MICRO-CREDENTIAL

SOFTWARE HACKING AND PROTECTION

SEPTEMBER - DECEMBER

GHENT UNIVERSITY

SOFTWARE HACKING AND PROTECTION

Since the start of the ICT-revolution, companies, organizations, private citizens, governments, and society at large have come to depend more and more on software. Today, software benefits many aspects of our private and public lives. At the same time, it is a key enabler of many business models.

Software can also be abused and weaponized in various ways, however, to disrupt private lives, business models, and society at large. There hence exists a strong need to defend (systems running) software against a range of attacks.

Doing so requires defensive software protection knowledge and skills, but also offensive training. After all, poachers make the best gamekeepers. Moreover, at the technical level, the required skills largely overlap: many technically neutral methods and tools can be used offensively as well as defensively, the difference solely depending on whether the targeted software is malware or goodware.

PROGRAMME

In this course, we focus on the technical knowledge and skills, so-called hacking skills, required to attack and protect software assets. These assets are the most valuable and sensitive parts of programs that need to remain confidential in the face of reverse engineering and of which the integrity needs to be maintained in the face of software tampering attempts.

We study and practice a wide range of software analysis and tampering techniques, including side channel and faultinjection techniques that rely on physical implementation features, as well as protections such as obfuscations that aim to mitigate unauthorized uses of those techniques to protect assets and their security requirements.

We study and practice the complex tasks of deploying good combinations of protections and of evaluating the achieved levels of protection, including the design and execution of empirical experiments in the domain of reverse engineering and software protection.

Furthermore, we study and practice how to use a range of software analyses and forensic techniques to analyze and detect malware, as well the techniques that malware authors deploy in an attempt to evade detection. The attacks and mitigations in the scope of this course are commonly called man-at-the-end techniques, as they are deployed by parties that have (almost) complete control over the end devices on which they attack and analyze the software, such that they don't need to rely on exploitable vulnerabilities for their attacks and analyses.

LECTURER-IN-CHARGE

Prof. dr. ir. Prof. Bjorn De Sutter

Department of Electronics and Information Systems, Ghent University

COMPETENCES

⇨ Understanding the man-at-the-end attack model, including its relevant constructs, models, and methods.
⇨ Knowing how to devise appropriate man-at-the-end attack strategies based on knowledge about the targeted assets.
⇨ Knowledge of, a deeper understanding of, and experience with the tools and techniques commonly deployed in man-at-the-end software attacks.
⇨ Capacity to execute a range of man-at-the-end attack steps on software (reverse engineering, software tampering) as part of such strategies.
⇨ Extended knowledge of the techniques used for software protection against man-at-the-end attacks, understanding their limitations and the need to combine and layer multiple techniques to obtain useful protection.
⇨ Basic experience in using software protection tools for deploying those techniques.
⇨ Understanding strategies for and the complexities of deploying, evaluating, and validating software protections, including applicable risk management approaches.
⇨ Knowing how to design, execute, and analyze empirical experiments involving human subjects for expanding the knowledge in software protection and man-at-the-end attack models.
⇨ Knowing the different types of malware and their core features.
⇨ Understanding the most used malware detection, classification, and analysis methods, and how malware tries to evade those.
⇨ Being able to deploy forensic malware analysis techniques and tools.
⇨ Communicating domain-specific knowledge in a correct and clear manner, with the appropriate language skills, incl. the use of correct terminology.

PRACTICAL INFO

⇨ **LOCATION** Universiteit Gent, Campus Sterre, Gent
⇨ SEPTEMBER - DECEMBER 2025

More info? Go to ⇨ **WWW.UGAIN.UGENT.BE/SOFTWAREHACKING**