DI-FCT-UNL
Segurança de Redes e Sistemas de Computadores
Network and Computer Systems Security

Mestrado Integrado em Engenharia Informática
MSc Course: Informatics Engineering

1st Sem. 2019/2020

Course Overview

Generic Information

Course Information and Documentation

Course / Regency, Lectures and Labs:

Henrique João Domingos

hj@fct.unl.pt

P2/6 DI/FCT/UNL, Ext 10727

Docs/Info:

- See the CLIP System
- Also: asc.di.fct.unl.pt/~hj/srsc1920
  - Materials to support LABs/Practical Classes

See available slots for face-to-face contact (CLIP) for any course questions or other related issues.

Please avoid the use of Email for this purpose

No timely response guaranteed

Course activities

- **Lectures**
  - Exposition of Program topics
    - Bibliography: suggested readings

- **Pract./Labs**
  - Practical presentations/demonstrations/verifications/ exercises/
  - Programming Exercises
  - Materials/elements for the development of Work-Assignments (work-assignments) /
  - Face-to-Face clarifications/discussion

Class attendance sheets for registration of students' participation. This is informative (no direct implications in evaluation)

Course activities and calendar

- **Lectures**
  - **Room 2B Ed VII**
    Thursday, 16h-18h
- **Pract./Labs**
  - **Lab 110 Ed.II**
  - **P2:** Tuesday 16h-18h
  - **P3:** Tuesday 18h-20h
  - **P1:** Thursday 18h-20h

Calendar (FCT/UNL) *

- **1st Week:**
  - **9-13/Sep**
- **+ 13 Class Weeks:**
  - **16/Sep – 13/Dec**
- **Final frequency evaluations:**
  - **16-21/Dec**
- **Exams**
  - **4-20/Jan**

) https://www.fct.unl.pt/sites/default/files/calendario_escolar_19-20.pdf)

Evaluation

Assessment

T1,T2: Frequency tests (midterm): 60%

- Individual tests, Registration on CLIP
- Cover program topics/bibliography ref.
  - 1h-1h30 (closed book questions)
  - 1h- 1h30 (open book questions)
    - Includes practical related questions:
      - » (Labs/Exercises/Demos, and TP1, TP2 Context)

TP1,TP2: Work-assignments as mini-projects: 40%

- Groups of two students
- Development + Proof of Work + Report and Evaluation Forms
  - Submission and evaluation criteria with Assessment Forms
  - Selected students can be asked for Demo-Proofs and Discussion

Assessment Components and Grade Conditions
(See also in the CLIP system)

F: Frequency

F = 15% TP1 + 25% TP2

Frequency if:

F > 9,5/20 with TP2>=7,5/20

Grade conditions

- **With midterm tests (no final exam):**

  AF = 25% T1 + 35% T2 + 15% TP1 + 25% TP2

  Pass (Grade) if: AF >= 9,5/20 and
  average (T1,T2) >=9,5/20

- **With final exam (E)**

  F > 9,5 / 20

  AF = 60% E + 15% TP1 + 25% TP2

  Pass (Grade) if: AF >= 9.5/20 and E >= 7.5/20

Work Assignments: Practical Evaluation

- Developed in Group (Max. 2 Students)
  - Requires Lab Presence of group members (more than 60% of presences in Labs)
    - Recommended !
  - Optionally can also be developed as individual work and individual evaluation
  - Registration in Labs (Practical Classes) until 30/Sep
  - Registration forms for practical evaluation are available for registration
- Students with frequency (2016/2017 to 2018/2019) can use the previous practical evaluation
  - Students w/ 2018/2019, 2snd semester frequency can reuse/improve projects previously developed, according to specific proposals that must be validated

Assessment Calendar

Final Dates (already fixed by the Pedagogic Comm.)

