GUIA DOCENT

SEGURETAT D'APLICACIONS I COMUNICACIONS

Coordinació: FERNANDEZ CAMON, CESAR

Any acadèmic 2016-17

SEGURETAT D'APLICACIONS I COMUNICACIONS 2016-17

Informació general de l'assignatura

Denominació	SEGURETAT D'APLICACIONS I COMUNICACIONS
Codi	102028
Semestre d'impartició	1R Q(SEMESTRE) AVALUACIÓ CONTINUADA
Caràcter	<table><tr><th>Grau/Màster</th><th>Curs</th><th>Caràcter</th><th>Modalitat</th></tr><tr><td>Grau en Enginyeria Informàtica</td><td>4</td><td>OBLIGATÒRIA</td><td>Presencial</td></tr></table>
Nombre de crèdits ECTS	9
Grups	1GG
Crèdits teòrics	6
Crèdits pràctics	3
Coordinació	FERNANDEZ CAMON, CESAR
Departament/s	INFORMATICA I ENGINYERIA INDUSTRIAL,MATEMATICA
Distribució càrrega docent entre la classe presencial i el treball autònom de l'estudiant	9 ECTS = 25x9 = 225 hores de treball 40% --> 90 hores presencials 60% --> 135 hores de treball autònom
Informació important sobre tractament de dades	Consulteu aquest enllaç per a més informació.
Idioma/es d'impartició	Català / Anglés Materials en anglés.
Distribució de crèdits	FERNANDEZ CAMON, CESAR, 3ECTS MATEU PIÑOL, CARLOS, 3ECTS

SEGURETAT D'APLICACIONS I COMUNICACIONS 2016-17

Professor/a (s/es)	Adreça electrònica professor/a (s/es)	Crèdits impartits pel profesor	Horari de tutoria/lloc
FERNANDEZ CAMON, CESAR	cesar@diei.udl.cat	3	
MARTÍNEZ RODRÍGUEZ, SANTIAGO	santi@matematica.udl.cat	3	
MATEU PIÑOL, CARLOS	carlesm@diei.udl.cat	3	

Informació complementària de l'assignatura

Per cursar l'assignatura es requereixen coneixements prèvis de sistemes operatius, programació, xarxes i comunicacions.

Objectius acadèmics de l'assignatura

- Entendre els conceptes, problemes i procediments de seguretat informàtica
- El·laborar auditories de seguretat senzilles
- Entendre els conceptes i mecanismes bàsics de la criptografia i autenticació
- Dissenyar esquemes de tallafocs
- Desenvolupar aplicacions en entorns de comunicacions segurs

Competències

CT2. Adquirir un domini significatiu d'una llengua estrangera, especialment de l'anglès.

CT3. Adquirir capacitació en l'ús de les noves tecnologies i de les tecnologies de la informació i la comunicació.
Competències específiques de la titulació

GII-TI2. Capacitat per seleccionar, dissenyar, desplegar, integrar, avaluar, construir, gestionar, explotar i mantenir les tecnologies de hardware, software i xarxes, dins dels paràmetres de cost i qualitat adequats.

GII-TI6. Capacitat de concebre sistemes, aplicacions i serveis basats en tecnologies de xarxa, incloent Internet, web, comerç electrònic, multimèdia, serveis interactius i computació mòbil.

GII-TI7. Capacitat per comprendre, aplicar i gestionar la garantia i seguretat dels sistemes informàtics.

EPS11. Capacitat de comprendre les necessitats de l'usuari expressades en un llenguatge no tècnic.

Continguts fonamentals de l'assignatura

SEGURETAT D'APLICACIONS I COMUNICACIONS 2016-17

1. Introducció
2. Preliminars
    1. Conceptes previs
    2. Virtualització (per als labs)
3. Sistemes bàsics de seguretat
4. Fallides de programació: stack exploits, etc.
5. Auditoria de seguretat bàsica
6. Criptografia
    - Criptografia simètrica
        - Xifrat de bloc
        - Xifrat de fluxe
    - Funcions Hash
    - Criptografia asimètrica
        - Fonaments matemàtics
        - El criptosistema RSA
        - Digital signature (DSA)
7. Tallafocs
    - Filtrat del tràfic de xarxa
    - Disseny de tallafocs per a estacions, servidors i routers.
8. Autenticació
    - Gestió de claus
    - Aplicacions d'autenticació
        - kerberos
        - X509
    - Infrastructura de clau pública
    - DNIe
9. Comunicacions segures
    - Programant en SSL
    - SMIME
    - HTTPS
    - OpenVPN

Eixos metodològics de l'assignatura

Cadascún dels temes que composen l'assignatura es presenta en classes magistrals. En funció dels continguts, es proposa la resolució de problemes pràctics i/o
casos pràctics. Tant els problemes com els casos pràctics es desenvolupen en grup, són parcialment tutoritzats a classe i són avaluats.

Pla de desenvolupament de l'assignatura

- Setmana 1,2. Temes 1,2
- Setmana 3,4. Tema 3
- Setmana 5,6. Temes 4 i 5
- Setmana 7-10, Tema 6
- Setmana 11,12, Tema 7
- Setmana 13,14, Tema 8
- Setmana 15,16, Tema 9

Sistema d'avaluació

L'avaluació consistira en un seguit d'exercicis i casos pràctics amb la puntuació següent:

1. Virtualització (5)
2. Sistemes bàsics de seguretat (7 + 7)
3. Fallides de programació: stack exploits, etc. (7)
4. Auditoria bàsica de seguretat: (8)
5. Criptografia simètrica (3+3+3+3)
6. Funcions Hash (3)
7. Criptografia asimètrica (3+ 3)
8. Tallafocs (4+4+4)
9. Clau pública amb OpenSSL (7.5)
    - DNIe (4.5)
    - PKI (3)
10. Programació amb SSL (7.5)
11. SMIME (6)
12. HTTPS (4.5)
13. OpenVPN (3)

De totes aquestes activitiats se n'ha d'aconseguir un mínim de 50 punts per superar l'assignatura.

Bibliografia i recursos d'informació

- 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