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

Mestrado Integrado em Engenharia Informática
MSc Course: Informatics Engineering
2º Semestre, 2018/2019

Course Overview

Course Info

CLIP System, Course #11619 (FCT/UNL)
See Ref. Information

Information (classes): asc.di.fct.unl.pt/~hj/srsc1819

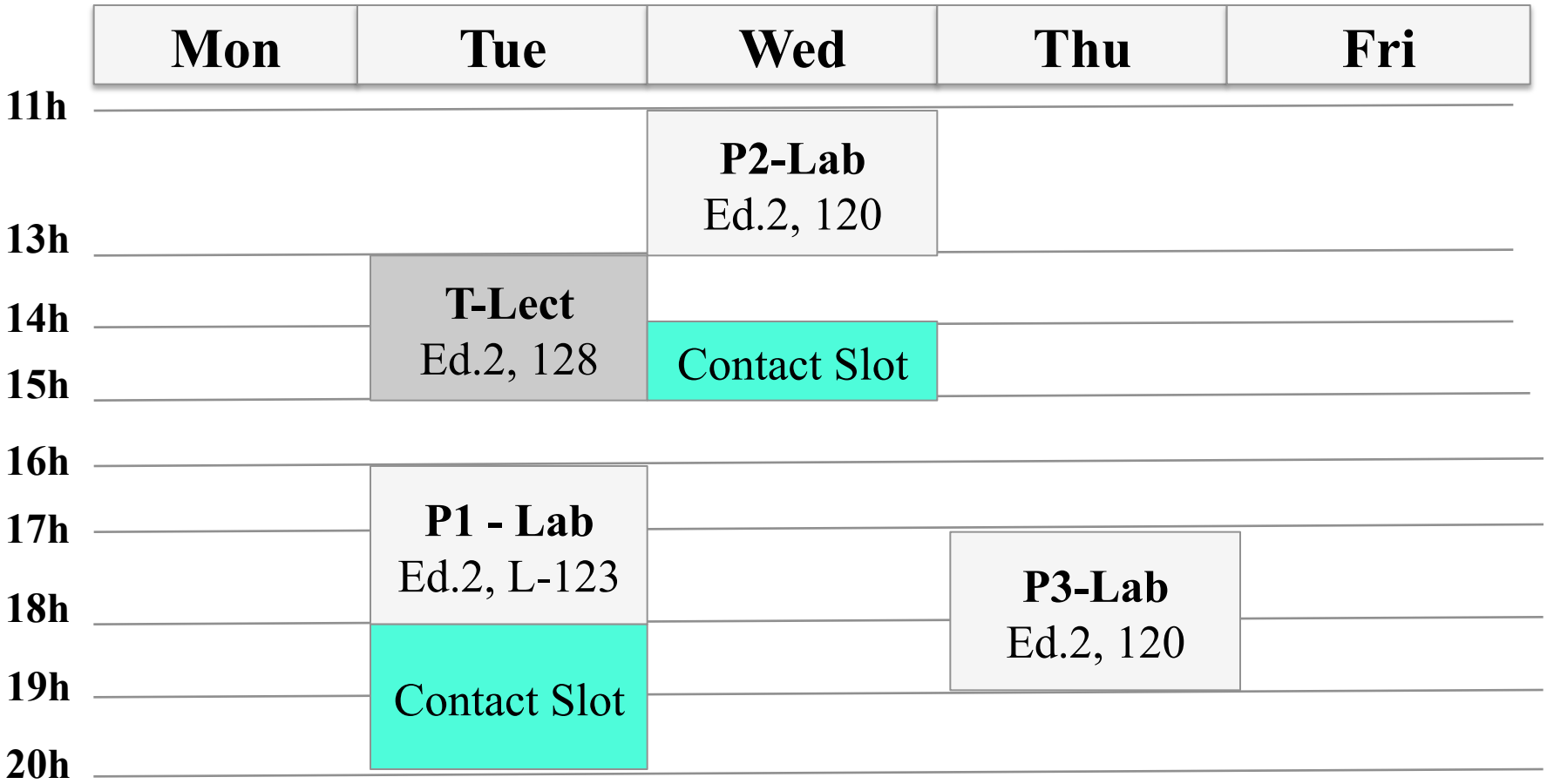
Lecturing/Contacts

Henrique João Domingos , hj@fct.unl.pt
P2/6 DI/FCT/UNL, Nova Lincs Research Center
asc.di.fct.unl.pt/~hj

