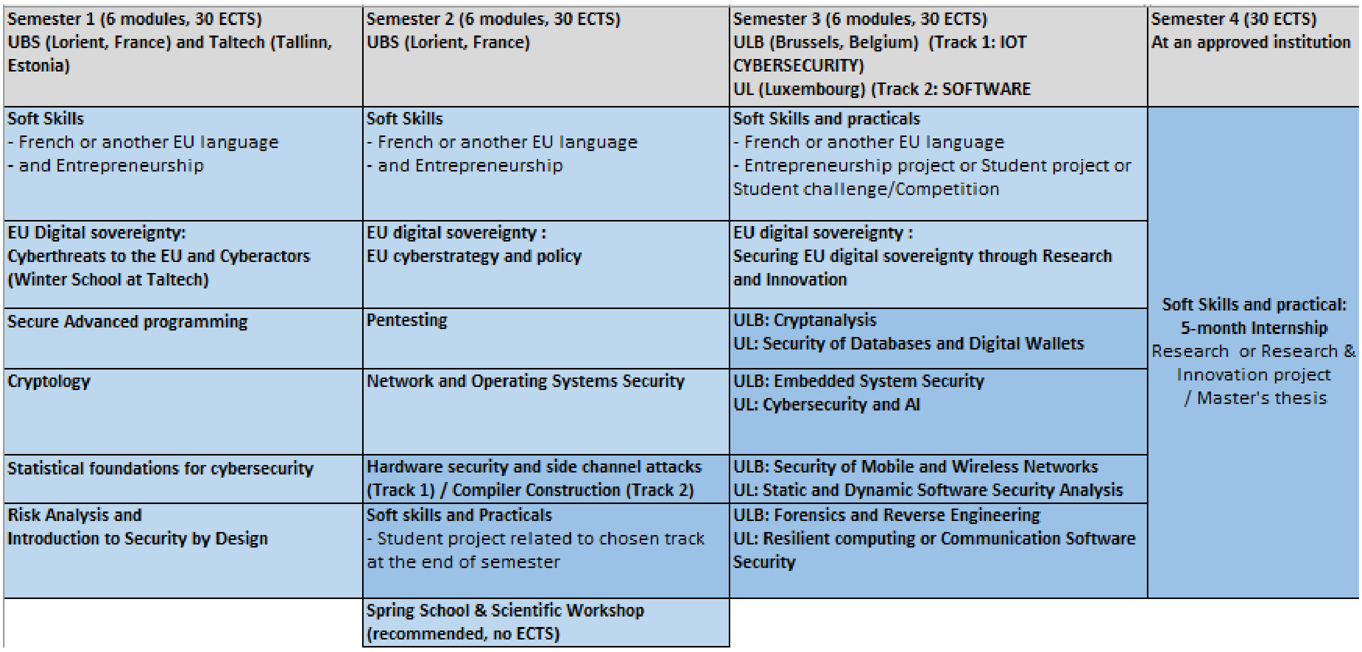
CYBERUS Syllabus

General structure of the programme



Semester 1 (6 modules, 30 ECTS) UBS (Lorient, France) and Taltech (Tallinn, Estonia)	Semester 2 (6 modules, 30 ECTS) UBS (Lorient, France)	Semester 3 (6 modules, 30 ECTS) ULB (Brussels, Belgium) (Track 1: IOT CYBERSECURITY) UL (Luxembourg) (Track 2: SOFTWARE	Semester 4 (30 ECTS) At an approved institution
Soft Skills - French or another EU language - and Entrepreneurship	Soft Skills - French or another EU language - and Entrepreneurship	Soft Skills and practicals - French or another EU language - Entrepreneurship project or Student project or Student challenge/Competition	Soft Skills and practical: 5-month Internship Research or Research & Innovation project / Master's thesis
EU Digital sovereignty: Cyberthreats to the EU and Cyberactors (Winter School at Taltech)	EU digital sovereignty : EU cyberstrategy and policy	EU digital sovereignty : Securing EU digital sovereignty through Research and Innovation	
Secure Advanced programming	Pentesting	ULB: Cryptanalysis UL: Security of Databases and Digital Wallets	
Cryptology	Network and Operating Systems Security	ULB: Embedded System Security UL: Cybersecurity and AI	
Statistical foundations for cybersecurity	Hardware security and side channel attacks (Track 1) / Compiler Construction (Track 2)	ULB: Security of Mobile and Wireless Networks UL: Static and Dynamic Software Security Analysis	
Risk Analysis and Introduction to Security by Design	Soft skills and Practicals - Student project related to chosen track at the end of semester	ULB: Forensics and Reverse Engineering UL: Resilient computing or Communication Software Security	
	Spring School & Scientific Workshop (recommended, no ECTS)		

Co-funded by
the European Union

UBS (Semester 1)

1. Entrepreneurship (mandatory)

Description:
This course extends over 3 semesters. It constitutes a half-module each time. It is compulsory in semesters 1 and 2. In semester 3, it is an elective and much like a student project.
There is no prerequisite. Students are deemed to have little or no knowledge of entrepreneurship.

Objectives:
The aim of this course is to introduce students to entrepreneurship and business considerations:
Understand management concepts and practices.
Understand business environments and legal frameworks.
Command tools (business plans, financial statements, risk analyses, indicators).
Understand marketing strategies.
Identify the elements of success of entrepreneurial ventures.

Learning outcomes:
Analyze business environments in order to identify business opportunities.
Evaluate the effectiveness of different entrepreneurial strategies.
Specify the basic performance indicators of entrepreneurial activity.