Midterm Tests: Required registration - CLIP System

Defined Dates:	Registration (CLIP):
T1: Test #1: 8/Nov/19, Friday, 18h	until 1/Nov/19
T2: Test #2: 9/Dec/19, Monday, 18h	until 2/Dec/19

Work-Assignments/Mini-Projects
Form (Group/Individual) Registration Required:

WA#1: Deliv./Submission until 31/Oct, 24h00
- Consider for your development plan: from 2 to 30/Oct

WA#2: Deliv./Submission until 6/Dec. 24h00
- Consider for your development plan: from 4/Nov to 5/Dec

Program Topics and Bibliographic References

Program: Main Topics (details in CLIP)

1. Introduction: initial concepts and terminology
2. CSNS Foundations, Frameworks and Standards
3. Applied cryptography: models, methods, algorithms and tools
4. Authentication services and protocols; User-authentication
5. Access control, OS-Based Access Control

6. Network Security Services, Protocols and Standards
   - Network Access Control
   - TCP/IP Security Stack: WEB Sec/HTTPS/TLS, SSH, IPSec and VPNs, Email Security Services, DNSSEC

7. Computer systems security:
   SW / OS Security
   Trust Computing: TPMs and TEEs
   Intrusion Detection and Intrusion Prevention

Main Bibliography

[WS-NSE] W. Stallings,
Network Security Essentials - Applications and Standards, Pearson-Prentice Hall (6th Ed., 2017)
http://www.williamstallings.com/NetworkSecurity/

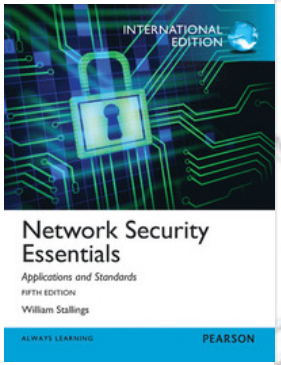
[WS-CS] W. Stallings, L. Brown, Computer Security
- Principles and Practice, Pearson (4th Ed., 2018)
http://www.williamstallings.com/ComputerSecurity/

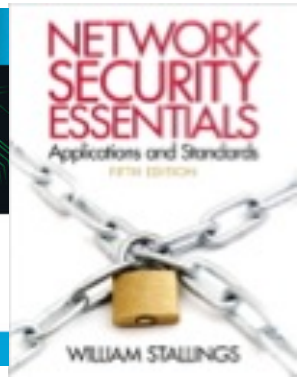
[WS-CNS] W. Stallings, Cryptography and Network Security, Pearson (7th Ed., 2017): More on Cryptography
http://www.williamstallings.com/Cryptography/

See complementary ref. of bibliography / materials in CLIP Additional Refs. Suggested for specific program topics on lectures and slides

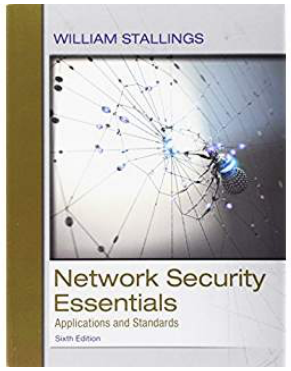
Main Bibliograhy (and prev. editions)

[WS-NSE]





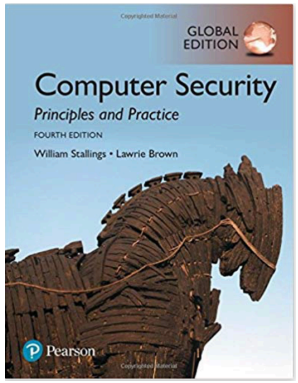
5th Ed. 2013



6th Ed. 2017

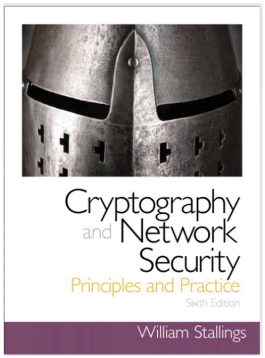
[WS-CS]

