

Information Systems Security (ISS)			14X021	
Eduardo SOLANA (CC)				
Nombre d'heures par semaine	cours	2	Semestre d'automne	<input checked="" type="checkbox"/>
	exercices	2	Semestre de printemps	
	pratique	2	Total d'heures	84
Cursus		Type		Crédits ECTS
Master en sciences informatiques (120 ECTS)		Obligatoire		6

OBJECTIFS :

This course proposes a formal description of the main basic blocks of computer security, namely the cryptographic techniques together with a detailed analysis of the solutions commonly used in secure environments. It combines theoretical and practical aspects enabling the student to understand the issues of information security while presenting concrete and current solutions. The last chapter discusses the ongoing transition to non-perimeter protection as well as the new challenges associated with securing the cloud.

CONTENU :

- Cryptographic building blocks: symmetric and asymmetric encryption, cryptographic hash functions, Message Authentication Codes, digital signatures, etc.
- Digital identity management: authentication, privilege management, Federated Services, Single-Sign-On, securing cryptographic parameters (certificates, Active Directory, Trusted Platforms, Hardware Security Modules, etc.).
- Secure transactions: Key establishment protocols, SSL/TLS, Signal, trusted networks intra/inter domain, Kerberos, Public Key Infrastructures (PKI).
- Perimeter and perimeter-less security, from the PC to the cloud: Trusted
- Computing, network security topologies, virtualization, Cloud Security, etc.

Forme de l'enseignement	Integrated courses and exercises
Documentation	List of reference books
Préalable requis	required: basic knowledge of computer theory
Préparation pour	-
Mode d'évaluation	Oral
Sessions d'examens	JF/AS