Industrial Internet of Things: Security of Interoperability

Fergal MARTIN-TRICOT, Cédric EICHLER, Pascal BERTHOMÉ
LIFO - INSA Centre-Val de Loire
88 Boulevard Lahitolle
18000 BOURGES
E-Mail: firstname.lastname@insa-cvl.fr

***Abstract*—Industry uses more and more IoT components to have a better control on production and logitistic processes. Unfortunately, as in every deep transformation, there are a lot of pitfalls in which one must not fall. In particular, security risks induced by this growing network openess must be thoroughly investigated.**

Furthermore, the multiplicity of devices manufacturers poses major fragmentation problems. Since being limited to one manufacturer is not acceptable in an industrial world, interoperability is paramount. Security solutions must thus integrate the joint use of multiple protocols and systems.

Fortunately, a well supported standard is a promising solution for the interoperability problem: oneM2M. It offers a common data structuring allowing different protocols to interact.

We therefore propose to study the intersection between industry and IoT, and particularly the data security, especially at the interface between the interoperability standard and third-party protocols.

I. Industrial world

During the last years, the industry began to adopt Machine to Machine (*M2M*), a paradigm of communication which allows direct machine to machine exchanges [1]. This approach provides some tools to have a better real-time vision and control on procedures. However, it faces two main problems.

First of all, a lot of industrial systems are based on closed and proprietary control and management protocols. For example, production machines usually use manufacturer's communication and software solution. However, the industrial world is slowly beginning a big IT transformation by the use of more open communication and standards to limit this problem.

Secondly, the attack surface can be considerably enlarged with the introduction of M2M devices in the production system. Indeed, introduction of more remote accesses on a system can largly extend the attack surface.

Nevertheless, the willingness to automate and rationalize control on procedures is pushing for M2M adoption and its next step: the IoT.

II. Internet of Things

The Internet of Things (*IoT*) is, in a certain way, the continuity of the M2M approach. According to Gubbi and al. [2], IoT can be defined as an "Interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications". IoT is thus the continuity of the openness policy on standards, protocols and technologies followed by the industry for the last years.

Frequently, those networks are based on wireless technologies (*e.g.*, Bluetooth, ZigBee, LoRaWAN, SigFox) [3]. Such technologies propose secured communication protocol relying on energy-efficient and cost-less devices.

Unfortunately, IoT poses a new security problem with the creation of attack vectors on some critical systems. Indeed, if a device is connected with a radio communication protocol, an attacker has more potential entrance.

The main question here is: what are the risks? To answer, we must investigate security dangers and, in first, study the protocols.

III. IoT common protocols

The most interesting protocols for industrial concerns can be divided into two main categories: Wireless Local Area Network (with Mesh Wireless Network and classical wireless ones) and Low Power Wide Area Network (LPWAN). They all address different issues.

The first one is suitable to make a communication network at room or building scale. This is the perfect choice to have, for example, a sensor network to monitor a facility production. This category comprises classical technologies such as WiFi or Bluetooth but also Mesh networking that offers some interesting properties such as better range and energy efficiency [4]. The most used and developped Mesh IoT technologies are ZigBee [5], Thread [6] and Z-Wave [7].

On the other hand, LPWAN usually rely on a network widely deployed and proposed by a service provider. The main difference with 3G or 4G networks is that the protocol is more optimized to reduce power consumption. These protocols can thus work in a big area and allow a device to be connected anywhere [8]. In an industrial approach, it can be used in shipment and supply chain.

The complementarity of these two facets of the IoT with regard to industrial needs raises a known problem in computer science (but immature in IoT): the protocol interoperability. It is an issue which must be solved, but which can raises security issues. We must therefore investigate it in our study.

IV. Interoperability problems

As presented before, interoperability is crucial in industrial IoT. Indeed, a single protocol cannot, for now, answer all the needs of the industry. Moreover, getting locked into one manufacturer environment is never a wise choice. So it is necessary to find solutions to assure interoperability.

The best way to solve this problem in the long term is the mass adoption of a common standard. Few standards and initiatives (*e.g.*, INTER-IoT, Intel IoT Solutions Alliance) are currently dedicated to this issue. One of them stands out by its international support and maturity: oneM2M. Based on the work made with smartM2M (an ETSI workgroup), it gathers now a lot of national and international standard institutes (Japan, Korea, United States, UE, China and India at the beginning) but also six industrial fora.

V. oneM2M

The oneM2M standard facilitates management and interoperability in M2M and IoT networks. This solution was designed to be network-agnostic and thus to work with every existing solutions [9].

One of the main feature of oneM2M is a data model based on an arborescent architecture. A data is associated with its creator and is stored into containers which enable to store and expose heterogeneous data through a common ontology.

