Security and Privacy Challenges in Industrial Internet of Things

Invited

Ahmad-Reza Sadeghi[1], Christian Wachsmann[2], Michael Waidner[1,3]

[1]Technische Universität Darmstadt, Germany
[2]Intel CRI-SC at TU Darmstadt, Germany
[3]Fraunhofer Institute for Secure Information Technology, Darmstadt, Germany

{ahmad.sadeghi, christian.wachsmann}@trust.cased.de,
michael.waidner@sit.fraunhofer.de

ABSTRACT

Today, embedded, mobile, and cyberphysical systems are ubiquitous and used in many applications, from industrial control systems, modern vehicles, to critical infrastructure. Current trends and initiatives, such as "Industrie 4.0" and Internet of Things (IoT), promise innovative business models and novel user experiences through strong connectivity and effective use of next generation of embedded devices. These systems generate, process, and exchange vast amounts of security-critical and privacy-sensitive data, which makes them attractive targets of attacks. Cyberattacks on IoT systems are very critical since they may cause physical damage and even threaten human lives. The complexity of these systems and the potential impact of cyberattacks bring upon new threats.

This paper gives an introduction to Industrial IoT systems, the related security and privacy challenges, and an outlook on possible solutions towards a holistic security framework for Industrial IoT systems.

1. INTRODUCTION

Current industrial trends and initiatives aim to "connect the unconnected." Today, millions of embedded devices are used in safety and security critical applications such as industrial control systems, modern vehicles, and critical infrastructure. In the last decades, classical production engineering, automation, and intelligent computation systems merged into the industrial Internet of Things (IoT). The number of computation components integrated into industrial control systems, production systems, and factories is steadily increasing. Programmable logic controllers are replaced by more advanced cyberphysical systems (CPS), which are freely programmable embedded devices that control physical processes. CPS typically communicate over closed industrial communication networks but are often also connected to the Internet.

DAC '15, June 07 - 11, 2015, San Francisco, CA, USA

http://dx.doi.org/10.1145/2744769.2747942.

With the integration of classical computing into production systems, emerging megatrends, such as mobile computing, cloud computing, and Big Data, are becoming important drivers of innovation in industry. Cloud-based services are used to monitor and optimize complex supply chains; Big Data algorithms predict machine failures, which reduces downtimes and maintenance costs; interconnected production systems enable tight integration and optimization of production and business processes as well as outsourcing production steps to other locations, companies, and freelancers. In the near future, cloud-based services will allow considering more customer requirements in the production process and planning, enabling a new level of product individualization at a minimal cost. This development driven by computation systems is also called the "fourth industrial revolution" [23].[1]

Devices in the Internet of Things (IoT) generate, process, and exchange vast amounts of security and safety-critical data as well as privacy-sensitive information, and hence are appealing targets of various attacks [52, 51, 31, 7, 70, 22, 27, 50, 40, 41, 21, 19]. To ensure the correct and safe operation of IoT systems, it is crucial to assure the integrity of the underlying devices, in particular of their code and data, against malicious modifications [75]. Recent studies have revealed many security vulnerabilities in embedded devices [10, 11, 43, 50, 27, 8, 41, 62, 21]. This poses new challenges on the design and implementation of secure embedded systems that typically must provide multiple functions, security features, and real-time guarantees at a minimal cost.

In this paper, we give an overview of the developments and trends of Industrial IoT systems (Section 2), point out related security and privacy risks and challenges (Section 3), and discuss potential solutions towards a holistic security framework for Industrial IoT systems (Section 4).

2. FROM CYBERPHYSICAL SYSTEMS TO INDUSTRIAL INTERNET OF THINGS

An increasing number of everyday objects is equipped

[1]The introduction of water and steam powered mechanical manufacturing facilities is considered as the first industrial revolution. The next revolution was the deployment of electrically powered mass production based on division of labor, followed by the third industrial revolution that introduced electronics and IT to production systems to enhance automation of manufacturing. [23] However, some publications count differently [53].

