Proceedings of APMS 2017: IFIP International Conference on Advances in Production Management Systems: The Path to Intelligent, Collaborative, and Sustainable Manufacturing, 3-7 September 2017, Hamburg, Germany, pp. 391-398
DOI:10.1007/978-3-319-66923-6_46

New threats for old manufacturing problems: secure IoT-enabled monitoring of legacy production machinery

Stefano Tedeschi[1], Christos Emmanouilidis[1], Michael Farnsworth[1], Jörn Mehnen[2], and Rajkumar Roy[1]

[1]Manufacturing Department, Cranfield University, Cranfield, United Kingdom;
{s.tedeschi, christosem, m.j.farnsworth, r.roy}@cranfield.ac.uk
[2]Design, Manufacture and Engineering Management Department, University of Strathclyde, Glasgow, United Kingdom;
jorn.mehnen@strath.ac.uk

Abstract. The digitization of manufacturing through the introduction of Industrie 4.0 technologies creates additional business opportunities and technical challenges. The integration of such technologies on legacy production machinery can upgrade them to become part of the digital and smart manufacturing environment. A typical example is that of industrial monitoring and maintenance, which can benefit from internet of things (IoT) solutions. This paper presents the development of an-IoT-enabled monitoring solution for machine tools as part of a remote maintenance approach. While the technical challenges pertaining to the development and integration of such solutions in a manufacturing environment have been the subject of relevant research in the literature, the corresponding new security challenges arising from the introduction of such technologies have not received equal attention. Failure to adequately handle such issues is a key barrier to the adoption of such solutions by industry. This paper aims to assess and classify the security aspects of integrating IoT technology with monitoring systems in manufacturing environments and propose a systematic view of relevant vulnerabilities and threats by taking an IoT architecture point of view. Our analysis has led to proposing a novel modular approach for secure IoT-enabled monitoring for legacy production machinery. The introduced approach is implemented on a case study of machine tool monitoring, highlighting key findings and issues for further research.

Keywords: Production machinery monitoring, internet of things; security

1. Introduction

Machine tools are among the key production equipment in manufacturing environments. Monitoring machinery health status enables preventive, predictive and proactive actions to be taken, leading to reducing downtime and breakdowns. When integrated with the overall production management considerations, including costs and planning considerations, this in turn can lead to improved production perfor-

adfa, p. 1, 2011.

mance through higher overall equipment efficiency (OEE), while offering additional support towards meeting production and costs/profits targets are met. In this context, the introduction of internet of things (IoT) technologies constitute a prime enabler for the integration of legacy production machinery to the digital factory era, enabling ubiquitous availability of machinery status and performance information through different networking technologies.

IoT technology, among other, enables a growing number of sensors, devices, assets and other human and non-human actors to communicate over wired and wireless networks, creating opportunities for new applications and services to be offered over the cloud. A typical manufacturing environment with legacy machine tools often lacks built-in sensors, external communication capabilities and applications or services for for real-time monitoring. Computer numeric control (CNC) machines are also often present, which do have communication capabilities (Ethernet) and an Application Programming Interface (API) for exchanging data through third-party applications [1]. The lack of provisions to easily monitor machine capabilities within the entire factory gives rise to a higher cost of integration through additional hardware and software in order to capture data autonomously and achieve some level of information integration in production environments. The use of IoT technologies can empower legacy machine tools to become smart and connected. In this setting, machines, sensors, devices, computing entities, human operators and the cloud become contributing constituents to a digital and smart manufacturing environment.

However, the introduction of such technologies also brings in additional challenges and in particular raises security concerns. Such concerns are yet to be sufficiently addressed in industry practice, especially concerning efforts to upgrade legacy equipment to the Industrie 4.0 era. Contributing in the direction of addressing such challenges, this paper analyses security risks associated with introducing IoT devices in production environments. We propose a monitoring architecture through a novel modular IoT unit for legacy machine tools, equipped with the introduction of a novel multi-stage and adaptive authentication protocol at the hardware level. The security advantages arising from its use, compared to standard practices, are outlined. The paper is organized as follows. Section 2 gives an overview of relevant literature. Section 3 presents the approach used for the design and development of the modular IoT unit, paying attention to security issues. Section 4 describes a number of case studies with a DMG Mori Seiki machine tool, and the pilot architecture to address security weaknesses. Section 5 states our conclusions and provides pointers to future work.