2. Secure Advanced Programming (mandatory)

Description:

For this course we consider knowing how to program as a prerequisite. An essential element for secure coding is a good knowledge of the standards and best practices, associated with the language used, which serve this objective.

This course introduces the first fundamentals to a secure development. This is the reason why it is in the first semester. Information technologies rely on software applications that need to be designed with care and have software vulnerabilities in mind.

Objectives:

New technology always introduces new security risks. Security concerns for modern operating systems (which are arguably more secure) or traditional desktop operating systems are not always well understood. In fact, problems can still appear when we don't carefully consider security during development. Data storage, inter-app communication, proper usage of cryptographic APIs, and secure network communication are only some of these considerations.

The aim of this course is to master the rules of good practice for secure coding and good knowledge on software vulnerabilities. Thus, making students able to produce code free from any exploitable vulnerabilities.

The standards learned target not only the security of the produced applications, but also other properties such as safety, reliability, resilience, etc. Before developing skills in software security, it is mandatory that students master secure software programming. This is the goal of this course.

Learning outcomes:

Develop secured applications.

Co-funded by
the European Union

3. Applied cryptography (mandatory)

Description:
Cryptology is one of the pillars for data security. Students will be taught algorithms providing authentication, integrity, and confidentiality using cryptography. This course covers basic concepts in cryptography including encryption/decryption, sender authentication, data integrity, non-repudiation, attack classification, secret key cryptography and public key cryptography.

Objectives:
The aim of this course is to provide students with knowledge to understand cryptographic algorithms and protocols and to understand cryptanalysis concepts.
The courses will be focused on applied cryptography, through different points of view:
Discover and understand some cryptographic algorithms from algorithmic aspects to implementations
Acquire a culture in the field of security Confidentiality, Integrity, Authentication, Non repudiation...
Understand their implementation and their complexity in hardware and software

Learning outcomes:
The ability to understand main cryptographic concepts and algorithms.
To understand the needs of clear security needs and corresponding cryptographic algorithms and protocols.
Hands-on experience of implementing main cryptographic primitives (symmetric encryption, hashing functions, asymmetric encryptions…) using Python.

Co-funded by
the European Union

4. Statistical Foundations for Cybersecurity (mandatory)

Description:

Supervised and unsupervised statistical tools are fundamentals to develop strong security analysis and to allow extensive security evaluation of information technologies. This course provides students with fundamental mathematical tools to allow them develop strong skills in machine learning, deep learning and big data applied to cybersecurity.

Objectives:

The aim of this course is to understand theoretical concepts required to develop and evaluate statistical approaches. This course will introduce statistical modelling, parametric estimation, nonparametric estimation and resampling, supervised learning, algorithms for regression, classification algorithms and applications of machine learning for cybersecurity.

Learning outcomes:

Students will be able to develop applications using statistical approaches and to analyze the quality of the results (precision, accuracy, robustness…).

Co-funded by the European Union

5. Risk Analysis and Introduction to Security by Design (mandatory)

Description:

The aim of risk analysis is to identify and understand the digital risks associated with a system. It makes it possible to determine the security measures adapted to the threat and to set up the framework for monitoring and continuous improvement. In software development, this analysis is associated with the requirement analysis and specification stage. In this course, we will visit two well-known risk analysis methods: EBIOS from ANSSI and SP 800-30 from NIST.

Regarding Security by design, in this course, we will revisit software development lifecycle to introduce the security concepts associated with each stage in order to build a secure software development lifecycle. This forms the basis of the "Secure by Design" concept.

Objectives:

The objective of the risk analysis course is to identify and understand the digital risks associated with a system.

The objective of the secure by design course is to master the stages of the secure software development life cycle for the objective of "Secure by Design".

Learning outcomes:

Students will be able to formalize the application's requirements in accordance with the adequate level of security.

Co-funded by the European Union

6. EU Digital sovereignty: Cyberthreats to the EU and Cyberactors (mandatory)

Description:
This course is organized by TalTech in Tallinn, Estonia (winter school taking place in January). Students spend two weeks where they follow several seminars and hands-on. They also conduct a research topic during the two weeks with an oral defense.

Objectives:
The winter school addresses the following topics: Introduction to international relations, Estonian cyber security since 2007, Low hanging Fruits in malware related incident handling, Cybersecurity and international law, Introduction to Digital Forensics, Modelling the cyber operational environment, The electromagnetic environment Influence operations, Open-source monitoring solutions for building SOC, TalTech Maritime Academy (visit), CCDCOE and CR14, Incident management, Open source intelligence and threat intelligence, Hacker mindset, Cyberphysical systems

Learning outcomes:
Students have a good evaluation of cyberthreats and cyberactors. This will increase their capacity to evaluate risk and actors in the domain of cyberdefense.

Co-funded by the European Union

UBS (Semester 2)

7. Entrepreneurship (mandatory)

Description:
This course extends over 3 semesters. It constitutes a half-module each time. It is compulsory in semesters 1 and 2. In semester 3, it is an elective and much like a student project.
There is no prerequisite. Students are deemed to have little or no knowledge of entrepreneurship.

Objectives:
The aim of this course is to introduce students to entrepreneurship and business considerations.
Understand management concepts and practices.
Understand business environments and legal frameworks.
Command tools (business plans, financial statements, risk analyses, indicators).
Understand marketing strategies.
Identify the elements of success of entrepreneurial ventures.

Learning outcomes:
Analyze business environment in order to identify business opportunities.
Evaluate the effectiveness of different entrepreneurial strategies.
Specify the basic performance indicators of entrepreneurial activity.

