Practical Security Aspects of the Internet of Things

Jörn Mehnen, Hongmei He, Stefano Tedeschi and Nikolaos Tapoglou

Abstract Industry 4.0 and with that the Internet of Things (IoT) are expected to revolutionize the industrial world. The vast amount of interconnected devices bear the great opportunity to collect valuable information for advancing decision making in management and technology to improve through-life management of a product. Cyber-physical systems and the Internet of Services will revolutionize our current world through fully interconnected communication where information and services are becoming ubiquitous. The availability of information across a system of systems can be very powerful when utilized properly and harnessed adequately. The vast network of small, power-sensitive and often deeply embedded devices that are streaming potentially commercially sensitive data over long periods of time poses an entirely different type of threat than known from the conventional PC world. Adequate and sensible measures need to be taken right at the design stage of IoT devices in order to take best advantage of Industry 4.0 technology. This chapter introduces a set of key security issues related to the implementation of IoT in an industrial mechanical engineering context. A real-world example concerning remote maintenance of CNC machine tools illustrates the different threat scenarios related to IoT in practice. The paper touches on Big Data and Cloud Manufacturing but will remain focused on improving security at the Edge of IoT, i.e. where data is collected, transmitted and eventually transferred back to the physical actuators. The aim of this chapter is to introduce a generic overview of real-world IoT security

J. Mehnen (✉)
University of Strathclyde, Glasgow G1 1XJ, UK
e-mail: jorn.mehnen@strath.ac.uk

H. He · S. Tedeschi
Cranfield University, Cranfield, Bedfordshire MK43 0AL, UK
e-mail: h.he@cranfield.ac.uk

S. Tedeschi
e-mail: s.tedeschi@cranfield.ac.uk

N. Tapoglou
AMRC with Boeing University of Sheffield, Advanced Manufacturing Park, Wallis Way, Catcliffe, Rotherham S60 5TZ, UK
e-mail: n.tapoglou@amrc.co.uk

© Springer International Publishing AG 2017

L. Thames and D. Schaefer (eds.), *Cybersecurity for Industry 4.0*,
Springer Series in Advanced Manufacturing, DOI 10.1007/978-3-319-50660-9_9

jorn.mehnen@strath.ac.uk

issues as well as giving a deeper technical example-supported insight into practical considerations for designing IoT systems for practical use in business.

Keywords IoT security · Industry 4.0 · Remote maintenance of CNC machines

1 Introduction

The term "Industry 4.0", though not very well defined yet, is used to describe in broad terms the move from the third Industrial Revolution or Digital Revolution, which encompasses the change from mechanical, and electronic technology to digital technology, to the fourth Industrial Revolution which covers the world of Cyber-Physical Systems, the Internet of Things and the Internet of Services (Kang et al. 2016). All three aspects of Industry 4.0 are hinging on secure communication. Hence, it is of utmost importance that business can utilize the opportunities that the Internet offers in a secure, confident, agile and prosperous way. Business needs to be equipped with the knowledge about the capabilities and limitations and potential risks the Cyberspace poses to fully exploit the rich opportunities of the digital era. Cyberattacks continue to create a Tier 1 risk. This has been expressed clearly in the National Security Risk Assessment of 2015 (UK Government 2015).

Security helps improving trust, collaboration, individual industrial competitive advantage and even maintaining national security and individual safety. Industry 4.0 requires maintaining strict access to confidential data as well as to digital services and physical processes that are linked to complex cyber-physical systems that can control whole factories at a physical as well as at the decisions level. Fast and agile security measures that are able to adapt to the quickly changing attack strategies in Cyberspace need to be in place to make Industry 4.0 work efficiently now and in the long term future.

The intention of this chapter is to address the concerns of industry which is trying to adopt IoT to secure new business opportunities. Section 2 of this chapter introduces generic security threats related to industrial IoT. Section 3 of this chapter discusses a practical real-world example with the intention to demonstrate the generic security topics from Sect. 2 in a practical mechanical engineering environment. Section 4 summarizes the previous sections and draws further conclusions.

2 IoT Security Threats

In an Industry 4.0 context, communication cannot be treated as an isolated process anymore. Systems are getting increasingly interconnected and this trend will continue also in the future. Readily available information at every level will be expected by managers as well as by the people on the ground who are running and

jorn.mehnen@strath.ac.uk

maintaining machines. Systems that may have been designed with the intention to be entirely isolated may, at a later stage, get connected to other systems to utilize their power more efficiently at a global level. For example, the connection of well-tested though isolated legacy systems with new and advancing services through the Internet can help retaining these useful legacy systems instead of making them obsolete. Systems—and particularly IoT systems—should be designed right from the start with the option to integrate them with other systems at any time in a well-controlled and comparatively easy and smooth way.

Industry 4.0 technology utilizes the Internet of Things to facilitate the concept of Cyber-Physical Systems (CPS) that offers new business opportunities through the Internet of Services. In the manufacturing domain, the Internet of Services is also known as Cloud Manufacturing (Li and Mehnen 2013). The concept of Servitization (Raddats et al. 2016; Huxtable and Schaefer 2016) introduces a new business approach where the conventional approach of selling a product is replaced by providing a service to a customer while the product itself often remains property of the manufacturer. This approach introduces new challenges to the manufacturer because the associated new availability contract schemes leave the manufacturer with the Through-Life service tasks which cover the whole life span of a product from its design and manufacture, over its repair, maintenance or overhaul to its final recycle or disposal. In this scenario, the Internet of Things can help in various aspects. Real-time data can be gathered for example for product and process monitoring purposes. Large amounts of data can be streamed together to form Big Data (Pääkkönen and Pakkala 2015) that can be exploited at a higher level, for example to support strategic condition based maintenance decisions based on thorough Big Data analytics or as feedback into design and manufacture. IoT can also help in converting the analytical decisions made in the Cloud into automated actions that influence processes and product utilization actively.

