Course guide
230157 - SPI - Information Security and Privacy

Last modified: 20/06/2024

Unit in charge: Barcelona School of Telecommunications Engineering
Teaching unit: 744 - ENTEL - Department of Network Engineering.

Degree: BACHELOR'S DEGREE IN TELECOMMUNICATIONS TECHNOLOGIES AND SERVICES ENGINEERING (Syllabus 2015). (Optional subject).
BACHELOR'S DEGREE IN ELECTRONIC ENGINEERING AND TELECOMMUNICATION (Syllabus 2018). (Optional subject).

Academic year: 2024 **ECTS Credits:** 6.0 **Languages:** English

LECTURER

Coordinating lecturer: Consultar aquí / See here:

Others: Consultar aquí / See here:

TEACHING METHODOLOGY

- Lectures
- Application lectures
- Teamwork
- Individual work
- Presentations
- Written exams

LEARNING OBJECTIVES OF THE SUBJECT

- Learning general concepts of information security and privacy.
- Knowing the main mechanisms of authentication and key management.
- Deepening the knowledge of the main security protocols used on the Internet.
- Introducing the main data anonymization algorithms and the associated privacy guarantees
- Introducing the main privacy guarantees defined by different application scenarios.
- Understanding the challenges and mechanisms of privacy in personalized information systems
- Introducing anonymous communication systems

STUDY LOAD

Type	Hours	Percentage
Self study	98,0	65.33
Hours large group	52,0	34.67

Total learning time: 150 h

CONTENTS

1. Network security fundamentals

Description:
Security services and mechanisms. Symmetric crytography and public-key cryptography; digital signature; Perimeter security.

Full-or-part-time: 30h
Theory classes: 10h
Self study : 20h

2. Authentication and Key Management

Description:
Authentication protocols and mechanisms; Key management protocols; Public Key infrastructures (PKI); Trust models.

Full-or-part-time: 16h
Theory classes: 6h
Self study : 10h

3. Internet Security Protocols

Description:
IP Security and Virtual Private Networks; Email security; Web security

Full-or-part-time: 24h
Theory classes: 8h
Self study : 16h

4. Introduction to data privacy

Description:
Motivation. Definition of basic concepts. Attackers and trusted parties. Privacy metrics

Full-or-part-time: 12h
Theory classes: 4h
Self study : 8h

5. Data anonymization algorithms

Description:
Statistical disclosure control. Data microaggregation algorithms. Measuring the commitment to privacy-utility.

Full-or-part-time: 26h
Theory classes: 10h
Self study : 16h

6. Privacy in personalised information systems

Description:
User profiles: measure of privacy risk. Privacy-enhancing mechanisms.

Full-or-part-time: 12h
Theory classes: 4h
Self study : 8h

7. Anonymous communication systems.

Description:
Traffic analysis. Anonymous communications systems: TOR, Crowds, Mix Networks

Full-or-part-time: 12h
Theory classes: 4h
Self study : 8h

8. Differential privacy

Description:
Syntactic vs. semantic privacy. Differential privacy in interactive databases.

Full-or-part-time: 18h
Theory classes: 6h
Self study : 12h

GRADING SYSTEM

The final grade for the subject will be obtained from the continuous assessment grade, which will include active participation in class, as well as tests, presentations and assignments proposed by the teacher throughout the course. The weighting will be as follows:

- Tests (50%)
- Active participation in class (10%)
- Assignments and presentations (40%)

If the continuous assessment is not passed, the student may take a final exam, which in this case is worth 100% of the grade.

BIBLIOGRAPHY

Basic:
- Templ, Matthias. Statistical disclosure control for microdata : methods and applications in R . Cham, Switzerland : Springer International Publishing AG, 2017. ISBN 9783319502724.
- Stallings, William. Cryptography and network security : principles and practice . 7th ed., global edition. Boston : Prentice Hall, cop. 2017. ISBN 9781292158587.