, no. C, pp. 112–127, Mar. 2015. [Online]. Available: http://dx.doi.org/10.1016/j.jnca.2014.11.011

[7] M. Abomhara and G. M. Kien, "Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks," in *Journal of Cyber Security and Mobility, Volume 4, Issue 1*, Jan 2015, pp. 65–88.

[8] J. Delsing and P. Varga, *Local automation clouds: Arrowhead Framework*. In book: IoT Automation – Chapter 2 – published by CRC Press, 2017.

[9] D. Dzung, M. Naedele, T. von Hoff, and M. Crevatin, "Security for industrial communication systems," *Proceedings of the IEEE*, vol. 93, no. 6, pp. 1152–1177, June 2005.

[10] M. Waidner and M. Kasper, "Security in industrie 4.0 - challenges and solutions for the fourth industrial revolution," in *2016 Design, Automation Test in Europe Conference Exhibition (DATE)*, March 2016, pp. 1303–1308.

[11] "Das Referenzarchitekturmodell RAMI 4.0 und die Industrie 4.0-Komponente," http://www.zvei.org/Themen/Industrie40/Seiten/Das-Referenzarchitekturmodell-RAMI-40-und-die-Industrie-40-Komponente.aspx.

[12] S.-W. Lin, Industrial Internet Consortium, Tech. Rep., 2015. [Online]. Available: http://www.iiconsortium.org/IIRA-1-7-ajs.pdf

[13] D. M. Pai, "Interoperability between IIC Architecture & Industry 4.0 Reference Architecture for Industrial Assets," Infosys, Tech. Rep., 2016. [Online]. Available: https://www.infosys.com/engineering-services/white-papers/Documents/industrial-internet-consortium-architecture.pdf

[14] Z. Ma, A. Hudic, A. Shaaban, and S. Plosz, "Security viewpoint in a reference architecture model for cyber-physical production systems," in *2nd IEEE European Symposium on Security and Privacy*, April 2017.

[15] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things," in *2015 IEEE World Congress on Services*, June 2015, pp. 21–28.

[16] M. Abomhara and G. M. Kien, "Security and privacy in the internet of things: Current status and open issues," in *2014 International Conference on Privacy and Security in Mobile Systems (PRISMS)*, May 2014, pp. 1–8.

[17] C. Zhang and R. Green, "Communication security in internet of thing: Preventive measure and avoid ddos attack over iot network," in *Proceedings of the 18th Symposium on Communications & Networking*, ser. CNS '15. San Diego, CA, USA: Society for Computer Simulation International, 2015, pp. 8–15. [Online]. Available: http://dl.acm.org/citation.cfm?id=2872550.2872552

[18] S. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks," *IEEE Communications Surveys and Tutorials*, vol. 57, no. 10, pp. 2046–2069, 2013.

[19] T. Pecorella, L. Brilli, and L. Mucchi, "The role of physical layer security in iot: A novel perspective," *Information*, vol. 7, no. 3, 2016. [Online]. Available: http://www.mdpi.com/2078-2489/7/3/49

[20] J. Y. Lee, W. C. Lin, and Y. H. Huang, "A lightweight authentication protocol for internet of things," in *2014 International Symposium on Next-Generation Electronics (ISNE)*, May 2014, pp. 1–2.

[21] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 128–139. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409960

[22] S. Plósz, C. Schmittner, and P. Varga, "Combining safety & security analysis for industrial collaborative automation systems," 2017, manuscript submitted for publication.

[23] R. L. Krutz and R. D. Vines, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Wiley Publishing, 2010.

[24] R. Canzanese, M. Kam, and S. Mancoridis, "Toward an automatic, online behavioral malware classification system," in *2013 IEEE 7th International Conference on Self-Adaptive and Self-Organizing Systems*, Sept 2013, pp. 111–120.

[25] Trendmicro, "Virtualization and Cloud Computing: Security Threats to Evolving Data Centers." [Online]. Available: http://www.trendmicro.tw/cloud-content/us/pdfs/about/rpt_security-threats-to-datacenters.pdf