SYLLABUS

1. Data about the program of study

1.1	Institution	The Technical University of Cluj-Napoca
1.2	Faculty	Faculty of Automation and Computer Science
1.3	Department	Automation Department
1.4	Field of study	Systems Engineering
1.5	Cycle of study	Research Master's
1.6	Program of study/Qualification	Cyber Physical Systems
1.7	Form of education	Full time
1.8	Subject code	10.00

2. Data about the subject

2.1	Subject name			Cyber-Physical Systems' Security		
2.2	Course responsible/lecturer			Assoc. prof. Stan Ovidiu – Ovidiu.Stan@aut.utcluj.ro		
2.3	Teachers in charge of seminars			Assoc. prof. Stan Ovidiu – Ovidiu.Stan@aut.utcluj.ro		
2.4 Year of study	1	2.5 Semester	2	2.6 Assessment		E
2.7 Subject category	Formative category					DA
	Optionality					DI

3. Estimated total time

3.1 Number of hours per week	3	of which	3.2 Course	2	3.3 Seminar	0	3.3 Laboratory	1	3.3 Project	0
3.4 Total hours in the curriculum	42	of which	3.5 Course	28	3.6 Seminar	0	3.6 Laboratory	14	3.6 Project	0

3.7 Individual study:	
(a) Manual, lecture material and notes, bibliography	20
(b) Supplementary study in the library, online and in the field	20
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays	13
(d) Tutoring	2
(e) Exams and tests	3
(f) Other activities	0

3.8 Total hours of individual study (sum (3.7(a)…3.7(f)))	58
3.9 Total hours per semester (3.4+3.8)	100
3.10 Number of credit points	4

4. Pre-requisites (where appropriate)

4.1	Curriculum	- Mathematical Algebra, Special Mathematics, Probability - Programming in a high-level object language
4.2	Competence	Computer usage basics.

5. Requirements (where appropriate)

5.1	For the course	- Classroom with, video projector, blackboard, - Internet connection

5.2	For the applications	Laboratory attendance is mandatory.

6. Specific competences

Professional competences	C3 Innovative design of complex control systems, industrial networks and related hardware and software components, using domain-specific tools. C3.1 Identification and description of advanced techniques, methods, methodologies and technologies for the analysis, design and implementation of computer applications based on programmable equipment and embedded systems. C3.2 The use of concepts, principles, techniques, methodologies and advanced technologies of analysis, design and implementation of computer applications based on programmable equipment and embedded systems.
Cross competences	CT1 Demonstrating knowledge of the economic, ethical, legal and social context of exercising the profession for identifying tasks, planning activities and opting for responsible decisions, culminating in the conception, drafting and presentation of a scientific paper. CT2 Clear and concise description of the activity flow, tasks and results in the domain, obtained either by assuming the role of leader / project head or as a member of a research team, thanks to: the ability to synthesize information in the field, global overall vision, communication skills with collaborators, the ability to define activities by stages.

7. Discipline objectives (as results from the *key competences gained*)

7.1	General objective	- Identify and master the main modern techniques in security in the current technological context of the CPS and Internet of Things - This course aims to introduce students to the concept of CPS & IoT and its impact on our daily lives, make them understand the architecture and components of CPS & IoT and address the challenges and solutions of implementing. - 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 CPS systems. From this course, students will become aware of the issues of cyber-security issues raised by IoT and will gain knowledge about 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 to secure data through encryption - Identification of vulnerabilities - Security assessment of smart devices - Understanding the impact of CPS & IoT technologies - Knowledge of emerging CPS & IoT technologies - Developing critical thinking skills

8. Contents

8.1. Lecture (syllabus)	Number of hours	Teaching methods	Notes
01. Course Logistics. Security Basics	2	Presentation and reading from course notes and references, questions and answers face-to-face and online, case studies.	
02. IoT and CPS System Architecture: Their Differences, Understanding Their Threat Models	2		
03. Program Analysis for IoT/CPS (Dynamic, Static Analysis, Symbolic Execution)	2		
04. Building Blocks of Binary Analysis (Program Slicing, Taint Tracking, Summarization, Binary Rewriting, Symbolic Execution), Binary Hardening, Information Leaks, and Side-channels.	2		
05. Side Channel Attacks; Definition, Attack Types, Threat Model	2		
06. Formal Analysis and Verification (Model Checking and Falsification with LTL/MTL)	2		
07. Defense Strategies, Static and Dynamic Enforcers	2		
08. Machine Learning for Perception and Decision Making (Autonomous Vehicle Controller Pipeline, Sensor Fusion, Kalman Filter)	2		
09. Models of Autonomous Systems, Data-driven Verification, Verification of Models with Black-box Components	2		
10. Voice-assistant Systems, Their Architectures, Integrated Algorithms (Voice Recognition, Intent Extraction, Conflict Resolution)	2		
11. Security Protocols and Their Verification, part 1	2		
12. Security Protocols and Their Verification, part 2	2		
13. Trusted and Confidential Computing (TCC), part 1	2		
14. Trusted and Confidential Computing (TCC), part 2	2		

