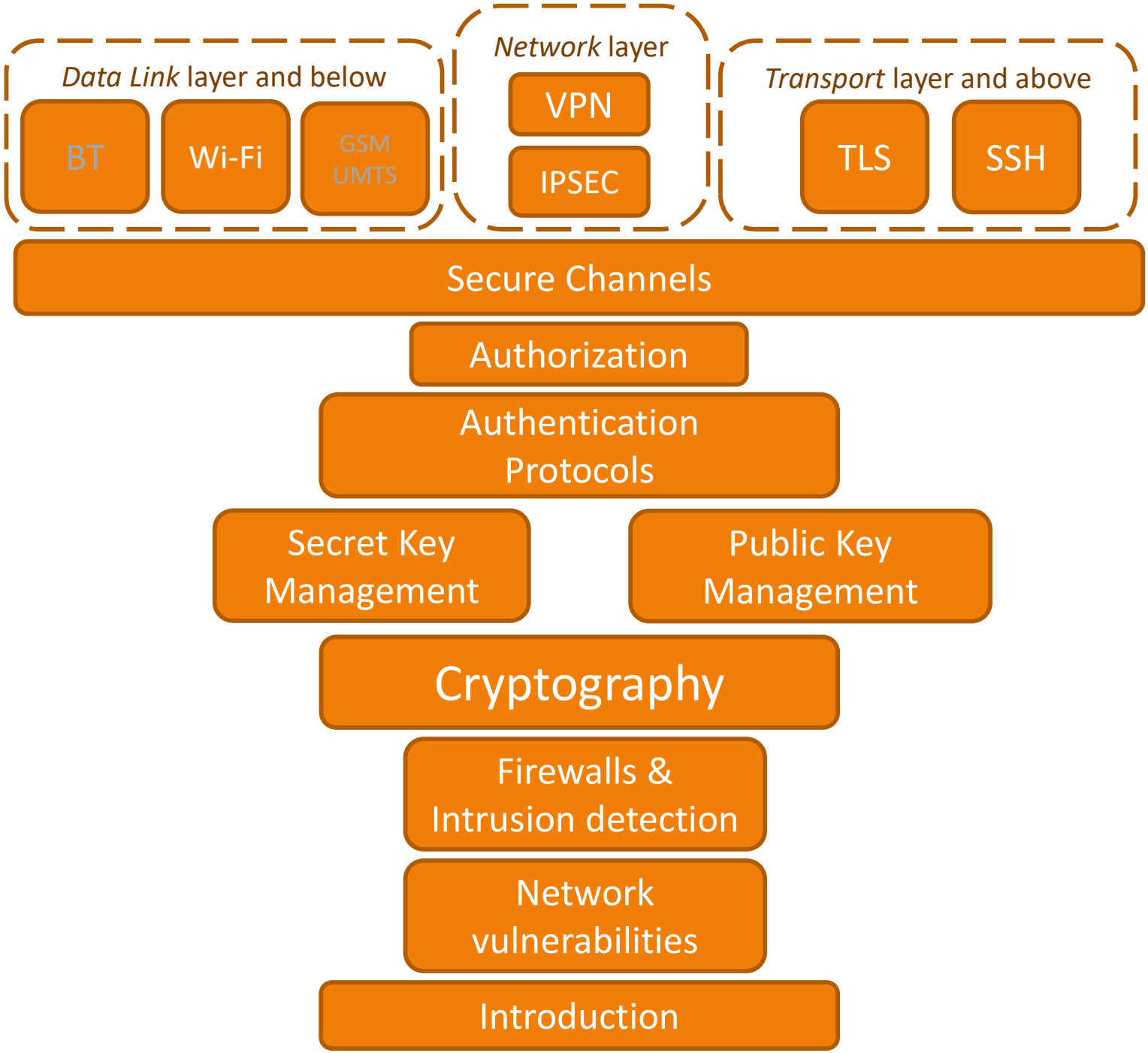
TÉCNICO LISBOA

General information on SIRS

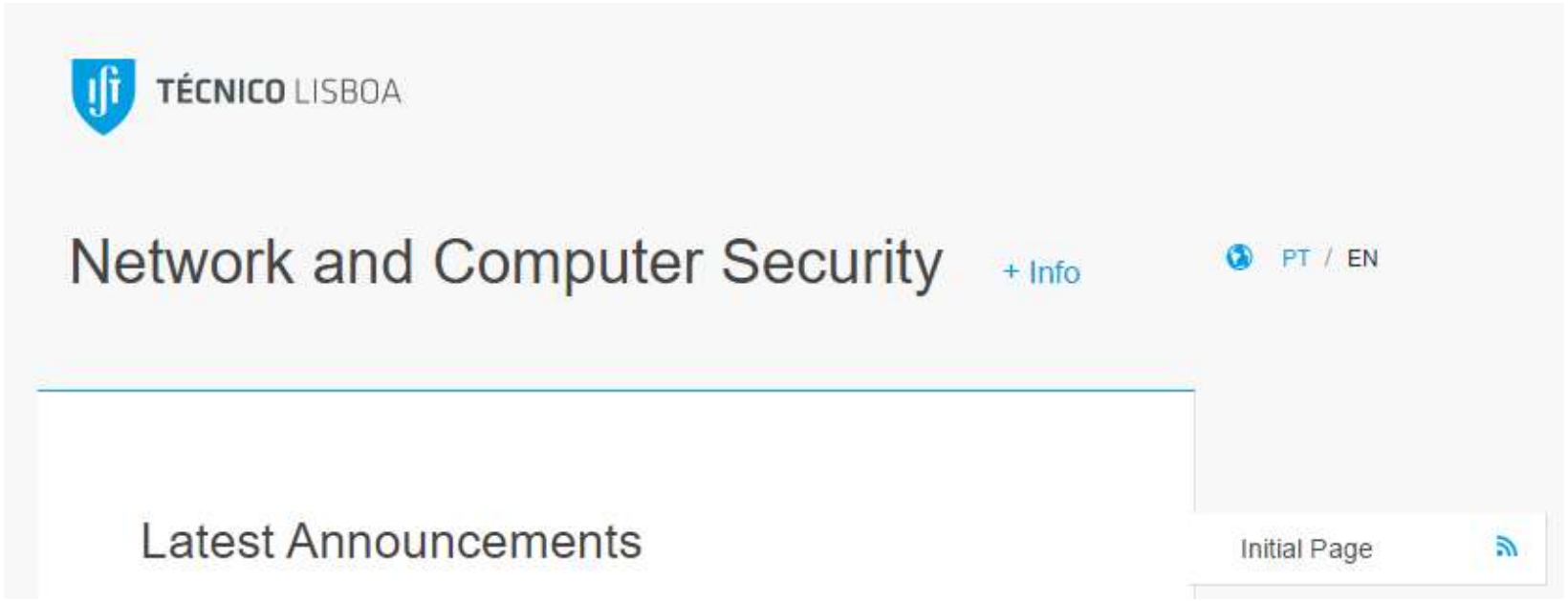
Security in Computer Networks and Systems

Segurança **I**nformática em **R**edes e **S**istemas
2022/23

Miguel Pardal


Data Link layer and below
BT
Wi-Fi
GSM
UMTS
Network layer
VPN
IPSEC
Transport layer and above
TLS
SSH
Secure Channels
Authorization
Authentication
Protocols
Secret Key
Management
Public Key
Management
Cryptography
Firewalls &
Intrusion detection
Network
vulnerabilities
Introduction

Official Page: Fénix



- All information in this presentation is superseded by whatever is in Fénix

General Information

- **meic-sirs**@disciplinas.tecnico.ulisboa.pt
  - Subject: **[SIRS]** …

- Lab Classes
  - Lab guides/assignments
    - Have them prepared before class!
  - Project

- Grades
  - Theory (50%) + Practice (50%)

Teaching staff

- Theoretical lectures:
  - Miguel Pardal
  - Ricardo Chaves
- Lab/project lectures:
  - João Garcia
  - David R. Matos
  - Miguel Guerreiro
  - Afonso Gomes
  - André Mendes


MP


RC


JOG


DRM


MG


AG


AM

Lecture Plan

Calendar Week	Teaching Week	Class	Lectures (2h+2h)	Teacher	Evaluation	Labs (1,5h+1,5h)	Project
21-Nov	1	1	Introduction Network basics (OSI, MAC, IP) + passive and active attacks Network vulnerabilities: layers 1 (sniffer), 2 (ARP spoofing), 3 (IP spoofing)	MP		Enroll groups /Install SEED Labs https://github.com/tecnico-sec/Setup	Assemble groups + Project overview + choice of project scenario
		2	Network vulnerabilities layers 4 (TCP spoofing, SYN flood), layer 7 (DNS, Kaminsky attack) Application layer vulnerabilities (example of remote code execution through code injection e.g. PHP and SQL)	MP		Virtual networking https://github.com/tecnico-sec/Virtual-Networking	
28-Nov	2	3	Firewall and IDS	MP		Traffic Analysis https://github.com/tecnico-sec/Traffic-Analysis	Project infrastructure (virtualize app/api server + db server) + configure firewalls
		4	Criptography overview: services, primitives, properties Symmetric ciphers: stream, blocks, block modes Hash functions and MAC	RC		Firewall https://github.com/tecnico-sec/Firewall	

Lecture Plan (cont.)

