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. 2020/2021

Course Overview

Course Lecturing and Lab-Instruction

Course: Reg., Lectures and Labs:
Henrique Domingos

Associate Professor @ DI/FCT/UNL
Integrated Researcher @ NOVA LINCS Research Center (FCT)

Course Overview

Initial information

- Information, documents and materials
- Course development: activities, calendar and initial (ref.) plan
- Evaluation (Components and Rules)
- Topics (Program)
- Bibliography / Coverage of Topics (Readings)
- Requirements / Initial Background

- Tools / Intial installations and setup

Information, Documentation and Materials

- CLIP System
  - **Course characterization**
    - Generic description, objectives, requirements
    - Program topics and Bibliography
  - **Course development / operation**
    - Expected student work (6 ECTS x 28h = 168h)
    - Assessment rules: frequency and grading conditions
  - **Materials**
    - **Docs.** See "Documentação de Apoio"
      - Lectures / Slides (Acetatos)
      - Also (past) tests, training quizzes
- LABs (On-going references, guidelines and pointers)
  - **http://vps726303.ovh.net/srsc2021/**

    yes ;-(… It is not HTTPS/TLS secured by now … you will understand why

Course Activities

- **Lectures, 2h/Week (Remote, Zoom Sessions)**
  - Program Topics, Suggested Readings

- **Slots for Labs-Activities, 3 x 2h/week (Remote, Zoom Sessions)**
  - Practical presentations/theoretical-practical demonstrations, hands-on experimental demos
  - Proposal of short practical exercises
  - Work-Assignments materials (evaluation projects)

- Contact slot: see in CLIP

Obs) Use classes or face-to-face / zoom contact slots (No Email)

Evaluation

Assessment components

Tests: T1, T2

- Individual tests, Registration on CLIP
- Cover selected program topics/bibliography references
  - 2h, closed book questions

PRESENCE

Practical (Frequency) Evaluation: TP1, TP2

- Practical / Development / Submission Forms
- Development: Individual or Group (max. 2 students)
  - Package to submit: Development (sources, executable components) + results from proof of correctness + form indicators + report

OffLine, Remote

- Individual Practical Tests (~30-45 m): until 20% of each TP evaluation
  - Open book / no networked devices

PRESENCE

Final (Appeal) Exam

- Individual exam
- Covers all the program topics/bibliography references
  - 2h30, closed book questions

PRESENCE

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

F: Frequency* = 40% TP1 + 60% TP2

Individual practical tests: until 20% of TP evaluations

Minimum grade for individual frequency: F > 8/20 and TP2>=8/20

Grade conditions

- **Minimal grade for individual frequency**

  AF = 25% T1 + 35% T2 + 40% F

  Approval if: F > 8/20 **AND** average (T1,T2) >=9,5/20 AND AF>=9,5/20

- **Grade with final (appeal) exam**

  AF = 60% E + 40% F

  Approval if: AF >= 9.5/20 and E >= 9,5/20

(*) Students with frequency (2018/2019 or 2019/2020) can use the frequency evaluation using the evaluation rules of 2020/2021

Assessment Dates (Initial Ref.)

These dates are only indicative (will be confirmed soon)*

- T1: [02/Nov/20 - 21/Nov/20] Possible Date: Sat, 14/Nov, 9h
- T2: [04/Jan /21 – 15/Jan/21] Possible Date: Sat, 09/Jan, 9h

- TP1 Deliveravle/Submission:
  [until ~30/Oct/20]
- TP2 Deliverable/Submissiom
  [until ~15/Dec/20]

- Final Exams (Appeal Date):
  [26/Jan/21 – 09/Feb/21]