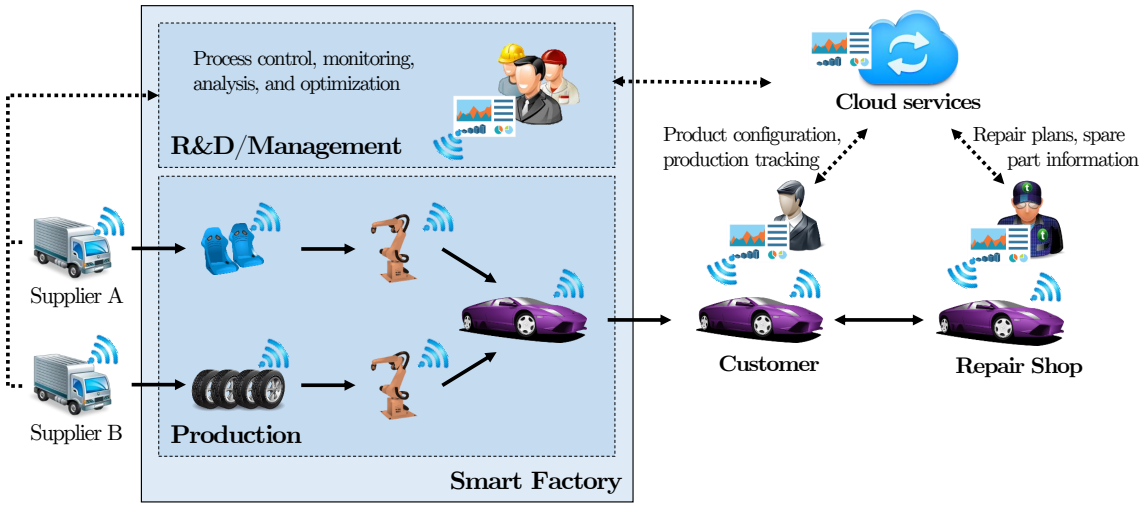

Figure 1: Industrial Internet of Things (IoT)

with electronics, which provides these objects with identification, computing, and communication capabilities. Examples include basic technology, such as Radio Frequency Identification (RFID) for the identification and tracking of products, packets, and pallets in supply chain scenarios, to smart devices, such as smart phones and wearables (e.g., smart watches) with considerable computing capabilities and Internet connections. This network of ubiquitous smart objects is known as the Internet of Things (IoT) and enables novel applications and services, in particular in the industrial sector [9, 37, 34, 42, 69].

Production facilities typically consist of several independently operating production systems with no or only limited communication capabilities. An emerging trend is to integrate more sophisticated electronics into production systems, interconnect them, and to integrate into conventional business IT systems. The resulting Industrial IoT is the basis for a new level of organization and management of industrial value chains and enables highly flexible and resource-saving production as well as enhanced individualization of products at the cost of mass production.

The foundation of Industrial IoT are cyberphsical systems (CPS), which are computing platforms that monitor and control physical processes [30]. CPS enable condition monitoring, structural health monitoring, remote diagnosis, and remote control of production systems in real-time. Further, CPS are the basis of smart factories that dynamically organize and optimize production processes with regard to resource-utilization (i.e., costs, availability, material, and labor) based on data generated and collected by the underlying CPS, even across company boundaries [1, 76].

In smart factories, smart products know their own identity, history, specification, documentation, and even control their own production process (cf. Figure 1). Beyond manufacturing, smart products are the basis of novel knowledge-based services, called smart services. Specifically, smart products do not only collect data during their production but also when they are deployed and used by customers. This allows to optimize them with regard to the way they are actually used. Smart products are equipped with a digital identity (e.g., stored in a barcode or RFID chip) and all information related to the product is stored in some backend-database. Alternatively, the product is equipped with electronics (e.g., memory and a processor) and stores this data itself.

Industrial IoT brings many new challenges with regard to different aspects, including security, privacy, standardization, legal, and social aspects. In particular increased diversity and large numbers of devices in IoT systems require highly scalable solutions for, e.g., naming and addressing, data communication, knowledge management, and service provisioning. Further, most IoT devices have only limited resources which demands for architectures supporting low power, low cost, fully networked integrated devices that are compatible with standard communication techniques.

3. SECURITY & PRIVACY CHALLENGES

In the context of industrial control systems, the notion of security has traditionally almost the same meaning as safety, i.e., the protection of humans, environment, and machines against consequences of system failures [73, 71]. Only with integration of information technology, protection against cyberattacks became increasingly important and today is a major design goal of Industrial IoT systems [71, 23, 75].

Attacks on Industrial IoT Systems

In the past, systematic integration of countermeasures against cyberattacks often followed integration of IT components with some delay. As a result, current Industrial IoT systems are vulnerable to a variety of cyberattacks [52, 51, 31, 7, 12, 70, 22, 27, 50, 74, 40, 41, 21, 19].