Co-funded by the European Union

8. EU Cyberstrategy and Digital Sovereignty (mandatory)

Description:

Cyberus students will acquire an introductory understanding of contemporary cybersecurity through a historical, legal and political science approach, using the EU as an example. From this foundation, they will have developed a better knowledge of the main concepts related to cyber, including those related to societal transformations – including personal data protection – and the influence on international relations – particularly states strategies inflection and the evolution of the notion of sovereignty in the digital realm – while focusing on an intercultural approach in order to better understand their future technical and non-technical interlocutors.

The course can be delivered on site and online. There is no prerequisite. Students will have little or no knowledge of EU Cyberstrategy and Policy. This course is about understanding where the EU and its member states stand vis-à-vis cyber threats.

Objectives:

The objective is to enlarge the students' perspective so that they do not consider cybersecurity just as a technical object but also as a phenomenon that impacts societies, countries and international organizations. This enlargement will be based more particularly on the EU example which can be considered (or not) as building its own cybersecurity specific path and through this path gaining global influence.

The aim of this course is to introduce students to the policies and strategies of the EU and its member states.

What are their strategic and legal texts, what tools have they designed, do they have strategies, how are they organize, who makes decisions? And how do they compare with other countries?

Learning outcome:

Cyber aspects in their individual and collective dimensions will be addressed.

Each section of this module will also have allowed students to improve their level of knowledge and reflection, having debated, presented issues and made a least one presentation on a specific topic as a group project.

As regards intellectual and transferable skills for all course sections, students will be able to:

- engage critically with a wide range of concepts and ideas relevant to cyberspace.
- exercise informed and independent critical judgment.
- communicate effectively and fluently in written and oral assignments.
- demonstrate abilities in primary and secondary research.
- find relevant information.
- advise top management on legal frameworks.
- make ethical decisions.
- balance risks in choice of technologies and suppliers.

Co-funded by
the European Union

9. Pentesting (mandatory)

Description:

The Pentest is the task to be carried out before deploying software in its execution environment, to verify that it does not contain exploitable flaws. This course aims to implement the techniques used during a penetration test service. Both on technical aspects (recognition, web intrusion, elevation of privileges, pivoting and intrusion of active directory) and business aspects (documentation of traces and audit evidence, client feedback). Moreover, this course will introduce the semantic Pentesting approach. For this, we will visit the design stage to introduce the notion of malicious cases, whose construction requires techniques based on adversarial thinking. The malicious cases will serve as the base for the semantic pentesting.

Objectives:

The objective is to master the principles and the different types of Pentest, process and organization, customer expectations, certifications, trace records and report writing.

Learning outcomes:

With this course, students will be able to carry out the Pentest before the application is deployed, but also to achieve certifications carried out through tests which are similar to the Pentest.

Co-funded by the European Union

10. Network and Operating Systems Security (mandatory)

Description:

Operating systems are omnipresent in computer systems and in the context of embedded systems, they have also been used for a long time (router, set-up-box, cars, …). There are several types of operating systems to study.
We have chosen to illustrate the concepts of security and hardening through the example of a Linux OS in the context of an embedded system. Consequently, this course is dedicated to Linux embedded system security.

Objectives:

The aim of this course is to allow students having a deep understanding of Linux operating system for embedded system, their security concerns and how to enforce security to build secured embedded systems.
The first objective is to introduce different concepts of Linux OS to harden a system.
It focuses precisely on the boot phase and on basic security concepts (DAC, MAC, …).
The second objective is to learn how to apply the principle of defense in depth for a Linux embedded system.
It focuses precisely on the principle of partitioning application services (cgroup, namespaces, capabilities, seccomp, containers) and defense in depth.
The third objective is to introduce different concepts related to audit, test/compliance and remediation.

Learning outcomes:

At the end of this course the student will be able to:

- understand and apply the principle of surface reduction of attack,
- understand and apply the principle of the least privileges,
- understand and apply secure administration procedures,
- understand and apply the principle of isolating application services,
- understand and apply the principle of defense in depth,
- understand and apply a consistent event logging policy,
- understand and apply a test/compliance policy.

Co-funded by the European Union

11. Hardware security and side-channel attacks (mandatory Track 1)

Description:
Hardware components are assembled to build information systems. Their security is a big issue as they can face several threats like side-channel (using timing, power consumption analysis, electromagnetic analysis) and fault injection attacks (using glitch on power supply or clock, electromagnetic radiation, laser shot). Thus, it is mandatory that any students have minimum skills to understand that hardware is not a secure black box but has its own vulnerabilities that need to be addressed. Students will understand how hardware can leak some information and how it can be attacked and what are existing countermeasures. Moreover, they will understand how to build a complete embedded system considering security properties such as firmware integrity and software isolation relying on hardware features.

Objectives:
The aim of this course is to allow students understand hardware vulnerabilities in order to develop countermeasures against side-channel and fault injection attacks. This course also introduces how to build Random Number Generators (RNG) and secure embedded systems. Students will be able to evaluate the security of an embedded system and to implement software and hardware countermeasures.

Learning outcomes:
Students will be able to implement hardware and software solutions against physical and software attacks targeting hardware architectures.

Co-funded by the European Union

12. Compiler Construction (mandatory Track 2)

Description:
An important element in the culture of a computer scientist is the mastery of the theory of programming languages and compilation process. This mastery becomes crucial for those who must build secure software systems. Indeed, it is necessary to know how the code written by the programmer is transformed into executable code in order to make the right decisions in terms of security. This is amplified by the fact that engineers often have to build Domain Specific Languages (DSL) to address specific problems in a formal way.

Objectives:
Students must master the programming language production chain, whether textual or graphical, from the specification to the compiler.

Learning outcomes:
Students should be able to detect security flaws originating from the compiler, but also be able to build a secure DSL.

