Syllabus

1. Data about the program of study

1.1 Institution	Technical University of Cluj-Napoca
1.2 Faculty	Automation and Computer Science
1.3 Departament	Automation
1.4 Field of study	Systems Engineering
1.5 Cycle of study	Bachelor of Science
1.6 Program of study/Qualification	Automation and Applied Informatics (English)
1.7 Form of education	Full time
1.8 Codul disciplinei	56.30

2. Data about the subject

2.1 Subject name	***Digital Security***				
2.2 Course responsible/lecturer	Conf.dr.ing. Ovidiu Stan, Ovidiu.stan@aut.utcluj.ro				
2.3 Teachers in charge of applications	Conf.dr.ing. Ovidiu Stan, Ovidiu.stan@aut.utcluj.ro				
2.4 Year of study	4	2.5 Semester	2	2.6 Assessment *(E/C/V)*	C
2.7 Type of subject	*DF – fundamental, DD – in the field, DS – specialty, DC – complementary*				DS
	DI – compulsory, DO – elective, Dfac – optional				DO

3. Estimated total time

3.1 Number of hours per week	3	of which:	Course	2	Seminar	0	Laboratory	0	Project	1
3.2 Number of hours per semester	42	of which:	course	28	Seminar	0	Laboratory	0	Project	14
3.3 Individual study										
(a) Manual, lecture material and notes, bibliography										20
(b) Supplementary study in the library, online and in the field										19
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										33
(d) Tutoring										6
(e) Exams and tests										4
(f) Other activities:										1

3.4 Total hours of individual study (sum of (3.3(a)…3.3(f)))	83
3.5 Total hours per semester (3.2+3.4)	125
3.6 Number of credit points	5

4. Pre-requisites (where appropriate)

4.1 Curriculum	- Mathematical Algebra, Special Mathematics, Probability - Programming in a high-level object language
4.2 Competence	C1. Use of knowledge of mathematics, physics, measurement engineering, technical graphics, mechanical, chemical, electrical and electronic engineering in systems engineering

5. Requirements (where appropriate)

5.1. For the course	Classroom with minimum 90 seats, computer, projector, blackboard, Internet connection
5.2. For the applications	Room with minimum 20 seats, minimum 10 computers, projector, whiteboard, 4 X SEcube dev board, 20 x Raspberry Pi 3+

6. Specific competences

6.1 Professional competences	- C1. Use knowledge of mathematics, physics, measurement engineering, technical graphics, mechanical, chemical, electrical and electronic engineering in systems engineering. - C2. Operating with fundamental concepts from computer science, information and communication technology. - C3. Use of basics of automation, modelling, simulation, process identification and analysis methods, computer-aided design techniques.

	- C4. Design, implement, test, operate and maintain general purpose and dedicated equipment systems, including computer networks, for automation and applied computing applications. - C5. Development of applications and implementation of algorithms and structures for automatic control, using project management principles, programming environments and technologies based on microcontrollers, signal processors, programmable logic controllers, embedded systems.
6.2 Cross competences	- CT2. Identify roles and responsibilities in a multi-skilled team, making decisions and assigning tasks, with the application of interpersonal and effective teamwork techniques. - CT3. Identify opportunities for further training and make effective use of learning resources and techniques for own development. - Written and oral communication skills - Time and material resource management skills - Skills in the use of scientific terminology in the field - Skills in interdisciplinary use of knowledge and terminology in the field

7. Course objectives

7.1 General objective	- Identify and master the main modern techniques in data security in the current technological context exposed by the Internet of Things - Internet of Things (IoT) is an emerging technology that is changing our world with its innovative products such as "smart homes", "autonomous vehicles", etc. This course aims to introduce students to the concept of IoT and its impact on our daily lives, make them understand the architecture and components of IoT and address the challenges and solutions of implementing IoT in reality. - Students will learn how to link and exchange communication costs and computing power, as well as hardware and software. In addition, digital security is a critical design issue for IoT systems. From this course, students will become aware of the cyber-security issues raised by IoT and gain knowledge of related security techniques. Students will also gain hands-on experiences about building IoT devices and implementing security techniques through team projects.
7.2 Specific objectives	- Use of specific algorithms/methods for securing data through encryption - Identification of vulnerabilities - Security assessment of smart devices - Understanding the impact of IoT technologies - Knowledge of emerging IoT technologies - Developing critical thinking skills

8. Contents

8.1 Lecture	No.hours	Teaching methods	Notes
Lecture 1 1. Introductory notes, context, subject structure, exam requirements 2. Introduction: data security and information security issues 3. Security services 4. Data access and control 5. Types of attacks (Dictionary and Brute Force, Lookup Tables, Reverse Look Tables, Rainbow Tables) 6. Classification of attacks 6.1 Protocol attacks 6.2. Estimation attacks 6.3. Reshaping attacks	2	Teaching using laptop and projector, interactive course, debate / or online on Teams platform	
Lecture 2 1. Classical encryption - general aspects, algorithms, authentication messages, digital signatures	4		