One of the first successful attacks against industrial control systems was the Slammer worm, which infected two critical monitoring systems of a nuclear power plant in the U.S.A. in 2003 [51]. In the same year, a computer virus infected the signal and dispatching control system of a major transportation network in the U.S.A. leading to complete stop of passenger and freight trains [52]. In the following years, many security incidents affecting industrial control systems and critical infrastructure have been reported in literature [31, 7, 22, 40]. While these attacks seem not to have specifically targeted industrial control systems, Stuxnet [70, 22, 40] indicates a new trend towards highly targeted attacks and sab-

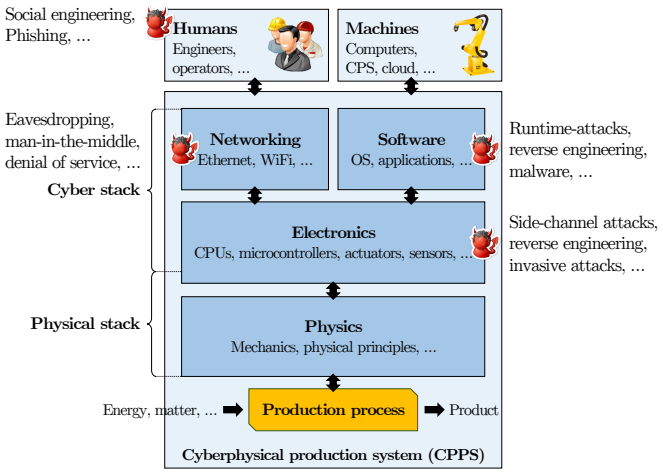

Figure 2: Cyberphysical production system (CPPS) architecture and attack surfaces

otage by powerful adversaries, e.g., nation states. Stuxnet exploited multiple zero-day vulnerabilities[2] and made centrifuges at an Iranian nuclear facility to fail.

Attack Surfaces

Industrial IoT systems provide various attack surfaces. Smart factories consist of several cyberphysical production systems (CPPS), which consist of electronics (e.g., processor and memory) and monitors that control physical processes through sensors and actuators (cf. Figure 2) [61]. The electronics are driven by software (e.g., embedded operating systems and applications) and interact with humans and other CPPS through various network connections (e.g., Ethernet or WiFi).

Attack surfaces exist on all these abstraction layers (cf. Figure 2) [12, 37, 74, 65, 33, 73, 2, 71, 30]. Electronics are subject to physical attacks, including invasive hardware attacks, side-channel attacks, and reverse-engineering attacks [55]. Software can be compromised by malicious code, such as Trojans, viruses, and runtime attacks. Communication protocols are subject to protocol attacks, including man-in-the-middle and denial-of-service attacks [28]. Even humans operating CPPS are subject to social attacks, such as phishing and social engineering.

Security Goals and Requirements

The most important objective of industrial production systems is availability, which should prevent any unnecessary delay in production that results in loss of productivity and loss of revenues. This particularly includes protection against denial-of-service attacks against cyberphysical production systems.

Another fundamental objectives is preventing any system failure that may result in physical damage or harm to humans. To achieve this objective, the integrity of Industrial IoT systems must be preserved. This includes protection against sabotage, which may lead to unnoticed loss of product quality and increased use of resources. Further, unnoticed and unintended use of counterfeit components, which may not fulfil the quality requirements of genuine components, should be prevented. With the interconnection of cyberphysical production systems, it must be ensured that system failures or malicious attacks do not propagate within smart factories or across company boarders.

One of the objectives of Industrial IoT is to realize smart products that know their own history and may control their own production process. Another example includes smart services, where companies outsource the production of their designs to smart factories operated by third parties. In both examples the authenticity and integrity of the smart factory infrastructure and any information related to the production process must be ensured to prove to third parties that the smart factory is trustworthy. Further, e.g., in the case of warranty claims, it may be necessary to provide evidence of quality of resource materials and correctness of production of a product to third parties.

The strong connectivity of IoT-based production systems and smart products demands for new mechanisms to protect against industrial espionage and privacy of customers and employees. Hence, the confidentiality of code, data, and configuration of production systems as well as blueprints of products is an important security requirement.

4. SECURING THE INDUSTRIAL IoT

Adapting existing information security concepts to cyberphysical production systems (CPPS) is not straightforward. There are many differences between classical IT systems and CPPS [44, 18, 74, 71]. Integrity and confidentiality are primary protection goals of classical enterprise IT systems and hence, protection against cyberattacks is often a tradeoff between security and availability. For instance, if a cyberattack occurs, affected IT systems are typically temporarily disabled and then restored after the attack. However, this approach cannot be applied to CPPS, where availability is a fundamental requirement.