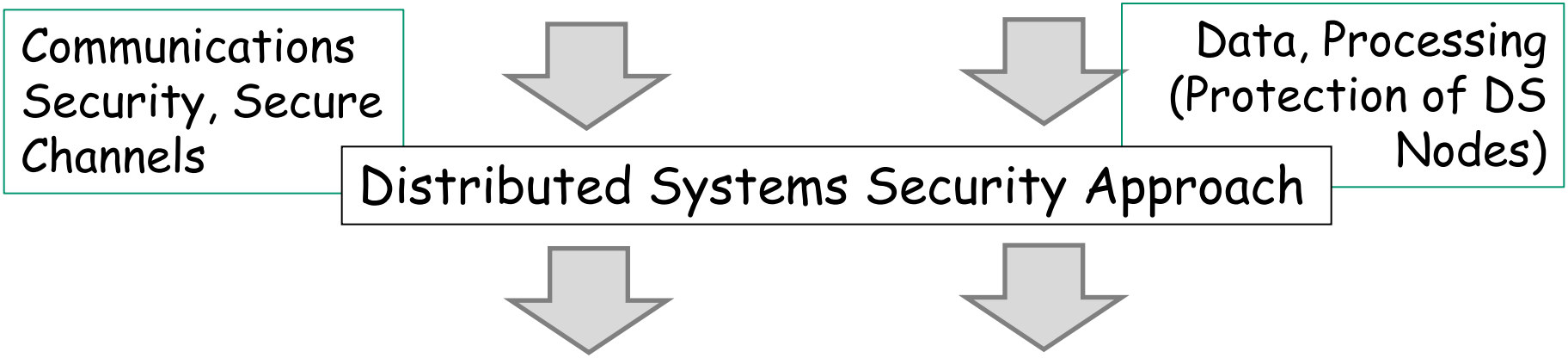
(*) Final dates decided/defined by CCMIEI Coordination (CLIP)

Topics

Program Topics

(See CLIP for more detail)

Consolidation Course – **Two Main Security Dimensions:**
Computer Networks **Computer Systems**



Engineering & Computer Science Approach:
Focusing on Concepts, Principles, Foundations, Paradigms, Techniques and Standards ….
To Design/Support Security Services and Mechanisms for Dist. Systems

Main Topics (in a nutshel)

Ex., CISSP/CBK
ISOC/IEC Cert.,
https://www.isc2.org/

Overview

1. Introduction
2. Foundations, Frameworks and models for CSNS – Concepts, Terminology, Principles

3. Applied Crypto Methods, Models, Alg. and Tools
   Details on Applied Crypto, Correct Use/Programming
   - Communications Security and Crypto. Protocols
   - Establishment of secure channels

4. Authentication
5. Access Control

6. Network Security Services and TCP/IP Security Stack: Protocols, Standards, Secure Channels, Design Principles
7. Systems' Security
   Computer Systems Security
   Security infrastructure elements

Foundations and Principles

Cryptographic Tools

Base security mechanisms, techniques and services

Communication / Network Security and Standards

Systems security Engineering

Bibliography

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/

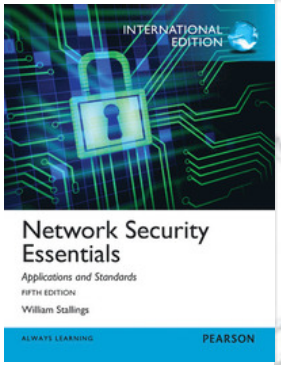
[WS-CNS] W. Stallings, Cryptography and Network Security, Pearson (7th Ed., 2017): More on Cryptography
http://www.williamstallings.com/Cryptography/

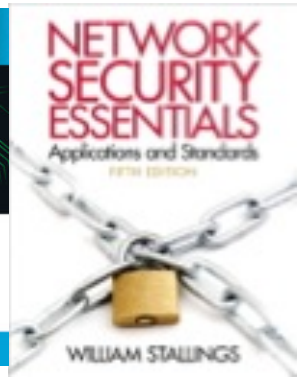
Complementary/On-going refs, bibliography, materials suggested for specific program topics …. Suggested readings in lectures and slides (evaluation + complementary)

Main Bibliograhy (different editions)

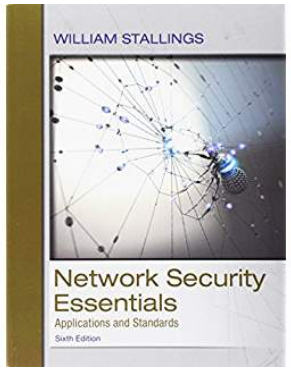
[WS-NSE]

. . . . . .





