TÉCNICO LISBOA

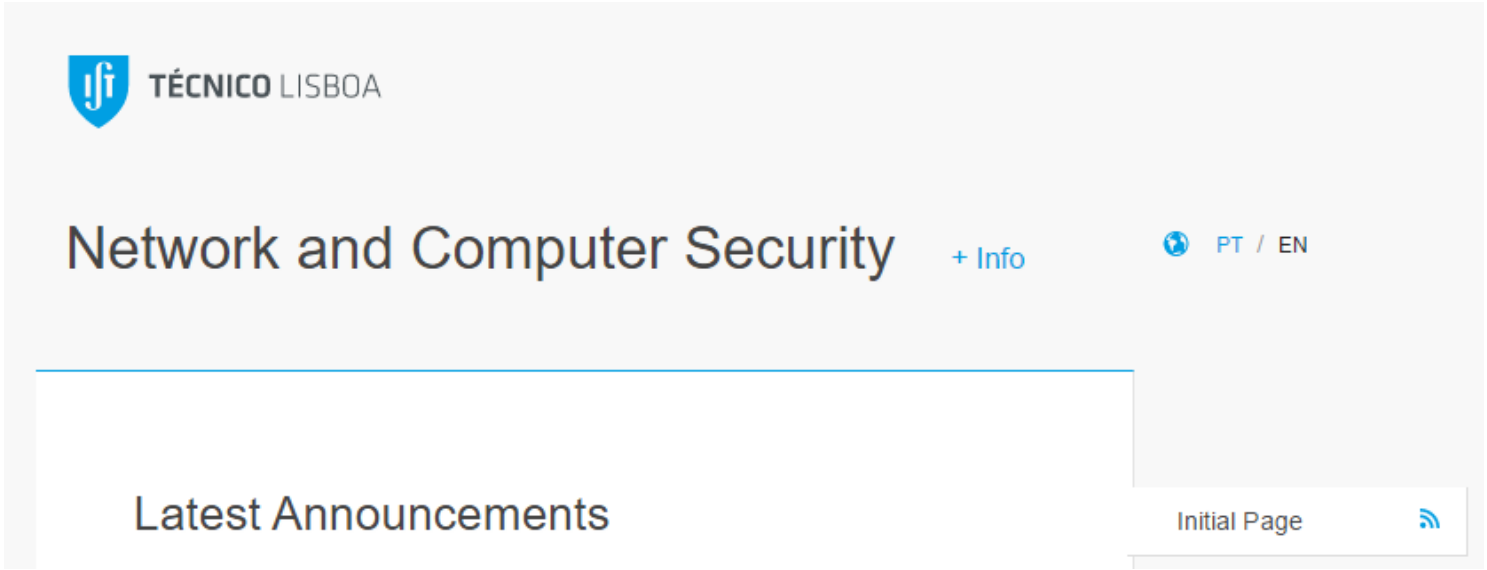
Course information

Security in Computer Networks and Systems

Segurança **I**nformática em **R**edes e **S**istemas
2024/25

David R. Matos, Ricardo Chaves

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- All information in this presentation is superseded by whatever is in Fénix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]** …

- Lectures
- Labs
  - Guides
    - Have them prepared before class
  - Project

- Grades
  - Theory (50%) + Practice (50%)
  - Passing grade: 9,5 values (out of 20)

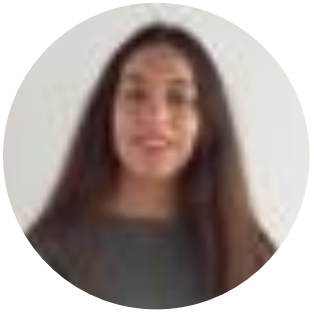
Teaching staff

- Theoretical lectures:
  - David R. Matos
  - Ricardo Chaves
- Lab/project:
  - Ricardo Chaves
  - David R. Matos
  - Christof Torres
  - Mafalda Ferreira
  - Martim Monis
  - Miguel Eleutério