Other differences are due to the strict real-time requirements of CPPS, their constrained computational, memory, and energy resources, and the long lifetime of industrial production systems. Other aspects are protection of design and configuration data (intellectual property) and detection of counterfeit components (product piracy). Many industrial areas have legal requirements with regard to logging of production steps (provenance and accountability). With the increasing number of interconnected CPPS and the possibility to use Big Data techniques to analyze data collected by CPPS, privacy becomes a fundamental aspect [42, 30]. For example, Big Data analysis may violate privacy of employees or leak sensitive customer information to the manufacturer or service personnel of CPPS equipment.

To counter these security and privacy risks, a holistic cybersecurity concept for Industrial IoT systems is required that addresses the various security and privacy risks at all abstraction levels. This includes different aspects, such as platform security, secure engineering, security management, identity management, industrial rights management [71]. In particular security and privacy aspects must be preserved during the lifetime of smart production systems and smart products. In the following, we will focus on solutions for protecting embedded devices which are at core of cyberphysical production systems.

[2]Zero-day vulnerabilities are those vulnerabilities which are unknown before they are exploited, i.e., not security patches are available to fix them.

Security Architectures for CPS

There is a rich body of literature on security architectures for embedded IoT systems, mainly due to the broad range of devices considered as embedded systems [11, 10]. On the upper end are Intel and ARM architectures, which are widely used in mobile devices (e.g, smartphones and tablets). For these systems, a variety of security architectures have been proposed: software-based isolation and virtualization [35]; Trusted Computing based on secure hardware (e.g., Trusted Platform Module [67]); and processor architectures providing secure execution (e.g., ARM TrustZone [72], AEGIS [64], OASIS [46], and Intel Software Guard Extensions (SGX) [36, 20]). However, all these approaches are too complex for low-end embedded systems, which are typically designed for specific tasks and optimized for low power consumption and minimal costs. Often they must provide multiple features and meet strict real-time requirements. Security solutions for these devices are typically based on hardware-enforced isolation of security-critical code and data from other software on the same platform. Examples are SMART [13], SPM [63], SANCUS [45], and TrustLite [25]. SMART protects the integrity of only one specific embedded application (task) with read-only memory, which does not allow code changes after deployment. SPM provides hardware-enforced isolation of tasks by granting access to a task's data region only to the task itself. However, these tasks have a fixed memory layout and cannot be interrupted. Further, the task measurement of SPM is performed in hardware, i.e., it is non-interruptible and at the same time dependent on the memory size of the measured task, which violates real-time requirements. SANCUS extends SPM with a mechanism to generate and manage cryptographic secrets of tasks but inherits SPM's limitations. TrustLite generalizes the concept of SPM [63] and SMART [13] and supports interrupting tasks. However, TrustLite requires all software components to be loaded and their isolation to be configured at boot time. In contrast to SMART, SPM, and SANCUS, TyTAN [6] provides dynamic loading and unloading of multiple tasks at runtime, secure inter-process communication (IPC) with sender and receiver authentication, and real-time scheduling.

Integrity Verification of CPS

A key mechanism to verify integrity of a system's software configuration is *attestation*, which enables the detection of unintended and malicious software modifications. Various approaches to remote attestation have been proposed to-date. Common to all of them is that the device to be attested, called *prover*, sends a status report of its current software configuration to another device, called *verifier*, to demonstrate that it is in a known and, thus trustworthy, state. Since malicious software on the prover's platform could forge this report, its authenticity is typically assured by secure hardware [49, 67, 48, 14, 29, 56, 26] and/or trusted software [3, 24, 60, 59, 58, 57, 16, 32, 29, 68]. Attestation based on secure hardware is most suitable for advanced computing platforms, such as smartphones, tablets, laptops, personal computers, and servers. However, the underlying security hardware is often too complex and/or expensive for low-end embedded systems. In contrast, software-based attestation [24, 60, 59, 58, 57, 16, 32], does not require secure hardware or cryptographic secrets. However, security guarantees of software-based attestation are often unclear since it usually relies on strong assumptions, such as (1) the adversary being passive while the attestation protocol is executed, and (2) optimality of the attestation algorithm and its implementation. Such assumptions are hard to achieve in practice [4]. Hence, a secure and practical attestation scheme requires at least some basic security features in hardware but these should be kept as small as possible [14, 15, 26].