Co-funded by the European Union

UL (Semester 3)

Code	Title	Credits ECTS	Semester	Validation	Compensation	Language	Type
Semester 3 organized by the University of Luxembourg - Software Cybersecurity specialization							
CYBERIUS-113	Soft Skills and practical	5	3	Obligation	Oui	Ang	Cours
CYBERUS-114	EU Digital sovereignty: Cyberthreats to the EU and Cyberactors	5	3	Obligation	Oui	Ang	Cours
CYBERUS-115	Cybersecurity and AI	5	3	Obligation	Oui	Ang	Cours
CYBERUS-116	Security of Databases and Digital Wallets	5	3	Obligation	Oui	Ang	Cours
CYBERUS-117	Static and dynamic software security analysis	5	3	Obligation	Oui	Ang	Cours
CYBERUS-118	Resilient Computing	5	3	Option	Oui	Ang	Cours
CYBERUS-119	Communication Software Security	5	3	Option	Oui	Ang	Cours
Semester 4 organized by Université de Luxembourg and Université Libre de Bruxelles							
CYBERUS-130	Soft Skills and practical: 5-month Internship and Master Thesis	30	4	Obligation	Non	Several	Stage

1. CYBERIUS-113 Soft Skills and practical: Entrepreneurship (mandatory)

Description:

The course will cover the following topics: Entrepreneurship in general, entrepreneurial personalities, business planning, lean startup, entrepreneurial marketing, entrepreneurial finance, entrepreneurial growth, entrepreneurial exit, select types of entrepreneurship (e.g., social entrepreneurship, sustainable entrepreneurship). The course also features case studies, in which students will apply the concepts of the lecture to real business cases, preferably from the cybersecurity sector.

Objectives:

The course provides a bird's-eye view of important fundamentals of entrepreneurship.

Learning outcomes:

Ability and skills to understand and critically evaluate business problems from the perspective of entrepreneurship; deep knowledge on the entire startup process (from ideation to venture exit); evidence-based insights on entrepreneurship rooted in latest research insights; ability to apply these insights in real-world case studies that feature highly relevant problems and their solutions.

2. CYBERUS-114 EU Digital sovereignty: Cyberthreats to the EU and Cyberactors (mandatory)

Description:

This course addresses the following topics:

Introduction to EU’s framework for digital sovereignty – tools, mechanisms, and actors; Chips market: the Chips Act as a mean to secure EU digital sovereignty; 5G infrastructure deployment: geopolitical and legal challenges; Digital infrastructure sharing imperative: perspectives on an EU Cloud; Software and software development: issues of liability in the context of automated processes/decisions; Artificial Intelligence (AI): opportunities and challenges for the EU digital sovereignty; Blockchain and Distributed Ledger Technologies: beyond the hype – socio-economic and legal perspectives for the EU digital sovereignty; Quantum technologies: securing strategic autonomy through quantum R&D; Data protection: General Data Protection Regulation (GDPR) as a flagship regulation for a digital sovereign EU; Digital services: the Digital Services Act for a safe and accountable online environment; Digital Markets Act: a bid for fairness towards and between ‘gatekeepers’?; European Digital Identity: the idea of a personal digital wallet for EU citizens and residents; Intellectual property: towards a harmonized EU patent rules to boost innovation, investment, and competitiveness; Beyond efficiency and legal niceties: Ethics and technology.

Objectives:

Analyze EU’s 'digital sovereignty' i.e. EU's ability to act independently in the digital world. This means studying protective mechanisms and offensive tools designed by the EU to foster digital innovation (including in cooperation with non-EU companies) as well as related challenges.

Learning outcomes:

Students will be able to:

(i) Identify and explain different levers used by the EU for its digital sovereignty (notably economic and legal (normative) levers);

(ii) breakdown legislative acts and proposals that aim at implementing EU’s digital sovereignty;

(iii) understand different UE budgetary instruments (including actors) to finance Research and innovation;

(iv) describe strategic technological innovation for EU’s digital sovereignty;

(v) explain challenges to EU’s digital sovereignty and suggest solutions;

(vi) discuss ethics and technology.

Co-funded by the European Union

3. CYBERUS-115 Cybersecurity and AI (mandatory)

Description:

This course addresses the following topics:

- Introduction to machine learning security and offensive AI / Basic tool setup
- Evasion attacks on computer vision systems, white-box and black-box threat models, transferability
- Malware detection using AI and its pitfalls / Introduction to the end of year project
- Dense task security with application to healthcare and autonomous driving
- Tabular attacks in constrained domains, with application to financial systems
- Attacks on NLP model / Escape game
- Privacy of AI systems / Detection of generated content
- Distribution drifts
- Poisoning attacks
- Attacks on biometrics systems
- Certified robustness
- Regulations and auditing

Objectives:

The objective of the course is to make the students familiar with the quality and security threats to AI systems, especially in light of (European) regulations. The course generally introduces the students to the foundations of security attacks, but enables also the manipulation of the related concepts through experiments (via Jupyter notebooks). The covered topics include: evasion attacks on computer vision, tabular data, NLP models; poisoning attacks; privacy concerns and threats; distribution drifts, presentation attacks on biometric systems, vulnerabilities in AI-based malware detectors, certifiable robustness, detection of generated content, regulation and auditing, etc. The course sessions will feature ex-cathedra presentations from the teaching team and external speakers, focused discussions, hands-on exercises, expert panels, paper reading and presentation by the students.

