**COURSE : Security and Privacy**

INSTRUCTOR : Giuseppe Bianchi

CONTACTS: Giuseppe Bianchi, Alberto Caponi

email : Giuseppe.bianchi@uniroma2.it, Alberto.caponi@uniroma2.it

**COURSE BACKGROUND -** No specific background beyond basic math, basic ICT, basic networking; familiarity with Linux may help laboratory activities.

**LEARNING OBJECTIVES -** The course has a threefold goal: i) provide an introductory know how to security and privacy technologies, protocols and solutions; ii) provide an hands-on understanding of cyber-attacks and relevant defenses, via laboratory activities and practice on security software and tools; iii) highlight some specific challenges emerging in big data scenarios, and provide some hints on the modern emerging methodologies and tools devised to address such emerging challenges.

**METHODOLOGY -** The course combines both frontal lectures (especially on goals I and iii) as well as laboratory activities (especially on part ii); based on the students’ skills and interests, the mix of theory and practice may be adapted during the course.

**EXAM -** Test + practical part

**CONTENTS -** Given the breadth of the topic (which could be the object of a dedicated master itself) the course will specifically address a subset of security and privacy issues revolving around i) infrastructure security and ii) data protection. The first part of the course will mainly focus on the analysis of the security best practices and protocols, along with the necessary review of the basic cryptographic and system security notions therein involved. Specific attention will be given to practical attacks as well as understanding of vulnerabilities. The course will finally briefly mention more specific and advanced topics, by providing an introduction to the emerging techniques (SMC, homomorphic encryption, etc) for the secure and private computation over protected data, with specific attention to scalable approaches.

**TEACHING MATERIAL -** Lecture slides will be provided during the course, along with supplementary ad-hoc material (book chapters, scientific works, standard documents, etc) complementing the slides.

 **SUGGESTED READING -** Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, ''***Handbook of applied cryptography***'', available at http://www.cacr.math.uwaterloo.ca/hac/

**ADDITIONAL SUGGESTED TEXTBOOKS**

William Stallings, “***Cryptography and Network Security***”, McGraw Hill

Stephen Thomas, “***SSL and TLS Essentials***”, Wiley