Bibliography

1. Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems 3rd Edition, ISBN 978-1119642787, Chapters 1, 2, 3
2. Trent Jaeger, Operating System Security, ISBN: 978-3-031-02333-0, Chapter 1
3. Greer, C. , Burns, M. , Wollman, D. and Griffor, E. (2019), Cyber-Physical Systems and Internet of Things, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.1900-202
4. Anders Møller, Michael I. SchwartzbachStatic Program Analysis, https://cs.au.dk/~amoeller/spa/spa.pdf Chapter 1
5. Compilers, Principles, Techniques and Tools (Dragon Book), Chapter 10
6. Celik et al., Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities, https://arxiv.org/pdf/1809.06962.pdf
7. What is soundness (in static analysis) https://tinyurl.com/749mt8n8

8. Shoshitaishvili et al., (State of) The Art of War: Offensive Techniques in Binary Analysis, https://sites.cs.ucsb.edu/~vigna/publications/2016_SP_angrSoK.pdf
9. Mathias Payer, Software Security Principles, Policies, and Protection (Book), Chapter 4 (Memory and Type Safety), https://nebelwelt.net/SS3P/softsec.pdf
10. Manes et al., The Art, Science, and Engineering of Fuzzing: A Survey (Paper), https://arxiv.org/pdf/1812.00140.pdf
11. Klees et al., Evaluating Fuzz Testing (Paper), https://cseweb.ucsd.edu/~dstefan/cse227-spring20/papers/klees:evaluating.pdf
12. Kapinski et al., Simulation-Based Approaches for Verification of Embedded Control Systems, https://viterbi-web.usc.edu/~jdeshmuk/teaching/cs699-fm-for-cps/Papers/B1.pdf
13. Michael Huth, Mark Ryan, Logic in Computer Science, Modelling and Reasoning about Systems, Chapter 3 (Verification by Model Checking), http://staff.ustc.edu.cn/~huangwc/book/LogicInCS.pdf
14. Yurtsever et al., A Survey of Autonomous Driving: Common Practices and Emerging Technologies (Paper), https://arxiv.org/pdf/1906.05113.pdf
15. Spreitzer et al. Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices, https://arxiv.org/pdf/1611.03748.pdf
16. Lentzsch et al., Hey Alexa, is this Skill Safe?: Taking a Closer Look at the Alexa Skill Ecosystem, https://anupamdas.org/paper/NDSS2021.pdf
17. Blanchet et al., Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif, https://bblanche.gitlabpages.inria.fr/publications/BlanchetFnTPS16.pdf
18. Cremers et al., A Comprehensive Symbolic Analysis of TLS 1.3, https://acmccs.github.io/papers/p1773-cremersA.pdf
19. Cerdeira et al., SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-assisted TEE Systems, https://www.cs.purdue.edu/homes/pfonseca/papers/sp2020-tees.pdf
20. Stan, O.P.; Enyedi, S.; Corches, C.; Flonta, S.; Stefan, I.; Gota, D.; Miclea, L. Method to Increase Dependability in a Cloud-Fog-Edge Environment. Sensors 2021, 21, 4714. https://doi.org/10.3390/s21144714

8.2. Seminars /Laboratory/Project	Number of hours	Teaching methods	Notes
01. Crypto and Crypto Protocols • Hashes and Message Authentication • Asymmetric & Symmetric Cryptography • Key Management	2	Documentation reading, presentation and exemplification, individual exercises on the computer, problem solving within a team.	
02. Crypto and Crypto Protocols • User Authentication • Authentication Protocols	2		
03. Network Security • Networking Background and TCP Attacks • Transport Layer Security • Routing Security • DNS Security • Firewalls and Tunnels • Intrusion Detection Systems	2		

04. Topic: Systems Security • Software Vulnerabilities • Access Control • Operating System Security	2		
05. Topic: Systems Security • Web Security • Mobile Security • IoT Security	2		
06. Machine Learning for Security Applications • Attacks on the Machine Learning Pipeline: Poisoning attacks, model theft attacks, adversarial examples, recovery of sensitive training data, and physical-world attacks • Threat Models: White Box, Black Box, and Grey Box • Transferability • Types of Defenses: Pre-processing, and robust optimization • Introduction to Privacy in Machine Learning: Membership inference and model inversion attacks	2		
07. Security of Machine Learning Systems	2		