Learning outcomes:

Students understand the security concerns that AI system raised and the limitations of using AI systems for cybersecurity. Students can experiment on specific security attacks and defenses through the use of established Python libraries. Students can read advanced scientific papers and reproduce previous experiments. Students can have some understanding of the meaning and implications of regulations related to AI systems and their security.

Co-funded by the European Union

4. CYBERUS-116 Security of Databases and Digital Wallets (mandatory)

Description:

This course addresses the following topics:

1. Introduction and Motivation; Cryptographic building blocks
   a. Digital wallets (Gilbert FRIDGEN)
   - Custodial vs. non-custodial wallets
   - Metamask
   - Cold vs. hot wallets

   b. Cryptographic building blocks (Johannes SEDLMEIR)
   - Symmetric and asymmetric encryption
   - Digital signatures, digital certificates, and the Internet PKI
   - Hashing, Merkle trees & Merkle proofs
   - Trusted hardware and secure elements
   - Elliptic curves, pairings, and BLS signatures

2. Digital identity wallets (Johannes SEDLMEIR)
   a. Challenges of fragmented and federated identity management
   b. Roles: Issuer, holder, and verifier
   c. Revocation and trust registries
   d. Demo: Lissi
   e. Machine-in-the-middle attacks and mitigations
   f. Secure key management and recovery
   g. Can we trust our phones?
   h. User experience

3. Foundations of zero-knowledge proofs (Johannes SEDLMEIR)
   a. Proof systems: Key definitions
   b. From graph three coloring to “everything is provable in zero-knowledge)
   c. Polynomial commitment schemes (PCS) □ Examples: KZG, FRI
   d. Interactive oracle proofs (IOPs) □ Examples: R1CS and PlonKish arithmetization
   e. zk-SNARKs from PCS and IOPs
   f. The Cambrian explosion of SNARKs
   g. Custom gates
   h. Recursion and proof composition

4. Anonymous credentials (Johannes SEDLMEIR)
   a. Privacy challenges in digital identity wallets
   b. Hardware-based solutions and landscape
   c. Software-based solutions and anonymous credentials
   d. Anonymous credential constructions based on special-purpose ZKPs

e. Anonymous credential constructions based on general-purpose ZKPs
f. Designated verifier proofs

5. Foundations of blockchain (Johannes SEDLMEIR)
a. Why blockchain?
b. From replicated state machines to cryptocurrencies
c. Consensus mechanisms
d. Smart contracts
e. Energy consumption
f. Attacks on proof of work (PoW) and proof of stake (PoS)
g. (De-) Centralization layers and PoW vs PoS security

6. Addressing key challenges of blockchain (Johannes SEDLMEIR)
a. Privacy solutions: Concepts (zero-knowledge proofs, multi-party computation, homomorphic encryption) and solutions (e.g., TornadoCash)
b. Scaling solutions (payment channels, optimistic and zk-rollups, bridges, stateless clients and Verkle trees, data availability sampling, succinct blockchains)
c. Implications of these constructions on system design and user experience

7. Decentralized finance (Johannes SEDLMEIR)
a. Coding-Session with Solidity/Remix
b. Token standards
c. Liquidity pools
d. Survey of DeFi applications
e. Flashloans, Oracles & DeFi attacks
f. Miner extractable value

8. Paper discussion: Privacy and compliance in mixers and central bank digital currencies (Johannes SEDLMEIR)
a. A history of digital cash: From e-Cash to Zcash
b. Software vs. hardware-based solutions
c. CBDCs
d. Sanctions lists
e. Money Mules and the role of digital identities

Objectives:

Getting familiar with technical and organizational foundations of digital wallets used in digital identity management and blockchain-based decentralized digital information systems:

(1) Cryptographic primitives (e.g., hashing, Merkle trees, digital signatures, zero-knowledge proofs), hardware security, and how they are used in digital identity management systems, blockchains, and the corresponding digital wallets that users and organizations use to interact with these systems,

(2) Deep dive into the constructions and applications of cryptographic proof systems, including zero-knowledge proofs to improve users' and organizations' control over data disclosure (e.g., in the form of anonymous credentials based on zero-knowledge proofs,
(3) Misconceptions about digital identities and blockchains,
(4) Security issues and attacks on these systems and how to mitigate them,
(5) User perspectives with regard to adoption of these technologies and in particular their interaction through digital wallets.

Learning outcomes:
Students can identify application areas of digital wallets and the corresponding decentralized information systems, detect potential design flaws and conceptualize appropriate solutions based on the cryptographic building blocks they learned, consider security threats and countermeasures, and are aware of common pitfalls from a user perspective.

Co-funded by the European Union

5. CYBERUS-117 Static and dynamic software security analysis (mandatory)

Description:
Software, whether developed by skilled programmers at the premises of Tech giants, or collaboratively produced in an open-source setting, will often include vulnerabilities. To address such vulnerabilities, scanners can be programmed that statically check software code for known rule violations or for dynamically exercising the app to detect exploitable behaviour. Such analyses techniques are at the core of most security assessment tools, and their reliability is essential to increase confidence in the software deployed in enterprise.

Objectives:
Through this course, the student will learn the fundamental theoretical concepts and techniques of static analysis. The student will be able to use this knowledge to implement static analyses to solve concrete security problems. In a second, smaller part of the course, the student will learn how to dynamically analyse programs with fuzzing.

Learning outcomes:
- The student should be able to critically read publications related to static and dynamic analysis (research paper, etc.)
- The student should be able to select an adapted approach to solve a specific static analysis problem
- The student should be able to implement static analysis techniques
- The student should be able to run a fuzzer.