2. IoT Security challenges in manufacturing environments

Networks of smart objects are employed in safety and security applications and are projected to scale up to involve millions of embedded devices in both commercial and industrial sectors [2, 3]. Solutions based on IoT technology can significantly upgrade the data-generation and integration capabilities of production systems, further pushing for the integration of cloud computing and big data into manufacturing environments. While process and safety-critical data can thus become integrated, the underlying

potential security and privacy vulnerabilities of such a process, if not appropriately handled, make the connected factory more susceptible to attacks [4, 5, 6]. This is particularly important as many studies have revealed security weaknesses in embedded devices [7, 8, 9]. Such threats have profound commercial, legal, safety and social implications. A smart manufacturing system may comprise several cyber physical production systems (CPPs), which involve monitoring hardware and software components as integrated circuits [10]. Based on the software interactions with humans and CPPs and the involved different communication protocols, such hardware is exposed to physical attacks, including invasive hardware attacks, side-channel attacks and reverse engineering attacks [11]. Software can be compromised by malicious code, such as Trojans, viruses and runtime attacks [12], while different denial-of-service (DoS) communication protocols can be subjected to various attacks, such as denial-of-service attacks [13, 14].

Currently, security limitations of IoT devices generate new challenges for the design and implementation of embedded solutions. Typical security issues for embedded systems involve compromising the boot process as in the Google Nest Thermostat [15], hardware exploitation which involves implementing parts of software / firmware [16], chip exploitation with invasive intrusion to take secret information stored in the chip [17], cryptographic vulnerability in applications [18], backdoors in remote access channels able to find out credentials for administrator access [19] and traditional software vulnerabilities. These devices are intended to be part of an industrial IoT architecture which may become under-attack too. For example, in [20], a successful attack against an industrial control system through a computer virus that infected the transportation network leading to a complete stop of passenger and freight train function is presented. Other industrial attacks are also described in the literature [21, 22] and one of the most famous is the Stuxnet attack [23] which caused the failure of centrifuges within Iranian nuclear facilities. It is therefore necessary to develop strategies, architectures and solutions which address such challenges. Relevant work includes common standard protocols used in SCADA systems, emphasizing security threats and vulnerabilities [24], with standard communication protocols considered at three different layers: the Physical/Link layer, the Network/Transport Layer and the Application Layer [25]. This paper analyses relevant requirements and presents the design and development of a new security architecture for IoT-enabled data exchanges in an industrial setting. This is introduced in the next section.

3. A modular approach for IoT security in manufacturing

The multiple vulnerabilities associated with the introduction of IoT technology in manufacturing and especially on legacy production machinery, require a re-thinking of the design approach to security. Instead of adding complexity at single security control mechanisms, such as in encryption or authentication for accessing a networked device, one approach would be to de-compose the whole device into multiple components, each contributing additional security barriers. Furthermore, the very nature of such security barriers may be adaptive, adding further complexity needs to

any mechanism design to attack an IoT-enabled solution. Our innovative modular approach to IoT security in manufacturing environments employs such concepts to increase the overall complexity needed for an attack to succeed, while remaining simple to implement. To illustrate this, we present a new modular design for an IoT data acquisition (DAQ) unit, aimed at machine tools monitoring

