270123 - SI - Computer Security

Coordinating unit: 270 - FIB - Barcelona School of Informatics
Teaching unit: 701 - AC - Department of Computer Architecture
Academic year: 2018
Degree: BACHELOR'S DEGREE IN INFORMATICS ENGINEERING (Syllabus 2010). (Teaching unit Optional)
ECTS credits: 6
Teaching languages: Catalan

Teaching staff
Coordinator: Antonio Rodriguez I Garcia (antonio.rodriguez.g@est.fib.upc.edu)

Prior skills
Those obtained at the Operating Systems and Computer Networks subjects.
Knowledge of technical English.

Requirements
- Pre-Corequisite XC
- Pre-Corequisite SO

Degree competences to which the subject contributes

Specific:
CTI1.1. To demonstrate understanding the environment of an organization and its needs in the field of the information and communication technologies.
CTI1.2. To select, design, deploy, integrate and manage communication networks and infrastructures in an organization.
CTI1.3. To select, deploy, integrate and manage information system which satisfy the organization needs with the identified cost and quality criteria.
CTI2.3. To demonstrate comprehension, apply and manage the reliability and security of the computer systems (CEI C6).
CTI3.1. To conceive systems, applications and services based on network technologies, taking into account Internet, web, electronic commerce, multimedia, interactive services and ubiquitous computation.
CT6.4. To demonstrate knowledge and capacity to apply the characteristics, functionalities and structure of the Distributed Systems and Computer and Internet Networks guaranteeing its use and management, as well as the design and implementation of application based on them.
CT7.1. To demonstrate knowledge about metrics of quality and be able to use them.

CT7.2. To evaluate hardware/software systems in function of a determined criteria of quality.
CT7.3. To determine the factors that affect negatively the security and reliability of a hardware/software system, and minimize its effects.
CT8.1. To identify current and emerging technologies and evaluate if they are applicable, to satisfy the users needs.

Generical:
G6. SOLVENT USE OF THE INFORMATION RESOURCES: To manage the acquisition, structuring, analysis and visualization of data and information of the field of the informatics engineering, and value in a critical way the results of this management.
270123 - SI - Computer Security

**Teaching methodology**

This course should give an overview and a technical view of the problems and possible solutions to computer systems and networks security. For this reason, it covers many topics and has a great descriptive component.

However, the teaching methodology will use examples and problems for introducing the concepts to which students attain the necessary skills. Also, we will try to encourage interactivity with students considering real situations in class to discuss possible solutions.

Moreover, the laboratory will complete the skills and knowledge acquired in theory / problems class.

**Learning objectives of the subject**

1. Being able to understand the threats and security risks of computer systems.
2. Being able to analyze malicious code such as viruses, Trojans, etc.
3. Being able to understand and identify mechanisms for access control of an operating system.
4. Knowing the problems of security in computer networks and be able to find solutions to protect them.
5. Being able to design protection mechanisms for distributed applications.
6. Being able to understand the need and operation of forensic computer security mechanisms.
7. Being able to use cryptographic mechanisms to protect resources.
8. Being able to understand, design and implement public key infrastructure (PKI).
9. Being able to understand the mechanisms of protection and security policies.

**Study load**

<table>
<thead>
<tr>
<th>Total learning time: 150h</th>
<th>Hours large group: 45h</th>
<th>30.00%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hours medium group: 0h</td>
<td>0.00%</td>
</tr>
<tr>
<td></td>
<td>Hours small group: 15h</td>
<td>10.00%</td>
</tr>
<tr>
<td></td>
<td>Guided activities: 6h</td>
<td>4.00%</td>
</tr>
<tr>
<td></td>
<td>Self study: 84h</td>
<td>56.00%</td>
</tr>
</tbody>
</table>

This course should give an overview and a technical view of the problems and possible solutions to computer systems and networks security. For this reason, it covers many topics and has a great descriptive component.

However, the teaching methodology will use examples and problems for introducing the concepts to which students attain the necessary skills. Also, we will try to encourage interactivity with students considering real situations in class to discuss possible solutions.