Pedro Medeiros , pm@fct.unl.pt
P3/9 DI/FCT/UNL, Nova Lincs Research Center
asc.di.fct.unl.pt/~pm

Classes (6/Mar to 7/Jun)

› See the FCT **Calendar, 2nd Sem. 18/19: FCT/UNL**



- Presence (control) and Participation (as indicative evaluation)

Activities

- **Lectures:**
  - Program topics + bibliog. and suggested readings
    - Registration of Students' Participation

- **Pract./Labs**
  - Practical demonstrations/verifications/tools
  - Prog w/Crypto / Security Protocols (Java JCA / JCE)
  - Prog. Exercices

  - Input/Clarifications: Materials and elements for the development of Work-Assignments (work-assignments)
  - WS/Project Development Observation

T1
T2
Eval.

TP1
TP2
Eval.

Assessment and Grade

Assessment components and evaluation rules

Assessment components

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

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

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

- Groups of two students
- Development + Proof of Work + Report and Evaluation:
  - Submission and evaluation criteria defined in Work-Assignment Statements and Specifications
  - Selected students can be asked for Demo-Proof and Discussion

Group registration / Work-Project Assignments

Groups (TPs): Regist. Required !

- Secretariat DI/FCT/UNL, 9h-12h, 13h-17h
  - Max.. 2 Students per Group
  - Ask for the SRSC Registration Forms for Workgroups
  - Registration until 15/Mar

- Students with frequency (2016/2017 and 2017/2018) can use the frequency for 2018/2019

Tests: Regist. In CLIP

T1: From 6/Mar to 8/Apr

T2: From 15/Apr to 27/May

Grade Conditions

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 T2>=7,5/20

- **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

Assessment Dates

Calendar:

- Lect. Sessions: ~12 weeks (+ 1,2 Supl. Sessions)
- P1: ~12
- P2: ~11
- P3: ~11

Assessment Dates

Tests and Exam

T1: Sat, 13/Apr, 10h
T2: Sat, 15/Jun, 10h
Exam: Sat, 6/Jul, 9h

TP Ref. Deliv. Dates (Submission periods):

TP1 15 … 18/Apr
TP2: 3 … 9/Jun

Assessment Dates

TP1: Subm: 18/Apr
T1 : 13/Apr, 9h-11h30

Março 2019

Seg	Ter	Qua	Quin	Sex	Sáb	Dom
				1	2	3
4	C	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Abril 2019

Seg	Ter	Qua	Quin	Sex	Sáb	Dom
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	P
22	23	Expo	25	26	27	28
29	30					

Maio 2019

Seg	Ter	Qua	Quin	Sex	Sáb	Dom
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

Junho 2019

Seg	Ter	Qua	Quin	Sex	Sáb	Dom
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	20	30

Julho 2019

Seg	Ter	Qua	Quin	Sex	Sáb	Dom
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Setembro 2019

Seg	Ter	Qua	Quin	Sex	Sáb	Dom
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
31						

TP2 : Subm: 9/Jun
T2 : 1/Jun, 11h30-14h

Exam (Appeal):
6/Jul, 9h-12h

Bibliography

Main References (base bibliography)

Complementary references

Other references

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/

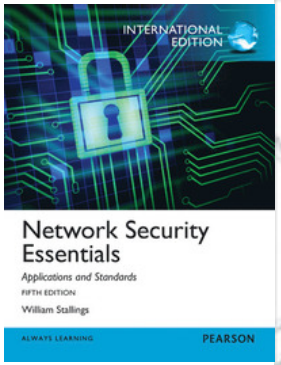
[WS-CNS] W. Stallings, Cryptography and Network Security, Pearson (7th Ed., 2017): More on Cryptography
http://www.williamstallings.com/Cryptography/