2.1 Top Security Issues in IoT Systems

The increasing use of the Internet and mobile devices means that the hard boundaries of enterprises are disappearing and, as a result, the risk landscape is increasing. IoT enabled Cyber-Physical Systems (CPS) are facing vulnerabilities and threats from the Internet (He et al. 2016). This has attracted the attention from researcher. For example, the European project E-CRIME (2016) provided a cyber-crime inventory and networks in non-ICT sectors. It has shown that the cause of system interference can range from viruses, worms, Trojan horses, software bombs, disrupting computer services, Denial of Computer Services to sabotage.

Advanced manufacturing systems are not secure like traditional systems. Cybersecurity has become a critical challenge in IoT enabled CPS, which could be threatened by a wide variety of cyber-attacks ranging from criminals and terrorists to hacktivists. As a consequence, Cybersecurity is critical for the success of Smart Manufacturing. Cyber-threats to the Industrial IoT are real, global and growing,

jorn.mehnen@strath.ac.uk

including theft of trade secrets and intellectual property, hostile alterations to data, and disruptions or denial of process control (Albert 2015). The public is becoming increasingly aware of the potential security threats caused by the malicious exploitation of poorly secured systems.

A distinct feature of Smart Manufacturing is that the manufacturing processes are connected to the suppliers through the Internet. Suppliers will have increased visibility of material consumption on the plant floor and can replenish stock just-in-time. Pervasive visibility and proactive replenishment are the two major benefits of IoT to the Manufacturing Supply Chain (NN 2016). However, organisations or enterprises within a connected supply chain will have different levels of security. A determined aggressor, e.g. an Advanced Persistent Threat (APT), usually identifies the organisation with the weakest cybersecurity within the supply chain and uses these vulnerabilities to gain access to other members of the supply chain. The smaller organisations within a supply chain, due to more limited resources, often have the weakest cybersecurity arrangements (CERT-UK 2015) (Fig. 1).

It is estimated that the number of connected devices will increase to 40 billion by 2020 (Baxter 2016). A huge number of connected devices (including sensors) will produce a huge amount of data. The data flow across all levels of the information exchange throughout the whole IoT infrastructure can potentially be open to vulnerabilities. Therefore, data protection and privacy is one of IoT priority challenges (Chen 2012).

IoT is where the Internet meets the physical world. This has some serious implications on security as the attack threat moves from manipulating information to controlling actuation. Consequently, it drastically expands the attack surface from known threats and known devices to additional security threats of new devices, protocols and work-flows. Many manufacturing systems are moving from closed systems (e.g. SCADA, Modbus, CIP) into IP-based Cyber-Physical Systems. This further expands the attack surface. Figure 2 shows the evolution from a legitimate Industry Control System (ICS) to a modern ICS. Cybersecurity risks are

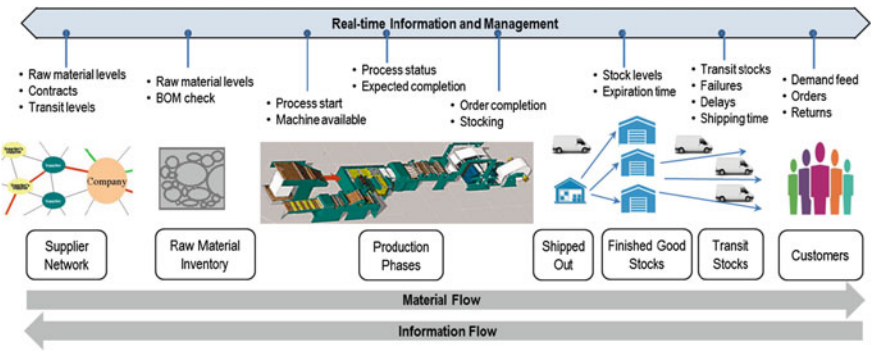

Fig. 1 IoT manufacturing supply chain (redrawn after NN 2016)

jorn.mehnen@strath.ac.uk

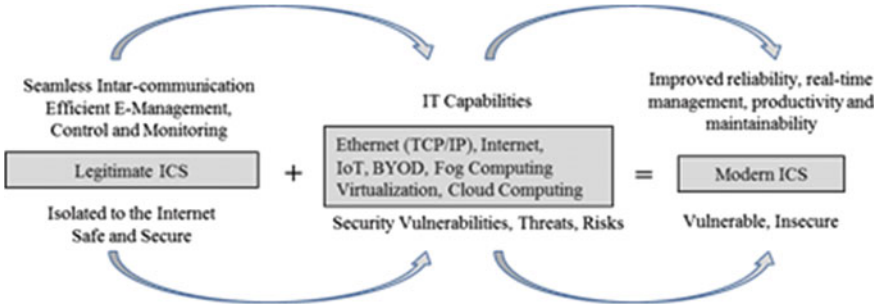

Fig. 2 Evolutions from legitimate ICS to modern ICS (redrawn after He et al. 2016)

brought to the modern ICS while a legitimate ICS is incorporated with IT capacity. The state of vulnerability is exacerbated by the fact that a legitimate ICS uses typically older equipment and is not yet well-secured against modern networked environments (Korolov 2016). This is because the components of a traditional ICS are communicating with specific protocols often without any security concern. Therefore, the big challenge is how to protect legitimate ICS from attacks when they are connected to the Internet.