3th Ed. 2014

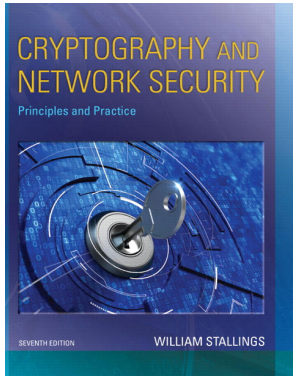


4th Ed. 2018

[WS-CNS]



6th Ed. 2014



7th Ed. 2017

Plan: Lectures vs. Weeks/Sessions

1. Overview/Introduction	W1-W2
2. Crypto Methods, Models, Alg. and Tools: Symmetric Encryption Assym. Cripto + Secure Hashing, MACs and Digital Signatures	W3-W4-W5
3. Authentication Services and Protocols	W5-W6
4. X509 Authentication and PKIs	
5. User Authentication	W6-W7
6. Access Control	W7-W8
7. TCP/IP Sec. Stack: HTTPS TLS/SSL, IPSec/VPNs + Email Security	W8-W10
8. Net. Access and LAN/WLAN Security	W11
9. OS Security and Virtualization	W11-W12
10. Trusted Computing and TEEs	W13
11. Intrusion Detection/Prevention/Recovery	W14

Program Topics vs. Bibliog.

	[WS-NSE]	[WS-CS]
1. Overview/Introduction	[WS-NSE], C1	[WS-CS], C1
2. Crypto Methods, … Symmetric Encryption Assym. Cripto + Secure Hashing, MACs and Digital Signatures	[WS-NSE], C2 [WS-NSE], C3	[WS-CS], C2
3. Authentication Services and Protocols	[WS-NSE], C4	[WS-CS], C23
4. X509 Authentication and PKIs		
5. User Authentication		[WS-CS], C3
6. Access Control		[WS-CS], C4
7. TCP/IP Sec. Stack: HTTPS TLS/SSL, IPSec/VPNs + Email Security	[WS-NSE] C6, C7, C8, C9	[WS-CS], C22, C24
8. Net. Access and LAN/WLAN Security	[WS-NSE] C5	[WS-CS], C24
9. OS Security and Virtualization		[WS-CS], C12
10. Trusted Computing and TEEs	Prov Readings	[WS-CS], C13
11. Intrusion Detection/Prevention/Recovery	[WS-NSE], C11, C12	[WS-CS], C8, C9

Program Topics vs. Bibliog.

	[WS-NSE]	[WS-CNS]
1. Overview/Introduction	[WS-NSE], C1	[WS-CNS], C1
2. Crypto Methods, …	[WS-NSE], C2	[WS-CNS], C1–C7
Symmetric Encryption	[WS-NSE], C3	[WS-CNS], C8–C10
Assym. Cripto + Secure Hashing, MACs and Digital Signatures		[WS-CNS], C11–C13
3. Authentication Services and Protocols	[WS-NSE], C4	[WS-CNS], C14
4. X509 Authentication and PKIs		
5. User Authentication		[WS-CNS], C15
6. Access Control		
7. TCP/IP Sec. Stack: HTTPS TLS/SSL, IPSec/VPNs + Email Security	[WS-NSE] C6, C7, C8, C9	[WS-CNS], C17 C18, C19, C20
8. Net. Access and LAN/WLAN Security	[WS-NSE] C5	[WS-CNS], C16
9. OS Security and Virtualization		
10. Trusted Computing and TEEs	Prov Readings	
11. Intrusion Detection/Prevention/Recovery	[WS-NSE], C11, C12	

SRSC / CSNS, 1920

Previous Skills
(Required Knowledge Base)