The next generation of IoT systems will consist of *device swarms*, i.e., large self-organizing heterogeneous networks of embedded devices. Verifying correct and safe operation of these systems requires an efficient *swarm attestation* mechanism to collectively verify the software integrity of all devices in order to detect unintended and malicious software modifications. However, naïve applications of remote attestation do not scale to these systems. In particular, device swarms with dynamic topologies, such as vehicular ad-hoc networks, robot swarms, and sensors in fluid environments, require novel and flexible solutions. We are aware of only one proposal to attest multiple provers running the *same* software at once [47]. The idea is that the verifier does not verify each individual attestation report, but compares integrity measurements of multiple provers. The design of an efficient attestation scheme for large dynamic and heterogeneous networks of embedded systems is a challenging open research problem.

Secure IoT Device Management

Many IoT devices (such as sensors) do not have appropriate user interfaces or suitable communication interfaces for performing pairing using legacy solutions, e.g., PIN codes as used in Bluetooth. Also, as the number of IoT devices grows, e.g., in smart home scenarios, it becomes increasingly burdensome for the user to introduce new devices, if it involves manually pairing the new device with each existing device. This becomes even more challenging with transient pairing. Therefore, pairing of devices should be achieved with *zero user interaction*, i.e., not require explicit involvement of the user. Once a device joins a group of devices, it can collaborate with all devices in this group and access the user's and the other devices' data (device-centric authentication [17]).

New ways of establishing trust among IoT devices have been presented with the premise of strongly improving user-experience by eliminating the need for the user to explicitly specify or point out the devices to be paired with each other [54, 39, 66, 38]. This can be achieved by utilizing the fact that devices that are located in the same place also consistently observe similar ambient context information. For example, IoT devices in the living room of a user's smart home will, for most of the time, observe similar changes in ambient contextual parameters like noise or light.

The management of IoT devices in future smart spaces will be extremely challenging due to their heterogeneity. Additionally, these devices will produce a large volume of nonuniform data that needs to be processed in real-time. In the context of secure pairing based on ambient data, local IoT systems need to process and analyze heterogenous data inputs with low latency to make appropriate decisions. Existing approaches rely on cloud-based services to perform these operations remotely. Unfortunately, critical privacy issues are raised when exporting substantial amounts of personal data to external services. Furthermore, the increasing number of devices connected to IoT will require highly scalable solutions with respect to data storage, latency of services,

and management of data and devices.

Local data management and local distributed analytics are expected to improve latency of local services because only minimal information will be exchanged outside local and low-latency network. For the same reason, local analytics and data management will improve user data privacy. These features will maximize usage of resources available in IoT systems and provide building blocks for developers to create innovative services.

Performing local data management and analytics, however, raises several challenges due to diversity of devices and the need for scalable solutions. For instance, computation capacity of devices varies considerably, and thus analytical tasks cannot be distributed uniformly among IoT devices. Moreover, devices have several non-negligible constrains such as power management, constrained resources (e.g., limited computation power, storage, communication means, and energy), and permeability to attacks. Finally, interoperability between devices requires a data abstraction model supported by an extensive RESTful API [5].

5. CONCLUSION

Internet of Things (IoT) is an emerging key technology that paves the way for the next generation of industrial production systems. Smart factories will consist of self-organizing production systems that optimize themselves with regard to resource availability and consumption, even across company boarders. These systems enable product individualization at costs of mass production and new smart services, including product optimization according to customer usage and de-centralized long-term product support.

Today's IoT systems are not sufficiently enhanced to fulfill the desired functional requirements and bear security and privacy risks. Particularly, attacks on cyberphysical systems may cause physical damage and threaten human life. Ubiquity of IoT devices may lead to a transparent society through seamless supervision of employees and customers.

Protecting IoT requires a holistic cybersecurity framework covering all abstraction layers of heterogeneous IoT systems and across platform boundaries. However, existing security solutions are inappropriate since they do not scale to large networks of heterogeneous devices and cyberphysical systems with constrained resources and/or real-time requirements. Further research is required to develop and design appropriate IoT security mechanisms, including novel isolation primitives that are resilient to run-time attacks, minimal trust anchors for cyberphysical systems, and scalable security protocols.

Acknowledgments

This work has been co-funded by the DFG as part of project S2 within the CRC 1119 CROSSING.

6. REFERENCES

[1] *SmartFactory — From Vision to Reality in Factory Technologies*. International Federation of Automatic Control, 2008.

[2] C. Alcaraz, R. Roman, P. Najera, and J. Lopez. Security of industrial sensor network-based remote substations in the context of the internet of things. *Ad Hoc Netw.*, 11(3), 2013.