2.2 The Architecture of IoT Systems

Considering the different areas of applications of IoT, one can, in general, divide IoT security issues into different areas which are either related to the fundamental IoT technical architecture and communication threats, the IoT application (threats from the environment, data flow and final use of data), or threats cause by IoT users (threats human interaction). It is also possible to divide IoT threats into logical (the use of data and meta-data and decision making), software threats and physical (hardware) threats. The categorization of IoT threats is closely related to the architectural structure of IoT and the use of IoT devices and its data.

Figure 3 shows the general IoT architecture as a multi-tiered hierarchical structure. The lowest level contains input and output devices—this level is often called the Edge. The second lowest level is the level where data is collected and processed but not sent into the Internet yet. Communication between devices at this level is generally referred to as Machine-to-Machine (M2M) communication. The third level concerns the transmission of data into the Internet and up into the related Cloud services. The highest level offers high level compute and/or memory intensive Cloud Services and Apps for either directly decision support or data storage and data exchange. Information can usually flow freely within this stack.

The Edge level itself can be further subdivided. The lowest tier of that level starts with the basic sensors or actuators which generally do not come with any particular intelligence per se. A simple data receiving and preprocessing device may

jorn.mehnen@strath.ac.uk

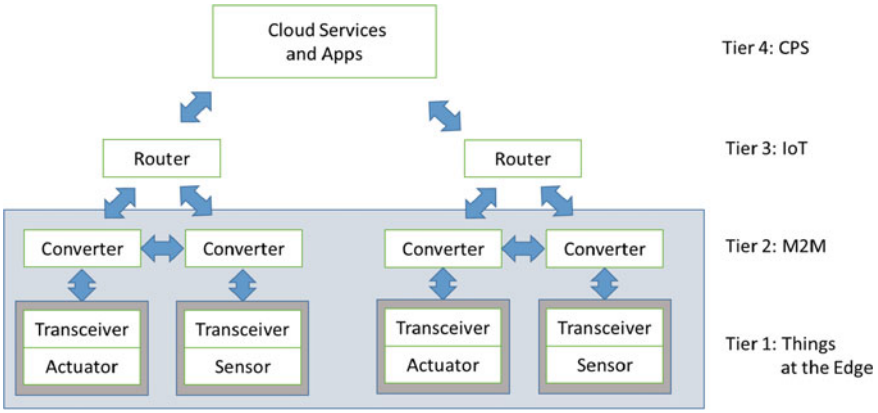

Fig. 3 IoT stack architecture

add additional basic intelligence to the sensor or actuator. An attached transceiver sends data from the intelligent sensor to an Internet connected element, for example a router. An additional transceiver may add an optional level for converting data protocols or switching between data communication technologies (e.g. Bluetooth to WiFi or NRF and LiFi and vice versa). This level is the typical domain of M2M communication which does not necessarily include any Internet connection. However, also this layer shall be considered in the following as an integral part of IoT. The approach of making IoT agnostic to the physical and transport layer protocols used by devices concept has been referred to as the Web of Things (WoT) (Guinard and Trifa 2016). Figure 3 shows the complete IoT stack including the detailed Edge.

2.3 Security Issues in the IoT Stack

Considering IoT security, one should consider the allover Internet protocol security down to the Edge. Concerning IoT security at Tier 3 and above only would imply ignoring any potential IoT security issues that are coming directly from the data generation and preprocessing levels. Security levels at Tier 3 and above are typically well-developed as these levels use conventional Internet technology. Security technology and threats at these levels are well understood and supported by agreed standards and controlled through strict regulations.

In the IoT world, however, several consortia such as AllJoyn, Thread, Open Interconnect Consortium (OCI) or the Industrial Internet Consortium (IIC) are developing (partially competing) IoT standards. At the communication/transport layer there are also various standards such as ISA100.11a, IEEE 802.15.4, NFC, ANT, Bluetooth, Eddystone, ZigBee, EnOcean, or WiMax. All these standards

jorn.mehnen@strath.ac.uk

offer different levels and schemata for implementing security. Typical security standards in IoT—which are also used in the wider Internet—are the Open Trust Protocol (OTrP) and X.509 with the latter being the most popular standard for Public Key Infrastructure (PKI) management using digital certificates and public-key encryption.

Security issues at the top two tiers of the IoT stack are typically addressed through Internet security measures which apply to the conventional Internet world. As this is well-discussed in literature, in the following only the two lowest tiers of the IoT stack will be discussed in more detail to highlight especially potential security threats at the IoT Edge.

2.3.1 Threats at the IoT Edge

Threats to security at the Tier 1 and Tier 2 level, i.e. security issues at the sensor, transceiver and converter layer level can be divided into security threats (Shahri and Ismail 2012; Di and Smith 2007) caused by

(A) humans,
(B) technical insufficiencies, and
(C) physical attacks of the actual IoT hardware.

Examples for Class A threats at the IoT level, i.e. security issues caused deliberately or involuntarily by humans considering sensors, communication, and data exchange are:

- Data entry errors or omissions
- Improper use or disposal of sensitive data
- Improper use and electronic setup of equipment
- Inadvertent acts or carelessness
- Ignorance of warnings and errors
- Ignorance due to the low cost of the equipment (“throwaway mentality”)
- Underestimation of technological complexity
- Insufficient password management
- Procedural violation
- Espionage and eavesdropping
- Impersonation and identity theft
- Shoulder surfing, i.e. the deliberate attempt to gain access to protected information through observation
- High level data analytics can reveal hidden information

Examples for Class B threats due to internal technical issues, i.e. software and hardware issues, are:

- Compromising emanations, i.e. unintentional data-related or intelligence-bearing signals, which, if intercepted and analyzed, could disclose sensitive information that is transmitted and/or processed

jorn.mehnen@strath.ac.uk

- Corruption by system errors or system failures
- Data and system contamination, i.e. the intermixing of data of different sensitivity levels can lead to an accidental or intentional violation of data integrity
- Insertion of malicious code or software
- Poor programming styles and habits
- Insufficient authentication methods (weak cryptography due to limited power, memory and speed of the Edge devices; weak random number generators)
- Misrepresentation of identity or authorization
- Insufficient and irregular firmware updates
- Data overload and improper error handling (poor Quality of Service)
- Inadequately managed and operated equipment that is mostly dormant
- Exploitation of network flaws (connections and data protocols)
- Power failures
- Obsolescence and system inconsistencies over time
- Inconsistent or changing communication protocols

Class C deal with attacks on hardware and communication through physical means. Examples of Class C issues are:

- Physical tampering with the hardware, i.e. unauthorized physical modification or alteration of equipment in a manner that degrades the security functionality of the asset
- Electromagnetic attacks through electromagnetic interference (EMI) to impact the signal transmission or the device electronics directly causing interruptions in the electronic operation of the system
- Introduction of detrimental environmental conditions, i.e. inadequate humidity or temperature causing the circuits to malfunction or deliberatively degrade or age quickly
- Introduction of hazardous materials which are flammable, oxidizing or combustible, explosive, corrosive, an irritant or radioactive
- Mechanical attacks (cutting of cables, ripping, breaking, bending)
- Deliberate power fluctuation, low power or power spikes
- Side channel attacks (timing attack, power-analysis attack, electromagnetic attack) (Di-Battista et al. 2010; Kim et al. 2015)

Different to conventional Internet and PC technology, IoT devices are often embedded and hard to reach. Ideally, IoT devices are virtually invisible and working unnoticed over long periods of time while requiring minimal maintenance and external energy. IoT devices are susceptible to security issues due to their need for constant power supply, their limited memory size as well as potentially inadequate firmware updates and maintenance.

Regular integrity scans such as virus detections are much harder to achieve in IoT networks than in the PC world due to the limited electrical and computational power of the device. Secure authorization in IoT devices is of special importance as it guarantees legitimate access to the device for servicing and data access. For very power and memory limited IoT devices even authentication can become a serious

jorn.mehnen@strath.ac.uk

issue as reliable cryptographic methods require power and memory. The use of poor pseudo number generators can compromise authentication and cryptographic exchange of data across the network.

The large number of IoT devices and their connectivity opens a potentially large attack surface. Re-organization of IoT networks, structures and data protocols and changing users with changing authorization rights require a strict and continuous maintenance of the IoT network already at the lowest levels. A single breach into one device can create a broad scale attack if many devices are following the same inadequate security setup.

A simple change of ownership of equipment containing embedded IoT devices can cause the leaking of potentially sensitive information to the new owner of the device. With the introduction of the EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 enters application in May 2018), this risk will require serious consideration by the liable OEMs.

The physical attack of the IoT hardware itself with regards to tempering or destruction is hardly mentioned in the literature. However, the physical Edge of IoT is very vulnerable to physical attacks as it is exposed to either physical degradation over time or active physical attacks. This holds for many IoT devices, from wearables to sensors that are embedded in industrial tools or military applications. Relying on the correctness of the data from these devices can be crucial. Important decisions, jobs and even lives can depend on the reliability of the communication. Physical protection of the devices is a research topic that concerns design, manufacture, programming, installation as well as the maintenance of the devices. Adding security as an "afterthought" to an existing design has the potential to be inadequate or causing long term issues that can become expensive or even dangerous. Hence, designing IoT devices right from the start with security in mind becomes an imperative that cannot be overlooked. Lessons learned from the current Internet and PC world can certainly help building new IoT technology that is reliable, safe and secure.

2.4 IoT Communication Technology

The current typical data communication protocols and techniques available for the IoT stack between the Internet, local area networks, individual machines, transceivers, sensors and actuators are summarized in Table 1.

The choice of the best technology depends on the application and its requirements. This concerns communication speed, the distance any data can be sent reliably, memory requirements, data processing and transmission power and the required security level. Another practical issue to be considered is the physical environment (electrical noise) as well as the ease of installation, use and maintenance. The management of a large number of devices with their individual identification, authentication and management can become a challenge in IoT as well. Some protocols such as WiFi and ZigBee offer identification, authentication and

jorn.mehnen@strath.ac.uk

Table 1 Technical aspects of IoT device communication

Mode	Technology	Protocols
Internet	WiFi, ethernet, cloud	SHTML, MQTT, XMPP, TLS/SSL, CoAP, AMQP, Mihini/M3DA, DDS, REST, SOAP, websockets, OPC UA
M2M	Wifi, bluetooth, Xbee various NRF techniques, LiFi, laser, infrared, sound (e.g. ultrasound), direct wire connection	SHTML, HTML, MQTT, XMPP-IoT, TLS/SSL, CoAP, AMQP, MQTT-SN, Mihini/M3DA, DDS, LWM2M, REST, SOAP, websocket, reactive streams
Sensor/transceiver/actuator	Mainly direct wire. In case of a detached modular combinations (see also Fig. 5) any of the M2M options are applicable	Plain secure wire communication; otherwise see above

build-in data security, while other technologies such as Near Radio Frequency (NRF), point-to-point laser communication, LiFi (Light Fidelity, i.e. communication via light), basic infrared communication or sound often do not offer these features by default.

Data transport protocols such as SHTML and TLS (Dierks and Rescorla 2008) offer current best secure data communication modes based on authentication and keys. Bluetooth builds on authentication through pairing. However, Bluetooth is not immune to Denial of Service (DoS) attacks and hence an appropriate IoT software design is required to minimize any such risks. Bluetooth data is typically encrypted by default to minimize eavesdropping, however, issues have been reported around in low-energy variants of Bluetooth models (Zhang et al. 2011).