Relationships w/ Other Courses

Previous Courses and Knowledge Base

- **SRSC is a Consolidation Course in the MIEI Curriculum**

- **Precedent Knowledge / Recommended**
  - Computer Networks
  - Distributed Systems
  - Operating Systems
  - Courses on Programming / Data Structures and Algorithms (Java/Web/Rest Programming)

Practical skills

Computer Networks, Distributed Systems

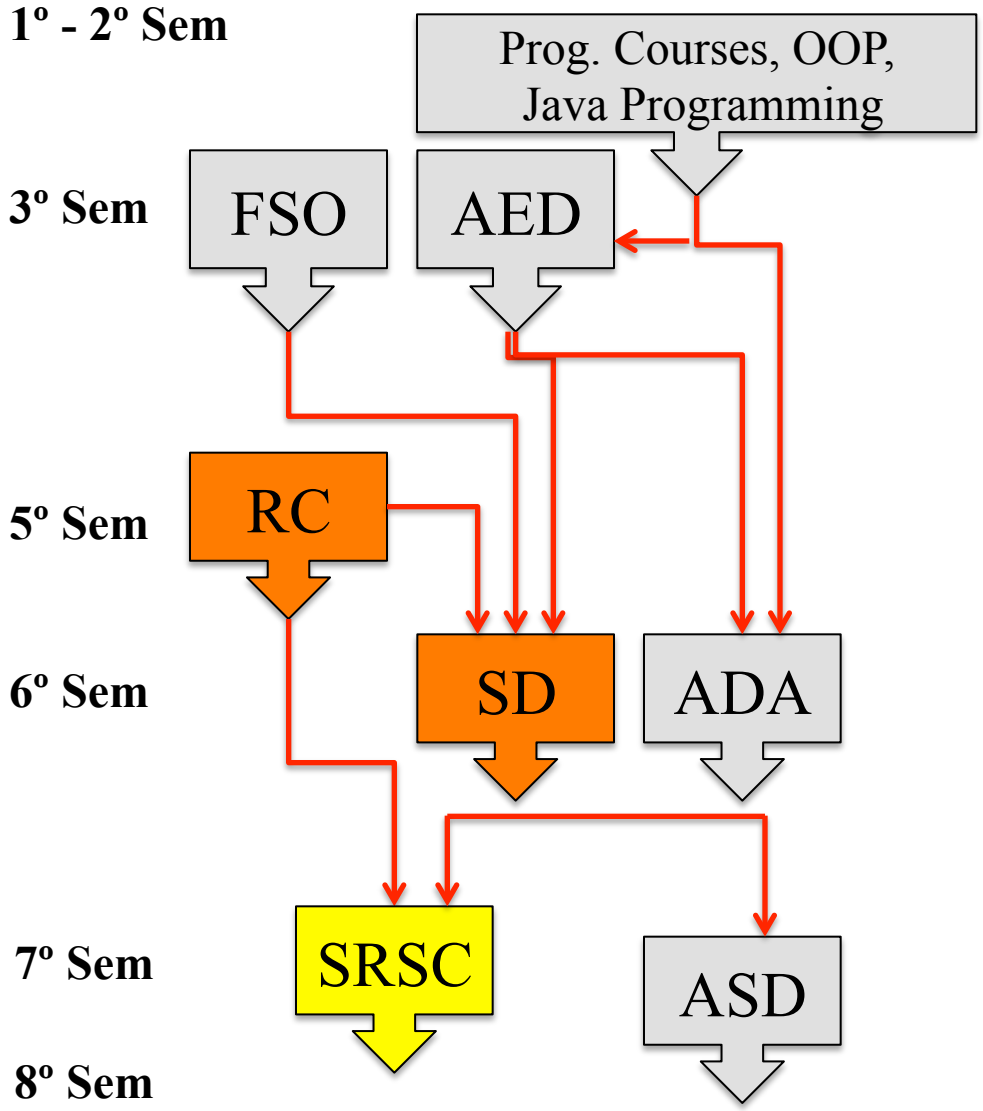
- Good Skills and Autonomy for **Distributed Systems Programming**

