Course guide
230995 - IAS - Applications Security

Unit in charge: Barcelona School of Telecommunications Engineering
Teaching unit: 701 - DAC - Department of Computer Architecture.

Degree: MASTER'S DEGREE IN CYBERSECURITY (Syllabus 2020). (Compulsory subject).

Academic year: 2021 ECTS Credits: 5.0 Languages: English

LECTURER

Coordinating lecturer: Jaime Delgado Mercé
Others: Silvia Llorente Viejo

PRIOR SKILLS

Basic knowledge of programming, communication networks, and coding and compression of audiovisual content.

TEACHING METHODOLOGY

The course is very interactive with subjects’ presentations from the Professor and assignments in which students present topics and discuss conclusions. Furthermore, some topics are complemented with laboratory sessions.

Concerning class assignments, there is one for analysis and discussion on specific advanced topics and standards, focusing either on research issues or software development or application. Students make a small research project led by the Professor (on a specific topic: what is done? what is not solved? ideas to solve it). They write a short paper and make a presentation where they answer questions and criticisms from the Professor and the other students. In addition, students lead a discussion on their results with the rest of students.

Laboratory work consists on the design and development of applications taking into account the principles of Security by Design and Privacy by Design. The students have to work in teams in order to provide a secure version of their application. The kind of applications to be implemented has to be based on some of the use cases presented in the course. Alternatively, some topics proposed by the students may be considered.

LEARNING OBJECTIVES OF THE SUBJECT

This subject on Applications Security covers advanced aspects of the very active area of Internet applications, its development and its security. Focus is not restricted to a specific sector, but some are used as examples, such as eHealth and multimedia applications.

With this main objective in mind, security and privacy are considered for application protocols, information or content formats, metadata, etc. Many aspects of security for Internet applications will be reviewed, including techniques for development of secure software.

Standards to achieve interoperability are key for understanding the relevant problems and their solutions, so they will be studied.

Topics will be introduced, analyzed and discussed, focusing on the new approaches and techniques. Students will work on specific assignments that will be discussed with their peers in order to understand current solutions and think on alternative ones.
STUDY LOAD

<table>
<thead>
<tr>
<th>Type</th>
<th>Hours</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hours small group</td>
<td>6,0</td>
<td>4.80</td>
</tr>
<tr>
<td>Self study</td>
<td>86,0</td>
<td>68.80</td>
</tr>
<tr>
<td>Hours large group</td>
<td>33,0</td>
<td>26.40</td>
</tr>
</tbody>
</table>

Total learning time: 125 h

CONTENTS

1. Introduction

**Description:**
- Subject introduction
- Application layer and HTTP review
- XML (eXtensible Markup Language) review
- Standardization

**Full-or-part-time:** 4h
Theory classes: 4h

2. Privacy and security by design

**Description:**
- Regulations: GDPR, ...
- Strategies
- Example approaches: W3C, OWASP
- Risk management
- Security by Design and secure development of software (SecDevOps)
- SecDevOps laboratory

**Full-or-part-time:** 11h
Theory classes: 5h
Laboratory classes: 6h

3. Security in Internet applications

**Description:**
- Security in application layer protocols
- XML and security: Encryption, Signature
- Specific security protocols: SAML, JWT, OAuth, OpenID Connect
- Internet applications privacy
- Privacy policies
- Access control languages (XACML, ...)
- Access control approaches: RBAC (Role Based), ABAC (Attribute Based), KC-RBAC (Knowledge-Constrained), ...
- Anonymization, pseudonymization, de-identification

**Full-or-part-time:** 9h
Theory classes: 9h
4. Security and privacy in eHealth

Description:
- Concepts and examples
- Privacy in eHealth: User identification, Patient consent, Access/privacy policies for health information, FAIR access, TRUST models, Genomic information
- Standards: HL7, OpenEHR, ISO Health Informatics, ISO Genomics Informatics, GA4GH, ...
- IoT for eHealth: Hospitals & Home, Security and privacy issues, Devices security
- Specific regulations (GDPR, HIPAA, ...)

Full-or-part-time: 8h
Theory classes: 8h

5. Security in multimedia content

Description:
- Intellectual rights for multimedia content
- Encryption in multimedia formats (ISO base media file format, ...)
- W3C approach: Encrypted Media Extensions (EME) & Media Source Extensions (MSE)
- Security in DASH streaming: encryption, authentication, ...
- Content authentication and metadata
- Permission and contracts languages (ODRL, MPEG CEL, ...)
- User privacy in web services and applications: Web tracking, Privacy in social applications/networks

Full-or-part-time: 7h
Theory classes: 7h

GRADING SYSTEM

Tests on the topics developed by the Professor (T1 and T2).
An assignment on research, analysis and discussion of a topic (A): Students provide documentation, presentation and lead class discussion. Students not presenting should make questions showing their understanding of the topic.
Laboratory work on SecDevOps (L).
Final grade: \((T1+T2)/2)*0,4 + (A*0,4) + (L*0,2)\)
Assessment of A includes: Content (35%), Presentation (30%), Lead discussion (10%), Others' discussion (5%), Report (20%).
T1 and T2 grades could be increased (factor F) with the evaluation of n (number to define) "daily short tests" (grade D for every daily test):
Increase factor \(F = 0,025 \times (\Sigma n \times D)/n\)
The increased Ti grade will be: \(Ti \times (1+F)\). 0 <= F <= 0,25.

EXAMINATION RULES.