Popular protocols for Internet data exchange in IoT are REST (Representational State Transfer), SOAP (Simple Object Access Protocol), CoAP (Constrained Application Protocol) and MQTT and AMQP (both OASIS standards for light weight Internet/IoT), XMPP-IoT (Extensible Messaging and Presence Protocol) or LWM2M (Lightweight M2M). These protocols co-exist with several other protocols and also next to less flexible proprietary direct peer-to-peer data exchange protocols depending on the communication technique adopted. OPC UA is an international standard for connecting devices on the plant floor with well-developed interfaces to the Internet and Cloud services providing a unified standard for user authentication and authorization, auditability and availability. OPC UA is also the recommended standard of secure connectivity in the Reference Architecture Model Industry 4.0 (RAMI4.0) (VDI/VDE 2016).

REST is used in local networks or across the Internet. REST uses standardized HTTP verbs (GET, POST, PUT, DELETE, etc.) to send data or request data packages from web resources identified by Uniform Resource Identifiers (URI). RESTful implementations make use of standards such as HTTP, URL, JSON, and XML for a structured data exchange. REST like SOAP are not secure protocols per

jorn.mehnen@strath.ac.uk

se. Security comes through other secure communication layers such as TLS, direct data encryption or Wi-Fi Protected Access (WPA) or through the implementation as in the case of Reactive Streams (Java/JavaScript).

MQTT (Message Queuing Telemetry Transport) was initially designed for oil pipeline maintenance through satellite communication. MQTT is an open data exchange protocol (OASIS standard since 2014, Banks and Gupta 2015) which is becoming increasingly popular in the IoT community due to its various light weight (i.e. small code size) implementations provided in many computer languages. It offers high data exchange speed and little overhead. MQTT supports scalability to manage very large numbers of IoT modules. MQTT requires a central data broker to which many clients can subscribe to receive messages related to topics that have been published on the broker by other clients. Clients can identify themselves at the broker through passwords. With respect to security, MQTT relies mainly on the security coming from underlying communication layers or the security offered by the application. Exchanged data is by default not encrypted but the MQTT payload can, of course, be encrypted. A major advantage of MQTT is the adjustable Quality of Service (QoS) that guarantee that messages reception can been acknowledged. This can be of particular interest for example in a TES manufacturing environment where e.g. information of machine downtime may need to be recorded reliably for contract reasons.

The enterprise-level Advanced Message Queuing Protocol AMQP (ISO/IEC 19464) provides a platform-agnostic method for ensuring information safe transport between applications and among organizations. Notable users of AMQP come from areas such as the financial sector, US Department of Homeland Security or operating systems. The framing and protocol definitions for security layers in AMQP are expected to be defined externally as in the case of TLS. An exception to this is the SASL (Melnikov and Zeilenga 2006) security layer which depends on its host protocol to provide framing.

The Cloud can provide a means to automate complex decision processes through secure Cloud computing services. When based on IoT technology, these services employ a variety of technologies that can process large amounts of data in a massively parallel way. Data may stream into these services at a continuous and rapid speed or at long time intervals when the device is dormant to save power. IoT means connecting systems with systems. Hence, one has to design IoT systems for a mix of different data speeds and data types. Devices and services with a variety of different properties and demands need to be managed in parallel using services that employ techniques such as asynchronous “lazy evaluation” (e.g. used in Node.js, Wilson 2013) in a non-halting manner to deal with different speeds of responses from the services to minimize waiting time for the service requesting clients. While this can be a challenge in itself, authentication and secure data exchange between the highest and the lowest IoT levels need to be maintained throughout the complex network of devices and services.

In contrast to the conventional PC world, where the communication is typically comparatively stable and error free; this might not be the case with IoT devices and their networks. IoT networks should to be designed with robustness against

jorn.mehnen@strath.ac.uk

communication errors in mind. Due to the simple characteristics of the basic sensors in IoT systems communication errors are more likely. Noisy data should not be misinterpreted as attacks. Tunneling solutions that improve software security can potentially get confused or work less efficient if they are overloaded by erroneous data due to poor communication channels or deeply embedded or poorly designed IoT devices.

3 Technical Example: Remote Maintenance of Machine Tools

Remote maintenance of machine tools requires reliable and safe communication from machine to machine and from the machine to the services that offer decision making support through the Cloud. Remote maintenance also requires a secure route for the information back to the machine tool and the human where the decisions are automatically actuated or manually executed.

3.1 IoT Remote Maintenance Architecture

In the context of this section, remote maintenance of machine tools will be regarded as all tasks that cover machine tool monitoring, data analysis for through-life service support and the actuation of any maintenance of the machine tool. Through-life service support for machine maintenance deals with machine performance and failure prediction of individual machine tools and machine tool components and globally interconnected machine tool assemblies. Through-life service support also covers maintenance support through dashboards and rule based decisions support considering the whole-life performance of a machine tool.

IoT serves remote maintenance through sensor networks, advanced data analytics, visualization as well as, if requested, active automated or semi-automated maintenance services that help extending the life of a machine tool. A particularly attractive aspect of IoT is that this technology can be applied not only to existing new machine tools but also to upgrade older (in the following called “legacy”) machine tools that are typically not well Internet enabled. Advancing legacy machines through IoT into the age of Industry 4.0 is not only attractive to industry as a technological means to maintain legacy machines but also to retain and upgrade existing and often very expensive equipment. IoT also offers the advantage that young machine tool operators can enjoy the quality of interaction with machines that a new generation of workers and technicians would be expecting after experiencing modern smart communication technology such as smart phones and tablets.

jorn.mehnen@strath.ac.uk

In this section an example of remote machine tool maintenance is presented that looks into security issues related to IoT sensors deployed in machine tools, the secure data transfer into the Cloud and secure data transfer back to the level of IoT actuators on the machine. Figure 4 illustrates the general setup of a possible IoT supported remote maintenance architecture for machine tools. In this setup, intelligent sensors and actuator units (see also Fig. 5) are embedded in the machine. The flexibility of small though powerful intelligent IoT Units and their application inside the machine tool makes the application of IoT technology a lot easier and more convenient than the use of large IoT devices. The setup in Fig. 4 can be applied to both, modern as well as legacy machines. Information from existing data interfaces directly from the machine tool such as MTconnect® or data from industrial ERP, PLM and Manufacturing Execution Systems (MES) can be augmented with Big Data from secure Cloud Services.

