Poster: Knowledge-enriched Security and Privacy Threat Modeling

Laurens Sion, Koen Yskout, Dimitri Van Landuyt, Wouter Joosen
imec-DistriNet
KU Leuven
Heverlee, Belgium
{laurens.sion,koen.yskout,dimitri.vanlanduyt,wouter.joosen}@cs.kuleuven.be

ABSTRACT

Creating secure and privacy-protecting systems entails the simultaneous coordination of development activities along three different yet mutually influencing dimensions: translating (security and privacy) goals to design choices, analyzing the design for threats, and performing a risk analysis of these threats in light of the goals.

These activities are often executed in isolation, and such a disconnect impedes the prioritization of elicited threats, assessment which threats are sufficiently mitigated, and decision-making in terms of which risks can be accepted.

In the proposed TMaRA approach, we facilitate the simultaneous consideration of these dimensions by integrating support for threat modeling, risk analysis, and design decisions. Key risk assessment inputs are systematically modeled and threat modeling efforts are fed back into the risk management process. This enables prioritizing threats based on their estimated risk, thereby providing decision support in the mitigation, acceptance, or transferral of risk for the system under design.

KEYWORDS

Security, design, threat modeling, model enrichment

ACM Reference Format:
Laurens Sion, Koen Yskout, Dimitri Van Landuyt, Wouter Joosen. 2018. Poster: Knowledge-enriched Security and Privacy Threat Modeling. In *ICSE '18 Companion: 40th International Conference on Software Engineering Companion, May 27-June 3, 2018, Gothenburg, Sweden.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3183440.3194975

1 INTRODUCTION

The principles of Security and Privacy by Design (SbD/PbD) are increasingly recognized as essential for preventing security and privacy design flaws [1]. Recent regulatory efforts such as the EU General Data Protection Regulation (GDPR) [7] even introduce the obligation to adhere to *privacy and data protection by design* and by default, for all systems or services that process personal data. Threat modeling approaches contribute to the realization of these principles by providing a systematic, rigorous, and methodical approach towards a security and privacy analysis.

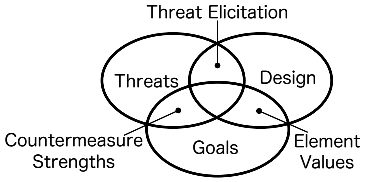

Figure 1: Three dimensions to approach security needs [20]

Threat modeling methodologies, such as STRIDE [9, 10] or LINDDUN [5, 21] use Data Flow Diagrams (DFDs) [4] as a representation of the system. Systematically iterating over all model elements leads to the identification of potential security or privacy threats. In a subsequent step, the identified threats must be manually assessed with respect to their importance (based on likelihood and impact). Such assessments ideally involve other stakeholders, tapping into existing risk analysis methodologies and architectural analysis approaches [8, 11]. In practice, these activities require substantial effort and expertise, partly due to their disconnected nature.

In this paper, we present a novel approach called TMaRA (Threat Modeling and Risk Analysis) which involves integrating threat modeling and risk analysis activities. Specifically, existing threat modeling artifacts are enriched with the information to conduct risk analyses, allowing for tighter integration between risk assessment and threat modeling. Similar to other approaches [12], this combined analysis provides a list of threats. A second distinguishing factor of the TMaRA approach is that the threat list is further enriched with risk estimates considering (i) the value of the threatened assets, (ii) the likelihood of various types of attackers to pose these threats, and (iii) the difficulty for attackers to overcome the security and privacy countermeasures in place. As such, the knowledge-driven approach allows continuously monitoring progress in terms of risks mitigated by existing countermeasures and residual risks, and provides a better basis for *what-if* or change impact analysis.

2 RELATED WORK

Türpe [20] discusses security needs as interactions from three dimensions: design, goals, and threats (as depicted in Figure 1), and observes that many existing efforts are focused on a single dimension. We structure this section by focusing on the threat-related interactions in this framework:

Threat–design interactions. Threat modeling, originally introduced by Microsoft and part of their security development lifecycle [9, 10, 15, 17, 18], is widely adopted, with multiple real-world applications in the industry [6, 15, 18], and readily-available tool

ICSE '18 Companion, May 27-June 3, 2018, Gothenburg, Sweden
© 2018 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-5663-3/18/05.
https://doi.org/10.1145/3183440.3194975

support from Microsoft [12]. In these existing approaches and applications, data flow diagrams remain largely security and privacy-agnostic models, with only minor, and often ad-hoc, additions for security or privacy. However, recently there have been several proposals for extensions to these data flow diagrams to more systematically representat of security- and privacy-relevant information and increase the efficiency of threat modeling approaches [2, 3, 16, 19].

Threat–goal interactions. Risk analysis approaches elicit security requirements starting from security goals or anti-goals, such as in CORAS [11]. They can be used in a complementary fashion to threat modeling [13]. Also related are attack trees [14], which start from attacker goals and explore the possible ways to achieve those.

3 TMARA: THREAT MODELING AND RISK ANALYSIS

We shortly outline the core principles behind the proposed TMaRA threat modeling approach, focusing on how it advances the state of the art for the threat–design and threat–goal interactions. Improvements in both are based upon *enriching* the input models.

Threat–design interactions: solution-awareness. Many threat modeling approaches start from a plain DFD model [5, 9]. which defines an abstract view of the system under design. This model is used at the basis for eliciting threats by matching model elements to certain predefined threat expressions. A key problem however is that such approach is completely agnostic to any existing security countermeasures. Tools such as the Microsoft Threat Modeling Tool [12] take these into account to a limited degree by attaching simple properties to individual elements which prevent certain threats from being generated. For example, each data flow has a predefined boolean property *Provides confidentiality*. While useful, such properties are very local and their expressiveness is limited.