5th Ed. 2013

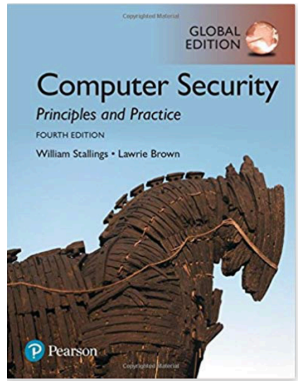


6th Ed. 2017

[WS-CS]

. . . . . .

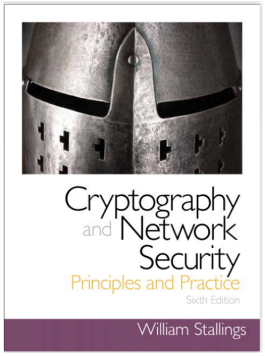
3th Ed. 2014



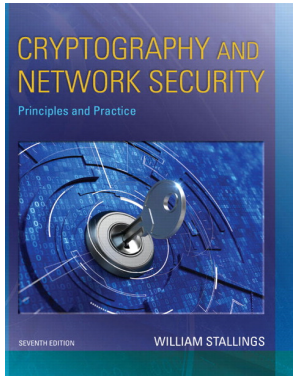
4th Ed. 2018

[WS-CNS]

. . . . . .



6th Ed. 2014



7th Ed. 2017 (8th Ed, 2020)

Program Topics vs. Bibliog.

1. Overview/Introduction
2. Foundations, Frameworks and models for CSNS
3. Applied Crypto Methods, Models, Alg. and Tools
4. Authentication and Access Control
5. TCP/IP Security Stack, Security services, Protocols and Standards
6. Systems Security

[WS-NSE]	[WS-CS]
[WS-NSE], C1	[WS-CS], C1
[WS-NSE], C2	[WS-CS], C2
[WS-NSE], C3	[WS-CS], C23
[WS-NSE], C4	[WS-CS], C23
	[WS-CS], C3, C4
[WS-NSE] C6, C7, C8, C9,	[WS-CS], C22, C23
	[WS-CS], C24
[WS-NSE] C5	
	[WS-CS], C12
Add. Readings	[WS-CS], C13
[WS-NSE], C11, C12	[WS-CS], C8, C9

Program Topics vs. Bibliog.

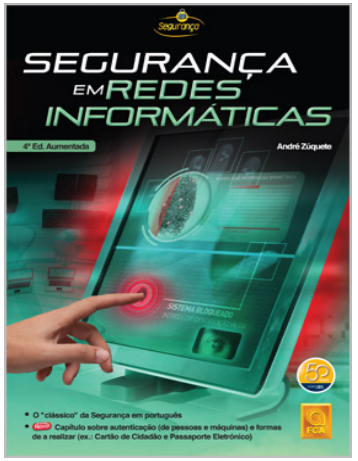
	[WS-NSE]	[WS-CNS]
1. Overview/Introduction	[WS-NSE], C1	[WS-CNS], C1
2. Foundations, Frameworks and models for CSNS		
3. Applied Crypto Methods, Models, Alg. and Tools	[WS-NSE], C2	[WS-CNS], C1–C2-C3 C4-C5-C6 C7-C8-C9-C10
	[WS-NSE], C3	
4. Authentication and Access Control	[WS-NSE], C4	[WS-CNS], C14-C15
5. TCP/IP Security Stack, Security services, Protocols and Standards	[WS-NSE] C6, C7, C8, C9,	[WS-CNS], C17 C18, C19, C20
	[WS-NSE] C5	[WS-CNS], C16
6. Systems Security		
	Add. Readings	
	[WS-NSE], C11, C12	

Other Bibliography (*Portuguese Lang.*)

A. Zúquete

Segurança em Redes Informáticas, FCA, 5ª Ed.