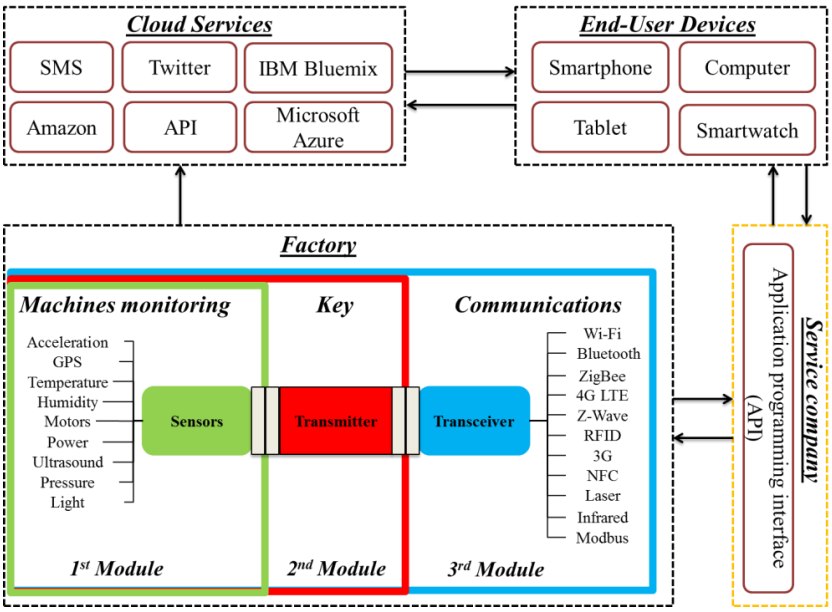

Fig. 1. The modular IoT DAQ

Fig. 1 illustrates the modular IoT DAQ proposed for communicating at the Machine-to-Machine (M2M) level, as well as with others IoT layers. The design decomposes the overall device to independent modules for sensing and communicating, indicated as 1st module and 3rd module. An intermediate unit, marked as 2nd module, is the key to mediate between collecting and processing data from several sensors and sending them outside the factory. The device size is small so to allow comfortably fitting into a machine tool. Such IoT modules can use different communication protocols to share information inside and outside the factory. The sensed data can be sent to the cloud, managed by different services, and shared with the end-user devices or sent to a service providing vendor, tasked with monitoring in real time the status of the machines. One of the advantages of this architecture is the flexibility in terms of easy replacement or re-use of individual components. The modularization yields low power needs in terms of device capability, making it also possible to isolate sensing by accommodating a single sensor instead of several sensors per module. Furthermore, the modular IoT DAQ can work as a modem able to convert one communication protocol into another. These features allow building a robust IoT device, which can work areas with high electronic noise, such as around the machine spindle and drives. At the same time, they maintain the flexibility of multi-connectivity, being

able to support different wireless protocols, each with own security provisions. The proposed modular IoT DAQ employs a hardware and software authorization protocol of cascaded complexity, allowing access to the module data for authorized users [25].

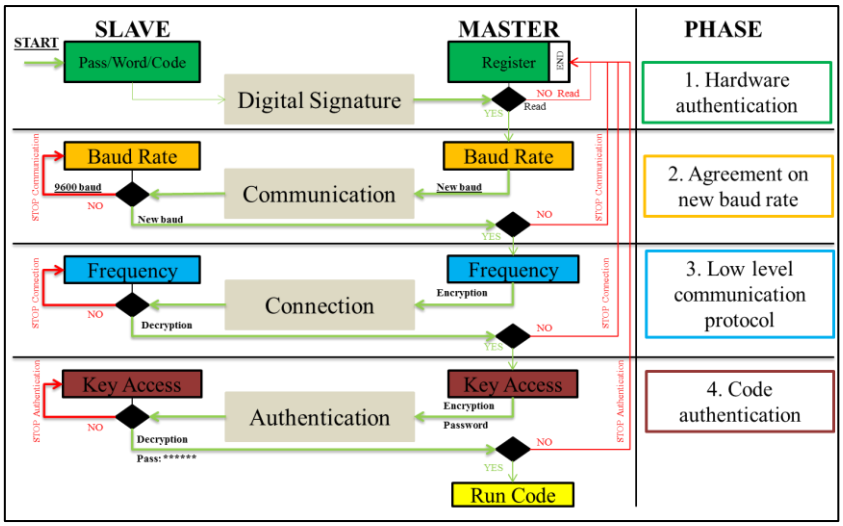

Fig. 2. Secure authentication protocol

The proposed authentication protocol is illustrated in Fig. 2. The slave unit represents sensing and communication entities (1st and 3rd modules) while the master is the key (2nd module). The protocol comprises four phases for enabling the sensor operation and accessing its data. The initial phase involves the physical authentication between the sensors, transceiver technologies, and the key. Each sensor and communication module is equipped with an ID number, to be recognized only by the key module. The next phase is an agreement about the baud rate to share signals, information and password. The master offers a new baud rate and the slave will accept after evaluating requirements, such as frequency and time. The third phase consists of sending the hardware password by the master to the slave. This hardware password is a specific frequency agreed beforehand between the two parts. The last phase consists of recognizing the alphanumeric password sent by the slave and executes the code to collect sensor data. All phases are supported with AES cryptography. Adopting a modular IoT approach, instead of employing monolithic IoT devices, offers the possibility to personalize the choice of the device setup, to replace single modules without compromising the entire device and to cascade the complexity of security provisions.

4. Case study and pilot implementation

We present an instantiation of the proposed architecture on a problem of considerable interest for industry, that of introducing legacy machine tools with IoT-enabled monitoring capabilities. Most legacy machine tools do not have built-in sensors and

do not have any local or external network communication. Interconnecting such machinery introduces security threats related not only to the machine tools but to everything around them and everything that interfaces with them.