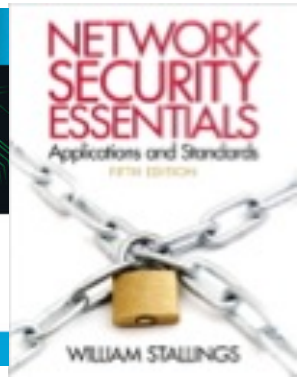
Selected chapters/sections:
Study references in the slides used for the lectures

Main Bibliograhy (and prev. editions)

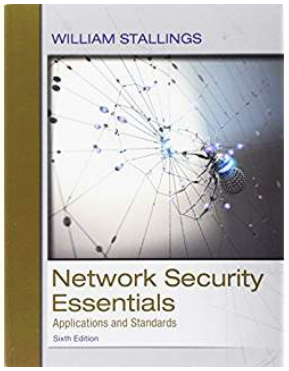
[WS-NSE]

. . . . . .





5th Ed. 2013

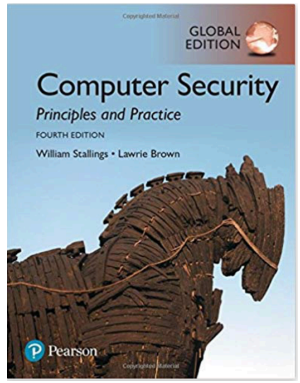


6th Ed. 2017

[WS-CS]

. . . . . .

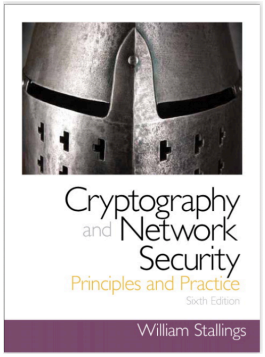
3th Ed. 2014



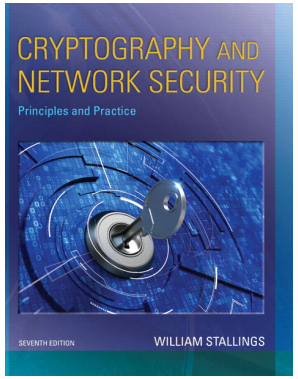
4th Ed. 2018

[WS-CNS]

. . . . . .



6th Ed. 2014



7th Ed. 2017

Program Topics vs. Weeks/Sessions

Refs

1. Overview/Introduction	S1-S2
2. Crypto Methods and Tools: Symmetric Encryption Assym. Cripto + Secure Hashing, MACs and Digital Signatures	S3-S4
3. Authentication systems and protocols	S5-S6
4. X509 Authentication and PKIs	
5. User Authentication	S6-S7
6. Access Control	S8
7. TCP/IP Sec. Stack: HTTPS TLS/SSL, IPSec/VPNs + Email Security	S8-W10
8. LAN/WLAN Net. Access Control	S11
9. Web Applications and Serv. Security	S12
10. Security at OS Level + Virtualization	S13
11. Trusted Computing and TEEs	S14
12. Intrusion Detection/Prevention/Recovery	

Program vs. Bibliograhy

	[WS-NSE]	[WS-CS]
1. Overview/Introduction	[WS-NSE], C1	[WS-CS], C1
2. Crypto Methods and Tools: Symmetric Encryption	[WS-NSE], C2	[WS-CS], C2
Assym. Cripto + Secure Hashing, MACs and Digital Signatures	[WS-NSE], C3	
3. Authentication systems 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. LAN/WLAN Net. Access Control	[WS-NSE] C5	[WS-CS], C24
9. Web Applications and Serv. Security	Prov Readings	
10. Security at OS Level + Virtualization		[WS-CS], C12
11. Trusted Computing and TEEs	Prov Readings	
12. Intrusion Detection/Prevention/Recovery	[WS-NSE], C11, C12	[WS-CS], C8, C9