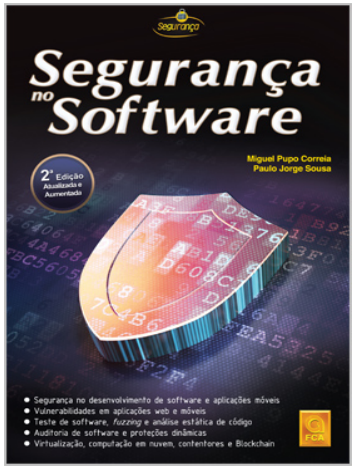
https://www.fca.pt/pt/catalogo/informatica/seguranca-ciberseguranca-protecao-de-dados/seguranca-em-redes-informaticas-2



M. P. Correia, P. Sousa

Segurança do Software, FCA, 2ª Ed.

https://www.fca.pt/pt/catalogo/informatica/seguranca-ciberseguranca-protecao-de-dados/seguranca-no-software-2/



SRSC / CSNS, 1920

Skills

Required Knowledge Base and Practice

Previous Courses, Knowledge Base and Course Requirements

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

- **Precedent Knowledge / Recommended**
  - Computer Networks
  - Distributed Systems
  - Operating Systems / OS Foundations
  - Courses on Programming / Design and implementation of Data Structures and Algorithms
  - Programming Languages: Java Programming
    - OK you could use C# too … But …

Practical skills and tools (1)

Computer Networks, Distributed Systems

- Autonomy for **Distributed Systems Programming**

TCP/IP Appl. Programming and Java Programming/Tools

- Network Programming and Distributed Programming
- Sockets, HTTP C/S Communication, WebSockets, Java RMI, Rest (WS)
- Autonomy with Eclipse IDE (or other) and Java or Maven Project Dev.
- Terminal/Console: Shell Environment
  - MacOS or Linux / Shell Environment
- Java Programming and Java Tools (including console-oriented tools)
  - (javac, java, keytool, javadoc, jdb, jar)
- Linux or MaOS Admin Basics (Installataions, Setup, Monitoring Tools, … simple shell scripting – sh, bash, ..)
- Development/Deployment with Docker (Docker Containers, Docker Composing)

Practical skills and tools (2)

- What about Windows and its multiple versions ? ;-("%&#/R(%#" rrrrrr
  - Black Consoles/Terminals / Linux/Shell based emulation on Windows , Java Tools, Executable Jars

- Practice w/ Virtual Environments (Linux VMs / VBox or Vmware)
  - Install a Linux VM …
  - or use a Cloud Remote Linux VM instance (good idea !)
    - FCT Azure Linux VM, OVH VPS Linux Instances, …

SRSC / CSNS, 1920

Practical Installations and Setup

Setting the schene with some initial tools

See: http://vps726303.ovh.net/srsc2021/

Setting the scene: tools and installations

- Initial Installations / Check these tools to be initially ready:
  - **wireshark** (www.wireshark.org)
  - **tcpdump** (native in your Linux Distro?) .. or
  - **openssl** (native in your Linux Distro … or www.openssl.org)
  - **KeyStore Explorer** (keystore-explorer.org)
  - **git** (Tool) and Individual Git Repository Accounts
  - **Java** (JDK or OpenJDK)
    - I will use lots of things in JAVA 8 but you can use other recent versions
    - Java tools (Check command-line): **javac, java, jar, keytool, ..**
  - **VirtualBox (**www.virtualbox.org)
    - Ubuntu or Debian VMs (why or why not Kali and other "like" Distros ?)
    - Ok, can use also VMWare
  - **Docker** (www.docker.com)

    ```
    $docker run hello-world …. $docker run -it ubuntu bash
    ```
  - **vlc** (www.videolan.org)

Complementary Information

Main Topics vs. ACM/IEEE CS2013 Information Assurance and Security (https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf)

Overview

1. Introduction
2. Foundations, Frameworks and models for CSNS – Concepts, Terminology, Principles

3. Applied Crypto Methods, Models, Alg. and Tools
   Details on Applied Crypto, Correct Use/Programming
   - Communications Security and Crypto. Protocols
   - Establishment of secure channels

4. Authentication
5. Access Control

6. Network Security Services and TCP/IP Security Stack: Protocols, Standards, Secure Channels, Design Principles
7. Systems' Security
   Computer Systems Security
   Security infrastructure elements