TMaRA involves creating a more extensive representation of security solutions in the form of architectural patterns for security and privacy [22]. By separating this information from the threat generation process, security solutions can be extended separately. Pattern instantiation happens by allocating roles to DFD elements. These roles specify the *Countermeasures* and the threats against which they protect. This approach leads to enriched DFDs [16].

Threat–goal interactions: asset value, strength of the countermeasures, and explicit attacker model. Risk analysis explicitly takes into account elements of uncertainty and is thus probabilistic in nature. Integrating risk analysis into threat modeling allows for the assessment of a threat's applicability on a continuous scale instead of a traditional binary scale (i.e. applicable or not).

This is accomplished in TMaRA in a knowledge-driven fashion, i.e. by taking into account three types of estimates: (i) the inherent value of affected assets in the DFD, (ii) the strength of countermeasures (the degree to which the probability of threat has been reduced as a result of implementing the countermeasure), and (iii) an explicit attacker profile that provides estimates on the technical capabilities of potential adversaries (probability that an attacker of this type will be able to realistically exert the threat).

The resulting threat prioritization is not final, which leads to more realistic assessment as no security/privacy mechanism is perfect, i.e. the strength may decline over time, as new vulnerabilities emerge, and as attacker capabilities (and assumptions) change.

4 CONCLUSION

Existing threat modeling practices lack grounding in data related to the security goals of the system under consideration. Additionally, risk analysis practices are disconnected from the concrete design of the system and the threats that such a design encompasses.

The presented TMaRA approach addresses this disconnect by extending DFD-based threat modeling and enrichment in terms of security and privacy solutions, and risk analysis simulations based on concrete element value estimates, countermeasure strengths, and attacker types. The resulting analysis is more tuned to reality, in which nothing is 100% secure, but countermeasures do represent a reduction of the risk of a certain threat manifesting itself. Additionally, the risk-enriched threat list enables the threat modeler to monitor progress in reducing and managing the overall risk.

In ongoing work, we are implementing a prototype in which threat modeling is augmented with risk analysis, and in which integration is accomplished with external knowledges sources (vulnerability databases, security solution catalogs, etc).

ACKNOWLEDGMENTS

This research is partially funded by the Research Fund KU Leuven.

REFERENCES

[1] Majed Alshammari and Andrew Simpson. 2016. Towards a Principled Approach for Engineering Privacy by Design. (2016).

[2] Thibaud Antignac, Riccardo Scandariato, and Gerardo Schneider. 2016. *A Privacy-Aware Conceptual Model for Handling Personal Data.* Springer, Cham, 942–957.

[3] Bernhard J. Berger, Karsten Sohr, and Rainer Koschke. 2016. Automatically extracting threats from extended data flow diagrams. *LNCS* 9639 (2016), 56–71.

[4] Tom DeMarco. 1979. *Structured Analysis and System Specification.* Yourdon Press.

[5] Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel, and Wouter Joosen. 2011. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering* 16, 1 (2011), 3–32.

[6] D Dhillon. 2011. Developer-Driven Threat Modeling: Lessons Learned in the Trenches. *IEEE Security Privacy* 9, 4 (jul 2011), 41–47.

[7] European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. OJ L 119, 04.05.2016, p. 1–88. *Official Journal of the European Union* 59, L 119 (may 2016), 1–88.

[8] Jack Freund and Jack Jones. 2014. *Measuring and managing information risk: a FAIR approach.* Butterworth-Heinemann.

[9] Shawn Hernan, Scott Lambert, Tomasz Ostwald, and Adam Shostack. 2006. Threat Modeling: Uncover Security Design Flaws Using The STRIDE Approach. *MSDN Magazine* 6 (nov 2006).

[10] Michael Howard and Steve Lipner. 2006. *The Security Development Lifecycle.* Microsoft Press.

[11] Mass Soldal Lund, Bjørnar Solhaug, and Ketil Stølen. 2010. *Model-driven risk analysis: the CORAS approach.* Springer Science & Business Media.

[12] Microsoft. 2016. Microsoft Threat Modeling Tool. http://aka.ms/tmt2016. (2016).

[13] Tobias Rauter, Nermin Kajtazovic, and Christian Kreiner. 2016. Asset-Centric Security Risk Assessment of Software Components. *2nd International Workshop on MILS: Architecture and Assurance for Secure Systems* (2016).

[14] Bruce Schneier. 1999. Attack trees. (1999).

[15] Adam Shostack. 2008. Experiences threat modeling at microsoft. In *Modeling Security Workshop. Dept. of Computing, Lancaster University, UK.*

[16] Laurens Sion, Koen Yskout, Dimitri Van Landuyt, and Wouter Joosen. 2018. Solution-aware Data Flow Diagrams for Security Threat Modelling. In *SAC2018: 6th track on Software Architecture: Theory, Technology, and Applications (SA-TTA).*

[17] Frank Swiderski and Window Snyder. 2004. *Threat modeling.* Microsoft Press.

[18] Peter Torr. 2005. Demystifying the threat modeling process. *IEEE Security & Privacy Magazine* 3 (2005), 66–70.

[19] Katja Tuma, Riccardo Scandariato, Mathias Widman, and Christian Sandberg. 2017. Towards security threats that matter. In *3rd Workshop On The Security Of Industrial Control Systems & Of Cyber-Physical Systems (CyberICPS 2017).*

[20] Sven Türpe. 2017. The Trouble With Security Requirements. *25th IEEE International Requirements Engineering Conference* (2017).

[21] Kim Wuyts. 2015. *Privacy Threats in Software Architectures.* Ph.D. Dissertation.

[22] Koen Yskout, Thomas Heyman, Riccardo Scandariato, and Wouter Joosen. 2006. A system of security patterns. (2006).