Program vs. Bibliograhy

	[WS-NSE]	[WS-CNS]
1. Overview/Introduction	[WS-NSE], C1	[WS-CNS], C1
2. Crypto Methods and Tools: Symmetric Encryption	[WS-NSE], C2	[WS-CNS], C1–C7
Assym. Cripto + Secure Hashing, MACs and Digital Signatures	[WS-NSE], C3	[WS-CNS], C8–C10 [WS-CNS], C11–C13
3. Authentication systems 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. LAN/WLAN Net. Access Control	[WS-NSE] C5	[WS-CNS], C16
9. Web Applications and Serv. Security	Prov Readings	
10. Security at OS Level + Virtualization		
11. Trusted Computing and TEEs	Prov Readings	
12. Intrusion Detection/Prevention/Recovery	[WS-NSE], C11, C12	

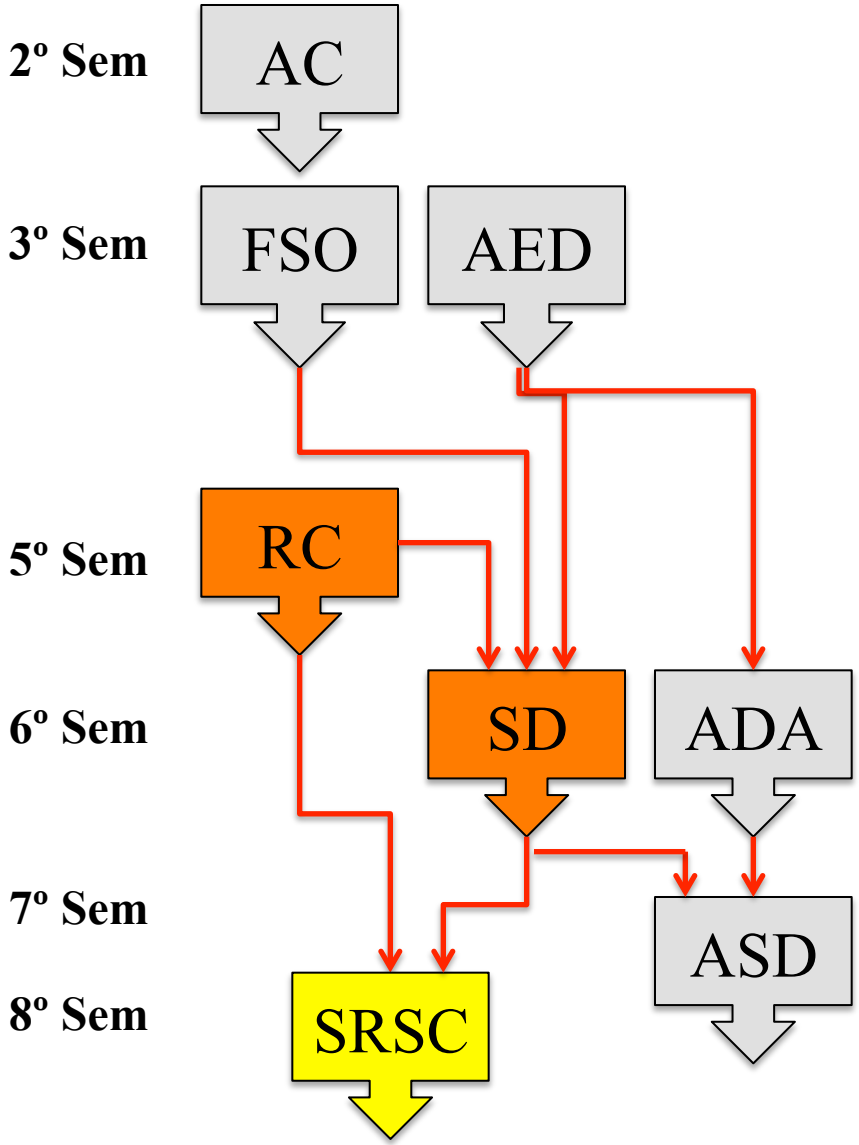
Other classic and additional references

- Complementary references: CLIP information
- Other references: suggested readings on the program topics
  - Ref. in classes

CSNS Course in the MIEI Program

Previous vs. Next Steps
(Preced. and Post.)

