From Attacker Models to Reliable Security

Heiko Mantel
TU Darmstadt
Darmstadt, Germany
mantel@cs.tu-darmstadt.de

ABSTRACT

Attack trees are a popular graphical notation for capturing threats to IT systems. They can be used to describe attacks in terms of attacker goals and attacker actions. By focusing on the viewpoint of a single attacker and on a particular attacker goal in the creation of an attack tree, one reduces the conceptual complexity of threat modeling substantially [1]. Aspects not covered by attack trees, like the behavior of the system under attack, can then be described using other models to enable a security analysis based on a combination of the models.

Despite the high popularity of attack trees in security engineering for many years, some pitfalls in their use were identified only recently [2]. In this talk, I will point out such difficulties, outline how attack trees can be used in combination with system models, and clarify the consequences of different combinations for security analysis results. After a security analysis of an abstract model, the insights gained need to be mapped to reality. I will introduce an automata-based model of run-time monitors [3] and will show how defenses in this model can be realized at runtime with the CliSeAu system [4,5].

CCS Concepts/ACM Classifiers

• Security and privacy~Security requirements
• Security and privacy~Formal security models
• Security and privacy~Software security engineering
• Security and privacy~Distributed systems security:

Author Keywords

Security engineering; threat modeling; security models; security policies; run-time monitoring and enforcement; usage control

BIOGRAPHY

Heiko Mantel is a full professor for Computer Science at TU Darmstadt. His research interests in IT security include language-based security, security engineering, information-flow security, and side-channel analysis. From 2010 to 2017, he was the spokesman of the national research initiative Reliably Secure Software Systems, funded by the German Science Foundation. Since 2018, he leads the Software-Factory 4.0 initiative, which aims for efficient, flexible and reliable solutions to software re-engineering, funded by the state of Hesse. He is or has been involved in many other research projects as principal investigator.

Previously, Heiko Mantel was assistant professor at the RWTH Aachen, postdoctoral researcher at the ETH Zurich, and researcher at the German Research Center for Artificial Intelligence. He received his Ph.D. from Saarland University in 2003.

REFERENCES

[1] B. Schneier, "Attack trees: Modeling security threats". Dr. Dobbs Journal, December 1999.

[2] H. Mantel and C. W. Probst. "On the Meaning and Purpose of Attack Trees". In IEEE Computer Security Foundations Symposium, 2019, to appear.

[3] R. Gay, H. Mantel, and B. Sprick. "Service Automata". In International Workshop on Formal Aspects of Security and Trust, LNCS 7140, 148-163, 2012.

[4] R. Gay, J. Hu, and H. Mantel. „CliSeAu: Securing Distributed Java Programs by Cooperative Dynamic Enforcement". In International Conference on Information Systems Security, LNCS 8880, 378-398, 2014.

[5] T. Hamann and H. Mantel. "Decentralized Dynamic Security Enforcement for Mobile Applications with CliSeAuDroid". In International Symposium on Foundations & Practice of Security, 29-45, 2018.

AsiaCCS '19, July 9–12, 2019, Auckland, New Zealand.

ACM ISBN 978-1-4503-6752-3/19/07.
DOI: https://doi.org/10.1145/3321705.3329915