Bibliography

1. Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems 3rd Edition, ISBN 978-1119642787, Chapters 1, 2, 3
2. Trent Jaeger, Operating System Security, ISBN: 978-3-031-02333-0, Chapter 1
3. Greer, C. , Burns, M. , Wollman, D. and Griffor, E. (2019), Cyber-Physical Systems and Internet of Things, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.1900-202
4. Anders Møller, Michael I. SchwartzbachStatic Program Analysis, https://cs.au.dk/~amoeller/spa/spa.pdf Chapter 1
5. Compilers, Principles, Techniques and Tools (Dragon Book), Chapter 10
6. Celik et al., Program Analysis of Commodity IoT Applications for Security and Privacy: Challenges and Opportunities, https://arxiv.org/pdf/1809.06962.pdf
7. What is soundness (in static analysis) https://tinyurl.com/749mt8n8
8. Shoshitaishvili et al., (State of) The Art of War: Offensive Techniques in Binary Analysis, https://sites.cs.ucsb.edu/~vigna/publications/2016_SP_angrSoK.pdf
9. Mathias Payer, Software Security Principles, Policies, and Protection (Book), Chapter 4 (Memory and Type Safety), https://nebelwelt.net/SS3P/softsec.pdf
10. Manes et al., The Art, Science, and Engineering of Fuzzing: A Survey (Paper), https://arxiv.org/pdf/1812.00140.pdf
11. Klees et al., Evaluating Fuzz Testing (Paper), https://cseweb.ucsd.edu/~dstefan/cse227-spring20/papers/klees:evaluating.pdf

12. Kapinski et al., Simulation-Based Approaches for Verification of Embedded Control Systems, https://viterbi-web.usc.edu/~jdeshmuk/teaching/cs699-fm-for-cps/Papers/B1.pdf
13. Michael Huth, Mark Ryan, Logic in Computer Science, Modelling and Reasoning about Systems, Chapter 3 (Verification by Model Checking), http://staff.ustc.edu.cn/~huangwc/book/LogicInCS.pdf
14. Yurtsever et al., A Survey of Autonomous Driving: Common Practices and Emerging Technologies (Paper), https://arxiv.org/pdf/1906.05113.pdf
15. Spreitzer et al. Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices, https://arxiv.org/pdf/1611.03748.pdf
16. Lentzsch et al., Hey Alexa, is this Skill Safe?: Taking a Closer Look at the Alexa Skill Ecosystem, https://anupamdas.org/paper/NDSS2021.pdf
17. Blanchet et al., Modeling and Verifying Security Protocols with the Applied Pi Calculus and ProVerif, https://bblanche.gitlabpages.inria.fr/publications/BlanchetFnTPS16.pdf
18. Cremers et al., A Comprehensive Symbolic Analysis of TLS 1.3, https://acmccs.github.io/papers/p1773-cremersA.pdf
19. Cerdeira et al., SoK: Understanding the Prevailing Security Vulnerabilities in TrustZone-assisted TEE Systems, https://www.cs.purdue.edu/homes/pfonseca/papers/sp2020-tees.pdf
20. Stan, O.P.; Enyedi, S.; Corches, C.; Flonta, S.; Stefan, I.; Gota, D.; Miclea, L. Method to Increase Dependability in a Cloud-Fog-Edge Environment. Sensors 2021, 21, 4714. https://doi.org/10.3390/s21144714

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

The course is essential in cyber-physical systems and familiarizes students with the basic security problems and solutions. The material is continuously adapted to the requirements of potential employers and to the feedback of already employed graduates.

10. Evaluation

Activity type	10.1 Assessment criteria	10.2 Assessment methods	10.3 Weight in the final grade
10.4 Course	Method of analysis, synthesis and integration of theoretical information	Exam	50%
10.5 Seminars /Laboratory/Project	Method of analysis, synthesis and integration of theoretical information	Project	30%
	Problem solving corresponding to laboratory meetings	Presentation of solutions, answers to questions	5%
	Scientific paper	1. Organization - adherence to IEEE format and structure; concordance and flow of work 2. Content - relevance and comprehensive coverage of subject matter; application of	15%

		concepts presented in the course; reflection of critical thinking skills 3. Inclusion of a minimum of 10 references	
10.6 Minimum standard of performance - Attend laboratory meetings and complete all assignments - Concurrent conditions for passing the exam - Minimum of 5 points from the exam - Minimum 5 points from project + scientific paper			

Date of filling in:		**Title Surname Name**	**Signature**
16.03.2023	Lecturer	Assoc.prof.Ovidiu Stan	
	Teachers in charge of applications	Assoc.prof.Ovidiu Stan	

Date of approval in the Automation Department _____	Head of department Prof. dipl. eng. Honoriu VĂLEAN, PhD
Date of approval in the Faculty of Automation and Computer Science _____	Dean Prof. dipl. eng. Liviu MICLEA, PhD