[3] W. Arbaugh, D. Farber, and J. Smith. A secure and reliable bootstrap architecture. In *IEEE Symposium on Security and Privacy (S&P)*, 1997.

[4] F. Armknecht, A.-R. Sadeghi, S. Schulz, and C. Wachsmann. A security framework for the analysis and design of software attestation. In *ACM Conference on Computer & Communications Security (CCS)*. ACM, 2013.

[5] M. Blackstock and R. Lea. Toward interoperability in a web of things. In *ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication (UbiComp)*. ACM, 2013.

[6] F. Brasser, P. Koeberl, B. E. Mahjoub, A.-R. Sadeghi, and C. Wachsmann. TyTAN: Tiny trust anchor for tiny devices. In *Design Automation Conference (DAC)*. ACM, 2015.

[7] E. Byres and J. Lowe. The myths and facts behind cyber security risks for industrial control systems. Technical report, PA Consulting Group, 2004.

[8] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Conference on Security*. USENIX Association, 2011.

[9] D. J. Cook and S. K. Das. How smart are our environments? An updated look at the state of the art. *Pervasive Mob. Comput.*, 3(2), 2007.

[10] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti. A large-scale analysis of the security of embedded firmwares. In *USENIX Conference on Security Symposium*. USENIX Association, 2014.

[11] A. Cui and S. J. Stolfo. A quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan. In *Annual Computer Security Applications Conference (ACSAC)*. ACM, 2010.

[12] D. Dzung, M. Naedele, T. von Hoff, and M. Crevatin. Security for industrial communication systems. *Proceedings of the IEEE*, 93(6), 2005.

[13] K. Eldefrawy, A. Francillon, D. Perito, and G. Tsudik. SMART: Secure and minimal architecture for (establishing a dynamic) root of trust. In *Network and Distributed System Security Symposium (NDSS)*, 2012.

[14] K. Eldefrawy, G. Tsudik, A. Francillon, and D. Perito. SMART: Secure and minimal architecture for (establishing a dynamic) root of trust. In *Network and Distributed System Security Symposium (NDSS)*. Internet Society, 2012.

[15] A. Francillon, Q. Nguyen, K. B. Rasmussen, and G. Tsudik. A minimalist approach to remote attestation. In *Conference on Design, Automation & Test in Europe (DATE)*. European Design and Automation Association, 2014.

[16] R. W. Gardner, S. Garera, and A. D. Rubin. Detecting code alteration by creating a temporary memory bottleneck. *Trans. Info. For. Sec.*, 4(4), 2009.

[17] E. Grosse and M. Upadhyay. Authentication at scale. *IEEE Security Privacy*, 11(1), 2013.

[18] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle. Security challenges in the ip-based internet of things. *Wirel. Pers. Commun.*, 61(3), 2011.

[19] G. Hernandez, O. Arias, D. Buentello, and Y. Jin. Smart Nest thermostat — A smart spy in your home. In *BlackHat USA*, 2014.

[20] M. Hoekstra, R. Lal, P. Pappachan, V. Phegade, and J. Del Cuvillo. Using innovative instructions to create trustworthy software solutions. In *Hardware and Architectural Support for Security and Privacy (HASP)*. ACM, 2013.

[21] A. G. Illera and J. V. Vidal. Lights off! The darkness of the smart meters. In *BlackHat Europe*, 2014.

[22] M. Kabay. Attacks on power systems: Hackers, malware, 2010.

[23] H. Kagermann, W. Wahlster, and J. Helbig. Securing the future of German manufacturing industry — Recommendations for implementing the strategic initiative Industrie 4.0, 2013.

[24] R. Kennell and L. H. Jamieson. Establishing the genuinity of remote computer systems. In *USENIX Security*. USENIX Association, 2003.

[25] P. Koeberl, S. Schulz, A.-R. Sadeghi, and V. Varadharajan. TrustLite: A security architecture for tiny embedded devices. In *European Conference on Computer Systems (EuroSys)*. ACM, 2014.

[26] J. Kong, F. Koushanfar, P. K. Pendyala, A.-R. Sadeghi, and C. Wachsmann. PUFatt: Embedded platform attestation based on novel processor-based PUFs. In *Design Automation Conference (DAC)*. ACM, 2014.

[27] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In *IEEE Symposium on Security and*

Privacy (S&P), 2010.

