DEGREE CURRICULUM

APPLICATIONS AND COMMUNICATIONS SECURITY

Coordination: FERNANDEZ CAMON, CESAR

Academic year 2018-19

APPLICATIONS AND COMMUNICATIONS SECURITY 2018-19

Subject's general information

Subject name	APPLICATIONS AND COMMUNICATIONS SECURITY
Code	102028
Semester	1st Q(SEMESTER) CONTINUED EVALUATION
Typology	<table><tr><th>Degree</th><th>Course</th><th>Character</th><th>Modality</th></tr><tr><td>Bachelor's Degree in Computer Engineering</td><td>4</td><td>COMPULSORY</td><td>Attendance-based</td></tr></table>
Course number of credits (ECTS)	9
Type of activity, credits, and groups	<table><tr><th>Activity type</th><td>PRALAB</td><td>TEORIA</td></tr><tr><th>Number of credits</th><td>3.6</td><td>5.4</td></tr><tr><th>Number of groups</th><td>1</td><td>1</td></tr></table>
Coordination	FERNANDEZ CAMON, CESAR
Department	MATHEMATICS
Teaching load distribution between lectures and independent student work	9 ECTS = 25x9 = 225 working hours 40% --> 90 working hours at class/lab rooms 60% --> 135 non guided working hours
Important information on data processing	Consult this link for more information.
Language	Catalan / English Course materials in english
Distribution of credits	FERNANDEZ CAMON, CESAR, 3ECTS MATEU PIÑOL, CARLOS, 3ECTS

APPLICATIONS AND COMMUNICATIONS SECURITY 2018-19

Teaching staff	E-mail addresses	Credits taught by teacher	Office and hour of attention
PINTÓ SUBIRADA, EVA JUDITH	judith.pinto@udl.cat	6	
SEBE FEIXAS, FRANCISCO	fsebe@matematica.udl.cat	3	

Subject's extra information

To properly follow this subject previous knowledge on operating systems, networks and programming is recommended.

Learning objectives

- To understand the concepts, issues and procedures related to computer security
- To create basic security audits
- To understand cryptography and authentication concepts and mechanisms
- To design basic firewalls
- To develop applications for secure communication environments

Competences

CT2. Mastering a foreign language, especially English.

CT3. Training Experience in the use of the new technologies and the information and communication technologies.

GII-TI2. Capacity to choose, design, deploy, integrate, evaluate, build, manage, explode and keep the hardware, software and network technologies inside the cost and quality requirements.

GII-TI6. Capacity to conceive systems, applications and services based in network technologies, including Internet, web, e-commerce, multimedia, interactive services and mobile computation.

GII-TI7. Capacity to comprise, apply and manage the computer systems guarantee and security.

EPS11. Capacity to understand the needs of the user expressed in a no technical language.

Subject contents

1. Introduction
2. Preliminaries
    1. Introductory concepts
    2. Virtualization (for use in labs)
3. Basic Systems security

4. Programming faults: stack exploits, etc.
5. Basic security auditing
6. Cryptography
    - Symmetric cryptography
        - Block ciphers
        - Stream ciphers
    - Hash functions
    - Asymmetric cryptography
        - Mathematical background
        - The RSA cryptosystem
        - Digital signature (DSA)
7. Firewalls
    - Network traffic filtering
    - Firewall design for workstations, servers and gateways.
8. Authentication
    - Key management
    - Authentication applications
        - kerberos
        - X509
    - Public Key Infrastructure
    - DNIe
9. Comms security
    - SSL programming
    - SMIME
    - HTTPS
    - OpenVPN

Methodology

Every topic of this subject is presented in master classes. Based on contents, practice problems are proposed, as well some practical cases. Both types of work are developed in group, partially advised by the professor at class time and finally subjected to avaluation.

Development plan

- Week 1,2. Themes 1,2
- Week 3,4. Theme 3
- Week 5,6. Themes 4 i 5
- Week 7-10, Theme 6
- Week 11,12, Theme 7
- Week 13,14, Theme 8
- Week 15,16, Theme 9

Evaluation

Evaluation consists on several problems and practical cases scored as:

1. Virtualization (5)
2. Basic Systems security 7+7)
3. Programming faults: stack exploits, etc. (7)
4. Basic security auditing: (8)
5. Symmetric cryptography (3+3+3+3)
6. Hash functions (3)
7. Asymmetric cryptography (3+3)
8. Firewalls (4+4+4)

9. Public Key with OpenSSL (7.5)
    - DNIe (4.5)
    - PKI (3)
10. SSL programming (7.5)
11. SMIME (6)
12. HTTPS (4.5)
13. OpenVPN (3)

A minimum of 50% from the total amount of points is mandatory to pass the course.

Bibliography

- Network Security with OpenSSL. Pravir Chandra, Matt Messier, John Viega. Ed. O'Reilly, 2002
- OpenSSL Documents
- Cryptography & Network Security, W. Stallings, 3-Ed, 2003
- Network & Internetwork Security, W. Stallings, 1995
- Advanced Penetration Testing for Highly-Secured Environments. Lee Allen. Packt Publishing. 2012.
- Threat Modeling. Adam Shostack. Wiley. 2014.
- Metasploit Penetration Testing Cookbook. Abhinav Singh. Pack Publishing. 2012.
- Gray Hat Hacking: The Ethical Hackers Handbook. Harper, Harris et al. McGraw-Hill.2011