Moreover, the laboratory will complete the skills and knowledge acquired in theory / problems class.

1. Being able to understand the threats and security risks of computer systems.
2. Being able to analyze malicious code such as viruses, Trojans, etc.
3. Being able to understand and identify mechanisms for access control of an operating system.
4. Knowing the problems of security in computer networks and be able to find solutions to protect them.
5. Being able to design protection mechanisms for distributed applications.
6. Being able to understand the need and operation of forensic computer security mechanisms.
7. Being able to use cryptographic mechanisms to protect resources.
8. Being able to understand, design and implement public key infrastructure (PKI).
9. Being able to understand the mechanisms of protection and security policies.

<table>
<thead>
<tr>
<th>Total learning time: 150h</th>
<th>Hours large group: 45h</th>
<th>30.00%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hours medium group: 0h</td>
<td>0.00%</td>
</tr>
<tr>
<td></td>
<td>Hours small group: 15h</td>
<td>10.00%</td>
</tr>
<tr>
<td></td>
<td>Guided activities: 6h</td>
<td>4.00%</td>
</tr>
<tr>
<td></td>
<td>Self study: 84h</td>
<td>56.00%</td>
</tr>
</tbody>
</table>

This course should give an overview and a technical view of the problems and possible solutions to computer systems and networks security. For this reason, it covers many topics and has a great descriptive component.

However, the teaching methodology will use examples and problems for introducing the concepts to which students attain the necessary skills. Also, we will try to encourage interactivity with students considering real situations in class to discuss possible solutions.

Moreover, the laboratory will complete the skills and knowledge acquired in theory / problems class.

1. Being able to understand the threats and security risks of computer systems.
2. Being able to analyze malicious code such as viruses, Trojans, etc.
3. Being able to understand and identify mechanisms for access control of an operating system.
4. Knowing the problems of security in computer networks and be able to find solutions to protect them.
5. Being able to design protection mechanisms for distributed applications.
6. Being able to understand the need and operation of forensic computer security mechanisms.
7. Being able to use cryptographic mechanisms to protect resources.
8. Being able to understand, design and implement public key infrastructure (PKI).
9. Being able to understand the mechanisms of protection and security policies.

<table>
<thead>
<tr>
<th>Total learning time: 150h</th>
<th>Hours large group: 45h</th>
<th>30.00%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hours medium group: 0h</td>
<td>0.00%</td>
</tr>
<tr>
<td></td>
<td>Hours small group: 15h</td>
<td>10.00%</td>
</tr>
<tr>
<td></td>
<td>Guided activities: 6h</td>
<td>4.00%</td>
</tr>
<tr>
<td></td>
<td>Self study: 84h</td>
<td>56.00%</td>
</tr>
</tbody>
</table>

This course should give an overview and a technical view of the problems and possible solutions to computer systems and networks security. For this reason, it covers many topics and has a great descriptive component.

However, the teaching methodology will use examples and problems for introducing the concepts to which students attain the necessary skills. Also, we will try to encourage interactivity with students considering real situations in class to discuss possible solutions.

Moreover, the laboratory will complete the skills and knowledge acquired in theory / problems class.

1. Being able to understand the threats and security risks of computer systems.
2. Being able to analyze malicious code such as viruses, Trojans, etc.
3. Being able to understand and identify mechanisms for access control of an operating system.
4. Knowing the problems of security in computer networks and be able to find solutions to protect them.
5. Being able to design protection mechanisms for distributed applications.
6. Being able to understand the need and operation of forensic computer security mechanisms.
7. Being able to use cryptographic mechanisms to protect resources.
8. Being able to understand, design and implement public key infrastructure (PKI).
9. Being able to understand the mechanisms of protection and security policies.

