Course guides
230995 - IAS - Applications Security

Last modified: 07/07/2020

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: 2020 **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 some introductory topics from the Professor and a few assignments in which students present topics and discuss conclusions. Furthermore, some topics are complemented with laboratory sessions.

Concerning class assignments, there are two of them, one for analysis and discussion on specific advanced topics and standards, and another one more focused on research issues. In the first assignment, students present the results of their analysis and lead a discussion on this with the rest of students.

In the other assignment, 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.

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 is 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

Type	Hours	Percentage
Hours small group	6,0	4.80
Self study	86,0	68.80
Hours large group	33,0	26.40

Total learning time: 125 h

CONTENTS

1. Introduction

Description:
- Subject introduction
- Application layer. Web protocols: HTTP
- XML (eXtensible Markup Language) review
- Standardization

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

2. Security in Internet applications

Description:
- Security in application layer protocols
- XML and security: Encryption, Signature
- Specific security protocols: SAML, OAuth, OpenID Connect
- Internet applications privacy
- XACML, access control
- Intellectual rights for multimedia content

Full-or-part-time: 6h
Theory classes: 6h

Security and privacy in eHealth

Description:
- Concepts and examples
- Privacy in eHealth: User identification, Health records' privacy policies, Access policies, FAIR access
- Some specific techniques: Anonymization, pseudonymization
- Standards: HL7, OpenEHR, Genomic information
- IoT for eHealth: Hospitals & Home, Security issues, Devices security

Full-or-part-time: 6h
Theory classes: 6h

4. Privacy and security by design

Description:
- Regulations: GDPR, …
- Methodologies for Privacy by Design
- Examples
- Security by Design and secure development of software, SecDevOps
- SecDevOps laboratory

Full-or-part-time: 10h
Theory classes: 4h
Laboratory classes: 6h

5. Security in multimedia content

Description:
- Common encryption in ISO base media file format
- Security in DASH: encryption, authentication
- W3C approach: Encrypted Media Extensions (EME) & Media Source Extensions (MSE)
- Permission and contracts languages (ODRL, MPEG CEL, …)

Full-or-part-time: 5h
Theory classes: 5h

6. Other security aspects in Internet

Description:
- User privacy in web services and applications: Web tracking, Privacy in social applications/networks
- Access Control approaches: RBAC (Role Based), ABAC (Attribute Based), KC-RBAC (Knowledge-Constrained), …
- Tor anonymity

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

GRADING SYSTEM

Tests on the topics developed by the Professor (T1 and T2).

An assignment on analysis and discussion (A) and an assignment on research (R):
- (A) Analysis & Discussion of a topic. Students provide documentation + short presentation and lead class discussion. Students not presenting should make questions showing their understanding of the topic.
- (R) Research work. Students provide documentation + "long" presentation + interview (if needed).

Laboratory work on SecDevOps (L).

Final grade: ((T1+T2)/2) * 0,35) + (A * 0,25) + (R * 0,25) + (L*0,15)

Assessment of A includes:
Content (35%), Presentation (30%), Lead discussion (20%), Others' discussion (15%).
Assessment of R includes:
Content (35%), Presentation (25%), Questions (15%), Report (25%).

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 * (Σn Di)/ n
The increased Ti grade will be: Ti * (1+F). 0

EXAMINATION RULES.

-