[28] F. Koushanfar, A.-R. Sadeghi, and H. Seudie. Eda for secure and dependable cybercars: Challenges and opportunities. In *Proceedings of the 49th Annual Design Automation Conference*. ACM, 2012.

[29] X. Kovah, C. Kallenberg, C. Weathers, A. Herzog, M. Albin, and J. Butterworth. New results for timing-based attestation. In *IEEE Symposium on Security and Privacy (S&P)*, 2012.

[30] J. S. Kumar and D. R. Patel. A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications*, 90(11), 2014.

[31] E. Levy. Crossover: Online pests plaguing the off line world. *IEEE Security Privacy*, 1(6), 2003.

[32] Y. Li, J. M. McCune, and A. Perrig. VIPER: Verifying the integrity of peripherals' firmware. In *ACM Conference on Computer and Communications Security (CCS)*. ACM, 2011.

[33] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen. Cyber security and privacy issues in smart grids. *IEEE Communications Surveys Tutorials*, 14(4), 2012.

[34] Y. Liu and G. Zhou. Key technologies and applications of internet of things. In *5th International Conference on Intelligent Computation Technology and Automation (ICICTA)*, 2012.

[35] J. McCune, Y. Li, N. Qu, Z. Zhou, A. Datta, V. Gligor, and A. Perrig. TrustVisor: Efficient TCB reduction and attestation. In *IEEE Symposium on Security and Privacy (S&P)*, 2010.

[36] F. McKeen, I. Alexandrovich, A. Berenzon, C. V. Rozas, H. Shafi, V. Shanbhogue, and U. R. Savagaonkar. Innovative instructions and software model for isolated execution. In *Hardware and Architectural Support for Security and Privacy (HASP)*. ACM, 2013.

[37] C. Medaglia and A. Serbanati. An overview of privacy and security issues in the internet of things. In *The Internet of Things*. Springer, 2010.

[38] M. Miettinen, N. Asokan, F. Koushanfar, T. D. Nguyen, J. Rios, A.-R. Sadeghi, M. Sobhani, and S. Yellapantula. I know where you are: Proofs of presence resilient to malicious provers. In *ACM Symposium on Information, Computer and Communications Security (ASIACCS)*. ACM, 2015.

[39] M. Miettinen, N. Asokan, T. D. Nguyen, A.-R. Sadeghi, and M. Sobhani. Context-based zero-interaction pairing and key evolution for advanced personal devices. In *Conference on Computer and Communications Security (CCS)*. ACM, 2014.

[40] B. Miller and D. Rowe. A survey SCADA of and critical infrastructure incidents. In *Research in Information Technology (RIIT)*. ACM, 2012.

[41] C. Miller and C. Valasek. A survey of remote automotive attack surfaces. In *BlackHat USA*, 2014.

[42] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac. Survey internet of things: Vision, applications and research challenges. *Ad Hoc Netw.*, 10(7), 2012.

[43] D. M. Nicol. Hacking the lights out. *Scientific American*, 305, 2011.

[44] P. Nixon, W. Wagealla, C. English, and S. Terzis. Security, privacy and trust issues in smart environments, 2004.

[45] J. Noorman, P. Agten, W. Daniels, R. Strackx, A. Van Herrewege, C. Huygens, B. Preneel, I. Verbauwhede, and F. Piessens. Sancus: Low-cost trustworthy extensible networked devices with a zero-software trusted computing base. In *USENIX Conference on Security*. USENIX Association, 2013.

[46] E. Owusu, J. Guajardo, J. McCune, J. Newsome, A. Perrig, and A. Vasudevan. OASIS: On achieving a sanctuary for integrity and secrecy on untrusted platforms. In *ACM Conference on Computer & Communications Security (CCS)*. ACM, 2013.

[47] H. Park, D. Seo, H. Lee, and A. Perrig. SMATT: Smart meter attestation using multiple target selection and copy-proof memory. In *Computer Science and its Applications*. Springer, 2012.

[48] B. Parno, J. McCune, and A. Perrig. Bootstrapping trust in commodity computers. In *IEEE Symposium on Security and Privacy (S&P)*, 2010.

[49] N. L. Petroni, Jr., T. Fraser, J. Molina, and W. A. Arbaugh. Copilot — A coprocessor-based kernel runtime integrity monitor. In *USENIX Security Symposium*. USENIX Association, 2004.

[50] J. Pollet and J. Cummins. Electricity for free — The dirty underbelly of SCADA and smart meters. In *BlackHat USA*, 2010.

[51] K. Poulsen. Slammer worm crashed Ohio nuke plant network, 2003.

