

Embedded System Security

Titulaire

Jan Tobias Mühlberg (Coordonnateur)

Mnémonique du cours

ELEC-H550

Crédits ECTS

5 crédits

Langue(s) d'enseignement

Anglais

Période du cours

Premier quadrimestre

Campus

Solbosch

Contenu du cours

- > The information security landscape and the role of safety, security, and data protection in embedded systems
- > Low-level vulnerabilities and defences in software and hardware
- > Vulnerabilities and defences in light-weight embedded systems
- > Automated detection, exploitation, and prevention of vulnerabilities in software
- > System security and secure hardware
- > Sustainability aspects in security and privacy engineering
- > Security assessment techniques

Objectifs (et/ou acquis d'apprentissages spécifiques)

The objective of this course is to provide insights on systems security with a focus on embedded systems. We focus specifically on software security in the Internet of Things and in Control Systems, and how computing equipment that is embedded into these systems can be securely integrated in the context of distributed systems engineering. Students will learn what software vulnerabilities are, how these vulnerabilities are exploited, and what development methodologies and security technologies are available to build sufficiently secure embedded systems.

The course strives to link theoretical knowledge with current industry practice and will feature a few interventions from guest lecturers who highlight and discuss recent industry trends, as well as a number of exercises and self-study tasks to provide hands-on experience and to deepen the students' knowledge on more specialised subjects.

The course is open to engineers/computer scientists from different backgrounds: computer sciences, computer engineering, telecommunications, and others.

Pré-requis et co-requis

Connaissances et compétences pré-requises

- > Understanding of processor architectures and computer systems
- > Understanding of operating systems, processes, memory management, concurrency
- > Programming skills, preferably some background in Rust/C/C++/Assembly

Méthodes d'enseignement et activités d'apprentissages

The course involves students in group projects to identify challenging problems in embedded systems security through extensive reading, practical challenges, and discussion.

Laboratories and self-study exercises include:

- > Exploration and exploitation of software-level vulnerabilities
- > Software fuzzing as a means to automatically detect vulnerabilities
- > Exploration of defensive techniques to harden embedded software
- > Research project on Internet of Things technology

Références, bibliographie et lectures recommandées

- > Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition, Ross Anderson, 2020: <https://www.cl.cam.ac.uk/~rja14/book.html>
- > Threat Modeling: Designing for Security, Adam Shostack, 2014: <https://shostack.org/books/threat-modeling-book>

Support(s) de cours

Université virtuelle

Autres renseignements

Lieu(x) d'enseignement

Solbosch

Contact(s)

Jan Tobias Muehlberg <jan.tobias.muehlberg@ulb.be>

Méthode(s) d'évaluation

Examen oral et Présentation orale

Examen oral

Question ouverte à réponse courte

Examen avec préparation

Langue(s) d'évaluation principale(s)

Anglais

Programmes

Programmes proposant ce cours à l'école polytechnique de Bruxelles

MA-IREL | **Master : ingénieur civil électricien** | finalité Spécialisée électronique et technologies de l'information/bloc 2 **et** MA-IRIF | **Master : ingénieur civil en informatique** | finalité Spécialisée/bloc 2

Programmes proposant ce cours à la faculté des Sciences

MA-SECU | **Master en cybersécurité** | finalité Conception et Analyse de Systèmes/bloc 1 et finalité Erasmus Mundus joint master in Cybersecurity (CYBERUS)/bloc 2