Fundamental Sec. Concepts (Tier 1)

Threats and Atacks (Tier 2)

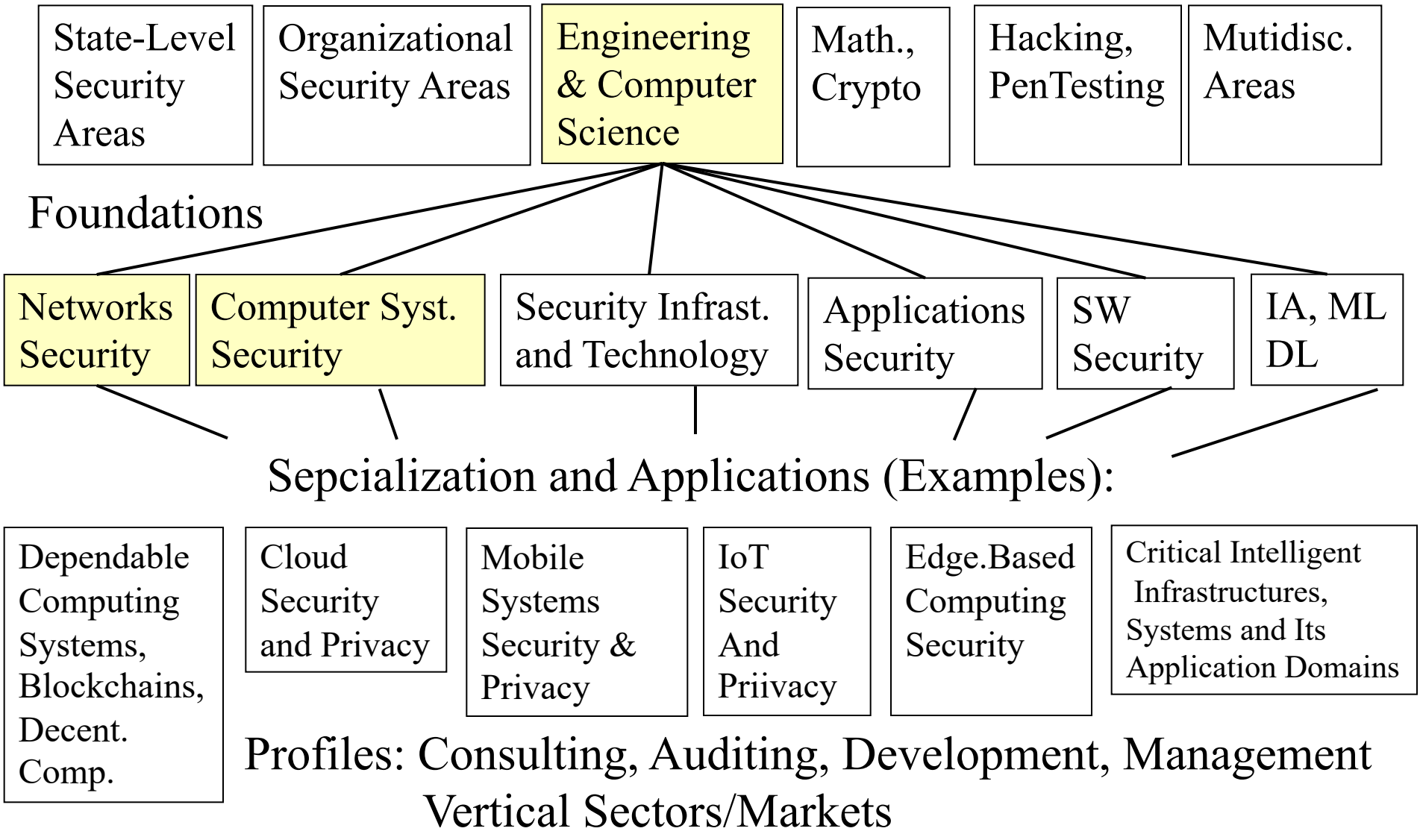
Cryptography (Tier 2)

Fundamental Sec. Concepts (Tier 1)

Network Security (Tier 2)

Defensive Prog & Spport (Tier 2)

