Detecting and Mitigating Cyberattacks against Microservice-Based Controllers for the Digital Factory (Extended Abstract)

Gabriele Gualandi, Emiliano Casalicchio,
Emanuele Gabrielli, and Luigi Vincenzo Mancini

Department of Computer Science, Sapienza Università di Roma, ITALY
lv.mancini@di.uniroma1.it

Keywords: Cybersecurity · Digital Industry · Cyber-phyisical systems

Evolution of the industry comes with the need of redefining the organization and management of the entire value chain along the lifecycle of products. The main goal is to improve flexibility in the production, for increasing the quality of the final products while using fewer resources. The improvements expected in the industry are supported by the recent advances in wireless sensor networks, artificial intelligence, big data and cloud computing. Such advances allow Cyber-Physical Systems (CPSs) to reduce the distance between digital computing and the physical world. By letting a digital system to perceive the environment and to actuate decisions (i.e. to "control"), the concept of feedback can be ported at many different levels of a value chain.

As an industry is a complex and heterogeneous eco-system, one of the main challenges is to integrate different domains of information which are historically seen as separated. For example, information related to business policies, market demand and supply, productivity trends, just to name a few, has to be integrated in a harmonious way with data sources of any kind (e.g. from data of sensors to decisions of human operators). Concrete scenarios and models have already been proposed under the name of Industry 4.0[1] or Digital Factory in what follow. What emerges from these studies is that a digital factory is indeed a complex system from many points of view. The complexity of the controller responsible for a whole Digital Factory increases with the multiplicity of heterogeneous data sources and actuators. Experts from different fields have to cooperate when developing the logic of the controller(s) and the relative integration with the systems or processes to be controlled. Moreover, there is the need for a continuous refinement and evolution of all the digital systems within a Digital Factory, including the logic of the controller and in related aspects (e.g. integration, deployment). As a complication, in a CPS the physical computational resources used by the digital systems are typically distributed, and there is the need to tolerate unexpected loads or failures which result from changes in the environment. Finally, CPS and the controller are targets for cyber attacks intended to leak information, compromise or destroy the Digital Factory.

The usage of a Service Oriented Approach has been proposed for realizing CPSs[2]. Among the Service Oriented approaches, the microservice approach was recently proposed for implementing CPSs [3] with the goal of solving limitations of current architectures in the scenario of Digital Factory where complexity, speed of evolution and required resources of applications is expected to increase in the coming years.

Microservices[4] is one of the latest architectural trends in software engineering, promising to address several open issues in software development. A microservice architecture is suitable to realize complex, distributed architectures, in which multiple teams of developers cooperate in all steps of software construction, from integration, testing, releasing to deployment and infrastructure management. This is reasonably in line with the requirements of a Digital Factory, where a complex, distributed application (in our case a controller - more likely a set of controllers hierarchically organized) has to evolve while remaining continuously available. Recently, has been proposed the integration of IoT technologies with a microservice architecture [5] with the goal of solving limitations of current architectures in the scenario of a Digital Factory. The IEC 61499 is an industrial standard proposing component-oriented models for developing distributed control systems. Given the modular nature of the microservices approach, we consider possible the implementation of an architecture following industrial standards such as the IEC 61499 into a microservice architecture.

Different microservices approach comes with different guidelines and patterns, having as a common point that of carrying advantages for developing, evolving and deploying complex applications. In this work we consider a Digital Factory adopting the Command Query Responsibility Segregation (CQRS) pattern [6] to implement the control plane. A CQRS application, the controller in our case, is split into two parts: command processing (i.e. inputs to the controller) and query processing (i.e. outputs of the controller). A CQRS application contains an Event Store, which can be used to determine the current and past state of the system, i.e the state of the controller.

Our contribution is twofold. First, we propose an architecture for implementing the controller as a set of containerized microservices that can be automatically deployed and orchestrated on cloud platforms. Compared to a monolithic design, our proposal has advantages when the controller is complex, constantly evolving and requires many computational resources.

Then, we focus on how to detect and mitigate cyber attacks to the controller. In our CQRS based controller, if the query or command services are compromised, the control system could be compromised as well, with catastrophic consequences for the Digital Factory.

The proposed solution consists of a detection and a mitigation mechanism. The detection technique involves the usage of redundant replicas with a voting scheme applied both to input and to the outputs of the controller. The mitigation is implemented by destroying and restoring the compromised microservices from their original image, together with a safe state taken from the Event Store. In the paper, we describe the CQRS-based architecture of the controller enhanced with the detection and mitigation schema and we show, by means of simulation, the effectiveness of the detection and mitigation mechanisms.

References

1. Zhong, Ray Y., et al. Intelligent manufacturing in the context of industry 4.0: a review. Engineering, 2017, 3.5: 616-630.
2. Feljan, A. V., Mohalik, S. K., Jayaraman, M. B., & Badrinath, R. (2015, December). Soa-pe: A service-oriented architecture for planning and execution in cyber-physical systems. In Smart Sensors and Systems (IC-SSS), International Conference on (pp. 1-6). IEEE.
3. Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18-23.
4. Kang, H., Le, M., & Tao, S. (2016, April). Container and microservice driven design for cloud infrastructure devops. In Cloud Engineering (IC2E), 2016 IEEE International Conference on (pp. 202-211). IEEE.
5. Thramboulidis, K., Vachtsevanou, D. C., & Solanos, A. (2018, May). Cyber-physical microservices: An IoT-based framework for manufacturing systems. In 2018 IEEE Industrial Cyber-Physical Systems (ICPS) (pp. 232-239). IEEE.
6. Betts, D., Dominguez, J., Melnik, G., Simonazzi, F., & Subramanian, M. (2013). Exploring CQRS and Event Sourcing: A journey into high scalability, availability, and maintainability with Windows Azure.