BUILDING THE EUROPEAN HIGHER EDUCATION AREA
A Subject in Information Systems Security

M. Gestal, J. R. Rabuñal, J. Dorado, D. Rivero and A. Pazos
Information and Communications Technologies Department
University of A Coruña, A Coruña, Spain

Keywords: European Higher Education Area, Computer Security, Syllabus, Evaluation, Course Design.

Abstract: This article describes the "Security in Information Systems" subject that is currently imparted at the University of A Coruña as part of its Master in Computer Sciences. This subject is organized as a response to the requirements of the European Higher Education Area (EHEA) and of extreme importance to future computer experts, since security is such a delicate and essential part of any information system. Special care has been given to the development of this subject, which requires continuous and timely updating.

1 INTRODUCTION

Our information society is, to a great extent, based on the idea that basic rights such as privacy, confidentiality, access to information, and authentification are not to be violated. In the world of information systems, security is particularly crucial because its advances take place at such a fast rate. Security requirements change with each new development, and since more and more information becomes accessible, security checks become increasingly exacting. As such, technological advances are catalysers that work in two directions: on the one hand they provide access to more and new information (entailing more security controls), on the other hand they allow for the implantation of more refined security mechanisms (which provide secure access to new information types).

The proposed subject is designed to provide students with the basic concepts and techniques for the protection of information systems. This knowledge is presented from a physical, logical, administrative, and legal point of view, and allows our future experts to understand and solve risks that threaten information systems in the present and in the future.

2 GLOBAL DESCRIPTION AND OBJECTIVES OF THE SUBJECT

Among the first basic concepts that are imparted is the evolution of several cryptographic algorithms (Ramió, 1998; Lucena, 2008). The enormous surge in electronic information exchange systems (electronic mail, web pages, e-commerce, digital signature, etc.), has increased the importance of first-level training on secure and reliable security infrastructures, with a strong focus on protocols, configuration, etc. (Stallings, 2006).

Operating Systems (Garfinkel et al., 2003) are also extremely dependent on security: they constitute the core of any computerized device and are the favourite target for computer attacks, so their vulnerabilities and possible defence strategies are especially interesting.

In general terms, this subject focuses on the weaknesses of Information Systems from both a physical (communications networks) and logical (operating systems, communications protocols, configurations, etc.) point of view, and broadly covers the following areas:

- Cryptography
- Cryptoanalysis
- Public-key cryptosystems
- Private-key cryptosystems
- Vulnerabilities in Information Systems
- Security in Operating Systems

Gestal M., Rabuñal J., Dorado J., Rivero D. and Pazos A. (2009).
BUILDING THE EUROPEAN HIGHER EDUCATION AREA - A Subject in Information Systems Security.
In *Proceedings of the First International Conference on Computer Supported Education*, pages 398-401
DOI: 10.5220/0001967003980401

- Security in Networks

These subjects provide students with extensive knowledge on basic security concepts, applicable to a wide range of fields, and allow them to manage and administrate the security aspects of information systems. The main purposes of this subject are the following:

- Become familiar with the security process
- Identify the risks for information systems
- Know the security mechanisms with which to equip an information system
- Understand the fundamental concepts of cryptography
- Understand the nature, definition, and application of a security policy

After completing this subject, the student will have of a series of competences with which to manage and administrate the security of information systems. These competences can be divided into three large groups:

- Competences related to conceptual capacity:
  - Summarize the foundations of cryptosystems
  - Know the legal aspects of information systems security
  - Define the risks and vulnerabilities of an information system
  - Analyse new advances in security and their repercussions
- Competences related to procedural capacities:
  - Use security tools
  - Organize the security of an information system
  - Express clearly and effectively the need for security measures and their implantation, advantages, and disadvantages
- Competences related to behavioural capacities:
  - Assume the existence of vulnerabilities in information systems and minimize them
  - Assess a system's security in a critical and objective manner
  - Collaborate with other professionals (such as system administrators, networks, databases, applications, etc.) in launching and maintaining security measures.

These competences will allow students to carry out their work in the systems security field. They will be able to design, implant, and evaluate the security mechanisms, the incident detection mechanisms, and the security policy of an information system.

3 TEACHING METHODOLOGY

The subject is based on three elements: theoretical classes, practical classes, and practical exercises. During the theoretical classes, the fundamental concepts of the subject are introduced so as to allow the student to study the proposed matter in depth. At this point, the teaching staff plays an essential role, but the students are also encouraged to participate actively and this participation will be evaluated.

Students receive the teaching material and a selection of bibliographical references, which enable them to prepare the classes in advance or focus on any given aspect. They may be exposed to written tests based on brief theoretical questions or on solving small problems, in order to check their level of assimilation of the concepts that were explained during class or analysed individually. These tests have a duration of approximately 30 minutes and are corrected and commented in class.

The practical classes are dedicated partly to the application of the exposed theoretical concepts to a practical case. During these classes, the students play a more relevant role; the professor merely presents the case and provides an individualized (or generalized, if relevant) support in case of doubt.

