PhD topic

Detection of cyberattacks in railway's remote monitoring systems

Host laboratory: Ampere Laboratory

Thesis director: Dr. Eric Zamaï

Co-advisors: **Dr. Cédric Escudero (contact)**, Dr. Quoc Bao Duong

Funding: Project RailMon PSPC (acquired)

Duration: 3 years

Type of contract: Full time

Doctoral School: EEA (Electronics, Electrical Engineering, Automatics and Signal Processing)

Keywords: cybersecurity, hardware design, embedded system, behavioral model, cyber-physical system, data analysis

1. Context

Since the beginning of the century, Industrial Control Systems (ICSs) have received a lot of attention in academics and industry. The integration of information and communication technology in the control of physical systems is commonly admitted as a requirement to improve the performance of industrial plants [1]. Therefore, controllers, sensors and actuators are nowadays embedded in computer-based systems, and legacy communication systems have been progressively replaced by network-based systems (e.g. ASI, Profibus, Modbus TCP/IP, Profinet) [2][3]. Nevertheless, this integration increases the attack surface of control systems. Therefore, ICSs are now exposed to cyberattacks leveraging the use of information and communication technology to alter the behavior of the control system [4][5][6][7][8][9]. Well-known cyberattacks examples are the Stuxnet malware on a uranium enrichment plant in 2010, the Crash Override malware on the Ukrainian power grid in 2015, the Triton malware on a petrochemical facility in 2018, or recently on water treatment systems in Israel and in USA. In particular, many cyberattacks against railway infrastructure have been demonstrated [9] and methods have been proposed recently in the literature [10][11][12].

Our industrial partner, a rail technology company, is in charge of the design and the deployment of the remote monitoring system for a national railway infrastructure. The remote monitoring is a critical part of such infrastructure as it allows operators to monitor the health of infrastructures in order to plan a maintenance if required. To this end, the remote monitoring system consists of two main parts:

- Local Measuring Stations (LMSs) compute safety information about each local railway infrastructure. More than 5 000 local measuring stations are disseminated throughout the railway infrastructure. Each of them acquires, collects and processes sensor measurements (app. 100 sensors);
- A centralized SIEM (Security Information and Event Management) collects the safety information from each LMS to supervise the health of the whole railway infrastructure.

2. Problematic

The remote LMS must be reconfigurable to be adapted to each local hardware to monitor. Integrators will configure each LMS based on the specificities of each local infrastructure (e.g. type of sensor measurements). Once installed, operators might reconfigure it for different reasons including failure of sensors or replacement of sensors. Although the reconfiguration is a requirement, it also increases the attack surface of the LMS. In fact, if an operator can reconfigure remotely the acquisition, the collection and the computation; then an attacker can do it also. Corruption of one LMS might allow an attacker to corrupt the computed safety information, for instance to mislead the health state of the local infrastructure. Furthermore, any corruption of one VOG will have a side-impact on the health state computed from the SIEM. Therefore, the attacks consider in this research work are the ones that aim to mislead the SIEM and the LMS about the health state of a local infrastructure (i) to trigger maintenance operations, or (ii) to hide an incoming failure of the equipment.

To deal with this security issue, the PhD final goal is the design of a non-configurable system that will analyze the remote LMS to detect anomalies in the collection and the computation of safety information based on trustable sensor measurements. Because the system will not be reconfigurable, it must be adaptable to automatically fit with the specificities of each local infrastructure.

Two main research approaches have been identified:

- On the first one, the research work will focus on hardware characteristics of the LMS's electronic card in charge of the acquisition and the collection of the sensor measurements (e.g. sampling time, sensor measurements amplitude);

- On the second one, it will focus on the safety of information computed by the LMS to detect anomalies. Based on information monitored from the LMS and the collected sensor measurements of the new LMS. Studying Algorithms and building programs in this class are impossible to configure remotely.

The following scientific problems have been pinpointed:

- How to model the normal behavior of the functioning of an electronic card?

- How to design an adaptable system be able to be self-configurable (e.g. for artificial intelligence-based methods, how to design a learning method with a short-period of learning? Or how to build a specific dataset to guaranty a safe learning stage.)

- How to analyze the computed variables in the LMS to detect anomalies based on the sensor measurements?

Beyond the scientific problems, the PhD candidate is expected to implement the proposed algorithms on an experimental electronic card (e.g. FPGA). It will include the following functionalities:

- acquiring the sensor measurements from the non-intrusive module (IOWINKS designed by WINKS-TECH company)
- collecting variables from the LMS
- detecting anomalies in the safety information computed by the LMS based on the trustable sensor measurements
- detecting anomalies in the functioning of the LMS card (hardware anomalies)

3. Organization

The PhD candidate will be in interaction with (i) WINKS-TECH, the company in charge of the design and the implementation of a secured acquisition system for the sensor measurements, i.e. the trustable sensor measurements; and (ii) SIEMA COGIFER, to access into the LMS. In addition, the PhD candidate will interact with the other candidates working on the cybersecurity subject located to the SIEM level.

4. Presentation of the host laboratory

Ampere Laboratory is a multidisciplinary laboratory split into three departments: Electrical Energy department, Automatic for System Engineering department, and Bioengineering department.

The department of Automatic for System Engineering is involved into a research axis focused on the diagnosis and the safety of industrial control systems. Historically, this research axis is interested on the abnormal functioning of systems. However, because of the massive integration of communication technologies into industrial control systems, the attack surface is increasing. Cyberattackers now benefit from such technologies to take control over the systems for degrading the performance of the system. Cybersecurity is now integrated in this research axis as the concern of industrials is growing each years.

