Basis for secure communication

Academic Year: (2019 / 2020) **Review date: 29-04-2019**

Department assigned to the subject: Telematic Engineering Department

Coordinating teacher: MUÑOZ ORGANERO, MARIO

Type: Compulsory ECTS Credits : 6.0

Year : 4 Semester : 1

REQUIREMENTS (SUBJECTS THAT ARE ASSUMED TO BE KNOWN)

Basic communication and network protocols concepts. In particular, it is recommended to have passed the following subjects:

- Communications networks and services

- Telematic Applications

A basic knowledge of probability and algebraic structures is also needed, so knowledge of the following subjects if recommended:

- Statistics

OBJECTIVES

Summary: To have the knowledge, to be ablo to analyze and design and know how to apply to the resolution of specific problems, the main cryptographic techniques, as well as their applications to security systems in telematic networks and services. Students should familiarize themselves with symmetric and asymmetric encryption techniques, hash functions, cryptographic checksums, digital signatures and certificates, authentication protocols and their combined applications.

Detail of specific competences of the subject in terms of knowledge:
- Know the generic environment of the cryptosystem together with the different agents that make it up.
- Know the evolution of the different classic security mechanisms as a basis for modern security mechanisms.
- Know the conventional encryption techniques (symmetric encryption) as well as the current encryption standard (AES) and the previous standard (DES).
- Know the main modes of operation used in symmetric encryption.
- To know the mathematical bases of the main mechanisms of public key encryption. Understand the RSA algorithm in depth.
- Know the different hash techniques and their use in conjunction with public key algorithms to create digital signatures and digital certificates (PKI).
- Know the different techniques of distribution of session keys, both based on public key and based on secret code.
- Know the joint use of the different mechanisms by studying different security protocols (IPSec, SSL, etc.)

Detail of specific competences of the subject in terms of analysis, design and resolution of problems:
- Ability to use the cryptosystem definition as a framework for comparing different security mechanisms to analyze communication systems and networks.
- Ability to use the acquired criteria to evaluate the security of a given protocol.
- Ability to analyze and know how to choose with criteria the most appropriate security algorithm in each circumstance and according to certain requirements.
- Ability to define a security protocol for the resolution of a given scenario and providing security services.
- Ability to use security tools that allow to apply the different mechanisms studied.
- Be able to solve in couple a series of cryptographic challenges such as breaking passwords, determine from encrypted messages how to encrypt and certain parameters of the algorithms as well as generate certificates and digitally sign information.
- Be able to understand recommendations about cryptographic standards.

- Basic capabilities of cryptanalyzing systems

DESCRIPTION OF CONTENTS: PROGRAMME

This is a basic and introductory subject to communication security covering the main technologies in order to create network security services and secure information transfer channels.

The programme is divided into 4 parts:

1. Introduction to security.
1.1.What is Security?
1.2 Security Mechanisms.
1.3 Security Services.
1.4 Information Theory.

2. Symmetric Cryptography.
2.1 Classical cryptography algorithms.
2.2 Symmetric Encryption algorithms.
2.3 DES. TDES. AES.
2.4 Modes of operation.
2.5 Key distribution mechanisms.

3. Asymmetric Cryptography
3.1 Asymmetric cryptography algorithms.
3.2 Digital Signatures.
3.3 Digital Certificates (identity and attribute certificates).

4 Applications.
4.1 IPsec
4.2 SSL/TLS

LEARNING ACTIVITIES AND METHODOLOGY

The learning activities and methodology include:

- Theoretical lectures, problem solving classes in small groups, student presentations, individual tutoring and personal work of the student, including study, tests and exams; oriented to the acquisition of theoretical knowledge.
- Laboratory practices and classes of problems in small groups, individual tutoring and personal work of the student, including study, tests and exams; oriented to the acquisition of practical skills related to the program of each subject.

ASSESSMENT SYSTEM

The evaluation system includes the continuous evaluation of the student's work (assignments, reports of laboratory practices, participation in class and tests of assessment of skills and theoretical-practical knowledge) and the final evaluation by means of a final written examination in which Assess the knowledge, skills and abilities acquired throughout the course.
Specifically:
- Continuous evaluation (40%):
+ Delivery of 4 laboratories performed in pairs on the different aspects of the course.
+ 2 in class assessment tests.
- Final exam (60%)

% end-of-term-examination:	60
% of continuous assessment (assigments, laboratory, practicals…):	40

BASIC BIBLIOGRAPHY

- A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone Handbook of Applied Cryptography, CRC Press, August 2001
- Mike Speciner; Radia Perlman; Charlie Kaufman Network Security: Private Communication in a Public World, Prentice Hall, 2002
- William Stallings Cryptography and network security . Principles and Practice, Pearson Education M.U.A., 2014

ADDITIONAL BIBLIOGRAPHY

- Martti Lehto, Pekka Neittaanmäki Cyber Security Power and Technology, Springer, 2018

- Xiaodong Lin, Ali Ghorbani, Kui Ren, Sencun Zhu Security and Privacy in Communication Networks: SecureComm 2017 International Workshops, ATCS and SePrIoT, Niagara Falls, ON, Canada, October 22¿25, ... and Telecommunications Engineering, Springer, 2018