A Broad Cybersecurity Scope



CNSS: Course orientation and emphasis

Cybersecurity (in its broad dimensions)

State-Level Security	Organizational Security	Mutidisciplinary Areas	Hacking
National/ Homeland Security and Defence	Human Resources Security	Other Engineering Areas/Disciplines	Hacking Tools, Methods and Techniques
CyberThreats, CyberAttacks Cyberspace Crisis Management	Security Auditing, Monitoring and Operational Security	Social and Human Sciences	Ethical Hacking
Military Security	IT Security: Security Mgmt, Risk Assessment and IT Security Controls	Law and Ethics	Vulnerability Assessment and PenTesting
Cyberwarfare and Ciberwar	Legal, Societal and Ethical Aspects	Regulation and Compliance	Hacking Tools and Methods
		Economy	
		Health and Medicalcare	

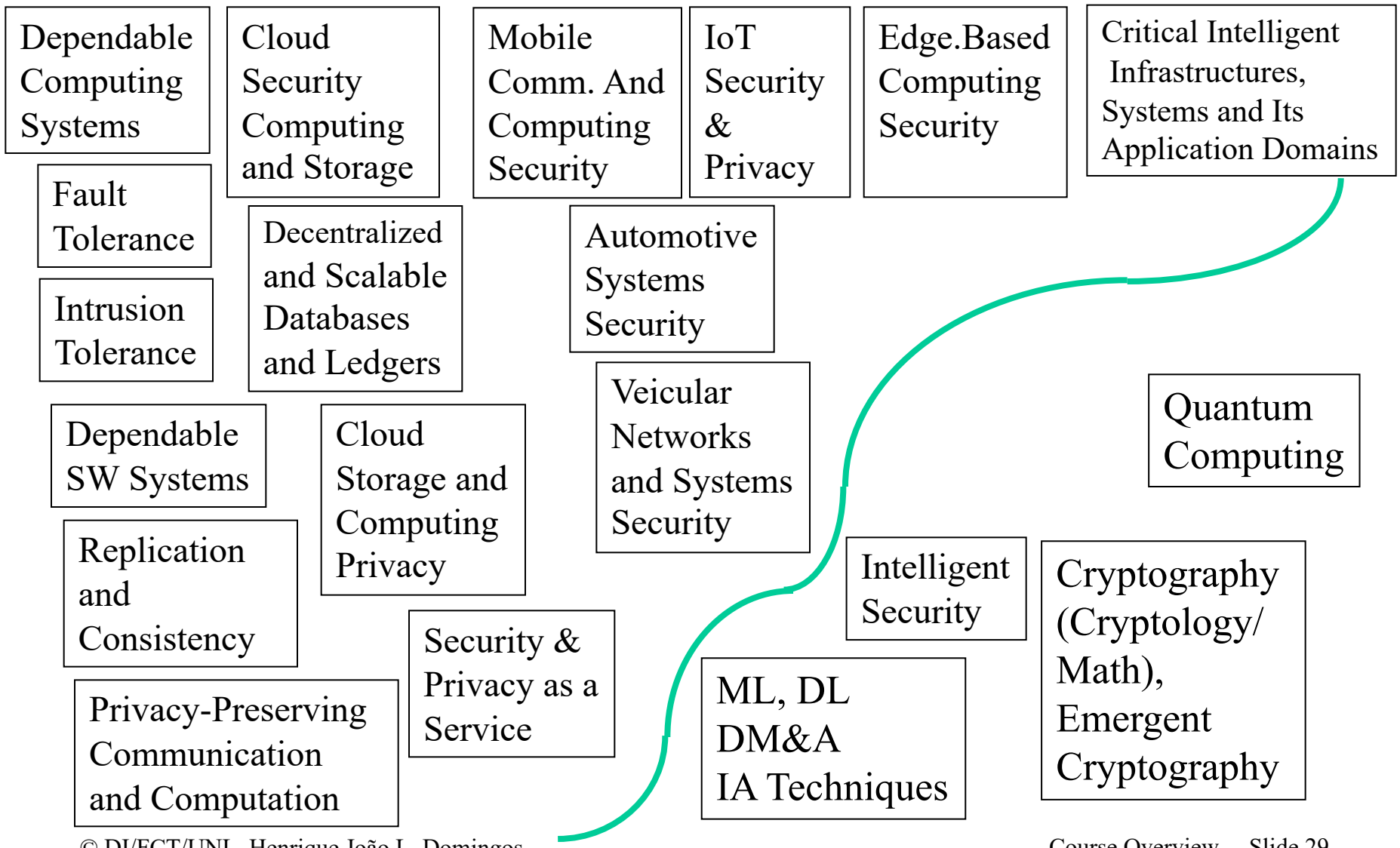
Course Coverage

Cybersecurity: Computer Science and Informatics Engineeirng