Co-funded by the European Union

6. CYBERUS-130 Soft Skills and practical: 5-month Internship and Master Thesis

Description:

The end of Master thesis gives is a personal, detailed and in-depth work in line with current research. An original contribution is expected. You will need to find an academic promoter to supervise your work. The promoter can suggest a topic or, if he or she agrees, you can choose the theme yourself. The thesis should be around 80 pages of polished text.

The internship provides the student with a full-time experience in cybersecurity by working with a participating employing firm, organization or academic research center. The student will be supervised by a faculty member acting as a liaison between the University and the employing organization.

Objectives:

Autonomous work based on feedback given by an academic supervisor.

Learning outcomes:

Master Thesis:

- Master complex subjects in line with current researches
- Autonomous work
- Correct exploitation of the results in the literature
- Write a clear text describing in detail the state of the art, as well as the personal contributions
- Cite existing literature correctly

Internship:

- Practical experiences

Co-funded by the European Union

Elective

7. CYBERUS-118 Resilient Computing (elective)

Description:
This course gives an overview of the fundamental design principles and protocols for the construction of fault and intrusion tolerant and cyber-resilient systems. The course serves as an introduction to the field and its concepts. It prepares to pursuing research in resilient computing or a related field (e.g., master projects or PhD theses). Concrete topics include:

- Introduction and taxonomy of faults;
- Consistency in the presence of faults;
- Group communication;
- Replication;
- Homogeneous byzantine fault tolerant protocols;
- Hybrid protocols;
- System-level aspects;
- Rejuvenation and Recovery.

Objectives:
This course aims at providing students with the knowledge necessary to construct systems that can tolerate and safely and securely operate through systems that have partially failed due to accidental reasons or that have partially been compromised.

Learning outcomes:
Understand fundamental limitations of fault and intrusion tolerant systems;
Analyse a specific system structure and propose a fault and intrusion tolerant alternative;
Knowledge in the construction of fault and intolerant systems and the protocols that govern their execution.

Co-funded by the European Union

8. CYBERUS-119 Communication Software Security (elective)

Description:

This course offers a comprehensive introduction and a small dive into the subject, structured over a semester with a blend of lectures, labs, and presentations. Each session is designed to build on the knowledge from the previous weeks, fostering a robust understanding and practical skills. The course is designed to not only provide foundational knowledge but also to engage students in active learning through quizzes, practical labs, presentations, and paper reviews. It aims to prepare students for advanced studies in the field and real-world applications.

Objectives:

- Familiarise with the intersection of cybersecurity and software-defined networking
- Grasp the foundational concepts of software-defined networking.
- Comprehend the distinction between the data plane and the control plane in SDN.
- Delve into SDN programming methodologies and techniques.
- Explore the diverse applications and use cases of software-defined networks.
- Recognize and assess the vulnerabilities and potential threats inherent to SDN.
- Implement strategies and measures to safeguard the SDN infrastructure
- Explore the security advantages of adopting SDN in modern network architectures.

Learning outcomes:

- Articulate the key components of SDN and their respective functions.
- Compare and contrast SDN security approaches with traditional network security methodologies.
- Illustrate the relevance and deployment of SDN in contemporary networking contexts.
- Evaluate the inherent security features and vulnerabilities of software-defined networking.
- Demonstrate proficiency in identifying and addressing SDN-specific security challenges.
- Critically analyse potential threats of SDN security and recommend preventative measures to ensure data integrity.

Co-funded by the European Union

ULB (Semester 3)

Mandatory

ELEC-H-423	Mobile and wireless networks	
ELEC-H-550	Embedded System Security	
INFO-Y-119	Forensics and Reverse Engineering	
INFO-F-537	Cryptanalysis	
MEMO-F-543	Master thesis and internship in cybersecurity	
LANG-F-XXX	LANG-Y9001	Français langue étrangère - Niveau A0 (F9)
	LANG-Y9011	Français langue étrangère - Niveau A1 (F9)
	LANG-Y9021	Français langue étrangère - Niveau A2 (F9)
	LANG-B9101	Français langue étrangère- Niveau perfectionnement
	LANG-B9061	Français langue étrangère – Niveau moyen 1
	LANG-F301	Anglais scientifique II

1. ELEC-H-423 Mobile and wireless networks (mandatory)

Description:

The course follows two objectives: 1) knowledge of advanced networking architectures (TelCo and IoT) and 2) understanding of the security of mobile and wireless architectures from the physical layer to the architecture as a whole.

It complements the course of networks and investigates the challenges related to the state-of-the-art wireless architectures. Novel security techniques are presented in the course protocols, cryptanalysis and mathematical cryptology. The course is supported by external speakers (researchers from the industry) and the research conducted at the ULB Cybersecurity Research Center.

Objectives:

This course will cover the fundamental aspects of wireless networks, with emphasis on current and next-generation wireless networks. The course should provide the students with a good understanding of the wireless networking concepts and research directions. We will also look at industry trends and discuss some innovative ideas that have recently been developed.

The course provides a solid understanding of the design and analysis of network security architectures, protocols, and services. Most of these protocols are based on cryptographic primitives and can be used as building blocks for more sophisticated networked systems. During the course, we will perform an in-depth coverage of today's network security standards, their functionality and limitations e.g., SSL/TLS, Kerberos, IPsec, Radius, IEEE 802.1x, WPA, etc. Furthermore, the students will acquire a practical knowledge and experience in deploying, configuring, and analyzing current network security tools and protocols. We will also discuss recent trends in network security attacks, and cyber-attacks in general, and analyze variety of attacks with in mind mobile and wireless specificities.