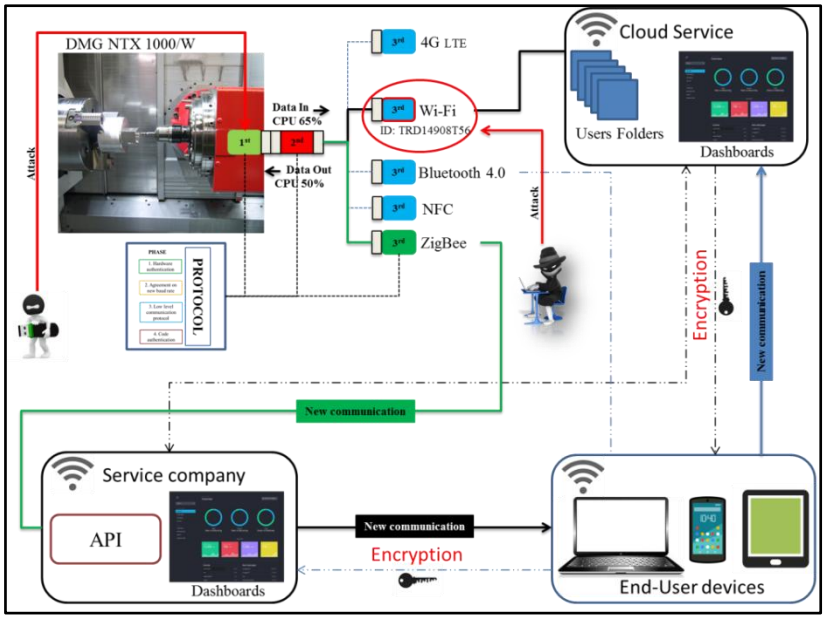

Fig. 3. The modular IoT implementation for legacy machine tools

Fig. 3, shows the implementation of the modular IoT DAQ with a legacy machine tool (DMG NTX 1000/W). A real industrial case was built around the machine to simulate and study possible weaknesses in implementing the IoT technology. The top left shows the spindle during normal operation, equipped with the sensor module (1st module), which is inactive until the connection with the key module (2nd module) is established. The key module executes code for sensing, processing and communicating, as well as the code to read the CPU usage for each authentication protocol phase. The communication module (3rd module) consists of different ways to share data into the local or external network. Typically, this configuration would be susceptible to the types of attacks discussed in section 2. Fig. 3 illustrates a case where RF component employs the Wi-Fi module (3rd module), which comes under attack, changing CPU from from 50% to 65%. The modular IoT will change the communication protocol into ZigBee protocol and will send data to the service company and the cloud or end-user devices, while the Wi-Fi operation shuts. All information shared within this IoT architecture is encrypted and only the key module is equipped with an SD card to store the data for limited time before transferring outside. In case of transferring malicious code to the IoT module, attempting to compromise the data, the authentication protocol prevents unauthorised users from accessing device files and codes. This case illustrates initial implantation steps of the modular secure IoT archi-

tecture for manufacturing environments, with minimal hardware costs, but significant data handling and CPU capacity.

5. Conclusion

This paper deals with integrating IoT technology with security provisions on legacy production machinery monitoring. The proposed approach adopts a modular architecture instantiated on an IoT DAQ, which employs a hybrid authentication protocol addressed both at the hardware as well as communication levels. The architecture was implemented on a DMG Mori Seiki machine tool as an example of the applicability to a wide ranging legacy systems, aimed at bringing them towards the Industrie 4.0 era. The next steps include extensive testing of the proposed solution, extension to handle additional security threats, as well as the migration of the components of the modular architecture into an industry-grade device, while also extending its' operation as a remote control system for different actuators. This architecture can be employed within a broader architecture for the predictive maintenance of legacy machine tools.

Acknowledgements

This work is being undertaken with the EPSRC, grant number EP/I033246/1 and in collaboration with the group Kennametal and has been conducted in the Through-life Engineering Services Centre at Cranfield. Many thanks to the DMG Mori which made the CNC turn-mill Centre NTX 1000/W available for this research.