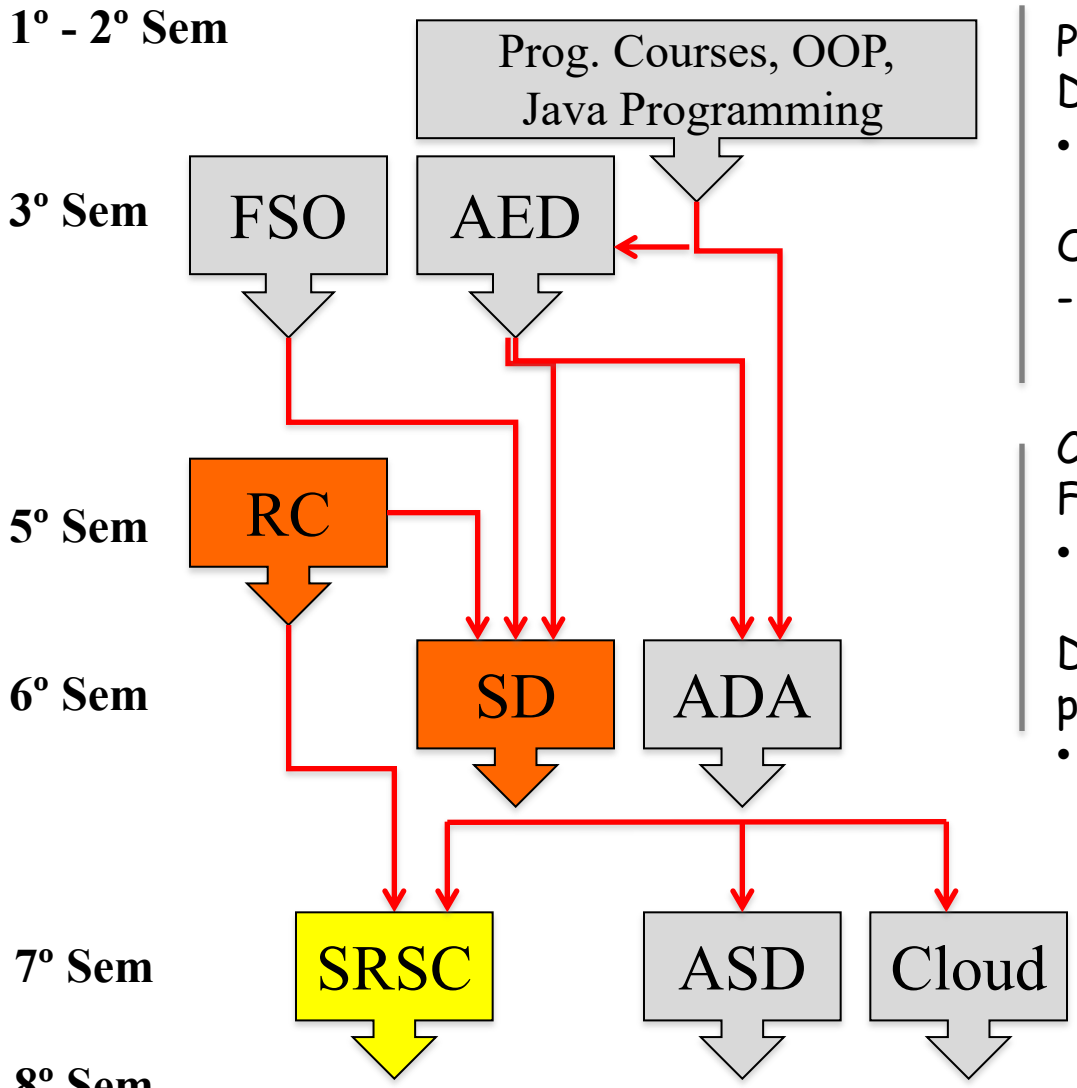
Networks Security	Computer Syst. Security	Security Infrast. and Tech.	Applications Security	SW Security
Secure Channels	Authentication	Perimeter Defense	Database Security	Design/ Implement. and verification of Secure SW Systems
Secure Communication Protocols & Stacks	Access Control	IPSs, IDSs	Web Security	Security Modeling and Analysis
Network Security Standards	OS Security	SIEM	Application Specific Security	Programming Languages and Tools
PtP vs. E2E Communications Security	OS SW Sec.	End-Systems Security and Devices	Cloud-Serv. and App. Security	Security and Usability
Internet Security Standards, TCP/IP Sec.	SW Attestation Environments	BackUp & Disaster Recovery	Mobile App. Security	
Wireless Nets. Security	Trusted Execution Environments	DataCenter Security		
	Virtualization Security	Cloud Security		
	HW/FW Security			

