Course Specifications

Valid as from the academic year 2020-2021

Software Hacking and Protection (E017941)

Due to Covid 19, the education and evaluation methods may vary from the information displayed in the schedules and course details. Any changes will be communicated on Ufora.

Course size (nominal values; actual values may depend on programme)

Credits	Study time	Contact hrs
6.0	180 h	60.0 h

Course offerings and teaching methods in academic year 2020-2021

A (semester 1)	English	Gent	self-reliant study activities	2.5 h
			guided self-study	2.5 h
			lecture: response lecture	6.25 h
			lecture	10.0 h
			microteaching	3.75 h
			practicum	23.75 h

Lecturers in academic year 2020-2021

De Sutter, Bjorn	TW06	lecturer-in-charge
Coppens, Bart	TW06	co-lecturer

Offered in the following programmes in 2020-2021	crdts	offering
Master of Science in Computer Science	6	A
Master of Science in Computer Science Engineering	6	A
Master of Science in Computer Science Engineering	6	A
Exchange Programme in Computer Science (master's level)	6	A

Teaching languages

English

Keywords

Security vulnerabilities, reverse engineering, software attacks, secure code, code injection, attacks, defenses, malware, defensive and offensive techniques, security policy, legal limitations

Position of the course

As more and more aspects of our lives are driven by, and dependent on, software, and as more and more infrastructure gets networked, illegitimate uses of software (such as malware and unauthorized copying and altering of software and content) are growing problems. To develop secure software that can resist attacks and that suffers from less vulnerabilities, it is important to acquire an understanding of existing attack vectors and attack methods, as well as of the protection techniques that can mitigate the attacks. Complementary to more traditional security-oriented courses that focus on cryptography, and hence on protection against so-called man-in-the-middle attacks in which communication channels are attacked, this course will focus on techniques used in and used against man-at-the-end attacks, in which the software running on the devices and systems performing the communications are attacked.

Contents

- General introduction into software security, risks, handling of issues, security requirements
- Native code reverse-engineering, incl. static and dynamic techniques overview, and debugging and disassembling in depth
- Software vulnerabilities & exploits thereof
- Secure software design and development practices
- Dynamic software attacks
- Code obfuscation and de-obfuscation

- Anti-tampering & anti-debugging
- Online software protection techniques
- Internet security, incl. browser, server, network vulnerabilities
- penetration testing
- Side channel and fault injection attacks and protection mechanisms
- Secure hardware based system design
- Malware classification, detection techniques and counter-measures

Initial competences

- Programming in C
- Basic knowledge in computer architecture
- Knowledge of operating system internals
- Knowledge of software engineering practices and paradigms
- Knowledge of databases, programming in SQL
- Basic knowledge of computer networks and Internet technology

Final competences

1. Have an understanding of, and be able to use the terminology of basic aspects of computer and software security, of risks, security requirements, handling of security issues, policy options, legal limitations.
2. Be able to place in context and execute man-at-the-end attacks (reverse engineering, debugging, tampering, ...). Knowledge of, a deeper understanding of, and experience with the tools and techniques commonly deployed in man--at--the--end software attacks
3. Deep understanding of vulnerabilities in software, exploits of those vulnerabilities, preventive counter-measures, and detection methods. Being able to use a range of tools and techniques thereto. Knowledge of security by design software development principles.
4. Knowledge of the techniques used for software protection against man-at-the-end attacks, and understanding their limitations and the need to combine multiple techniques to obtain useful protection. Basic capability in using tools and techniques thereto.
5. Understanding of online security requirements. Understanding in the aspects of penetration testing methods and online security testing. Be able to deploy popular tools thereto and to apply techniques thereto.
6. Understanding of ethical hacking (white hat vs. black hat) en responsible handling and disclosing of sensitive information.
7. Understanding of hardware based attack options (side channels and fault injection) and of protections to mitigate those attacks.
8. Understanding of the different types of malware and detection methods. Being able to deploy analysis techniques and tools.

Conditions for credit contract

Access to this course unit via a credit contract is determined after successful competences assessment

Conditions for exam contract

This course unit cannot be taken via an exam contract

Teaching methods

Guided self-study, lecture, microteaching, practicum, self-reliant study activities, lecture: response lecture

Extra information on the teaching methods

- Online movies and exercises (flipping the classroom)
- Some classical lectures, mostly QA lectures (response colleges)
- Labs/Practica (on campus if COVID-19 het toelaat)
- Normal labs are performed individually; no communication or collaboration between students is allowed.
- Peer presentations with guided preparation are done in small groups.
- Due to COVID19 alternative teaching methods might be adopted when necessary.

Learning materials and price

- Course website
- Online videos
- Online exercises
- Handouts labs
- Description terminology to know
- Academic publications (accessible for free)
- Course nodes and slides (in English), provided for free through the electronic learning platform

References

- Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection, by Christian Collberg & Jasvir Nagra, 2009, ISBN-13: 978-0321549259
- Software Security - Building Security In, by Gary McGraw, 2006, ISBN-13: 978-0321356703

Course content-related study coaching

- Interactive support and coaching through the electronic learning platform appointments
- Teachers and assistants are available for extra help before and after contact hours, and via chat and conf calls
- Use of flipping the classroom and blended learning techniques

Evaluation methods

end-of-term evaluation and continuous assessment

Examination methods in case of periodic evaluation during the first examination period

Written examination with open questions

Examination methods in case of periodic evaluation during the second examination period

Written examination with open questions

Examination methods in case of permanent evaluation

Oral examination, participation, assignment, peer assessment, report

Possibilities of retake in case of permanent evaluation

examination during the second examination period is possible in modified form

Extra information on the examination methods

- Periodic evaluation: written examination with open and closed questions on theory and practice (exercises), with closed-book
- During semester: graded lab sessions (written reports and possibly oral evaluation); participation 'flipping the classroom' activities, evaluation (including peer assessment) of peer presentations

Calculation of the examination mark

- 50% on continuous assessment, 50% on periodic exam.
- Lack of participation in continuous assessment for no valid reason results in a zero for that part.
- In the case of group assignments, the students in a group get the same score by default. Only when there is a clear difference in contribution to the solution and report, the students will be given different scores.
- The student must pass (<=10/20) both parts to pass the whole course. If he fails for one part while still scoring >=10/20 on average, the final score becomes 9/20.

Facilities for Working Students

Option to be freed from presence in labs with alternative assignment after consultation with the responsible teacher. Option for oral exam with written preparation at another time in the academic year. Option for feedback by appointment during and after business hours.