TCP/IP Appl. Programming and Java Programming/Tools

- Network Programming and Distributed Programming
- Sockets, WebSockets, Java RMI, Rest (WS)

- Eclipse IDE (or other)
- Basics in OS Management/Admin Experience (Terminal/Console) Shell Environment
- MacOS or Linux / Shell Environment
- Java Programming,
- Windows Console / Linux/Shell based emulation on Windows , Java Tools, Executable Jars
- Practice w/ Virtual Environments (Linux VMs / VBox or Vmware)
- Development/Deployment with Docker (Docker Containerized Services and Applications)

MIEI Sequence / Requirements



Programming Techniques and Dev. Environments

- Java Programming and Java Dev. Tools/Env.

Operating Systems

- Principles and Practice

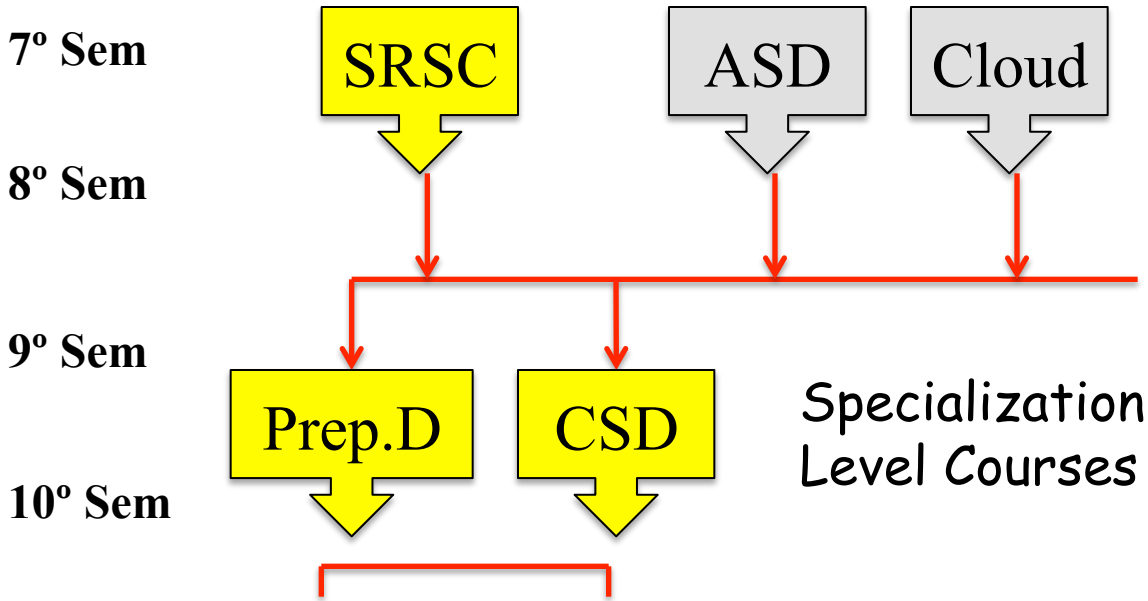
Computer Networks Foundations and Practice

- Services/Standards and Protocols in the TCP/IP Security Stack

DS Foundations, principles and paradigms

- DS Programming: WS/REST, Docker Containment

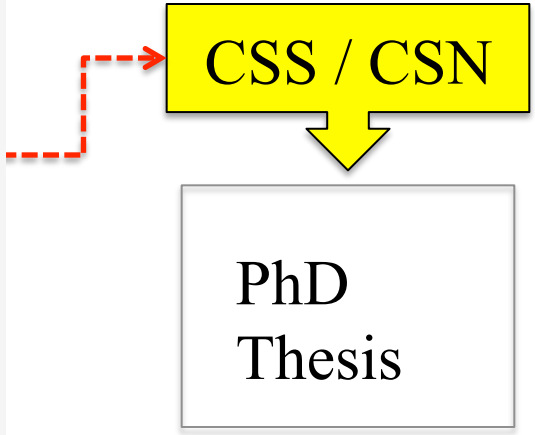
Future projection on MIEI and PhD Program



