Component-Based Refinement and Verification of Information-Flow Security Policies for Cyber-Physical Microservice Architectures

Christopher Gerking [1], David Schubert[2]

Abstract: This publication is based on our paper presented at the IEEE International Conference on Software Architecture 2019 [GS19].

Keywords: security policy; information flow; microservice architecture; cyber-physical systems

1 Composable Security for Cyber-Physical Systems

Cyber-physical systems (CPS) are closely interconnected with the outside world, exchanging information with different parties. From a security viewpoint, it is therefore crucial for software engineers to ensure that confidential information is never leaked to unauthorized third parties. To protect CPS against such security leaks, the flow of information must be regulated and analyzed in the early design phase. Formal methods for regulation and analysis are provided by the theory of *information-flow security*. Due to the popularity of component-based design principles (e.g., such as the *microservice* architectural style), the software of CPS is increasingly composed of multiple components. Thus, each component must be provided with an individual security policy that regulates the flow of information between the component's interfaces. To satisfy the security regulations of the composite system, these policies must be composable in a way that prevents unauthorized information flows from end to end.

However, the composability of properties like security is a problem that requires careful investigation by software engineers. Over the last decade, secure information flow has become known as a so-called *hyperproperty* [CS10]. Due to their formal characteristics, such properties are hard to compose in general. Therefore, a careless composition of secure components is at risk of leading to an insecure system [Ma02]. In our publication [GS19], we provided software engineers with means to ensure the composability of information-flow security in the presence of domain-specific CPS characteristics. Thereby, we enable microservice architectures of CPS to be composed securely. Our contributions address both regulation and analysis of the information flow.

[1] Karlsruhe Institute of Technology (KIT), Software Design and Quality, Am Fasanengarten 5, 76131 Karlsruhe, Germany, christopher.gerking@kit.edu, https://orcid.org/0000-0001-5531-9607

[2] Fraunhofer Institute for Mechatronic Systems Design (IEM), Software Engineering and IT Security, Zukunftsmeile 1, 33102 Paderborn, Germany, david.schubert@iem.fraunhofer.de

doi:10.18420/SE2021_10

2 Refining Information-Flow Regulations

As our first contribution, we address the refinement of security regulations during the decomposition of systems into components. To this end, we provide software engineers with a set of architectural well-formedness rules for the security policies of components. These rules are used to distinguish regular refinements from those that are irregular because they put the composite system at risk of unauthorized information flows. Our work is based on a well-founded theory of composability for information-flow properties [Ma02], but applies these theoretical foundations to the engineering practice at the architectural level. To ensure applicability in the domain of CPS, our rule set is tailored to the asynchronous communication between components, exchanging information by passing messages to each other. Applying our rules ensures that, as long as all constituent components adhere to their refined security policies, the composite system is free of any information leaks.

3 Timing-Sensitive Analysis of the Information Flow

Our second contribution is a tool-supported verification technique that enables engineers to analyze the message-passing behavior of a component for unauthorized information flows. To account for the fact that CPS are real-time systems, our technique is timing-sensitive. Thus, it detects so-called *timing channels*, which are information leaks that are exploitable by observing the instant of time at which messages are passed. In combination, our contributions enable a compositional security analysis, in which the analysis results are securely composable out of the box [Ge20]. Thereby, we assure software engineers that a composition of secure components is riskless because it will always lead to a secure system. To evaluate the accuracy of our contributions, we conducted a security-related extension of the community case study CoCoME for component-based systems.

References

[CS10] Clarkson, M. R.; Schneider, F. B.: Hyperproperties. Journal of Computer Security 18/6, pp. 1157–1210, 2010, DOI: 10.3233/JCS-2009-0393.

[Ge20] Gerking, C.: Model-driven information flow security engineering for cyber-physical systems, PhD thesis, Paderborn University, 2020, DOI: 10.17619/UNIPB/1-1033.

[GS19] Gerking, C.; Schubert, D.: Component-Based Refinement and Verification of Information-Flow Security Policies for Cyber-Physical Microservice Architectures. In: IEEE International Conference on Software Architecture, Proceedings. ICSA 2019. IEEE, pp. 61–70, 2019, DOI: 10.1109/ICSA.2019.00015.

[Ma02] Mantel, H.: On the Composition of Secure Systems. In: 2002 IEEE Symposium on Security and Privacy, Proceedings. IEEE Computer Society, pp. 88–101, 2002, DOI: 10.1109/SECPRI.2002.1004364.