CS-721 **Privacy at the communication layer**

Troncoso Carmela

Cursus	Sem.	Type
Computer and Communication Sciences		Opt.

Language of teaching	English
Credits	2
Session	
Exam	Multiple
Workload	60h
Hours	**40**
Lecture	26
Exercises	14
Number of positions	**20**

Remark

Not offered this year

Summary

In this seminar course students will get in depth understanding of mechanisms for private communication. This will be done by reading important papers that will be analyzed in the class. Students will also propose their own privacy attacks or defenses which can become a publication.

Content

Often, privacy is understood as keeping data secret with respect to unauthorized parties. To achieve this one can use cryptography to ensure confidentiality, or modern obfuscation techniques, such as differential privacy, to prevent adversaries from inferring values in a database. However, recent events, such as the Snowden revelations, have made it apparent that privacy goes beyond protecting data at the application layer. To ensure users' protection, so-called meta-data, for example communicating partners and communication time or frequency, must be also protected from adversaries.
The goal of this seminar is to provide students with the knowledge to understand the privacy threats related to metadata of communication, as well as give them tools to design and analyze protection mechanisms. Topics to be covered include:

- Low-latency and high latency anonymous communication systems
- Architectures and topologies: centralized, peer-to-peer, hybrid
- Routing strategies
- Dummy traffic strategies for creation and deployment
- Protecting protocols
- Censorship resistance

Every week of the course, students attending the seminar will read one relevant paper on the topics above, and they will provide a critical summary (a conference review like). Then we will discuss the paper in group, with two students leading the discussion: one defending and one criticizing the paper. Once a number of papers have been read and discussed in class, students will propose a project to either attack or defend communication privacy which they will develop individually or in pairs.

Keywords

Privacy, anonymous communications, censorship resistance

Learning Prerequisites

Required courses

Recommended to have an understanding of probablities and statistics, and notions of networking