Information theoretic Methods in Security

Prof. Nicola Laurenti[1]

[1] *University of Padova*
Department of Information Engineering
Email: nil@dei.unipd.it

Timetable: 20 hrs. (two lectures of two hours each per week). Class meets every Tuesday and Friday from 2:30 to 4:30, starting on Tuesday, November 11-th, 2014. Meeting Room DEI/G (3-rd floor, Dept. of Information Engineering, via Gradenigo Building).

Course requirements: Basic notions of Information Theory

Examination and grading: Each student must submit a project, and grading will be based on its evaluation. I encourage students to work from an information theoretic point of view on a security problem related to their research activities.

Aim: Provide the students with an information theoretic framework that will allow formal modeling, and understanding fundamental performance limits, in several security-related problems

Course contents: Topics will be chosen, according to the students' interests from the following list:

Measuring information. Measuring information. Review of basic notions and results in information theory: entropy, equivocation, mutual information, channel capacity.

The Holy Grail of perfect secrecy. Shannon's cipher system. Perfect secrecy. Ideal secrecy. Practical secrecy. The guessing attack.

Secrecy without cryptography. The wiretap channel model. Rate-equivocation pairs. Secrecy capacity for binary, Gaussian and fading channel models.

Security from uncertainty. Secret key agreement from common randomness on noisy channels. Information theoretic models and performance limits of quantum cryptography.

A different approach. Secrecy capacity from channel resolvability. Secret-key capacity from channel intrinsic randomness.

The gossip game. Broadcast and secrecy models in multiple access channels. The role of trusted and untrusted relays.

Secrets in a crowd. Information theoretic secrecy in a random network with random eavesdroppers. Secrecy graphs and large networks secrecy rates.

A cipher for free? Information theoretic security of random network coding.

Who's who? An information theoretic model for authentication in noisy channels. Signatures and fingerprinting.

Writing in sympathetic ink. Information theoretic models of steganography, watermarking and other information hiding techniques.

The jamming game. Optimal strategies for transmitters, receivers and jammers in Gaussian, fading and MIMO channels.

Leaky buckets and pipes. Information leaking and covert channels. Timing channels.

The dining cryptographers. Privacy and anonymity. Secure multiparty computation.

Information theoretic democracy. Privacy, reliability and verifiability in electronic voting systems.

Alea iacta est. Secure and true random number generation. Randomness extractors and smooth guessing entropy.

The Big Brother. An information theoretic formulation of database security: the privacy vs utility tradeoff.

References:

1. Y. Liang, H.V. Poor, and S. Shamai (Shitz), Information Theoretic Security, Now, 2007.

2. M. Bloch, J. Barros, Physical-Layer Security: from Information Theory to Security Engineering Cambridge University Press, 2011.

A short list of reference papers for each lecture will be provided during class meetings.