Calendar Week	Teaching Week	Class	Lectures (2h+2h)	Teacher	Evaluation	Labs (1,5h+1,5h)	Project
5-Dec	**3**	5	Asymmetric ciphers (RSA, ECC) + Digital Signatures	RC		Java Crypto https://github.com/tecnico-sec/Java-Crypto	Project standard secure channel (e.g. TLS configuration between app/api-db) + Project custom security protocol proposal
		6	Public key management + digital certificates X.509 Secure channels with TLS and SSH	RC		Secure Messages https://github.com/tecnico-sec/Secure-Messages	
12-Dec	**4**	7	Secret key management + secret key distribution protocols (DH, Kerberos)	RC		Project proposal	Project custom security protocol development + feedback
		8	Autentication + authentication protocols (EKE)	RC			
19-Dec	**5**	9	Authorization (XACML, Oauth, tokens, mobile apps)	RC		Project support	Project implementation + feedback
		10	Wi-Fi Security WEP, WPA, WPA2 + 802.1X + WPA3	RC			
26-Dec	Christmas Holidays						
2-Jan	**6**	11	IPsec + TLS + SSH (in depth)	MP		Project support	Project advanced implementation + report draft feedback
		12	VPN (topologies host-to-host, host-to-net, net-to-net; using IPsec, TLS)	MP	P (6-Jan 17:00)		
9-Jan	**7**	13	Certification & Assurance (Common Criteria)	MP		Project presentations	Project evaluation
		14	Overview/Conclusion	MP			

Labs feedback

- Labs
  - Laboratory guides
    - During first half of period
    - Should be prepared before the lab session
  - Group teamwork
  - No grades, but individual progress is recorded, and feedback is provided
    - Red - lab goals not met/demonstrated
    - Yellow - lab goals partially met/demonstrated
    - Green - lab goals fully met/demonstrated
  - First parts of project should be made in the labs

Grade assessment (practice)

- Project
  - 3 Students per group
  - Enrollment is done in lab of first week
  - Minimum grade: 8 out of 20
  - Can be reused from last year (only)
- Overview
  - Choice of scenario
    - this week
  - Infrastructure
  - Configuration of secure channels
  - Security challenge
    - Solution Proposal
    - Feedback
  - Development with feedback on labs
  - Report is built iteratively
  - Submission
    - Jan 6th
  - Presentations and Discussions
    - Week of Jan 9th
    - Each group member will answer individual questions

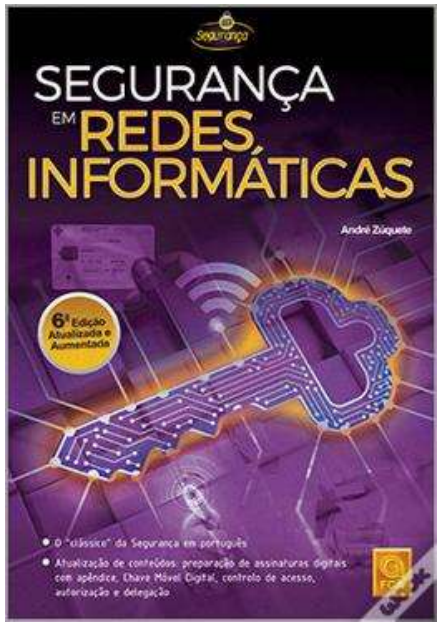
Grade assessment (theory)

