Software systems are constantly under threat from cyber-attacks. To protect their software, organizations design blueprints of future software and scrutinize them for security holes, even before any line of code written. Usually, this thorough analysis is performed manually by security experts, who strive to find as many issues as possible. However, due to resource constraints, only the most critical issues will be addressed. Not only is this way of working time-consuming, but it also leads analysts to discuss less important issues while possibly overlooking other critical issues. Further, even when analysts do find critical issues and require countermeasures to be put in place, there is no guarantee that the software developers will implement the security defenses as planned.

This thesis contributes to solving these problems. First, we improve an existing manual technique which enables the analysts to identify twice as many critical issues in our case studies. Second, we propose two techniques that detect security design flaws automatically and help in reducing the number of overlooked issues. Finally, we introduce a semi-automated approach to link the intended design to the implemented constructs and automatically verify that the implementation complies with the planned security requirements.

Katja Tuma
Department of Computer Science and Engineering
Software Engineering Division

ISBN 978-91-8009-154-1

DOCTORAL THESIS

Katja Tuma Efficiency and Automation in Threat Analysis of Software Systems

2021

DOCTORAL THESIS
IT FACULTY

Efficiency and Automation in Threat Analysis of Software Systems

Katja Tuma

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

UNIVERSITY OF GOTHENBURG