
GUIA DOCENT

# SEGURETAT D'APLICACIONS I COMUNICACIONS

Any acadèmic 2013-14

# SEGURETAT D'APLICACIONS I COMUNICACIONS 2013-14

## Informació general de l'assignatura

| | |
|---|---|
| **Denominació** | SEGURETAT D'APLICACIONS I COMUNICACIONS |
| **Codi** | 102028 |
| **Semestre d'impartició** | 1r Q Avaluació Continuada |
| **Caràcter** | Obligatòria |
| **Nombre de crèdits ECTS** | 9 |
| **Crèdits teòrics** | 0 |
| **Crèdits pràctics** | 0 |
| **Informació important sobre tractament de dades** | Consulteu aquest enllaç per a més informació. |

# SEGURETAT D'APLICACIONS I COMUNICACIONS 2013-14

FERNÁNDEZ CAMÓN, CÉSAR
MATEU PIÑOL, CARLES
SEBE FEIXAS, FRANCISCO

## Continguts fonamentals de l'assignatura

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

## Pla de desenvolupament de l'assignatura

1. Introduction (1t)
2. Preliminaries
    1. Introductory concepts (2t)
    2. Virtualization (for use in labs) (2t, 4l, 1ex)
3. Basic Systems security (6t, 10l, 2ex)
4. Programming faults: stack exploits, etc. (2t, 4l, 1ex)
5. Basic security auditing: (4t, 6l, 1x)
6. Cryptography
    - Symmetric cryptography (6t,4l,4ex)
        - Block ciphers
        - Stream ciphers
    - Hash functions (1t,1l,1ex)
    - Asymmetric cryptography (4t,2l,2ex)
        - Mathematical background

        - The RSA cryptosystem
        - Digital signature (DSA)
7. Firewalls (5t,7l,3ex)
    - Network traffic filtering
    - Firewall design for workstations, servers and gateways
8. Authentication
    - Key management (1t)
    - Authentication applications (2t)
        - kerberos
        - X509
    - Public Key with OpenSSL (2t, 2l, 2ex)
        - PKI (1t, 2l, 1ex)
        - DNIe (2t, 3l, 1ex)
9. Comms security
    - SSL programming (2t, 3l, 2ex)
    - SMIME (1t, 2l, 1ex)
    - HTTPS (1t, 2l, 1ex)
    - OpenVPN (1t, 3l)

## Sistema d'avaluació

L'avaluació consistira en un seguit d'exercicis i problemes, marcats al Plà de desenvoluament com **ex**), i que valdràn:

1. Virtualization (2t, 4l, 1ex-5 punts)
2. Basic Systems security (6t, 10l, 2ex-7 i 7 punts)
3. Programming faults: stack exploits, etc. (2t, 4l, 1ex-7 punts)
4. Basic security auditing: (4t, 6l, 1ex-8 punts)
5. Symmetric cryptography (6t,4l,4ex - 4x3punts)
6. Hash functions (1t,1l,1ex - 3 punts)
7. Asymmetric cryptography (4t,2l,2ex - 2 x 3 punts)
8. Firewalls (5t,7l,3ex - 3 x 4 punts)
9. Public Key with OpenSSL (2t, 2l, 2ex, 7.5pts)
    - DNIe (2t, 3l, 1ex, 4.5pts)
    - PKI (1t, 2l, 1ex, 3pt)
10. SSL programming (2t, 3l, 2ex, 7.5pts)
11. SMIME (1t, 2l, 1ex, 6pts)
12. HTTPS (1t, 2l, 1ex, 4.5pts)
13. OpenVPN (1t, 3l)

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