EIIN906B	Blockchain and Privacy	CM 18h	TD 7h	HNE 25h

Cours proposé dans la mineure / *Course offered in the minor* :

AL	CyberSec	IA-ID	IHM	IoT-CPS	Ubinet	IF	M1 EIT DSC	M2 EIT DSC	M2 Fintech
	x				x		x	x	x

Responsable / *In charge of* : **Legout Arnaud** (Arnaud.LEGOUT@inria.fr)

Résumé / *Abstract* :

Distributed applications are used daily by tens of millions of users. They therefore constitute perfect candidates for large scale security attacks, whose goal is notably to obtain undue financial gains. We will also present state of the art solutions to integrity, which will notably be illustrated through the blockchain approach and its applications to applications, notably through smart contracts. Distributed applications also constitute perfect candidates for large scale privacy attacks, whose goal is to retrieve personal information on those users. Such situations have for instance been shown on popular application such as Skype, Tor, Bittorrent, Bitcoin. This course will also show how such attacks are possible, in particular through the exploration of poor design choices. We will also present large scale measurement techniques that can be used to perform privacy attacks in the Internet. We discuss the design principles that enable such attacks and present recent approaches to distributed security and privacy solutions

Prérequis / *Prerequisite* :

- Network, TCP/IP, Internet.
- Basic crytographie (symetric, asymetric encryption principles, signatures, etc.) is a plus, but not a requirement.

Objectifs / *Objectives* :

Master the basics of blockchains, understand how difficult it is to design private systems, learn privacy attacks to design more secure systems.

Contenu / *Contents* :

- Chaum networks
- Shamir shared secret
- Introduction to the concepts of privacy
- Description of privacy attacks (targeting Skype, Bittorrent, Tor, Bitcoin)
- Blockchains basics
- Bitcoin inners
- Distributed consensus
- Proof of work

Références / *References* :

- https://cel.archives-ouvertes.fr/cel-00544132/en/
- https://bitcoin.org/bitcoin.pdf

Acquis / *Knowledge* :

- How Tor works
- How shared secrets systems (with people with conflicting interests) works
- How bitcoin works
- How we define privacy
- How privacy attacks are designed and how to make systems more robust

Evaluation / *Assessment* :

50% final written exam grade on the privacy part, 50% lab grade on the blockchain part