The practical sessions take place individually (or in groups of two persons), except for one of the classes which requires 2 or 3 sessions with groups of 4 to 6 persons. This particular class consists in a collaborative learning experience in which the group works on a previously indicated and structured theme (e.g. the application of security policy to a concrete case). The group indicates one person responsible for each part of the work; the persons responsible for the same part work together and explain what they do to the rest of their group, so that in the end all the components of one group have acquired knowledge on all the parts. In order to stimulate the explanation of concepts between the members of one group, a written test takes place after the work and the obtained result is common to the entire group, i.e. the average of the results of the individual members. This method enhances the interest of each student in making a fellow student understand the part for which he/she is responsible.

The practical classes can be complemented with seminaries that develop a subject related to the objective of the subject.

Finally, the practical exercise is carried out by groups of 2 to 4 persons and either chosen from a list proposed by the professor or directly proposed by the students. The proposed exercises have to be related to one of the subjects of the subject and seek to expand it. They are followed-up continuously during obligatory tutorials and finally exposed, as part of the theoretical classes, for a duration of 30 minutes. Time is given for questions and comments, and the content of these exercises is considered part of the subject material.

4 PROGRAMME

4.1 Theoretical Programme

The classes are within one semester, with four classes each week. The programme is divided into 5 large sections of very different nature. The subjects are the following:

- SECTION 1: Basic notions
  1.- Basics of the Security Theory
  2.- Physical and logical Security

- SECTION 2: Cryptography
  3.- Classical Cryptographic Systems
  4.- Private-key cryptographic systems
  5.- Public-key cryptographic systems
  6.- Digital signature

- SECTION 3: Security in Operative Systems
  7.- Security in Linux systems
  8.- Security in Windows systems

- SECTION 4: Security in Networks
  9.- Communciations Networks: Introduction
  10.- Security elements in communications networks: firewalls, , proxy
  11.- Vulnerabilities and Security on the Internet: WWW, electronic mail

- SECTION 5: Advanced Concepts
  12.- Steganography, visual cryptography
  13.- Forensic analysis

4.2 Practical Programme

For a correct and adequate follow-up of the theoretical programme, a practical programme is imparted that consists of a series of practices:

- Security Policies
- Classical Cryptography and Cryptoanalysis
- Security configuration and intruder detection in operative systems
- PGP
- Security configuration and intruder detection in web servers
- Forensic Analysis

5 EVALUATION

The evaluation process of this subject is continuous and consists of several sections: assimilation of theoretical concepts, execution of practices, and exposition of exercises that are evaluated according to the weighting criteria mentioned in Table 1.

Table 1: Weighting criteria for the evaluation of the subject.

Aspect	Criteria	Instrument	Weight
Attendance and Participation	▪ Active participation in theoretical and practical classes. ▪ Participation and output tutorials	▪ Observation and teacher’s notes	10%
Concepts	▪ Command of theoretical and operative notions	▪ Final theoretical exam	40%
Continuous assimilation of concepts	▪ Assimilation and compression of theoretical and operative notions	▪ Partial exams	10%
Monitored Practical Exercise	▪ Output of tutorials ▪ Quality of work ▪ Clarity of exposition	▪ Observation and teacher’s notes	25%
Elaboration Practical Classes and Exercices	▪ Output and elaboration of exercise during practical classes	▪ Observation and teacher’s notes ▪ Presentation exercises and practical classes	15%

In order for students to pass this subject, the sum of their qualifications in the above sections must be at least 5, and the results of the theoretical exam, the practical exercises, and the exposition of the work must each reach at least 40% of the highest mark.

The practical exercises will be retained for one year. The students who have already passed these during the previous year may repeat them but are not required to do so.

6 EXPERIENCE

This subject has been very well received by the student population, who was particularly interested in the “Hacking techniques in web applications” seminar that was organized in collaboration with Microsoft.

The monitored works have in many cases exceeded the required level, the students themselves being the ones who proposed additions or improvements to the initial proposal. We have even been obliged to organize additional classes so as to make room for all the expositions and subsequent debates and rounds of questions.

7 CONCLUSIONS

Good notions on security in information systems is an essential element in the training of any computer professional. Our subject is structured in a way that allows students to easily assimilate the programme but at the same time requires the highest level of participation (by means of practical classes and exercises). We believe that this can do nothing but stimulate their interest and implication in the subject.

REFERENCES

Ramió, J. *Aplicaciones Criptográficas*. Universidad Politécnica, Escuela Universitaria de Informática, 1999.

Lucena, M.J. 2008. *Criptografía y seguridad en Computadores, 4ª Edición.* Electronic book available at http://wwwdi.ujaen.es/~mlucena

Stallings, W. 2006. Cryptography and Network Security: Principles and Practice, Fourth Edition; Prentice Hall.

Garfinkel, S., Spafford, G., Schwartz, A. 2003. *Practical UNIX and Internet Security,* Third Edition. O’Reilly.