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	Computer Science
1.4 Field of study	Computer Science and Information Technology
1.5 Cycle of study	Master
1.6 Program of study / Qualification	Cybersecurity Engineering / Master
1.7 Form of education	Full time

2. Data about the subject

2.1 Subject name	***Mobile Security***			Subject code	**4.10**
2.2 Course responsible / lecturer	Assoc. prof. dr. eng. Ciprian-Pavel OPRIȘA				
2.3 Teachers in charge of seminars / Laboratory / project	Assoc. prof. dr. eng. Ciprian-Pavel OPRIȘA				
2.4 Year of study	I	2.5 Semester	1	2.6 Type of assessment (E - exam, C - colloquium, V – verification)	E
2.7 Subject category	Formative category: DA – advanced, DS – speciality, DC – complementary				DA
	Optionality: DI – imposed, DO – optional (alternative), DF – optional (free choice)				DO

3. Estimated total time

3.1 Number of hours per week	4	of which:	Course	2	Seminars	0	Laboratory	2	Project	0
3.2 Number of hours per semester	56	of which:	Course	28	Seminars	0	Laboratory	28	Project	0
3.3 Individual study:										
(a) Manual, lecture material and notes, bibliography										18
(b) Supplementary study in the library, online and in the field										24
(c) Preparation for seminars/laboratory works, homework, reports, portfolios, essays										50
(d) Tutoring										0
(e) Exams and tests										2
(f) Other activities:										0

3.4 Total hours of individual study (suma (3.3(a)…3.3(f)))	94
3.5 Total hours per semester (3.2+3.4)	150
3.6 Number of credit points	6

4. Pre-requisites (where appropriate)

4.1 Curriculum	Software Design, Operating Systems
4.2 Competence	Using mobile devices

5. Requirements (where appropriate)

5.1. For the course	blackboard, beamer, computers
5.2. For the applications	blackboard, beamer, computers

6. Specific competence

6.1 Professional competences	develop information security strategy perform ICT security testing manage system security manage IT security compliances identify ICT security risks define security policies educate on data confidentiality provide ICT consulting advice ensure information privacy monitor developments in field of expertise keep up with the latest information systems solutions
6.2 Cross competences	The graduate • develop an analytical approach • taking a proactive approach • developing strategies to solve problems • being open minded • coordinate engineering teams

7. Expected Learning Outcomes

Knowledge	The student has knowledge of: • ICT security standards • Internet of Things (IoT) • computer programming • cyber attack counter-measures • digital systems • security engineering • cloud technologies • ICT network security risks • Internet of Things (IoT) • mobile device management • network standards • operating systems • cloud monitoring and reporting • cloud security and compliance • computer forensics • cyber security • information confidentiality • building systems monitoring technology • security threats • attack vectors • web application security threats

Commented [BI1]: 2529.08 cybersecurity risk manager

Skills	The student is able to: • analyse ICT systems • define security policies • define technical requirements • identify ICT security risks • identify ICT system weaknesses • interpret technical texts • keep up with the latest information systems solutions • perform ICT security testing • perform risk analysis • provide ICT consulting advice • use software design patterns • use software libraries • perform project management • manage ICT data architecture • manage IT security compliances • manage digital identity • manage keys for data protection • monitor system performance • optimise the choice of ICT solutions • perform project management • perform risk analysis • perform scientific research • protect personal data and privacy • provide information • provide user documentation • remove computer viruses or malware • manage systems • develop with cloud services • implement anti-virus software • implement cloud security and compliance
Responsibilities and autonomy	The student has the ability to work independently in order to: • develop an analytical approach • take a proactive approach • develop strategies to solve problems • be open-minded • coordinate engineering teams

Commented [BI2]: 2529.3 embedded systems security engineer

8. Discipline objective (as results from the *key competences gained*)

8.1 General objective	After this course, the students will be familiar with mobile and IoT security concepts and will be able to build secure Android applications. They will also be able to perform reverse engineering on mobile applications, for detecting malware and discovering security and privacy issues.
8.2 Specific objectives	1. Understanding how the Android and iOS operating system work, how their applications work and how their applications markets work. 2. Acquiring the skill to develop mobile applications. 3. Acquiring the skill to reverse engineer a mobile application. 4. Understanding how IoT devices work and their relationship with mobile applications.

