# Network Security

Course 2021/2022

Universidad
Politécnica
de Cartagena

# Presentation

- Objectives - Become familiar with different security mechanisms, services and solutions:
  - The theoretical bases of cryptography will be examined
  - Authentication, digital signature, key management and access control services will be studied
  - Different techniques, protocols and security mechanisms used on the Internet and Intranets will be analyzed.
  - Secure protocols at the network, transport and application level
  - Firewalls and virtual private networks

# Faculty

- Teachers:
  - Mª Dolores Cano Baños (mdolores.cano@upct.es)
  - Francesc Burrull Mestres (francesc.burrull@upct.es)
  - Jose Maria Malgosa Sanahuja (josem.malgosa@upct.es)

- Consultation:
  - Tuesday from 9:00 to 11:00 and Wednesday from 9:00 to 13:00.
  - Appointment by email or MS Teams

# Theory (1/2)

## SECTION 1. INTRODUCTION TO SECURITY IN COMMUNICATIONS NETWORKS

Definition and types of attacks, vulnerabilities and threats. Basic concepts such as confidentiality, integrity, availability and authentication.

Security policy. Definition and characteristics of a security policy.

## BLOCK 2. CRYPTOGRAPHY

Block encryption. Study the operation of the main block, symmetric and asymmetric encryption algorithms (for example: AES; DES, RSA, elliptic curve,Diffie-Hellman, etc.).

Encryption in Stream. Study the operation of the main stream encryption algorithms (for example: RC4, A5, etc.)

## SECTION 3. INTERNET SECURITY

Authentication. Authentication systems and protocols, certificates and digital signature, content protection.

Application level and transport level security. Description, advantages and disadvantages. Study cases.

Network level and link level security. Description, advantages and disadvantages. Study cases.

Virtual private networks and firewalls. Description, advantages and disadvantages. Study cases.

# Theory (2/2)

- Two groups:
  - Spanish - Tuesday 15: 00-17: 00
  - English - Monday 15: 00-17: 00
  - Classroom “Aula 1.3” (or On-line by MS Teams)
- Classes will be divided into synchronous activities (live streaming on MS Teams) and into asynchronous activities
- The planning of activities will be updated in the “Aula Virtual”

# Labs (1/3)

- One group:
  - Monday - 17: 30-19: 30
  - Lab IT-2 (or Online MS Teams)
- Labs performed Individualy
- The practices start on week 2 (from today’s date, mid September approx.)
- Practices are compulsory

# Labs (2/3)

- Internal web portal: http://labit201.upct.es/seguridad/GkhJTRa2b
- In http://labit201.upct.es/seguridad/GkhJTRa2b/vm/vm.html a Linux image is available for VirtualBox, identical to the one installed in the laboratory
- It is recommended to use this image. However, if any of you already have Linux installed on your computer (probably ubuntu) or already have a Linux virtualbox image (i.e. from another course), you can use it, as long as you install the following packages: openssl, steghide, pwgen, nmap, self-signature, gpg, thunderbird, apache2 and mininet
- Download the image by mid September. It is a relatively slow process. Should not be done during class hours

# Labs (3/3)

- At the end of each practice, there will be a small control (no reports have to be submitted)
- The final mark of practices is the **average of each control**

# Labs

- PRACTICE 1: Hash functions applied to user authentication
- PRACTICE 2: Everyday uses of cryptography
- PRACTICE 3: Setting up a secure portal
- PRACTICE 4: Configuring a firewall

# Continuous evaluation

- The final grade is divided into the following parts:
  - Theory exam (to be carried out during the week of the second partal exams). Through questions, tests and/or problems the theoretical concepts presented in class will be evaluated: **50%**
  - Activities proposed by the teacher in class or other means: **20%** (throughout the semester)
  - Laboratory questionnaires: **30%** (throughout the semester)

- In order to pass, you need a **minimum grade of:**
  - 4 out of 10 in the exam and in the laboratory questionnaires
  - 3 out of 10 in class activities

  Only then the average mark gets calculated.

# Bibliography

Check for recent editions of these books in the library

- "Handbook of applied cryptography", Menezes, Oorschot, Vanstone, CRC Press, 1996. ISBN: 0-8493-8523-7.
- "Cryptography and network security principles and practice", William Stallings, Prentice Hall International Editions, 1999.
- "Internet and Intranet security", Rolf Oppliger, Artech House, 1999.
- "Computer Communications Security. Priciples, Standard Protocols and Techniques", W. Ford, Prentice Hall, 1994. ISBN 0137994532.
- "Seguridad y comercio electrónico en la web", Simson Garfinkel, Gene Spafford, Osborne McGranw-Hill /International from Spain, ISBN 970-10-2142-8.
- "Network Security, Private Communications in a Public World", C. Kaufman, R. Perlman, M. Speciner, C. Kaufman, Prentice Hall, 2002, ISBN 0130460192.
- "Building and Managing Virtual Private Networks ", D. Kosiur. JohnWiley & Sons, 1998.
- "Introducción a la criptografía", Pino Caballero Gil. Editorial Ra-Ma. 2nd edition, 2002. ISBN: 84-7897-520-9.
- "Applied cryptography: protocols, algorithms and source code in C ", Bruce Schneier, John Willey &Sons Inc., 1996.
- "Network and Internetwork Security: Principles and Practice", W. Stallings, Prentice Hall, 2nd edition, 1999, ASIN: 0024154830.
- "Firewalls and Internet Security: Repelling the Wily Hacker ", WR Cheswick, YE Bellovin, AD Rubin, 2nd Edition, Addison Wesley, 2003, ISBN 020163466X.
- "Secure Electronic Commerce: Building the infrastructure for Digital Signatures and Encryption", W. Ford, MS Baum, 2nd Edition, Prentice Hall, 1997, ISBN 0130272760.
- "Protect your Privacy: The Pgp User's Guide", W. Stallings, Prentice Hall, 1994, ISBN 0131855964.
- "Security Technologies for the World Wide Web ", R.Oppliger, Artech House, 2000, ISBN 1580530451.
- "Criptografía digital: fundamentos y aplicaciones", José Pastor Franco, Miguel Ángel Sarasa López. University Publications, University of Zaragoza.