2. Modern encryption - principles and algorithms 3. Public key cryptography - principles, standards and algorithms 4. Cryptographic (secret) key cryptography 5. Hash function (MD5, SHA256, SHA512, RipeMD, Whirlpool)			
Lecture 3 1. Steganography 1.1 General aspects 1.2. Technical steganography 1.3. Linguistic steganography 2. Use of steganographic methods to enhance the security of cyber-physical systems 3. Basic principles of transparent marking 3.1. Mark insertion 3.2. Mark detection 3.3. Least Significant Bit Shift Method 4. Fragile marking for various forms of digital information 4.1 Fragile marking for images 4.2. Marking for audio signals 4.3. Marking for video sequences 5. Image storage 5.1. Storing images in memory 5.2. Storing images in files	4		
Lecture 4 1. Introduction to Internet of Things (IoT) 1.1. Benefits and applications of IoT 1.2. Growth of IoT 1.3. Security issues with IoT 1.4. The basic architecture of the IoT 2. IoT Attack Surface and Threats 2.1. OWASP top 10 for IoT 2.2. IoT Attack Surface 2.3. Software and cloud components 2.4. Device firmware 2.5. Web application dashboard 2.6. Mobile application used for device control, configuration and monitoring 2.7. Threat assessment 3. Ethics and privacy	2		
Lecture 5 1. The need for IoT security 1.1. Basic requirements and properties 1.2. Main challenges 1.3. Main security issues 1.4. Confidentiality, Integrity, Availability 1.5. Non-replay 2. Introduction to IOT hardware and its components 2.1. Tools and techniques 2.2. Electronic communication protocols 2.3. JTAG 3. Introduction to HydraBus, Raspberry PI 3.1. Understanding Raspberry Pi 3.2. Setting up Raspberry Pi 3.3. Installing the operating system in Raspberry PI (Noobs and Kali Linux) 3.4. Setting up Raspberry PI remote access 4. Side channel analysis 5. Firmware analysis 6. Conventional attack vectors	4		
Lecture 6	4		

1. Understanding IoT architecture 1.1. Device to device 1.2. Device to Coud 1.3. Device to Gateway 1.4. Cloud to Gateway 2. IOT- communication protocols 2.1. OSI vs TCP/IP reference model 2.2. Transport level protocols (TCP, UDP) 2.3. Network layer protocols (IPv4, IPv6, LowPAN) 2.4. Link layer protocols (Ethernet, WiFi, WiMax, cellular) 2.5. Introduction to RF module 2.5.1. Types of RF modules 2.5.2. Wireless protocols used in RF modules 2.5.2.1. Introduction to BLE 2.5.2.2. Introduction to ZigBee 2.5.2.3. Introduction to SDR 2.7 Extracting sensitive data from Signals			
Lecture 7 1. IoT application layer security issues 1.1. Message Queue Telemetry Transport (MQTT) 1.2. Restricted Application Protocol (CoAP) 1.3. Understanding COAP with Wireshark 1.4. HTTP, Web socket, DDS, AMQP 2. IoT technology standards 2.1. Wired communication protocols (UART, USART, I2C, SPI, Ethernet, JTAG) 2.2. Wireless communication protocols (Bluetooth, Zigbee, 6lowPAN, WiFi, Z-wave)	4		
Lecture 8 1.Attacks and implementation 1.1. IoT risk 1.2. Vulnerability exploitation 1.3. Privacy attacks (Phishing, Pharming, DNS hijacking, Defacement, Eavesdropping, Cyber Espionage) 1.4. Web-based attacks (malware, password, access, social engineering, data and identity theft, reconnaissance) 2. Identity and Access Management 2.1. Key management 3. Case studies and discussion 3.1. Smart homes 3.2. Smart agriculture 3.3. Smart retail provision 3.4. Smart Healthcare 3.5. Smart Grid 3.6. Smart cities	4		

Bibliography

1. Lilya Budaghyan, Construction and Analysis of Cryptographic Functions, 2014, ISBN 978-3-319-12991-4
2. Kristian Beckers, Pattern and Security Requirements, 2015, ISBN 978-3-319-16664-3
3. KPMG International, Security and the IoT ecosystem, 2015
4. Shancang Li, Li Da Xu, Securing the Internet of Things, 2017, ISBN-13: 978-0128044582
5. Perry Lea, Internet of Things for Architects: Architecting IoT solutions by implementing sensors, communication infrastructure, edge computing, analytics, and security, 2018, ISBN-13: 978-1788470599
6. European Research Cluster , Internet of Things: IoT Governance, Privacy and Security Issues"