<table>
<thead>
<tr>
<th>Total learning time: 150h</th>
<th>Hours large group: 45h</th>
<th>30.00%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hours medium group: 0h</td>
<td>0.00%</td>
</tr>
<tr>
<td></td>
<td>Hours small group: 15h</td>
<td>10.00%</td>
</tr>
<tr>
<td></td>
<td>Guided activities: 6h</td>
<td>4.00%</td>
</tr>
<tr>
<td></td>
<td>Self study: 84h</td>
<td>56.00%</td>
</tr>
</tbody>
</table>
## Content

### Introduction

**Degree competences to which the content contributes:**

**Description:**
Threats, risk analysis, protection mechanisms, security of communications, security forensics, policies, recovery, legal aspects, ...

### Cryptography

**Degree competences to which the content contributes:**

**Description:**

### Security in operating systems

**Degree competences to which the content contributes:**

**Description:**
Malicious Code: Viruses, Trojan horses, worms, spyware, etc. Access Control.

### PKI Infrastructure

**Degree competences to which the content contributes:**

**Description:**

### Network security

**Degree competences to which the content contributes:**

**Description:**

### Security in applications

**Degree competences to which the content contributes:**

**Description:**
Forensic analysis

Degree competences to which the content contributes:

Description:
Collection of evidence. Analysis.
### Planning of activities

| Development of theme 1. Introduction. | Hours: 10h  
Theory classes: 6h  
Practical classes: 0h  
Laboratory classes: 0h  
Guided activities: 0h  
Self study: 4h |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong> Learning the concepts and objectives associated with this item.</td>
<td></td>
</tr>
</tbody>
</table>
| **Specific objectives:**  
1, 10 | |

| Vulnerabilities in web applications | Hours: 7h  
Theory classes: 0h  
Practical classes: 0h  
Laboratory classes: 3h  
Guided activities: 2h  
Self study: 2h |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong> Understanding the secure programming techniques described in the session. Understanding the webscarab and webgoat applications included in the OWASP linux distribution</td>
<td></td>
</tr>
</tbody>
</table>

| Development Topic 2. Cryptography. | Hours: 15h  
Theory classes: 7h  
Practical classes: 0h  
Laboratory classes: 0h  
Guided activities: 0h  
Self study: 8h |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong> Learning the concepts and objectives associated with this item.</td>
<td></td>
</tr>
<tr>
<td><strong>Specific objectives:</strong> 7</td>
<td></td>
</tr>
</tbody>
</table>

| Security in wireless networks | Hours: 4h  
Theory classes: 0h  
Practical classes: 0h  
Laboratory classes: 2h  
Guided activities: 0h  
Self study: 2h |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description:</strong> Understanding the protocol WEP. Being able to use the tools Airodump linux, aircrack and Aireplay</td>
<td></td>
</tr>
</tbody>
</table>
### Development of item 3. Infrastructure PKI

**Description:**
Learning the concepts and objectives associated with this item.

**Specific objectives:**
8

**Hours:** 18h
- Theory classes: 8h
- Practical classes: 0h
- Laboratory classes: 0h
- Guided activities: 1h
- Self study: 9h

### Using digital certificates and apache (HTTPS)

**Description:**
Being able to create a X.509 certificate with openssl and install it on an Apache web server to configure HTTPS

**Hours:** 4h
- Theory classes: 0h
- Practical classes: 0h
- Laboratory classes: 2h
- Guided activities: 0h
- Self study: 2h

### PKCS: Public-Key Cryptography Standard

**Description:**
Understanding the different formats of the PKCS messages. Being able to create PKCS messages using the linux tool openssl

**Hours:** 4h
- Theory classes: 0h
- Practical classes: 0h
- Laboratory classes: 2h
- Guided activities: 0h
- Self study: 2h

### First theory exam

**Description:**
Theory exam of the following topics: Introduction, Criptography, PKI infrastructure.

**Specific objectives:**
1, 7, 8, 10
### Development of item 4. Security in operating systems.

**Hours:** 10h  
Theory classes: 5h  
Practical classes: 0h  
Laboratory classes: 0h  
Guided activities: 0h  
Self study: 5h

**Description:**  
Learning the concepts and objectives associated with this item.

**Specific objectives:**  
2, 3

### Malware analysis

**Hours:** 4h  
Theory classes: 0h  
Practical classes: 0h  
Laboratory classes: 2h  
Guided activities: 0h  
Self study: 2h