Other (specialization) Dimensions

Other Specialized Disciplines 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

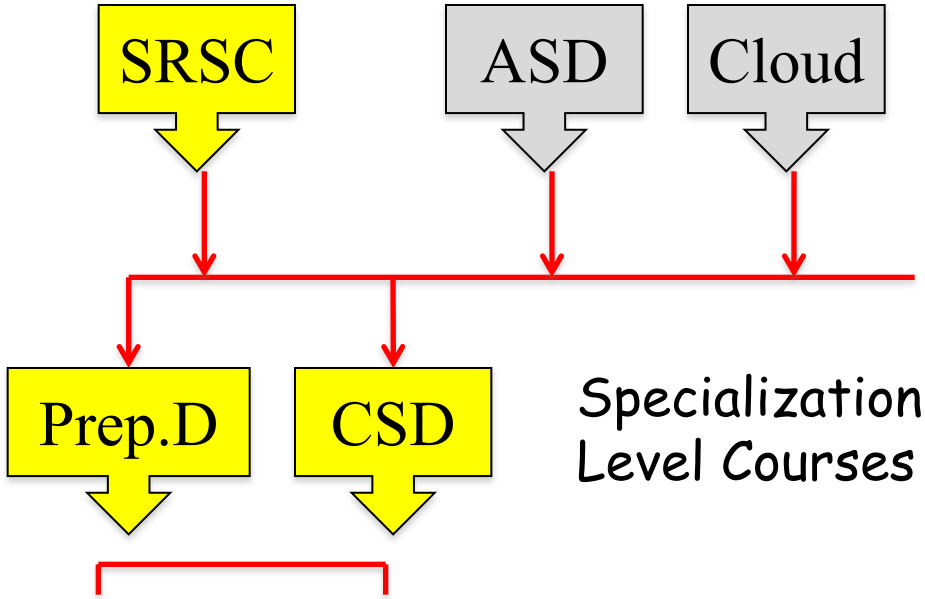
Future projection on MIEI and PhD Program

7º Sem

8º Sem

9º Sem

10º Sem



Specialization Level Courses

- Advanced Distributed Systems
- Cloud Computing and Storage

- Dependable Distributed Systems
- Advanced Network and Internet Security
- Privacy-Enhanced Systems / Privacy Preservation
- Cloud-Security and Privacy
- Privacy-Enhanced Storage, Privacy Preserving Data Analytics
- Blockchains and Current Research Challenges
- Anonymization and Censorship Circumvention
- Mobile Computing Security
- IoT Security
- Secure Vehicular and Automotive Systems and Networks
- Trusted Computing Systems, Trustworthy Computing
- Intrusion Tolerant Systems
- Cybersecurity Auditing, Operational Security, SIEMs

PhD Program
(Research-Oriented Courses and Modules)