References

1. Deshpande, A., Pieper, R.: Legacy machine monitoring using power signal analysis. Proceedings of the ASME 2011 International Manufacturing Science and Engineering Conference (MSEC), Corvallis, Oregon, USA, 13-17 June 2011.
2. Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I.: Survey internet of things: Vision, applications and research challanges. Ad Hoc Netw. **10**(7), 2012.
3. Vermesan, O., Friess, P.: Internet of Things - From Research and Innovation to Market Deployment. River Publishers, 2014.
4. Eric Byres, P., Lowe J. The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. In: VDE congress, VDE Association for Electrical, Electronic & Information Technologies, Berlin; October 2004.
5. Chae H., Shahzad A., Irfan M., et al.: Industrial control system vulnerability and security issues and future enhancements. Adv Sci Techno Lett [Internet]; **95**; pp: 144-148. Available from: Http://onlinepresent.org/proceedings/vol95_2015/27.pdf
6. Uchenna P., Daniel Ani, Hongmei (Mary) He & Ashutosh Tiwari.: Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. Journal of Cyber Security Technology. **1**(1), 2017.

7. Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T.: Comprehensive experimental analyses of automotive attack surfaces. In USENIX Conference on Security. USENIX Association, 2011
8. Costin, A., Zaddach, J., Francillon, A., Balzarotti, D.: A large-scale analysis of the security of embedded firmwares. In USENIX Conference on Security Symposium. USENIX Association, 2014.
9. Cui, A., Stolfo, S.J.: 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.
10. Shahrjerdi, D., Rajendran, J., Garg, S., Koushanfar, K., Karri, R.: Shielding and securing integrated circuits with sensors. In Computer-Aided Design (ICCAD), International Conference on. IEEE, 2014.
11. Rostami, M., Koushanfar, F., Karri, R.: A primer on hardware security: Models, methods, and metrics. Proceedings of the IEEE, 2014.
12. Szekeres, L., Payer, M., Wei, T., Song, D.: Eternal war in memory. In 2013 IEEE Symposium on Security and Privacy (SP), 2013.
13. The Guardian. Available online: https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service (access on 21 October 2016).
14. Koushanfar, F., Sadeghi, A.R., Seudie, H.: Eda for secure and dependable cybercars: Challenges and opportunities. In Proceedings of the 49th Annual Design Automation Conference (ACM), 2012.
15. Hernandez, G., Arias, O., Buentello, D., Jin, Y.: Smart nest thermostat: A smart spy in your home. In Black Hat USA, 2014.
16. Wurm, J., Arias, O., Hoang, K., Sadeghi, A.R, Jin, Y.: Security analysis on consumer and industrial iot devices. In 21st Asia and South Pacific Design Automation Conference (ASP-DAC), 2016.
17. Skorobogatov, S.: Fault attacks on secure chips: from glitch to flash. In Design and Security of Cryptographic Algorithms and Devices (ECRYPT II), 2011.
18. Lemos, R.: Sony left passwords, code-signing keys virtually unprotected. eWeek, 2014. [Online]. http://www.eweek.com/security/sony-left-passwords-codesigning-keys-virtually-unprotected.html.
19. Ray, S., Bhadra, J. Security challenges in mobile and IoT systems. 29th IEEE International System on Chip Conference, SOCC 2016; Seattle; United States; 6 September 2016; pp: 256-361.
20. Newswire, P.R.: Computer virus strikes CSX transportation computers, 2003.
21. Kabay, M.: Attacks on power systems: Hackers, malware, 2010.
22. Miller, M., Rowe, D.: A survey SCADA of and critical infrastructure incidents. RIIT '12 Proceedings of the 1st Annual conference on Research in information technology, Calgary, Alberta, Canada, October 11-13, 2012.
23. Vijayan, J.: Stuxnet renews power grid security concerns, 2010.
24. Igure, V.M., Laughter, S.A., Williams, R.D.: Security issues in SCADA networks. Computer & Security, **25**(7), pp. 498-506, 2006.
25. Tedeschi, S., Mehnen, J., Roy, R.: IoT Security Hardware Framework for Remote Maintenance of Machine Tools, Second International Conference on Internet of Things, Data and Cloud Computing (ICC'17), Cambridge, Churchill College, UK, 22-23 March 2017. (in press)

New threats for old manufacturing problems: Secure IoT-enabled monitoring of legacy production machinery

Tedeschi, Stefano

2017-08-31

Tedeschi S, Emmanouilidis C, Farnsworth M, et al., (2017) New threats for old manufacturing problems: Secure IoT-Enabled monitoring of legacy production machinery, Proceedings of APMS 2017: IFIP International Conference on Advances in Production Management Systems: The Path to Intelligent, Collaborative, and Sustainable Manufacturing, 3-7 September 2017, Hamburg, Germany, pp. 391-398

http://dx.doi.org/10.1007/978-3-319-66923-6_46