[52] PR Newswire. Computer virus strikes CSX transportation computers, 2003.

[53] J. Rifkin. *The Third Industrial Revolution: How Lateral Power is Transforming Energy, the Economy, and the World*. Palgrave MacMillan, 2011.

[54] M. Rostami, A. Juels, and F. Koushanfar. Heart-to-heart (h2h): authentication for implanted medical devices. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013.

[55] M. Rostami, F. Koushanfar, and R. Karri. A primer on hardware security: Models, methods, and metrics. *Proceedings of the IEEE*, 2014.

[56] S. Schulz, A.-R. Sadeghi, and C. Wachsmann. Short paper: Lightweight remote attestation using physical functions. In *ACM Conference on Wireless Network Security (WiSec)*. ACM, 2011.

[57] A. Seshadri, M. Luk, and A. Perrig. SAKE: Software attestation for key establishment in sensor networks. In *Distributed Computing in Sensor Systems*. Springer, 2008.

[58] A. Seshadri, M. Luk, A. Perrig, L. van Doorn, and P. Khosla. SCUBA: Secure code update by attestation in sensor networks. In *ACM Workshop on Wireless Security (WiSe)*. ACM, 2006.

[59] A. Seshadri, M. Luk, E. Shi, A. Perrig, L. van Doorn, and P. Khosla. Pioneer: Verifying code integrity and enforcing untampered code execution on legacy systems. In *ACM Symposium on Operating Systems Principles (SOSP)*. ACM, 2005.

[60] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla. SWATT: Software-based attestation for embedded devices. In *IEEE Symposium on Security and Privacy (S&P)*, 2004.

[61] D. Shahrjerdi, J. Rajendran, S. Garg, F. Koushanfar, and R. Karri. Shielding and securing integrated circuits with sensors. In *Computer-Aided Design (ICCAD), 2014 IEEE/ACM International Conference on*. IEEE, 2014.

[62] A. Soullie. Industrial control systems: Pentesting PLCs 101. In *BlackHat Europe*, 2014.

[63] R. Strackx, F. Piessens, and B. Preneel. Efficient isolation of trusted subsystems in embedded systems. In *Security and Privacy in Communication Networks*. Springer, 2010.

[64] G. E. Suh, D. Clarke, B. Gassend, M. van Dijk, and S. Devadas. AEGIS: Architecture for tamper-evident and tamper-resistant processing. In *Annual International Conference on Supercomputing (CIS)*. ACM, 2003.

[65] H. Suo, J. Wan, C. Zou, and J. Liu. Security in the internet of things: A review. In *International Conference on Computer Science and Electronics Engineering (ICCSEE)*, 2012.

[66] H. T. T. Truong, X. Gao, B. Shresthab, N. Saxena, N. Asokan, and P. Nurmi. Using contextual co-presence to strengthen zero-interaction authentication: Design, integration and usability. *Pervasive and Mobile Computing*, 2014.

[67] Trusted Computing Group (TCG). Website, 2011.

[68] A. Vasudevan, J. McCune, J. Newsome, A. Perrig, and L. van Doorn. CARMA: A hardware tamper-resistant isolated execution environment on commodity x86 platforms. In *ACM Symposium on Information, Computer and Communications Security (ASIACCS)*. ACM, 2012.

[69] O. Vermesan and P. Friess. *Internet of Things — From Research and Innovation to Market Deployment*. River Publishers, 2014.

[70] J. Vijayan. Stuxnet renews power grid security concerns, 2010.

[71] M. Waidner, M. Kasper, T. Henkel, C. Rudolph, and O. Küch. Eberbacher Gespräch zu "Sicherheit in der Industrie 4.0", 2013.

[72] J. Winter. Trusted computing building blocks for embedded linux-based ARM Trustzone platforms. In *ACM Workshop on Scalable Trusted Computing (STC)*. ACM, 2008.

[73] K. Zhao and L. Ge. A survey on the internet of things security. In *Computational Intelligence and Security (CIS)*, 2013.

[74] B. Zhu, A. Joseph, and S. Sastry. A taxonomy of cyber attacks on SCADA systems. In *International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing*. IEEE, 2011.

[75] S. Zonouz, J. Rrushi, and S. McLaughlin. Detecting industrial control malware using automated PLC code analytics. *IEEE Security and Privacy*, 12(6), 2014.

[76] D. Zuehlke. Smartfactory — towards a factory of things. *Annual Reviews in Control*, 34(1), 2010.