Aaron Guzman, IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices, 2017, ISBN-13: 978-1787280571

8.2 Aplications (seminar/laboratory/project)	No.hours	Teaching methods	Notes
Project 1 1. Introduction 1.1. Introductory notes 1.2. Background 1.3. Structure of the laboratory/project 1.4. Prerequisites - basic knowledge required 1.5. Simple practical lessons for premises 1.6. Open discussion 2. Encryption algorithms: analysis and software systems 3. Random number generators 4. Public key encryption. Algorithm implementation	4	Presentation of examples, demonstrations, discussions, practical applications / or online on Teams platform	Mandatory attendance
Project 2 1. Steganography: analysis and applications 2. XML standard and asymmetric key encryption 3. Scientific article 3.1. Requirements 3.2. IEEE Template 3.3. Suggested article structure	4		
Project 3 1. SEcube 1.1. What is SEcube 1.2. Use-cases 1.3. Hardware overview 1.4. Overview of libraries 1.5. Setup 1.5.1. Examples and low-level code analysis 2. Qt Framework 3. SEfile examples 4. SElink examples 5. Building a simple application	4		
Project 4 1. Securing Cloud Applications using SEcube 2. Securing IoT communication protocols using SEcube and Raspberry Pi 3+	4		
Project 5 1. IP-core manager 1.1 FPGA-based design using SEcube	4		
Project 6 1. Penetration testing 1.1. Disclaimer and how to learn safely (bounty bug, capture the flag, hack the box) 1.2. Workflow presentation (detailed) 1.2.1. Collecting information 1.2.2. Scanning 1.2.3. Enumeration 1.2.4. Exploitation 1.2.5. Post-exploitation 1.2.6. Reporting 1.3 Examples 1.4. Setting up a portable hacking station 1.4.1. Installing Kali on Raspberry Pi 1.4.2. Setting up SSH to connect to the Raspberry Pi remotely 1.4.3. Cracking a WI-FI password, creating a fake network, spying on device traffic 1.4.4. Monitoring a network	4		
Project 7	3		

1. Penetration testing 1.1 Website assessment OR Host assessment 1.2. Solving a Hack-the-box 2. Submit the scientific article			
Project 8 1. Submit the project	1		

Bibliography

1. Fei Hu, Security and Privacy in Internet of Things, 2016, ISBN-13: 978-1-4987-2319-0
2. Francis daCosta, Rethinking the Internet of Things: A Scalable Approach to Connecting Everything, 2013, ISBN: 978-1-4302-5740-0
3. Federal Trade Comission , Internet of Things: Privacy & Security in a Connected World, 2015
4. Georgia Weidman, Penetration Testing: A Hands-On Introduction to Hacking, 2014, ISBN-13: 978-1593275648
5. Wil Allsopp, Advanced Penetration Testing: Hacking the World's Most Secure Networks, 2017, ISBN-13: 978-1119367680
6. Aaron Guzman, IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices, 2017, ISBN-13: 978-1787280571

9. Bridging course contents with the expectations of the representatives of the community, professional associations and employers in the field

- Digital security is a constant concern in almost all industry sectors,
- Knowledge of digital information security is important for all components (software or hardware) in IT&C domains.
- The content of the subject is in line with that taught at other university centers at home and abroad;
- In order to better adapt the content of the subject to the requirements of the labor market, meetings with representatives of employers are held;
- The most important theoretical and empirical achievements in the field have been taken into account in the development of the subject.

10. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade
Course	Assessment of knowledge through a test based on the knowledge gained following participation in the course	Written exam / online exam using Teams	50%
Project	How to analyse, synthesise and integrate theoretical information	Practical assessment / online assesment using Teams	30%
	Problem solving corresponding to project meetings	Practical presentation or online presentation using Teams	5%
	Scientific article	1. Structure - compliance with IEEE format and structure; concordance and flow of the paper 2. Content - relevance and comprehensive coverage of subject matter; application of concepts presented in the course; reflection of critical thinking skills 3. Inclusion of a minimum of 6 references	15%

Minimum performance standard:
- Attend project meetings and complete all assignments
- Concurrent conditions for passing the exam:
  - o Minimum of 5 points from the exam
  - o Minimum 5 points from project + scientific paper

Date of filling in:		Title Firstname NAME	Signature
15.03.2023	Course	Conf.dr.ing. Ovidiu Stan	
	Project	Conf.dr.ing. Ovidiu Stan	

Date of approval by the Department Board Automatica _____	Head of Departament Automatica Prof.dr.ing. Honoriu VĂLEAN
Date of approval by the Faculty Council Automatica si Calculatoare _____	Dean Prof.dr.ing. Liviu Cristian MICLEA