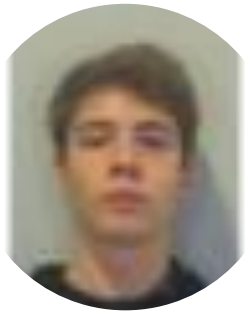

DRM

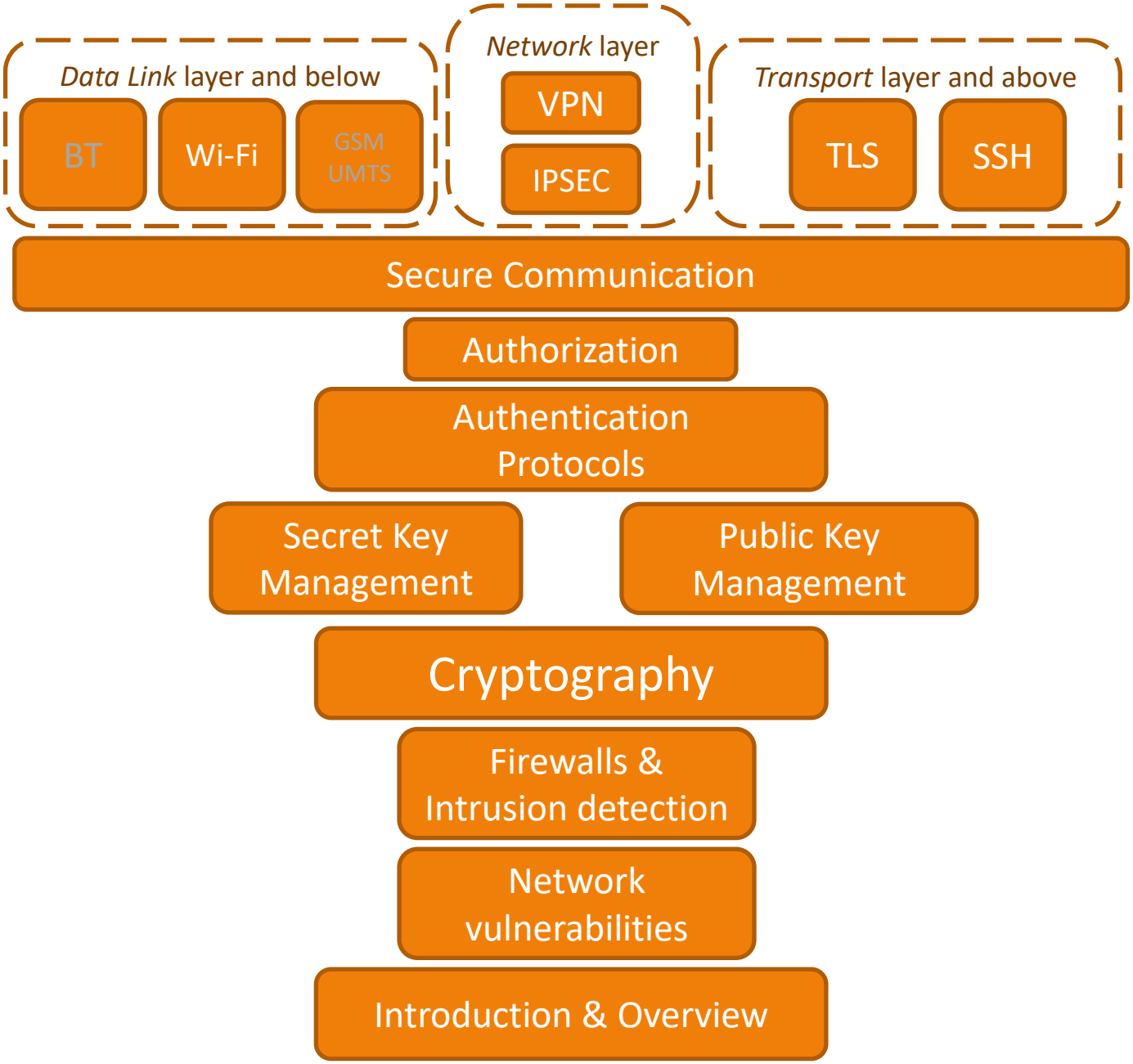

RC


CT


MF

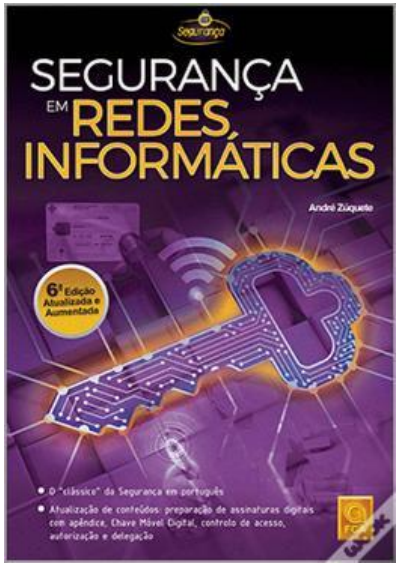

MM

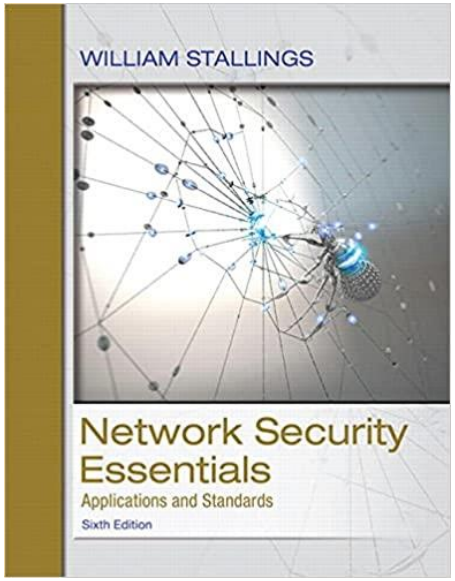

ME

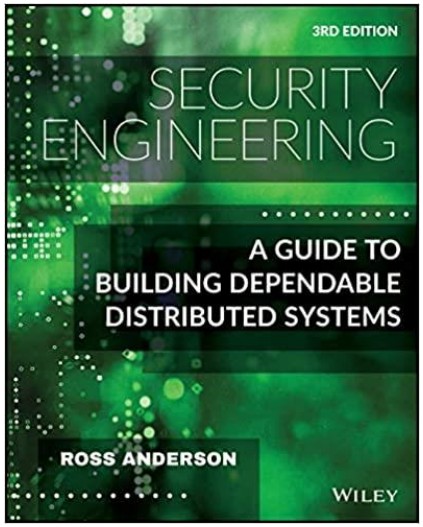

Data Link layer and below
BT
Wi-Fi
GSM
UMTS
Network layer
VPN
IPSEC
Transport layer and above
TLS
SSH
Secure Communication
Authorization
Authentication
Protocols
Secret Key
Management
Public Key
Management
Cryptography
Firewalls &
Intrusion detection
Network
vulnerabilities
Introduction & Overview

Bibliography

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