Learning outcomes:

- To understand the fundamentals of cellular communication, mobile radio propagation, cellular engineering, multiple access techniques, mobility support, channel allocation, mobile ad-hoc networks, sensor networks, Internet of Things.
- To get involved in research projects on advanced topics in IoT, and be able to present and write high quality technical reports on protocol design, analysis and simulation.
- To learn how to read and review publications in the wireless networking field.

2. ELEC-H-550 Embedded System Security (mandatory)

Description:

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.

Objectives:

- The information security landscape and the 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

Learning outcomes:

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

- 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

Co-funded by the European Union

3. INFO-Y-119 Forensics and Reverse Engineering (mandatory)

Description:

Reverse engineering is generally accepted as reviewing the disassembled code of a potentially malicious binary, or piece of malware, usually using a disassembler or hex editor, to gain a better understanding of how a binary function operates when executed. This type of analysis is geared toward capturing the behavioral aspects of the malicious binaries as they are executed in a controlled environment. Analytical information such as environment changes (file, system, network, process, etc.), communication with the rest of the network, communications with remote devices, and so on are closely observed for actionable information. This information is analyzed, and a complete picture is reconstructed as to what the binary is doing to a computer when executed. It is important to extract information from the malware that can be used to establish actionable information.

Objectives:

Emphasis is placed on analyzing the way the malware interacts with any associated networks, identifying the type of information being targeted, and finding commonalities with previously analyzed malware. Although not always known, features such as vulnerabilities exploited are of interest and are identified as possible malware infection vectors.

Homework labs will be provided to students over the course to allow students to apply the methods discussed in class. These assignments will be provided in class and announced via the course website. Homework assignments are due two weeks following the assigned date.

The capstone of the class will consist of a student project that will presented and defended at the end of the semester.

Learning outcomes:

The objective of this course is to familiarize students with the practice of reverse engineering suspicious files by utilizing static and dynamic tactics, techniques, and procedures in order to gain an understanding as to what impact the suspicious file may have on a particular computer system when executed.

Co-funded by the European Union

4. INFO-F-537 Cryptanalysis (mandatory)

Description:

The course will cover advanced topics on cryptography, including advanced cryptographic protocols, advanced mathematical tools, cryptanalysis and applied cryptography. The course will be organized each year around one main theme, with several related theoretical and practical topics covered.

Examples of topics that could be covered include homomorphic encryption, zero-knowledge proofs, multi-party computation, cryptanalysis, quantum cryptography, post-quantum cryptography (lattices, codes, multivariate, isogenies), side-channel attacks, secure communication protocols (TLS, Signal, PGP), key management, trusted computing, secure machine learning).

Students will be encouraged to read and analyze cryptography research papers.

Objectives

The course will cover advanced topics on cryptography, including advanced cryptographic protocols, advanced mathematical tools, cryptanalysis and applied cryptography. It will also aim to introduce students to cryptography research.

Learning outcomes:

1. Use rigorous approaches to evaluate the security of cryptographic constructions.
2. Understand advanced mathematical tools used in cryptography protocols and cryptanalysis.
3. Describe advanced cryptographic protocols used for tackling contemporary security problems.
4. Identity limitations of formal security abstractions to capture real-world security protocols.

Co-funded by
the European Union

5. MEMO-F-543 Master thesis and internship in cybersecurity (mandatory)

Description:
The end of Master thesis gives is a personal, detailed and in-depth work in line with current research. An original contribution is expected. You will need to find an academic promoter to supervise your work. The promoter can suggest a topic or, if he or she agrees, you can choose the theme yourself. The thesis should be around 80 pages of polished text.
The internship provides the student with a full-time experience in cybersecurity by working with a participating employing firm, organization or academic research center. The student will be supervised by a faculty member acting as a liaison between the University and the employing organization.

Objectives:
Autonomous work based on feedback given by an academic supervisor.

Learning outcomes:
Master Thesis:

- Master complex subjects in line with current researches
- Autonomous work
- Correct exploitation of the results in the literature
- Write a clear text describing in detail the state of the art, as well as the personal contributions
- Cite existing literature correctly

Internship:

- Practical experiences

Co-funded by the European Union

Electives

GEST-S-482	The digital firm
GEST-S-706	Entrepreneurship
INFO-F-409	Learning dynamics

6. GEST-S-482 The digital firm (elective)

Description:

Over the past five years, the increase in market capitalization of the five largest digital companies (the GAFAM) has exceeded the total market value of the largest global CPG and retail firms. In 2020, the total turnover of these 5 companies alone more than doubled the total GDP of Belgium. Facebook generates 140 times more income per employee than Walmart. Clearly, digital businesses run on a very different type of software. Digital technology and business are now so deeply interwoven, that it no longer makes sense to talk about one without talking about the other. Yet few business leaders are IT-savvy and few IT experts fully grasp the strategic and organizational impact of technology. This course aims at bridging this gap. More specifically, its core objective it to provide an overview of information systems (IS) and digital technologies (Digital), and their impact on the organization and strategy of firms and institutions. It is therefore meant to introduce the role of CIOs (Chief Information Officer) and CDOs (Chief Digital Officer), enriched with practical exercises ("Hands-On Digital") to understand and experience digital technology from the inside.

Objectives:

The first part of the course, "Digital Technology and the Organization", is structured around the notion of an operational model of the firm's activities, which is defined by its core processes. These processes are characterized by their degree of standardization and integration, which determine the extent to which workflows need to be harmonized and codified (process standardization) and data needs to be shared (process integration). This leads us to base the course on data modelling (Entity-Relationship Diagrams or ERD) on the one hand, and process modelling (Business Process Modeling and Notation or BPMN) on the other. Information Systems are technologies supporting the standardization, integration, and automation of business processes, thereby implementing and crystallizing the operational model of the firm. One chapter will review the main families of Information Systems and their functional scope. Given how IS and organizational processes are interwoven, deploying and exploiting IS requires strong change management. In business terms, one would say that information systems require strong complementary investments in organisational capital. One chapter of this first part will uncover why and how to deal with such change. Once implemented, Information Systems generate or capture data, which can inform management and strategy, a field called Business Analytics that will be introduced in the last chapter of Part I.

