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

Explainability of Cyber-Physical Security Threats

Christopher Gerking[1]

1 Explaining Secure Design Decisions

Developing software requires engineers to ensure consistency between the *design* of a system and the quality *goals* of the system's stakeholders. Such goals ultimately determine the design of a system, and the design decisions made by engineers affect the degree to which goals are achieved. In this regard, *security* is a quality property that is special as it involves *threats* as an additional dimension beside design and goals [Tü17]. A threat represents the source of a security incident, and thereby relates to both goals and design: security goals must cover a reasonable amount of threats in order to be consistent, whereas threats may be mitigated or even facilitated by particular design decisions.

However, design decisions that are made to mitigate threats are often hard to explain. The reason is that decisions are no longer clearly traceable to security goals. Instead, they are motivated in terms of unimaginable and seemingly unreal threats. Due to the vague and fast-moving nature of threats, explaining the harm they cause is often only possible in a post-incident way, i.e., if a threat has already materialized in form of a security incident. The intention to prevent such incidents beforehand is known as *security by design*, but the successful application of this principle suffers highly from the aforementioned problems in terms of explainability. Systems with unexplainable mitigations may either be used or operated in an insecure way, or fully rejected by users. In the worst case, unexplainable mitigations may even be neglected by engineers, thereby introducing serious security vulnerabilities.

Engineers may encounter this problem not only when explaining mitigations to stakeholders, but also when it comes to the explainability of results produced by automated security analyses. In particular, analyzable security properties like *noninterference* [GM82] are known to be *hyperproperties* which are properties of sets of execution traces [CS08]. Therefore, a counterexample that indicates a security vulnerability refers to more than one trace. Thus, it is hard to map such a counterexample to a real-life security incident with a clear indication of harm, thereby affecting the explainability of the analysis results.

[1] Paderborn University, Software Engineering Research Group, Fürstenallee 11, 33102 Paderborn, Germany
christopher.gerking@upb.de

2 Challenging Characteristics of Cyber-Physical Systems

The nature of cyber-physical systems implies several characteristics that further intensify the need to explain security threats. First of all, cyber-physical systems integrate artifacts from multiple engineering disciplines. Accordingly, security threats such as *side channels* exploit physical effects. Therefore, detecting and mitigating such threats involves disciplines other than software engineering and requires a discipline-spanning explanation at the level of *systems engineering*.

Second, the physical environment of systems imposes hard real-time constraints on their behavior. However, this real-time behavior must not enable attackers to infer sensitive information indirectly from the response times of a system. Such leaks, called *timing channels*, must be detected by corresponding analyses. Therefore, the time aspect needs to be taken into account during the explanation of threats as well.

Third, cyber-physical systems are increasingly self-adaptive by reconfiguring their structure or behavior according to a certain situational context. Such adaptations must not compromise the security of a system, which is why security considerations need to be taken into account during the analysis and planning of adaptations. Thereby, a system might even adapt its level of protection to a specific security situation. However, when it comes to the explainability of such adaptations, the corresponding security threats need to be integrated into the explanations as well.

3 Expertise

My field of expertise is model-driven engineering of cyber-physical systems that are *secure by design*. A specific focus of my work is on using model transformation techniques to apply formal security analyses that take the real-time behavior of systems into account. In this respect, the counterexamples obtained from the analyses suffer from a missing link to concrete, explainable security threats. To improve the explainability of analysis results, expertise is needed in order to link counterexamples to explainable threat *scenarios*. Furthermore, additional expertise is required with respect to the challenge of executing and explaining self-adaptations in a way that takes security threats into account.

References

[CS08] Clarkson, Michael R.; Schneider, Fred B.: Hyperproperties. In: CSF 2008. IEEE Computer Society, pp. 51–65, 2008.

[GM82] Goguen, Joseph A.; Meseguer, José: Security Policies and Security Models. In: IEEE S&P. IEEE Computer Society, pp. 11–20, 1982.

[Tü17] Türpe, Sven: The Trouble with Security Requirements. In: RE 2017. IEEE Computer Society, pp. 122–133, 2017.