5. Thesis funding

This thesis will be funded by the acquired project RailMon PSPC. The PhD candidate will be registered as the University of Lyon and at the EEA Doctoral School (Electronics, Electrical Engineering, Automatics and Signal Processing).

6. Candidate profile

The candidate will have to demonstrate a strong motivation for scientific research and good level of English language skills. He or she will have to demonstrate a great rigor in work, method, autonomy, and ease in experimenting, analyzing and presenting data. He or she will have to hold a Master 2 or

Engineering degree or equivalent degree and to know main notions of automation, control, industrial computing, and embedded systems.

The candidate is expected to have skills in the following fields: signal analysis, data analysis, real-time system design, automation and control system design, computer programming, electronic card design, microcontroller programming.

7. PhD roadmap

1st year: (a) State-of-the-art of (i) cybersecurity approaches with a focus on approaches detecting anomalies based on sensor measurements, (ii) adaptable methods including artificial intelligence-based methods, (b) understanding the functioning of the LMS's electronic card and identifying the expected functions of the security system to develop, (c) Identify the research group working on this area and develop the research problems.

Scientific dissemination: 1 conference paper on the scientific positioning

2nd year: (c) Explore and implement methods for detecting anomalies in the LMS.

Scientific dissemination: 1 conference paper on the existing methods (benefits, drawbacks, …), 1 conference paper on the proposed method

3rd year: (d) Develop the approach based on the explored methods, (e) implement the approach in an experimental electronic card, (f) write the thesis manuscript.

Scientific dissemination: 1 conference paper on the proposed approach, 1 journal paper on the proposed approach, the thesis manuscript

8. List of documents to be provided

The interested candidate can send an email to the contact Cédric Escudero (cedric.escudero@insa-lyon.fr) to have more information. Also, the following documents need to be provided:

- Curriculum Vitae
- A letter of motivation
- Academic transcript and ranking of Master 1 and 2 (or equivalent)
- 1 or 2 recommendation letters

Bibliography

[1] Lee, E. A: Cyber physical systems: design challenges, 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), pp. 363-369, IEEE, Piscataway, NJ (2008)

[2] McLaughlin, S., et al., "The cybersecurity landscape in industrial control systems", Proc. IEEE 104 (5), 1039-1057 (2016)

[3] C. Escudero, F. Sicard and E. Zamai, "Process-Aware Model based IDSs for Industrial Control Systems Cybersecurity: Approaches, Limits and Further Research," *2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA)*, 2018, pp. 605-612, doi: 10.1109/ETFA.2018.8502585.

[4] Hamed Farsi, Ali Fanian, Zahra Taghiyarrenani, A novel online state-based anomaly detection system for process control networks, International Journal of Critical Infrastructure Protection, Volume 27, 2019, 100323, ISSN 1874-5482, https://doi.org/10.1016/j.ijcip.2019.100323.

[5] H. Fawzi, P. Tabuada and S. Diggavi, "Secure Estimation and Control for Cyber-Physical Systems Under Adversarial Attacks," in IEEE Transactions on Automatic Control, vol. 59, no. 6, pp. 1454-1467, June 2014, doi: 10.1109/TAC.2014.2303233.

[6] Flammini F., Mazzocca N., Pappalardo A., Pragliola C., Vittorini V. (2011) Augmenting Surveillance System Capabilities by Exploiting Event Correlation and Distributed Attack Detection. In: Tjoa A.M., Quirchmayr G., You I., Xu L. (eds) Availability, Reliability and Security for Business, Enterprise and Health Information Systems. CD-ARES 2011. Lecture Notes in Computer Science, vol 6908. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-23300-5_15

[7] C. Escudero, P. Massioni, E. Zamaï, B. Raison. Analysis, prevention, and feasibility assessment of stealthy ageing attacks on dynamical systems. *IET Control Theory and Applications*, Institution of Engineering and Technology, 2021. ⟨hal-03278990⟩

[8] E. M. Merouane, C. Escudero, F. Sicard and E. Zamai, "Aging Attacks against Electro-Mechanical Actuators from Control Signal Manipulation," *2020 IEEE International Conference on Industrial Technology (ICIT)*, 2020, pp. 133-138, doi: 10.1109/ICIT45562.2020.9067147.

[9] Kour, R., Aljumaili, M., Karim, R., & Tretten, P. (2019). eMaintenance in railways: Issues and challenges in cybersecurity. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 233(10), 1012-1022.(Published)

[10] Ravdeep Kour, Adithya Thaduri and Ramin Karim, 2019. Railway Defender Kill Chain to Predict and Detect Cyber-Attacks, Journal of Cyber Security and Mobility, Vol. 91, 47–90. doi: 10.13052/jcsm2245-1439.912

[11] S. Lakshminarayana, Z. Teo, R. Tan, D. K. Y. Yau and P. Arboleya, "On False Data Injection Attacks Against Railway Traction Power Systems," 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Toulouse, France, 2016, pp. 383-394, doi: 10.1109/DSN.2016.42.

[12] Subhash Lakshminarayana, Teo Zhan Teng, Rui Tan, and David K. Y. Yau. 2018. Modeling and Detecting False Data Injection Attacks against Railway Traction Power Systems. ACM Trans. Cyber-Phys. Syst. 2, 4, Article 28 (September 2018), 29 pages. DOI:https://doi.org/10.1145/3226030