IoT security has to be considered especially in industrial networks where data security is associated with company integrity but also directly with safety on the plant floor. In a machine tool, IoT devices can get exposed to very harsh environments. Corrosive liquids, destructive heat and vibrations can be the source of device degradation and the sometimes intense electrical noise coming from the drives or the spindle can cause communication issues. Interception of data about machine performance and machine availability can be harmful to the reputation and competitiveness of a company. Unauthorized use or manipulation of IoT devices

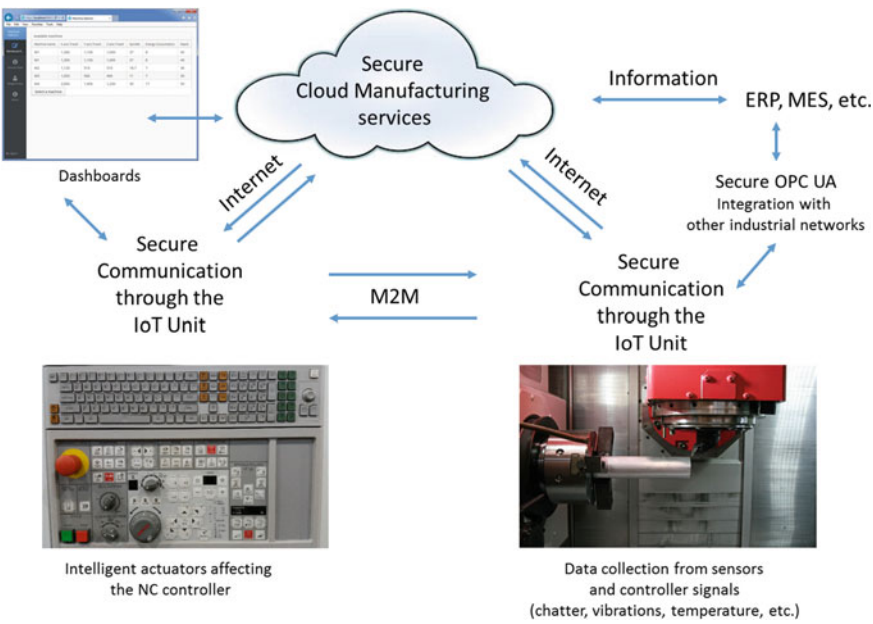

Fig. 4 An example of a Secure IoT supported remote maintenance architecture for modern as well as legacy machine tools

jorn.mehnen@strath.ac.uk

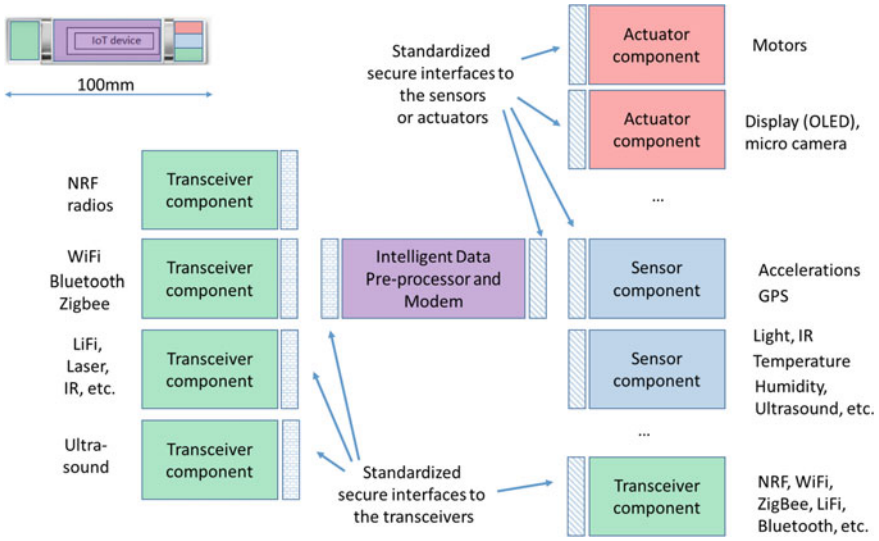

Fig. 5 Secure modular sensor/actuator/communication IoT Unit

can cause threats to the machine and potentially even to the operator. When embedded in the working space of a machine tool, IoT devices should be virtually unnoticeable, i.e. they should use as few wires and setups as possible. They should work robustly over long periods of time without any interruptions while needing none or only minimal maintenance (e.g. firmware updates or low power supply). This makes the selection of the right and reliable IoT technologies a non-trivial task.

Having a machine tool that can be controlled and operated remotely can safe cost and time, increase convenience and flexibility and even open new business opportunities. For example, remote maintenance can help saving cost on maintenance personnel that can otherwise be more efficiently deployed for complex tasks where human intelligence is really required. Employing secure IoT sensors and actuators should not be complex or expensive while requiring only a minimum amount of variation (i.e. non-invasive) to the machine tool. Augmenting machine tools should be gradually scalable, i.e. it should be possible to add, remove or replace as many IoT devices as deemed necessary while maintaining an entirely secure IoT environment. One approach to address these requirements is modularization of IoT devices.