**Description:**  
Understanding the different forms to analyze a malicious code. Being able to properly use the analysis tool IDAPro

### Development of item 5. Internet security

**Hours:** 18h  
Theory classes: 8h  
Practical classes: 0h  
Laboratory classes: 0h  
Guided activities: 1h  
Self study: 9h

**Description:**  
Learning the concepts and objectives associated with this item.

**Specific objectives:**  
4

### Iptables i snort

**Hours:** 5h  
Theory classes: 0h  
Practical classes: 0h  
Laboratory classes: 3h  
Guided activities: 0h  
Self study: 2h

**Description:**  
Understanding how the iptables command works as well as its internal operations based on tables and chains. Being able to create snort rules
### Documentation about malicious code.

<table>
<thead>
<tr>
<th>Hours: 10h</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theory classes: 0h</td>
</tr>
<tr>
<td>Practical classes: 0h</td>
</tr>
<tr>
<td>Laboratory classes: 0h</td>
</tr>
<tr>
<td>Guided activities: 0h</td>
</tr>
<tr>
<td>Self study: 10h</td>
</tr>
</tbody>
</table>

**Description:**
Being able to find high quality information about malware. Learning how to filter relevant information. Being able to correctly cite the information sources used.

**Specific objectives:**
2

### Development of item 6. Security applications.

<table>
<thead>
<tr>
<th>Hours: 12h</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theory classes: 6h</td>
</tr>
<tr>
<td>Practical classes: 0h</td>
</tr>
<tr>
<td>Laboratory classes: 0h</td>
</tr>
<tr>
<td>Guided activities: 0h</td>
</tr>
<tr>
<td>Self study: 6h</td>
</tr>
</tbody>
</table>

**Description:**
Learning the concepts and objectives associated with this item.

**Specific objectives:**
5

### Second theory exam

<table>
<thead>
<tr>
<th>Hours: 5h</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guided activities: 1h</td>
</tr>
<tr>
<td>Self study: 4h</td>
</tr>
</tbody>
</table>

**Description:**
Theory exam of the following topics: Security in operating systems and Security in computer networks

**Specific objectives:**
2, 3, 4, 5

### Development issue 7. Security forensics.

<table>
<thead>
<tr>
<th>Hours: 6h</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theory classes: 3h</td>
</tr>
<tr>
<td>Practical classes: 0h</td>
</tr>
<tr>
<td>Laboratory classes: 0h</td>
</tr>
<tr>
<td>Guided activities: 0h</td>
</tr>
<tr>
<td>Self study: 3h</td>
</tr>
</tbody>
</table>

**Description:**
Learning the concepts and objectives associated with this item.
Specific objectives:
6

<table>
<thead>
<tr>
<th>Final exam lab</th>
<th>Hours: 3h</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Guided activities: 1h</td>
</tr>
<tr>
<td></td>
<td>Self study: 2h</td>
</tr>
</tbody>
</table>

Description:
Review on all laboratory practices carried out throughout the course.

Specific objectives:
2, 3, 4, 5, 7, 8

<table>
<thead>
<tr>
<th>Third theory Exam</th>
<th>Hours: 10h</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Guided activities: 2h</td>
</tr>
<tr>
<td></td>
<td>Self study: 8h</td>
</tr>
</tbody>
</table>

Description:
Theory exam of the following topics: Computer Forensics and Security in computer networks

Specific objectives:
4, 5, 6

Qualification system
Theory (70%) - Laboratory (25%) - Generic competence (5%).
The laboratory mark is obtained from the grades of each practice (50%) and the laboratory final exam (50%), but taking into account that the practices, which can be done either at the lab or at home, are mandatory in order to do the laboratory exam. The theory grade will be the average of three course exams (ET1, ET2 and ET3). In other words, the theory grade will be NT = (ET1+ET2+ET3)/3. The grade for the generic competence is obtained from the evaluation of the activity "Bibliographic Internet Research and analysis".
Bibliography

Basic:


Complementary: