TEK5510 – Security in Operating Systems and Software

Digital threats and malware have become part of our daily digital life. Clicking on a malicious link, visiting the wrong website or failing to keep your systems updated may give threat actors access to your systems. This course aims to give the students understanding of how malware works, how threat actors can use vulnerabilities to gain access to a system, and how to prevent attacks.

The course focuses on security in a computer, not network security. We start by explaining how legit programs run on a computer and introduce the concept of security in operating systems and software. Threat actors often use a vulnerability in a software on the victim's computer as a way in, and this course gives an overview of various types of vulnerabilities and how they can be exploited and mitigated. We also consider how to write secure code to prevent introducing new vulnerabilities.

We cover password security and cracking, and give a brief introduction to how malware uses cryptography, for example for hiding and obfuscation. Hardware vulnerabilities are also explained, and how they differ from software vulnerabilities. We also touch on the importance of integrity and trust in the boot process.

Even though the focus is on security in a computer, no computer these days lives in isolation. The course therefore also covers web security and mobile devices.

In short: The main subjects are software vulnerabilities and malicious software, and techniques for mitigating these threats.