3.2 A Novel Modular IoT Unit

In the following a new modularization concept for IoT devices is introduced. The advantage of modularization is the flexibility to easily replace specialized secure

jorn.mehnen@strath.ac.uk

and temper-hardened components. Modularization also helps with flexible scaling of the device capabilities and adapting the device to the individual local requirements. Modular devices are lean and flexible and can adapt and scale to the actual engineering needs while minimizing the potential attack surface.

Figure 5 illustrates the concept of a modular and standardized IoT Unit for sensing, actuating and communicating at the M2M level as well as into the Cloud.

The standardized secure interfaces allows for quick replacement of individual sensors, actuators or transceivers. The IoT Unit can also act as a modem, i.e. it can convert one communication protocol and technology into another. This allows for building rapidly complex heterogeneous and robust IoT Unit networks. Although machine tool data will be collected in areas with potentially high electrical noise, all the data should be preferably transferred wirelessly to increase convenience of deployment. A modular approach allows to pick and choose the combination of the most robust communication means. Small and modular IoT devices also have the advantage to be comparatively cheap and easy to maintain and replace.

For the actual design of the IoT Unit a small and robust build size (estimated size between 50 and 100 mm excluding the power source embedded in epoxy) is preferred so that the actual unit fits easily into any machine tool. The power source uses ideally an energy harvesting unit or solar panel to allow longevity and independence. Although the current battery powered solutions are often feasible, a final choice of the power source will depend on the amount of power required for transferring data or for actuating e.g. motors.

The IoT Unit displayed in Fig. 5 shows an intended design of a sealed secure IoT Unit. Standardized communication interfaces between the components using an elaborate hardware and software authorization protocol allow access to the component data only for authorized users (Tedeschi et al. 2017). The whole approach is designed to be auditable so that any misuse can be spotted and prosecuted if necessary. The data preprocessing unit (in the middle of the IoT Unit) encrypts and decrypts data streams continuously to guarantee data security at all times. For that a miniature hardware AES cryptography low power IC solution has been developed and successfully tested.

To minimize the physical attack surface and also to accommodate for the small physical built size, the limited power supply and the typically limited memory to process data, the secure modular IoT sensor/transmitter/actuator device prefers a setup that uses only a single sensor or actuator and a single communication component at a time. In a machine tool environment the ZigBee protocol and hardware has shown to be a robust and secure communication solution (Tapoglou et al. 2015). Direct point-to-point communication through lasers is fast (e.g. for data streaming) and robust against electrical noise. However, this technique requires a clear line of sight and good geometric alignment of sender and receiver. Small IoT WiFi solutions (TCP/IP, UDP, etc.) offer the fidelity and convenience of classic Internet protocols with its associate security. Depending on the underlying protocols (e.g. MQTT is fast, reliable and scalable), WiFi protocols offer high speed (realistically between 20 Mbps and 100+ Mbps for 802.11 g/n and 802.11 ac, respectively) and reliability. The proposed IoT Unit offers the opportunity to

jorn.mehnen@strath.ac.uk

flexibly configure hybrid solutions. NRF, WiFi, ZigBee and other technologies can be utilize and combined to make the best of all individual technologies.

The current cost for the hardware of the proposed and tested IoT Unit lies on the average around £10 (excl. the power source). The actual hardware cost of the IoT Unit depends, of course, on the cost of the individual components with GPS, micro cameras and ZigBee being the most expensive while light and temperature sensors and accelerometers being comparatively cheap. The small and extremely cost efficient ESP8266/NodeMCU® modules as well as the technically well-advanced Intel Edison® are very versatile and programmable IoT units (both low power 3.3 V technology). All sensor and actuator technologies shown in Fig. 5 have been implemented and successfully tested as prototypes. However, the proposed design is still in its early stage and under constant research and development.

Remote machine maintenance offers great opportunities for the end user on the machine through improved awareness of the current and predicted machine performance, information about potential optimization options of the use and setup of a machine tool as well as potential active remote repair and control of the machine tool. Remote maintenance is also a flexible platform for software and service developers that want to offer new machine tool related services. The interconnection of the IoT solutions offers opportunities to improve project planning through simulation and information of the supply chain well in advance before a tool breaks or a spare part is required. Secure remote maintenance can play an important role in providing new services and business opportunities for Through-life Engineering and Industry 4.0.

4 Summary and Conclusion

The Internet of Things is a phenomenon that is currently receiving immense attention due to the rapid move of industry to adopt Industry 4.0. The concept of Cyber-Physical Systems is an integral component of the Industry 4.0 idea. It requires that objects are connected through the Internet or amongst themselves to create a fully interconnected industrial networked environment that offers smart solutions that improve decision making or direct automated process control. However, the large number of interconnected things requires secure and safe communication so that any decisions and actions made are based on reliable and properly authorized information. The risks posed in the IoT world are different to those in the classic Internet world that runs on PCs. In IoT, devices may be very limited in size, computational power and physical power supply, difficult to access, and exposed to harsh environments and unreliable networks. IoT offers great opportunities for the manufacturing industry to utilize the power of communication —this applies both for new as well as legacy equipment. However, even under the extreme conditions some IoT devices have to operate, security of the data needs to be guaranteed at all times to provide the highest quality of service. This article describes various IoT threats. It also introduces an example of an IoT application in

jorn.mehnen@strath.ac.uk

a real-world machine tool environment. A novel design—the IoT Unit—is proposed that thrives to lower the barriers to a more secure, easy and efficient application of IoT for a prosperous Industry 4.0 world.

Acknowledgements This work is partially supported by the EPSRC High Value Manufacturing Catapult Fellowship with the AMRC project "BAUTA: A non-invasive remote maintenance tool for legacy CNC machine tools". The project gratefully acknowledges the support of Kennametal and the EU project LegInt in collaboration with the University of Patras (LMS) and Formtec GmbH. The authors would also like to thank the reviewers for their helpful comments and suggestions.