Grade assessment (theory)

- 1 exam
  - January 23rd, 10:30
  - Exam has a minimum grade of 8 out of 20 values
- There is a recovery exam
  - February 6th, 18:00
  - Theoretical grade is the best of the two exams

Ethics and law

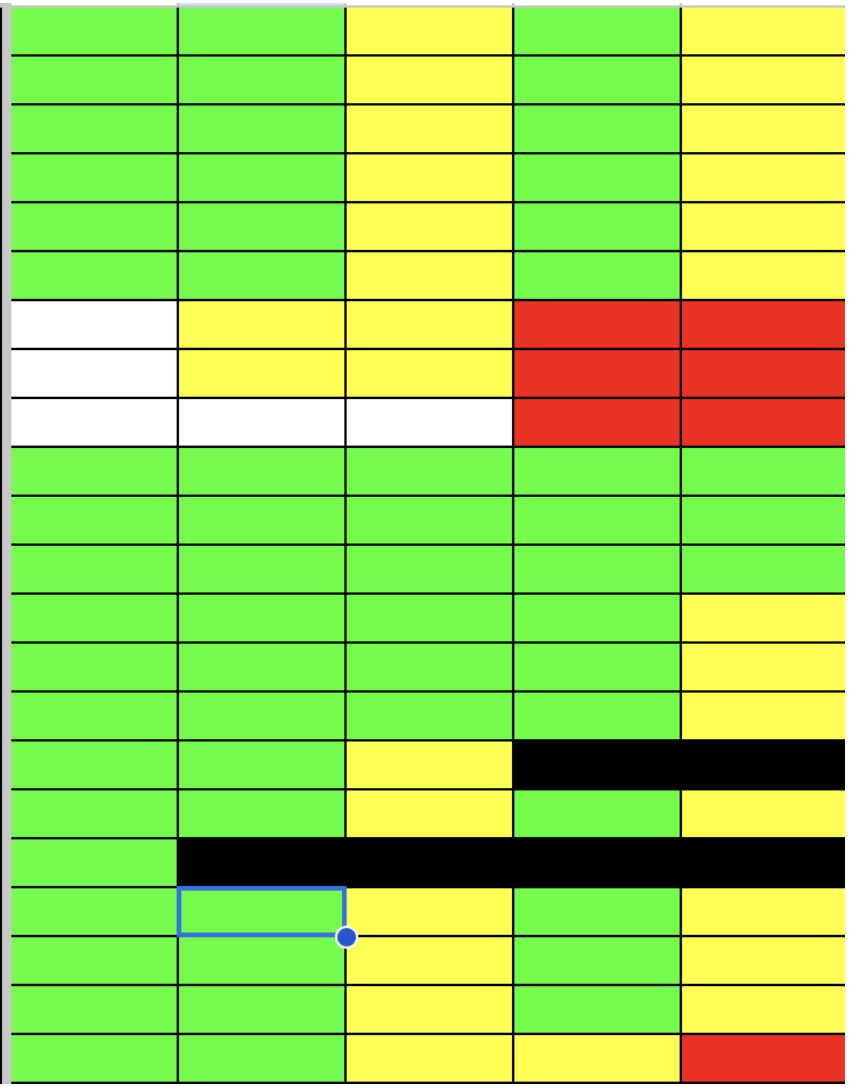
- The purpose of the course is to learn how to protect computer systems from cyber-attacks
  - but some of the things you learn may also be used to attack them
- Notice that
  - Attacking systems is unethical and punished by law
  - Even just "testing" systems without written permission is punished by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

