UNICUSANO
ROME

**Code: ING/INF05** **Credits: 9**
**Matter:** Systems Security
**Main language of instruction:** Italian
**Other language of instruction:** English

**Teaching Staff**

**Head instructor**
**Prof. Antonino LONGO MINNOLO - antonino.longo@unicusano.it**

## Introduction

1. *Objective of the course :*

The Systems Security Course aims to provide the student with a good knowledge of the principles that govern the security of processing systems. The course proposes the basic concepts in the field of security of processing systems, and declines them in the study of cryptography techniques and their application to the various aspects of computer security. Furthermore, the educational objective of the course is to provide the student with a detailed knowledge of the functioning of the main protocols at the basis of the design of secure distributed systems. The Etivities associated with the Course develop the skills necessary to analyze security protocols and computer vulnerabilities through the use of special tools and computer environments.

## Objectives

2. *Course Structure:*

- Illustrate the basic concepts in the field of security of processing systems
- Describe the main cryptographic techniques
- Illustrate the application of cryptography in the IT field
- Describe the main security protocols in distributed systems

**Competencies:**

A. Knowledge and understanding

At the end of the course, the student will have knowledge of the methodologies for dealing with problems related to the security of information processing systems. Furthermore, the student will acquire the ability to analyze authentication protocols and applications, e-mail and Web security, and all aspects related to the security of computer systems. Finally, the student will be made able to compare the consequences deriving from the architectural choices to be made in the design of a secure information system. In addition, through the Etivity, students will acquire the ability to analyze vulnerabilities of information systems, and test their permeability to intrusions, within forensic analysis and IT security testing environments such as Kali.

B. Applying knowledge and understanding

The student will be able to apply knowledge and methodologies to test, design and implement secure computer systems that make use of the techniques and tools analyzed during the course. The Etivities provide for the application of theoretical knowledge to practical problems, such as simulating attacks and solving vulnerabilities, to be solved with the help of forensic analysis and testing environments for information security (Kali).

C. Making judgements

The student will have acquired an analysis methodology of the mechanisms that guarantee the security of a computer system; will also be able to judge the validity of secure systems designs for processing information. Finally, the student will be able to carry out bibliographic searches, to analyze and interpret the relevant sources, in order to analyze new security protocols.

D. Communication skills

The student will be able to describe and hold conversations on issues relating to complex issues related to the security of information processing systems and networks, using appropriate terminology.

E. Learning skills.

At the end of the course, the student will have knowledge of the fundamental notions necessary to independently face any problem relating to the security of computer and network systems. Will be able to investigate data encryption, digital signature, authentication, integrity and non-repudiation techniques.

**Syllabus**

3. *Programme of the course:*

**Subject 1 - Systems security theoretical foundations**

Network Security. The evolution of ICT systems and the security problem. The problems and the lexicon of ICT security, The technological attacks (sniffing, spoofing, ...). Non-technological attacks (social engineering). Malicious Software. Methods for analyzing the security risks of an IT system. Authentication and authorization in complex security infrastructures..

**Subject 2 – Cryptography**
Cryptographic algorithms. Secret key encryption. Public key encryption. Diffie-Helman algorithm. Hash algorithms. SHA-1. Digital signature. Exercises..

**Subject 3 – Web applications security**
SQL injection. Cross-site scripting. State management. Buffer overflow.

**Subject 4 – IP security systems**
Security of IT systems. IP security overview. IPsec. EAP. RADIUS. Wireless Network Security. VPN. Tutorial on security protocols.

**Subject 5 - Web**
Email Security, Network Level Security, Web Security, Firewall. Tutorial on Web Security and Firewall..

**Subject 6 - Authentication**
User Authentication, Access Control. Authentication Applications: Kerberos. Exercises on user authentication..

**Subject 7 – IDS and IPS**
Intrusion Detection System(IDS). Intrusion Prevetuon System (IPS). Esercitazioni.

**Evaluation system and criteria**
The exam consists in carrying out a written test aimed at ascertaining the ability to analyze and rework the concepts acquired and a series of activities (e-tivity) carried out during the course in virtual classrooms.

The expected learning outcomes about the knowledge of the subject and the ability to apply them are assessed by the written test, while the communication skills, the ability to draw conclusions and the ability to self-learn are assessed in itinere through e-tivities.

**Bibliography and resources**

4. *Materials to consult:*

Notes written by the instructor are available in English. The notes cover the course contents and examination programme.

5. *Recommended bibliography:*

Suggested readings are:

- W. Stallings – Cryptography and Network Security, 7th Ed., Pearson
- W. Stallings – Computer security: principles and practice, 4th Ed., Pearson