References

Albert M (2015) 7 Things to know about the Internet of Things and Industry 4.0. Modern Mach Shop Mag 88(4):74

Banks A, Gupta R (2015) MQTT version 3.1.1 plus errata 01 OASIS standard incorporating approved errata 01, 10 December 2015, OASIS Open 2015. http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/errata01/os/mqtt-v3.1.1-errata01-os-complete.pdf. Accessed 10 Nov 2016

Baxter RJ (2016) Bluemix and the internet of things. https://developer.ibm.com/bluemix/2014/07/16/bluemix-internet-things/. Accessed 10 Nov 2016

CERT-UK (2015) Cyber-security risks in the supply chain. http://www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risksin-the-supply-chain.pdf. Accessed 2015

Chen Y-K (2012) Challenges and opportunities of internet of things. In: 17th Asia and South Pacific design automation conference (ASP-DAC), Sydney, Australia, 30 Jan–2 Feb 2012, pp 383–388

Di J, Smith S (2007) A hardware threat modeling concept for trustable integrated circuits. In: IEEE region 5 technical conference, 20–22 April 2007, pp 65–68. doi:10.1109/TPSD.2007.4380353

Di-Battista J, Courrege J-C, Rouzeyre R, Torres L, Perdu Ph (2010) When failure analysis meets side-channel attacks, cryptographic hardware and embedded systems. In: CHES 2010, Series lecture notes in computer science, vol 6225, pp 188–202. doi:10.1007/978-3-642-15031-9_13

Dierks T, Rescorla E (2008) The transport layer security (TLS) protocol version 1.2. IETF RFC 5246, RTFM Inc

EU FP7 E-Crime (2016) The economic impacts of cyber crime, D2.2 Executive summary and brief: cyber crime inventory and networks in non-ICT sectors. http://ecrime-project.eu/wp-content/uploads/2015/02/E-CRIME-Deliverable-2.2.pdf. Accessed 10 Nov 2016

Guinard D, Trifa V (2016) Building the web of things: with examples in node.js and raspberry pi. Manning Publications, ISBN-13: 978-1617292682

He H, Watson T, Maple C, Tiwari A, Mehnen J, Jin Y, Gabrys B (2016) The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In: WCCI2016, Vancouver, Canada, 24–29 July 2016

Huxtable J, Schaefer D (2016) On servitization of the manufacturing industry in the UK. Proc CIRP 52:46–51

Kang HS, Lee JY, Choi S, Kim H, Park JH, Son JY, Kim BH, Noh SD (2016) Smart manufacturing: Past research, present findings, and future directions. Int J Precis Eng Manuf Green Technol 3(1):111–128. doi:10.1007/s40684-016-0015-5

Kim HH, Bruce N, Lee H-J, Choi Y, Choi D (2015) Side channel attacks on cryptographic module: EM and PA attacks accuracy analysis, information science and applications, pp 509–516. doi:10.1007/978-3-662-46578-3_60

jorn.mehnen@strath.ac.uk

Korolov M (2016) Dell report: attacks against industrial control systems double. http://www.techpageone.co.uk/technology-uk-en/dell-report-attacks-industrial-control-systems-double. Accessed 10 Nov 2016

Li W, Mehnen J (2013) Cloud manufacturing: distributed computing technologies for global and sustainable manufacturing. Springer, London, ISBN-10: 1447149343

Melnikov A, Zeilenga K (eds) (2006) Simple authentication and security layer (SASL). IETF RFC 4422, OpenLDAP Foundation

NN (2016) Smart manufacturing—IoT enables fourth industrial revolution. http://www.smarttechforyou.com/2015/03/smart-manufacturing-iot-fourth-industrial-revolution.html. Accessed 10 Nov 2016

Pääkkönen P, Pakkala D (2015) Reference architecture and classification of technologies, products and services for big data systems. 2(4):166–186. doi:10.1016/j.bdr.2015.01.001

Raddats C, Baines T, Burton J, Story VM, Zolkiewski J (2016) Motivations for servitization: the impact of product complexity. Int J Oper Prod Manage 36(5):572–591. doi:10.1108/IJOPM-09-2014-0447

Shahri AB, Ismail Z (2012) A tree model for identification of threats as the first stage of risk assessment in HIS. J Inf Secur 3:169–176. doi:10.4236/jis.2012.32020

Tapoglou N, Mehnen J, Vlachou A, Doukas M, Milas N, Mourtzis D (2015) Cloud-based platform for optimal machining parameter selection based on function blocks and real-time monitoring. J Manuf Sci Eng 137(4):040909, Paper no: MANU-14-1548. doi:10.1115/1.4029806

Tedeschi S, Mehnen J, Roy R (2017) IoT security hardware framework for remote maintenance of machine tools. In: Second international conference on internet of things, data and cloud computing (ICC'17), March 2017, Cambridge, Churchill College, UK (in print), pp 22–23

UK Government (2015) The controller of her majesty's stationery office. National Security Strategy and Strategic Defence and Security Review 2015, OGL, ISBN 9781474125956

VDI/VDE (2016) Reference architecture model industries 4.0 (RAMI4.0), Status report, 2015. http://www.zvei.org/. Accessed 28 Sept 2016

Wilson J (2013) Node.js the right way, practical, server-side javascript that scales, Pragmatic Bookshelf

Zhang GH, Poon CCY, Zhang YT (2011) A review on body area networks security for healthcare, ISRN Commun Netw 2011:8, Article ID 692592. doi:10.5402/2011/692592

jorn.mehnen@strath.ac.uk