Labs

- Labs
  - Laboratory guides
    - Should be prepared before the lab session
  - Group teamwork
    - To learn and build the project
  - Feedback to individual progress is recorded (not graded)
    - We expect you to **proactively show your work**
    - Red – no evidence of progress
    - Yellow – progress partially demonstrated
    - Green – progress demonstrated

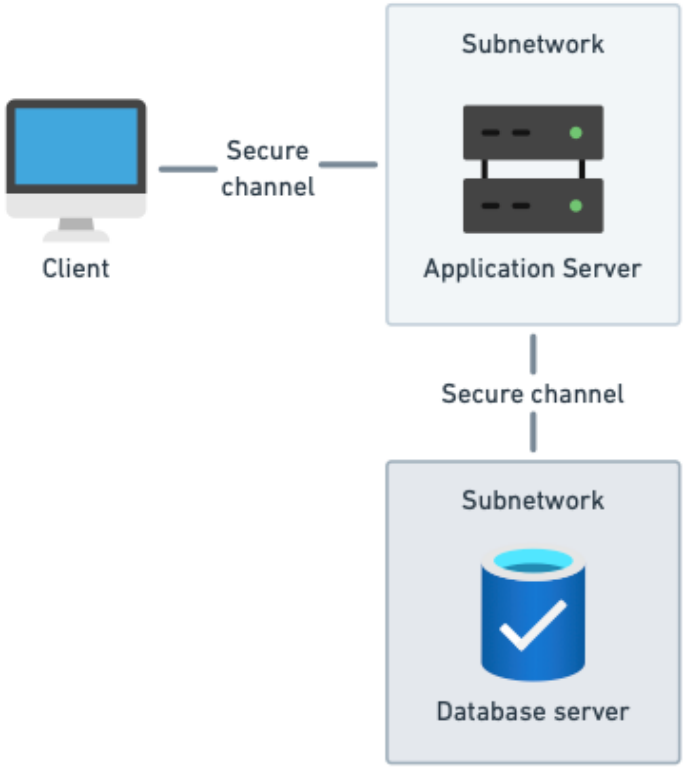
Feedback sheet

Alameda	26
Alameda	26
Alameda	26
Alameda	27
Alameda	27
Alameda	27
Alameda	63
Alameda	63
Alameda	63
Tagus	4
Tagus	4
Tagus	4
Tagus	5
Tagus	5
Tagus	5
Tagus	9
Tagus	9
Tagus	9
Tagus	10
Tagus	10
Tagus	10
Tagus	11



Project

- Overview
  - Choice of business scenario
  - Secure document/message library
  - Server Infrastructure
  - Configuration of secure channels
  - Security challenge
- Feedback
  - Demonstrate progress in labs
  - Build report gradually
- Dates
  - Mid point status: November 29th
  - Submission: December 20th
  - Presentations/Discussions: January 6th – 12th



Grade assessment (practice)

- Project
  - 3 Students per group (of the same class slot)
  - Enrollment is done in lab of first week
  - Minimum grade: 8 out of 20
  - Can be reused from last year (only)
    - If you want to reuse, **do not** enroll in the lab
- Each group member will answer individual questions

Assessment: Special Season

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

Summary Plan

Week		Theoretical	Practical
1		Introduction	(groups) + Virtual Machine
2		Cryptography	Project: cryptography
3		Network vulnerabilities	Virtual Networks + Traffic analysis
4		Firewall and Intrusion Detection	Project: infrastructure + firewalls
5		Key management and distribution	Project: security challenge
6		Authentication and authorization	Project
		Secure Communication: Wi-Fi, TLS	finalization
		(Christmas break)	
7			Project presentations/discussions