- Advanced Distributed Systems
- Cloud Computing and Storage

- Dependable Distributed Systems
- Privacy-Enhanced Systems / Privacy Preservation
- Cloud-Security and Privacy
- Privacy-Enhanced Data Analytics
- Blockchains
- Mobile Computing Security
- IoT Security
- Trusted Computing Systems, Trustworthy Computing
- Intrusion Tolerant Systems
- Cybersecurity Auditing

PhD Program
(Research-Oriented Courses and Modules)



Practical Installations and Setup

Initial Tools

Setting the Scene: Prepare your Own Installations

- **Linux, MacOS !**
  - **Windows: your are on your own …** ☹ !!!
- **OSes (Linux) – Native or VMs / Vbox or VMware**
  - Ex., Ubuntu, Debian Distros
  - Kali Distro

  | Shell-Env … ☺ !
- **GIT**. Use it for the work-assignments/ can share your Git Developments with the professor (in Labs)

  > git client ready (Shell and/or Eclipse IDE)
- **Virtualization: Virtualized Environment in your Computer**
  - VirtualBox (virtualbox.org): VMs w/ Linux OVA Images or Vmware
- **Do you have a VM somewhere ? It will be interesting** ☺ !
- **Do you have a Rasp.PI ? …**

Setting the Scene: Prepare your Own Installations

Important Tools:

- **openssl** (www.openssl.org) (openssl tool …)
- **wireshark** (www.wireshark.org), **ettercap**
  - **Other possible tools/demos during classes …**
- **Web (Dev/Inspect. Tools)**
- **Docker** (https://www.docker.io)
  - Install (if you don't have) it !

If youy have it … Check your Docker installation:

Shell command-line:

```
$docker run hello-world
```

Try in a next step …

```
$docker run -it ubuntu bash
```

Setting the Scene: Prepare your Own Installations

- **Java (JDK+JRE) 8.0 ref is ok (Oracle JDK Dist. Or Open JDK)**
  - As you know you can manage the use of this version even if you have other versions installed
- **Java JCE/JCA: install the Bouncy Castle Crypto provider**
  - https://www.bouncycastle.org
- **Dev Tools: Console-Based ☺ & Eclipse IDE**
  - www.eclipse.org // Eclipse IDE for Java Developers … Including git, gradle, maven …etc …
  - Other IDEs (if you prefer …)
- **Java tools / Shell-Based use:**
  - **javac, java, jar, …. keytool, javadocs**
  - Relevant: how to build jar apps:

    https://docs.oracle.com/javase/tutorial/deployment/jar/build.html

Setting the Scene: Prepare your Own Installations

- **Java Cryptography: JCA, Cryptographic Providers and JCE Programming / See Lab 1**
  - Try to compile and run the provided code …
    - Crypto-providers / JAVA JCA / JCE Programming Environment
  - Bouncy Castle Installation (used by LAB-demos / exercises)

  See the Bouncy Castle Web Site:

  https://www.bouncycastle.org/

  https://www.bouncycastle.org/latest_releases.html

  http://www.bouncycastle.org/wiki/display/JA1/Provider%2BInstallation

To prepare the next week lab …

- Check the provided documentation/bibliography in the CLIP system
  - http://vps726303.ovh.net/csns1920/
  - Follow and Test initially Materials for LAB 1:
    - Verif-JCE-CriptoProviders-Policy
    - Encryption-Decryption
  - Try to compile and run examples in LAB 1 (to check your JAVA/JCE Cryptographic Providers) and try to use tools (javac, java) in the Java Shell Environment
  - This will also check your java installation (JCA/JCE)

Questions

?