9. Contents

9.1 Lectures	Hours	Teaching methods	Notes
Mobile Devices and Mobile Platforms	2	Presentations using slides and the blackboard,	
Activities, Intents and GUI Basics	2		
Services, BroadcastReceivers and ContentProviders	2		

Permissions, Network Access and the NDK	2	discussions, individual assignments consisting in reading and presenting research papers	
The Publication and Monetization of Mobile Apps	2		
Reverse Engineering: Static Analysis	2		
Reverse Engineering: Dynamic Analysis	2		
Anti-Analysis Techniques	2		
Android Malware	2		
Privacy Threats on Mobile Platforms	2		
Privilege Escalation	2		
Security in Telecommunication Networks	2		
Security in the Internet of Things	2		
Summary, Recap and Exam Preparation	2		

Bibliography:

- Hacking Exposed: Mobile Security Secrets & Solutions (Berman, Neil – 2013 – McGraw-Hill)
- Mobile Application Security (Dwivedi, Himanshu – 2010 – Mc-Graw Hill)
- Android Forensics (Hoog, Andrew – 2007 – Syngress)
- Android Native Development Kit Cookbook (Liu, Feipeng – 2013 – Packt Publishing)
- Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It (Zdziarski, Jonathan – 2012 – O'Reilly)
- Professional Android 4 Application Development (Meier, 2012)

9.2 Applications - Seminars/Laboratory/Project	Hours	Teaching methods	Notes
Introduction to Android Application Development	4	Short presentations, work guides, live demos, discussions, problems solving	
Developing Android Applications that Interact with External Services	4		
Developing Android Applications that Interact with System Components	4		
Developing Android Applications that Interact with Mobile Sensors	4		
Static Reverse Engineering on Mobile Applications	4		
Dynamic Reverse Engineering on Mobile Applications	6		
Lab Evaluation	2		

Bibliography

- Hacking Exposed: Mobile Security Secrets & Solutions (Berman, Neil – 2013 – McGraw-Hill)
- Mobile Application Security (Dwivedi, Himanshu – 2010 – Mc-Graw Hill)
- Android Forensics (Hoog, Andrew – 2007 – Syngress)
- Android Native Development Kit Cookbook (Liu, Feipeng – 2013 – Packt Publishing)
- Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It (Zdziarski, Jonathan – 2012 – O'Reilly)
- Professional Android 4 Application Development (Meier, 2012)

**Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.*

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

It is done through discussions with representants with the most significant employers, especially those active in the cybersecurity field.
Multiple master programs abroad offer mobile security optional courses:

- XACS215 - Mobile Security, Stanford, USA https://online.stanford.edu/courses/xacs215-mobile-security
- Mobile Systems Security (with Aalto), University of Helsinki, Finland https://www.cs.helsinki.fi/en/courses/582704/2016/k/k/1

10. Evaluation

Activity type	Assessment criteria	Assessment methods	Weight in the final grade
Course	Problem-solving skills specific to the mobile security field	Written exam, including online quiz tests (e.g. on Moodle	70%

	Attendance and active participation during lectures	platform) and presentation(s) of different subjects / paper in the course's field during semester time.	
Seminar	-	-	-
Laboratory	Problem-solving skills specific to the mobile security field Attendance and active participation during labs	Evaluate lab activity. Evaluate lab assignments (homework). Evaluate solutions of problems given in a final lab exam.	30%
Project	-	-	-
Minimum standard of performance:			

Date of filling in: 01.09.2025	**Responsible**	**Title First name Last name**	**Signature**
	Course	Assoc. prof. dr. eng. Ciprian-Pavel OPRIȘA	
	Applications	Assoc. prof. dr. eng. Ciprian-Pavel OPRIȘA	

Date of approval in the department 17.09.2025	Head of department, Prof.dr.eng. Rodica Potolea
Date of approval in the Faculty Council 19.09.2025	Dean, Prof.dr.eng. Vlad Mureșan