



Segurança em Redes de Computadores (SRC) / Computer Networks Security



Redes de Comunicação de Dados

Departamento de Engenharia da Eletrónica e das Telecomunicações e de
Computadores

Instituto Superior de Engenharia de Lisboa

Polytechnical University of Lisbon (IPL)



**POLITÉCNICO
DE LISBOA**

Computer Networks Security (SRC) – Syllabus (1)



- Facts about safety.
- Threats, vulnerabilities and attacks.
- Cryptography (hash algorithms, key distribution, symmetric (substitution and transposition, algorithms from Cesar to AES) and asymmetric ciphers (introduction to number theory/modular mathematics, elliptical curves, RSA), digital certificates x.509 and certification authorities, digital signatures (DSA, Schnorr)).
- Security for dial-in access (access control - 802.1x, RADIUS, support for VPN - PPTP, L2TP).
- Communications security at the various layers of the OSI model (IPsec, IKEv2).
- Security in Web (SSH, SSL / TLS, HTTPS)
- Security in wireless networks (WLAN – from WEP to WPA 3).
- Security services in email (security in SMTP, POP, IMAP, MIME; Sender Policy Framework (SPF), Domain keys)

Computer Networks Security (SRC) – Syllabus (2)



- Security concepts applied in Blockchain e Smart Contracts.
 - Security in IoT.
 - Security policies.
 - Security in network management.
- Security practices: Routers, firewalls, IDS and traps.

Bibliography



Bibliografia de consulta/existência obrigatória (1.000 carateres).

- Folhas/Slides da disciplina
- “Cryptography and Network Security - Principles and Practice, 8th edition”, William Stallings, Prentice-Hall, 2020
- “Internet Security: A Hands-on Approach, Second Edition”, Wenliang DU, CreateSpace, 2019

Outra bibliografia

- “Computer security - Hands-on approach, Second Edition”, Wenliang DU, CreateSpace, 2019
- “Segurança em Redes Informáticas, 5ª edição”, André Zúquete, FCA, 2018



- Componentes de avaliação:

- 2 testes parciais ou um teste global nas datas de exame
- Fichas teóricas
- Trabalhos práticos

Pode ser realizada melhoria de nota de um dos testes parciais durante o exame da 1ª época

Os testes parciais são com consulta de uma folha A4 manuscrita que não pode ser fotocópia. Os testes globais são com consulta de duas folhas A4 manuscritas que não podem ser fotocópias.

- Para obter aprovação nesta UC um aluno deve:

- Realizar as componentes da avaliação pedagogicamente fundamentais: Maioria das fichas teóricas e os trabalhos práticos.
- Ter média da componente teórica igual ou superior a 10 valores
- Ter média da componente prática igual ou superior a 10 valores
- Ter média final igual ou superior a 10 valores
- Nota igual ou superior a 8 valores nos testes parciais que contarem para a média da nota da componente teórica

Nota final = 60% nota componente teórica + 40% nota componente prática + [-1..1] valores pelas fichas teóricas

Em caso de dúvida consultar: “NORMAS DE AVALIAÇÃO DE CONHECIMENTOS” do ISEL