Advanced Security	14X040

Eduardo SOLANA (CC)

Nombre d'heures par semaine	cours	2	Semestre d'automne	
	exercices	-	Semestre de printemps	☒
	pratique	2/3*	Total d'heures	56/70*

Cursus	Type	Crédits ECTS
Master en sciences informatiques 90 ECTS	Option	4
Master en sciences informatiques 120 ECTS	Option	5

OBJECTIFS :

The Advanced Security course expands and deepens the concepts covered in the Information Systems Security course in the fall semester. It relies on a combination of theory and practice enabling students to assimilate the cryptographic foundations of current protocols and solutions and to become familiar with the professional aspects of cybersecurity. Finally, the students are confronted with a mini-project in the second part of the semester addressing a specific problem related to cryptography and/or selected topics of information security.

CONTENU :

- Foundations of modern cryptography: Deterministic and probabilistic encryption, indistinguishability, malleable cryptography and repudiability, known attacks on cryptographic protocols.
- Current cryptographic protocols: Cryptographic protection in social networks and remote conferencing solutions, cryptocurrencies, blockchain technology, e-voting schemes, ransomware cryptographic fundamentals, etc.
- Cloud security solutions and trends: Virtualization, protected execution platforms and secure enclaves, searchable cryptography, homomorphic cryptography, etc.
- Professional aspects of computer security: Description of common positions in the cybersecurity job market. The role of the Chief Information Security Officer (CISO).
- Project addressing multiple aspects of information security: The students are required to submit an individual written assignment blending theory and practice that will determine the final grade of the Advanced Security course.
- External experts from the corporate security world and the academia will present topics related to their domains of expertise.

Forme de l'enseignement	Theoretical and practical course
Documentation	List of reference books
Préalable requis	Required : Information Systems Security
Préparation pour	-
Mode d'évaluation	Written work
Sessions d'examens	J/AS