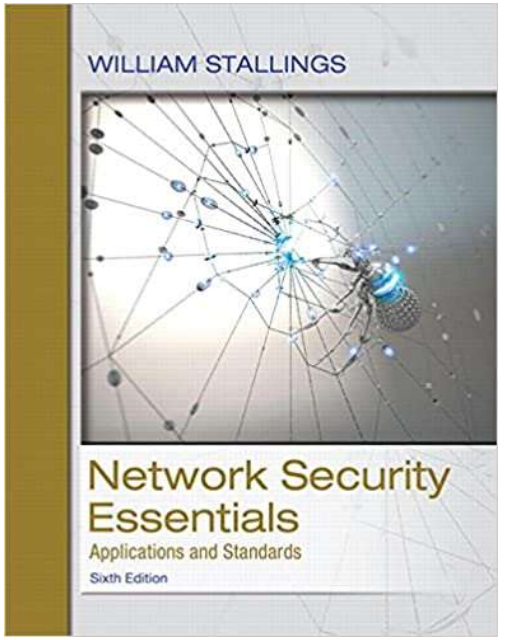
- 1 exam
  - Exam has a minimum grade of 8 values
- There is a recovery exam

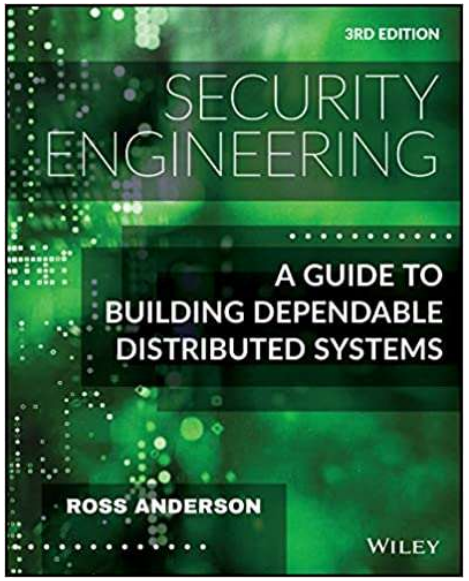
- Theoretical grade is the best of the two exams

Bibliography

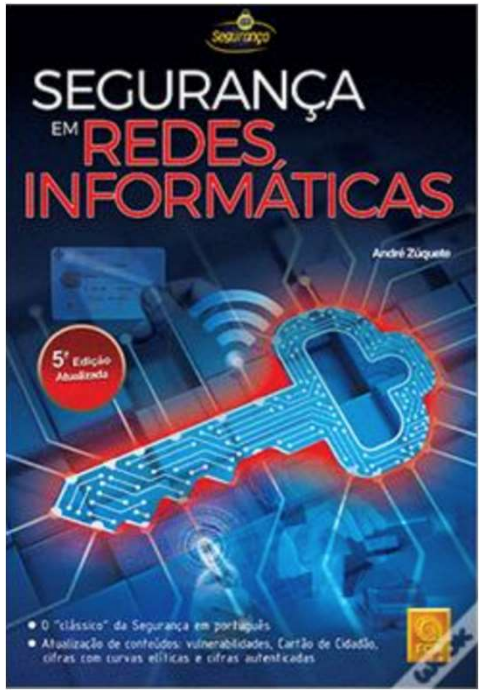
- Primary:
  - Zúquete21 (PT)
  - Stallings17 (EN)
- Secondary:
  - Anderson21 (EN)

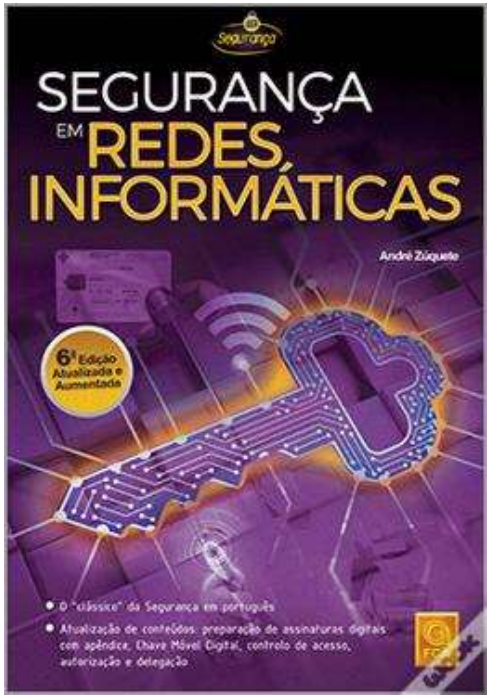






New edition of Zúquete





Both are OK, but latest is better

Ethics and law

- The purpose of the course is to learn how to protect computer systems from cyber-attacks
  - but some of the things you learn may also be used to attack them
- Notice that
  - Attacking systems is unethical and punished by law
  - Even just “testing” systems without written permission is punished by law
- “~~Do not try this at home~~”
  → “Try this only at home”

Assessment: Special Season

- Isolated from the regular period
- Grades from the normal period cannot be reused
- Exam (50%)
- Individual project (50%)