Joel Greenyer, Malte Lochau, and Thomas Vogel (Hrsg.): Explainable Software for Cyber-Physical Systems (ES4CPS), GI-Dagstuhl Seminar 19023, January 2019,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2019 11

Security Explainability Challenges in Cyber-Physical Systems

Narges Khakpour[1]

The growth in development and deployment of Cyber-Physical Systems (CPS) has lead to emerging new security problems and challenges. A CPS can be vulnerable to attacks that target its cyber elements, its physical parts, its communication link or a combination of them. Attacks to single components or single layers are usually easier to detect and mitigate,while attacks raised and amplified by the inter-dependence and interactions between cyber and physical components, that are usually provided by different vendors, are harder to detect, explain and protect against. In particular, coordinated attacks that target multiple components in a CPS and exploit different vulnerabilities in cyber and physical layers are very challenging to identify, explain, asses and mitigate.

The characteristics of CPS, specially their complexity and components heterogeneity, demand new techniques to design, explain, analyze and enforce security that consider such specific features. We point to a few challenges that should be addressed to realize more explainable security in CPS.

Security Explainability by Design Many CPSs are not usually designed with security in mind [Hu17], or the focus is usually on security of individual components. We need new design methods for CPS in which security is considered from the beginning of the system life-cycle, consider the specific security requirements of CPS and develope the software in a way that one can detect and troublshoot malicious behaviors or security weaknesses in future. One approach to tackle this challenge is to use domain-driven security [BCE11] that aims to facilitate secure software development by integrating security requirements with software development processes.

The model-driven security methods express security requirements in addition to the system design, propose analysis techniques to reason about the system security, and generate the code automatically from the models to enforce security policies. Such design techniques, tailored to CPS, should (i) take into account interactions of the physical and cyber layers and their potential security implications, (ii) provide proper technical documentations to discover, explain and fix security violations in future, e.g. the (verified) security implications of a change in a component in interaction with other components of the eco-system, or components' compatibility information, (iii) use advanced logging mechanisms and formats that enable us to extract helpful information about the system behavior in case of a suspicious

[1] Linnaeus University, Sweden narges.khakpour@lnu.se

behavior to explain and root-cause analyze the undesired behaviors, (iv) offer secure logging mechanisms that don't lead to confidential information leakage.

Evolving Security Mechanisms Today's CPS are designed in a way to get evolved at runtime, and adapt themselves to the changing requirements and the operational environment, e.g. by applying a security patch, and as such, any change in the system can introduce new vulnerabilities and make its protection mechanisms ineffective. Hence, with an increasing number of attacks and systems that become increasingly more adaptive and evolving, the protection mechanisms must subsequently evolve and be improved over time to face future attacks and dependability concerns. Reactive security techniques (like encryption, Intrusion Detection Systems (IDSs) etc), although very useful, can no longer be solely effective in such dynamic environments, and developing proactive and adaptive mechanisms is becoming an indispensable need.

To realize effective self-protecting systems, the security implications of any change should be checked before application, and as such, each system component must be provided with (verified) security signatures that explain the potential vulnerabilities, security threats and their implications. This will allow us to explain any undesired behavior in the eco-system by analyzing components' security signatures and their interactions. This will let us evaluate and explain the security impact of an adaptation too.

Cyber-Physical Interactions Due to the strong cross-layer interactions between physical and cyber layers in CPS, that can magnify and complicate the impact of an attack, analyzing security of each layer in isolation is insufficient to assess security of the whole system. Techniques and tools are required for security analysis and enforcement of CPS that consider both cyber and physical aspects of the system and their interactions. In particular, the security implications of cyber-physical interactions must be specified and verified that enable us to explain and troubleshoot any undesired behavior due to the cyber-physical interactions.

Required Expertise The competences required to address the above challenges include expertise in (physical) security, hybrid behavioral modeling and verification, self-adaptive systems and model-based development. The author's research interests lie in security, formal methods, (discrete-event) supervisory controller synthesis and self-adaptive systems. She has also experience in modeling hybrid systems. The required external expertise include physical security, verification of hybrid systems and model-based development.

The project PROSSES (Provably Secure Self-Protecting Systems) at Linnaeus University, led by the author, focuses on (i) proposing tools and techniques to enforce security in adaptive and evolving systems, and (ii) designing adaptive and provably secure security enforcement mechanisms. PROSSES focuses only on cyber-security. To address the second and third challenges, the research results of PROSSES should be extended and enhanced to consider physical layer's behavior and its interaction with the cyber layer.

References

[BCE11] Basin, David A.; Clavel, Manuel; Egea, Marina: A decade of model-driven security. In: SACMAT. 2011.

[Cy16] Cyber-Attack Against Ukrainian Critical Infrastructure, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[Hu17] Humayed, A.; Lin, J.; Li, F.; Luo, B.: Cyber-Physical Systems Security?A Survey. IEEE Internet of Things Journal, 4(6):1802–1831, Dec 2017.