Cyber Security and Defense (CySD)

1. Objectives

Todays, we are facing a tremendous growth and resilience to cyberspace infrastructures. These infrastructures promote the development of new business models, facilitate and improve communication, enable the design of value-added services, and contribute to our national defense. The flip side of this increased reliance, however, makes the cyber infrastructures highly vulnerable to threats and attacks. Network outages, theft and alteration of user data, malware propagation, viruses' contamination, and denial of service, are, among others, examples of security incidents that may affect personal, enterprises, and national assets.

The engineering curriculum of Cyber Security and Defense (CySD) provides students with the framework and knowledge to protect national, organization and enterprise's cyber assets. The courses to be taught focus on the different facets of cybersecurity engineering, namely prevention, detection, countering, and recovery from incidents affecting cyber infrastructures. The students will be provided with a broad analytical framework for evaluating and solving cybersecurity problems. They will acquire the skills and knowledge to protect and security audit infrastructures, detect intrusions, assess vulnerabilities, eliminate threats, and investigate incidents.

Graduate students will be ready for careers within industry such as Chief Information Security Officer, Security Systems Administrator, incident responder, security investigator, security auditor, and many other career paths within the field of security engineering.

2. Competences to develop

The courses taught in CySD curriculum will provide students with the knowledge and capacities related to the following areas:

- Cyber security and defense techniques and protocols
- Cryptographic algorithms and protocols
- Network security prevention
- Operating systems security
- Intrusion detection and response

- Cyber security forensics
- E-services security
- Wireless and mobile security
- Economics of security
- Legal aspects in cyber security and privacy
- Cyber security management
- Security Auditing

3. Career Paths

Future engineers who follow the career paths in cyber security and defense can apply for jobs in the following domains:

- Chief Information Security Officer
- Security consultant
- IT Security engineer
- Security Systems Administrator
- Security architect
- Incident responder
- Computer forensics expert
- Penetration tester
- Security analyst
- Security software developer
- Security auditor

4. Prospective employers

- Network operators and service providers
- Software development firms (secure coding, design and development of security solutions, integrate security into applications, …)
- National security authorities (ANCE, ANSI, ATT, …)
- Companies whose business model is highly sensitive to security (Banks, airline companies, e-commerce firms, grid operators, …)
- IT service firms (auditing, cyber security solutions deployment, …)

5. Curriculum at a glance

5.1. INDP2-SIRT (A module option in the 4th Semester)

Teaching Unit	List of courses	Hourly volume				Total Hours	Evaluation technique
		Total	Course	Practices	Exercises		
Fundamentals of cyberspace and cyber security	**Cryptographic algorithms and protocols**	21	15		6	63	Exam
	Cyber infrastructures security	21	15		6		Exam
	Labs	21		21			Labs grading

5.2. INDP3-CySD (The content of the 5th Semester)

Teaching Unit	List of courses	Hourly volume				Total Hours	Evaluation technique
		Total	Course	Practices	Exercises		

Legal, economic and management aspect in Cybersecurity	**Telecommunication Security Legal Aspects**	10,5	7,5		3	42	Exam
	Economics of Security	10,5	7,5		3		Exam
	Security Engineering and risk management	21	15	6			Exam (70%) Labs grading (30%)
Security auditing and intrusion prevention	**Security Auditing**	21	15	6		63	Exam (70%) Labs grading (30%)
	Intrusion detection	21	15	6			Exam (70%) Labs grading (30%)
	Ethical Hacking and Penetration testing	21	15	6			Exam (70%) Labs grading (30%)
Public and Emerging Networks Security	**Security of mobile and wireless networks**	21	15	6		84	Exam (70%) Labs grading (30%)
	Mobile networks: architectures and new functionalities	21	15	6			Exam (70%) Labs grading (30%)
	Cloud Computing and Big Data Security	21	15	6			Exam (70%) Labs grading (30%)
	IoT architectures, protocols, and security	21	15	6			Exam (70%) Labs grading (30%)
Cyber Crimes defense and investigation	**Cyber infrastructures protection**	21	15	6		84	Exam (70%) Labs grading (30%)
	Security Certification	21	21				
	Computer, Networks, and Mobile Forensics	21	15	6			Exam (70%) Labs grading (30%)
	Incident Response, Disaster Recovery, and Business Continuity	21	15	6			Exam (70%) Labs grading (30%)
Cybersecurity Capstone	**Tutored Projects**	126				177	Midterm evaluation (40%) Final evaluation (60%)
	Seminars on Security	21					
	Enterprise communication	30					