In oneM2M, a node is the heart of the interoperability: the *Interworking Proxy Entity (IPE)*. Its main purpose is to bind data and instructions between the oneM2M network and the specific protocol used by the non-oneM2M Device Node [10]. This is thus an interface between two worlds, and so a pillar for the data security. In fact, the *IPE* is part of the many oneM2M-specific nodes that constitute the oneM2M infrastructure.

Proprietary networks works normally, but will be connected to this central infrastructure. Its role is to transmit -and sometimes store- data and instructions between all existing protocols.

For example, if a device *A*, part of a ZigBee network, needs to have access to some data from a device *B*, part of a Thread network, it will communicate with oneM2M which will interact with the ZigBee network to retrieve these data, from *B*, and send them back to *A*.

All in all, oneM2M seems to answer interoperability problematic. However, as in every standard, there can be a gap between specification and implementations. Therefore, we made a small testing platform to highlight and study oneM2M operation.

VI. Implementation of an oneM2M architecture

First, our research approach was to investigate existing implementations of oneM2M and then create an experimental platform with the most relevant one.

A. Test scenario

The objective of our platform is to experiment the operating mode of oneM2M with a third party protocol: ZigBee. It will highlight the mechanisms used by oneM2M to interact with another protocol, and allows us to study the security of them.

The test scenario is as followed: a temperature sensor communicates its measurements to another node which has a display to show the value. Since the sensor and display are communicating with ZigBee, we need to have a specific node to be able to get those values into a oneM2M network.

B. Chosen solutions

In addition to proprietary oneM2M implementations, it exists today three main open source ones: IoT Ocean (KETI), OM2M (Oracle) and OpenMTC (Fraunhofer). We choose the most actively developped open-source solution: IoT Ocean. This solution is also interesting thanks to its software modularity: every logical actor into oneM2M is implemented as a specific software component.

On the hardware side, we use two Arduino programming boards for the temperature sensor and display. They are communicating with each other with ZigBee using an XBee radio module. The oneM2M part is provided by two RaspBerry Pi 3 board. One of them uses also an XBee radio module to communicate with the ZigBee network.

C. Implementation

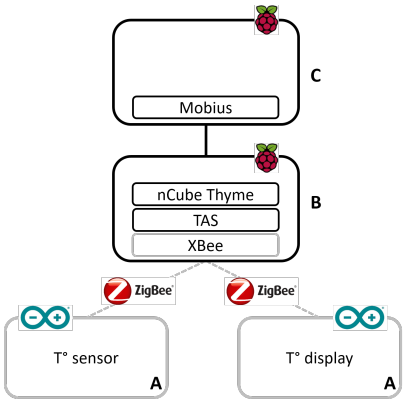

Figure 1. Architecture implemented

As depicted in Figure 1, the two Arduino boards (**A**) are communicating with one of the Raspberry Pi (**B**) using ZigBee. The oneM2M part is composed of two Raspberry Pi boards (**B** and **C**).

The first one, **C** uses Mobius, the IoT Ocean's implementation of an Infrastructure Node: a central node in which some data are stored.

The second one, **B** is connected at the same time to the oneM2M and ZigBee network. The oneM2M part is provided by nCube, an IoT Ocean's application which implements an Application Node. In IoT Ocean, the *IPE* is implemented with the *TAS*: a software component wich translates communication between oneM2M and a custom protocol (here, ZigBee). This part is totally homemade because of its specificity to a proprietary protocol.

Each *IPE* implementation relates to a specific protocol. Integrating a new one in an architecture thus requires solely to implement an appropriate *IPE*.

D. Conclusion

The establishment of this platform allowed us to study the power and limits of oneM2M's most mature open-source implementation, IoT Ocean. It is an in-developement solution which proposes the basic functionalities of oneM2M.

It appears that the *IPE* (TAS in IoT Ocean) is, as previously intuited, a major point of interest into data security. It must be a part of a trusted component because it transmits and translates all data through oneM2M.

VII. Security concerns

In data security within industrial IoT, there are a lot of security problematics which are related to two main domains: IoT or interoperability.

A. Inherent to IoT

Obviously, protocols themselves must be secured. However, the security in the most popular ones has already been widely studied.

For example, the last Zigbee's version (3.0) security has been analyzed by Zillner [11], Fan et al. [12] or more recently by Celebucki, Lin, & Graham [3]. They all agree that ZigBee proposes robust security features and that common security issues stem from improper implementations.

Z-Wave, a general public IoT protocol for home automation, has also been attacked by Rouch et al. [13] who shown an attack relying on some device-specific features and not directly linked to the protocol security.