The second part of the course, "Digital Technology Management" looks at digital infrastructure. Information Systems (and digital technologies more broadly) run on a given infrastructure, which falls under the responsibility of the CIO. This infrastructure includes networks, servers, desktops and mobile devices, but also external resources (e.g. Cloud services) and security. It will lead to questions about IS Architecture and design choices. We will finally cover the roles of the CIO more broadly and specific challenges in IT and IS Management, with an emphasis on new challenges in highly digitized environments, such as business continuity planning, data governance, cyber criminality, and privacy.

The third part of the course, "Digital Technology and Strategy" will explore the impact of digitalization on firm competitiveness. It will examine the main categories of digitally-enabled business models: digital distribution channels (e-commerce and mobile commerce), data-driven strategies, and platforms, ecosystems and crowdsourcing (e.g. P2P and open source models). This part will focus on how incumbent firms may respond to digital disruption. The course will conclude with a discussion of the social and environmental impacts of digitalization.

Learning outcomes:

More specifically, at the end of the course students should be able to:

- identify and model business processes
- model relational enterprise data
- recognize and criticize the scope of typical IS applications
- produce simple code in Python to automate a simple business task
- analyze business data with SQL and Python
- identify key IT implementation challenges
- identify and describe high-level building blocks of information systems and infrastructure
- describe and criticize high-level IT architectures
- recognize and evaluate IT risks and priorities
- anticipate and leverage the impact of digitization on businesses
- describe the logic of typical digital business models

Co-funded by the European Union

7. GEST-S-706 Entrepreneurship (elective)

Description:

Entrepreneurship in the broadest sense of the term has always been at the heart of the renewal of the economic fabric and, in particular today, of the acceleration of the transition to a sustainable world. It is also an increasingly common means of personal development. There are an increasing number of examples of successful businesses created by entrepreneurs who are guided by their vision and conviction. Entrepreneurship is also at the heart of strategic thinking about organisation and innovation in larger companies, which want to remain or become more 'entrepreneurial' in order to cope with ever more rapid and unpredictable market changes.

Although there are many definitions of entrepreneurship, there is a consensus on a set of key ideas that will be discussed during the course:

- Entrepreneurship is about identifying, evaluating and exploiting new opportunities.
- Entrepreneurship is about starting with limited - sometimes non-existent - resources at hand.
- Entrepreneurship requires dealing with highly uncertain situations and having limited access to relevant quantitative data on future markets and trends.
- The typical entrepreneurial context is one where people do things that are new to the market (innovation) and/or new to them (first time).

Objectives:

The aim of the course is to present the best practices and key concepts in the creation (start-up) and development of young companies (scale-up) by highlighting the entrepreneur's toolbox through the discovery of effectuation, design thinking, lean start-up, business modelling, business planning, venture capital, etc. as well as the fundamentals of creation and growth strategies.

The aim is to broaden the scope of entrepreneurship and show how an 'entrepreneurial management' approach is also relevant to existing organisations.

More specifically, the course will focus on the characteristic elements of the entrepreneurial approach, i.e.:

- The entrepreneur, his characteristics, his motivations, etc.;
- The notion of opportunity and a method for assessing its quality;
- The development and implementation of a business plan;
- The search for resources (human and financial) which are very often absent when an opportunity is identified.

Throughout the course, the above concepts are analysed in different contexts and in different sectors.

Learning outcomes:

At the end of the course, each student should be able to:

1. evaluate an opportunity;
2. draw up a business plan for an idea to create a start-up or develop a scale-up;
3. understand the importance of entrepreneurial behaviour in different organisational settings.

Generally speaking, the course also enables students who are not planning to become entrepreneurs to understand and master the thinking and action logics that are relevant to all managers.

The notion of sustainable development is not at the heart of the course, but its implications in the context of entrepreneurship will be systematically addressed.

Co-funded by
the European Union

8. INFO-F-409 Learning dynamics (elective)

Description:

The course addresses the question how agents learn to act in environment where there are other agents also learning how to act. Hence it is a course on multi-agent learning.

We address this question from the perspective of the learning or adaptation algorithm, which can be:

- the perspective of an individual agent, where learning how to act occurs internally,
- the perspective of the collective, where one examines how the distribution of agent behaviours changes over time.

Objectives:

Essentially, we focus in the first perspective on the basis and state-of-the-art of multi-agent reinforcement learning and in the second perspective on evolutionary dynamics.

In the first 5-6 weeks of this course, the basis of game theory, evolutionary dynamics and multi-agent RL are explained.

In the second part we dive into a number of more advanced topics to expand the knowledge in these topics and to prepare you further for the exam work.

At the end of each theory session, if feasible, you will have the chance to play with some simple coding examples. These sessions will also include a number of assignments, that will be graded individually. The exam is the reproduction of a paper on the topic, for which you will provide a report and a presentation in the exam session.

Learning outcomes:

The students will learn the basic principles of both domains, the mathematical and computational methods and the typical problems they are trying to solve. The students will also obtain a basic understanding of (evolutionary) game theory which will allow them to understand the standard literature in that field and the relevance of this domain to learning in general. The students will obtain the skills to address independently problems within these fields. In addition, they will be capable of presenting their work to an audience of specialists and non-specialists.

Co-funded by the European Union