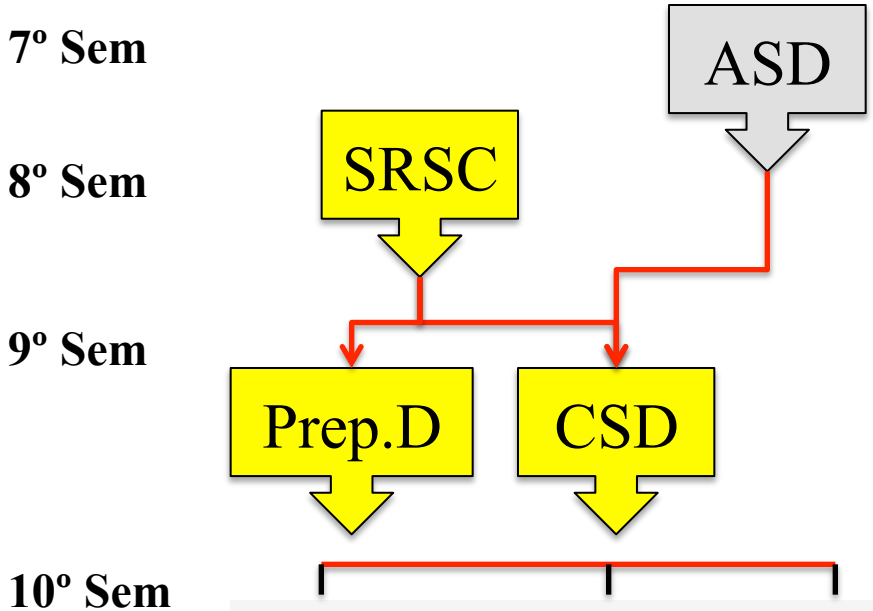
MIEI Sequence / Requirements



Practical Skills and Autonomy for Distributed Systems Programming and development of Internetworking Protocols in TCP/IP

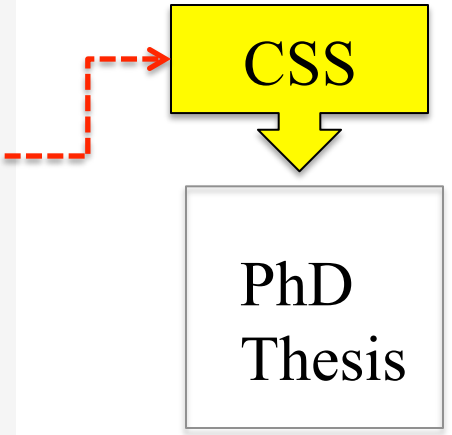
- Eclipse IDE (or other)
- JAVA Programming
- Network Programming and Distributed Programming)
- Sockets, WebSockets, Java RMI, Rest (WS)
- Basics in OS Management/Admin Experience (Terminal/Console) Shell Environment
  - Installation/Setup VMs w/ Virtualization Tools

Future projection on MIEI and PhD Program



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

PhD Program
(Research-Oriented Courses and Modules)



Setup

Tools, Environments, Installations

Setup: Installations (1st Week)

- **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 … Includes git, gradle, maven ...etc …
  - Other IDEs (if you prefer …)
- **openssl** (www.openssl.org) (openssl tool …)
- **wireshark** (www.wireshark.org)
- **Web (Dev/Inspect. Tools)**
- **Docker** (https://www.docker.com)

Setup: Installations (2nd Week)

- **GIT (or Bitbucket) Account**. For the work-assignments you will share the account with the professor (later instructions)
  - git client ready (reM you can also use git in your Eclipse IDE)

- **Virtualization Tools**
  - VirtualBox (virtualbox.org) // Orcacle … Ready for OVA Images
  - Can use also … Vmware

- **OSes (Linux) – Native or VMs**
  - Ubuntu (18.10.4 Cosmic Cuttlefish)
  - Kali distro

- **Other Tools (+ Work Assignments) – Ref, on Classes**

Questions

?