Popular science summary of the PhD thesis

PhD student	Alyzia-Maria Konsta
Title of the PhD thesis	Synthesis and Optimal Observability for Attack Trees
PhD school/Department	Compute

Science summary

* Please give a short popular summary in English (approximately half a page) suited for the publication of the title, main content, results and innovations of the PhD thesis also including prospective utilizations hereof. The summary should be written for the general public interested in science and technology.

As electronic device usage grows, vast amounts of sensitive data are stored and processed on local or remote servers, making the need of security crucial. One method to assess system security is through graphical security models like attack trees, which depicts all possible attack paths in a hierarchical structure. Traditionally, security experts design these trees manually, a process that can be tedious and error-prone. This thesis explores the automatic synthesis of attack trees using event logs from attacked systems, providing insights into exploited vulnerabilities. Additionally, it examines how to automatically apply countermeasures by controlling an attacker's observability, such as obfuscating data. For example, in a login system, if a user enters incorrect credentials, the system can either specify whether the username or password is wrong or provide a generic error message. The latter approach increases security by preventing attackers from narrowing down valid credentials but may reduce usability. Hence we explore ways of how a security expert can obfuscate (hide) specific aspect of the system under a budget (for example usability) in order to keep the attackers reward (for example gained knowledge) under a given threshold. This work provides a solid starting point for improving security analysis and countermeasures. The results are promising and offer new ideas and tools for future research in automated security and decision-making.

Please submit the summary to the department PhD coordinator together with your thesis