More generally, a global security threat analysis on IoT Security has been done by Tuna et al. [14] in 2017. They highlight a lot of security issues M2M and IoT manufacturer have to take into account.

Moreover, a security analysis has been done on the LoRaWAN protocol by Miller [15]. He presented the security mechanisms that are included into the protocol and concluded that security provided by LoRaWAN is correct and sufficient but that IoT application developpers must be very careful about data security when implementing applications.

In conclusion, the IoT protocols' security is a very important challenge. However, it is a well treated research subject and it emerges that the majority of security issues are, on matures protocols, caused by improper implementations.

B. Inherent to Interoperability

Another aspect is the data security within a oneM2M network. As stated before, oneM2M should allow secure data storage and transmission through heterogeneous networks. Even ignoring technical issues, one major conceptual problem is not yet solved: how is it possible to secure a data from end-to-end in an heterogeneous deployment?

The first obvious step is to investigate the security mechanisms in oneM2M. Unfortunatly, such a study would remain theoretical as no open source implementaton implements all of these envisionned mechanisms. Indeed, open-source security implementation remains a work in progress [16]. Furthermore these mechanisms are merely internal; they do not cover end to end data security when several protocols co-exist.

The second one is to study the security of the communication interface between oneM2M and a third-party protocol (the *IPE*) which is a critical yet mildly studied research point. Indeed, data authenticity, integrity and confidentiality are generally ensured by the IoT protocol from the device up to the border of the network.

VIII. Conclusion

There are some strong security functionalities into oneM2M (up to the *IPE*) and into the classicals IoT protocols (up to the edge) that ensure a proper data security.

Indeed, for now, when a data is shared by a device using a third-party protocol, it is authenticated and protected by the protocol until it is transmited to the *IPE*. It is thus, for the time being, necessary to have a blind trust into the *IPE*.

To ensure end-to-end security into heterogeneous deployments, it is essential to solve this problematic, relatively ignored until now.

References

[1] J. Latvakoski, A. Iivari, P. Vitic, B. Jubeh, M. B. Alaya, T. Monteil, Y. Lopez, G. Talavera, J. Gonzalez, N. Granqvist, M. Kellil, H. Ganem, and T. Väisänen, "A survey on M2M service networks," *Computers*, vol. 3, no. 4, pp. 130–173, 2014.

[2] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[3] D. Celebucki, M. A. Lin, and S. Graham, "A security evaluation of popular internet of things protocols for manufacturers," in *Consumer Electronics (ICCE), 2018 IEEE International Conference on*. IEEE, 2018, pp. 1–6.

[4] C. Gomez and J. Paradells, "Wireless home automation networks: A survey of architectures and technologies," *IEEE Communications Magazine*, vol. 48, no. 6, 2010.

[5] ZigBee, "ZigBee: Securing the IoT," ZigBee Alliance, Tech. Rep., 2017.

[6] Thread, "Thread technical overview," Thread, Tech. Rep., Oct. 2015.

[7] ABR, "Introduction to the Z-Wave security ecosystem," Sigma Design, Tech. Rep., 2016.

[8] K. E. Nolan, W. Guibene, and M. Y. Kelly, "An evaluation of low power wide area network technologies for the internet of things," in *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, sep 2016.

[9] OneM2M, "The interoperability enabler for the entire M2M and IoT ecosystem," oneM2M, Tech. Rep., 2015.

[10] J. Yun, R. C. Teja, N. Chen, N.-M. Sung, and J. Kim, "Interworking of oneM2M-based IoT systems and legacy systems for consumer products," in *2016 International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, oct 2016.

[11] T. Zillner, *ZigBee Exploited - The Good, The Bad and The Ugly*, Cagnosec, August 2015.

[12] X. Fan, F. Susan, W. Long, and S. Li, "Security analysis of Zigbee," 2017.

[13] L. Rouch, J. François, F. Beck, and A. Lahmadi, "A Universal Controller to Take Over a Z-Wave Network," in *Black Hat Europe 2017*, London, United Kingdom, Dec. 2017, pp. 1–9.

[14] G. Tuna, D. G. Kogias, V. C. Gungor, C. Gezer, E. Taşkın, and E. Ayday, "A survey on information security threats and solutions for machine to machine (M2M) communications," *Journal of Parallel and Distributed Computing*, vol. 109, pp. 142–154, nov 2017.

[15] R. Miller, "LoRa security: Building a secure LoRa solution," *MWR Labs Whitepaper*, 2016.

[16] S. Sicari, A. Rizzardi, A. Coen-Porisini, L. A. Grieco, and T. Monteil, "Secure OM2M service platform," in *Autonomic Computing (ICAC), 2015 IEEE International Conference on*. IEEE, 2015, pp. 313–318.