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	Department	Computer Science
1.4	Field of study	Computer Science and Information Technology
1.5	Cycle of study	Master of Science
1.6	Program of study / Qualification	Cybersecurity Engineering / Master
1.7	Form of education	Full time
1.8	Subject code	4.1.

2. Data about the subject

2.1	Subject name			***Mobile Security***	
2.2	Course responsible/lecturer			Assoc. Prof. Dr. Eng. Ciprian OPRIȘA- ciprian.oprisa@cs.utcluj.ro	
2.3	Teachers in charge of seminars			Assoc. Prof. Dr. Eng. Ciprian OPRIȘA - ciprian.oprisa@cs.utcluj.ro	
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	3.2 Course	2	3.3 Seminar	0	3.3 Laboratory	2	3.3 Project	0
3.4 Total hours in the curriculum	56	of which	3.5 Course	28	3.6 Seminar	0	3.6 Laboratory	28	3.6 Project	0

3.7 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

3.8 Total hours of individual study (sum (3.7(a)…3.7(f)))	94
3.9 Total hours per semester (3.4+3.8)	150
3.10 Number of credit points	6

4. Pre-requisites (where appropriate)

4.1	Curriculum	Software Design, Operating Systems
4.2	Competence	N/A

5. Requirements (where appropriate)

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

6. Specific competences

Professional competences	**C1. Identify and understand the security issues specific to the different contexts of computing system usage. Appropriately apply the basic elements of security management and methods of evaluation and management of information security risks.** • **C1.1.** Knowledge of advanced theoretical and practical terminology, concepts, and principles specific to cybersecurity field. Knowledge of concepts about cybersecurity risk evaluation, and management. • **C1.2.** Understanding cybersecurity risks specific to new situations and their relationship with previously experienced situations and risks. Be able to predict possible threat scenarios when using cybersecurity solutions in new fields or situations. • **C1.3.** Capability to identify and model new types of cybersecurity risks affecting end users, computing systems, and software applications, and identify and evaluate possible solutions against such risks. **C4. Design and develop highly secure software, security solutions and tools.** • **C4.1.** Knowledge of basic concepts and principles of secure software development and evaluation. Knowledge of common types of security software and tools. Knowledge of different operating system architectures, hardware and software infrastructures and frameworks needed to develop effective security solutions. • **C4.2.** Be able to identify new situations and scenarios when it is needed to develop a new cybersecurity solution or use an existing one. Be able to analyze proposed cybersecurity solutions and compare them with existing ones. • **C4.3.** Capability to develop complex secure software, complying with recommended good practices of built-in security and secure coding. Capability to develop software tools used for cybersecurity pentesting and assessment. • **C4.5.** Capability to develop software modules and tools that could provide a high degree of cybersecurity. Capability to propose new methods to assess the cybersecurity of computing systems and devices and ways to improve it. **C5. Develop rigorous and efficient security solutions to complex real-life problems and situations. Be able to use security mathematical tools and models, engineering approaches and technologies specific and appropriate for the information and computing system security field.** • **C5.1.** Knowledge of complex relationship between cybersecurity and real-life aspects. Knowledge of mathematical theory some cybersecurity mechanisms and solutions are based on. • **C5.4.** Capability to identify and assess limitations of existing cybersecurity solutions and tools used in real-life situations, their residual cybersecurity risks, and their criticality. Capability to identify and research new cybersecurity fields and methods that could be used to reduce the limitations of existing cybersecurity solutions.
Cross competences	N/A

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

7.1	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.
7.2	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

8. Contents

8.1. Lecture (syllabus)	Number of hours	Teaching methods	Notes
Mobile Devices and the Android Platform	2	Presentations using slides and the blackboard, discussions, individual assignments consisting in reading and presenting research papers	
Activities, Intents and GUI Elements	2		
Services, Broadcast Receivers and Content Providers	2		
Permissions, Network Access and the NDK	2		
Publishing and Monetizing Mobile Applications	2		
Static Reverse Engineering on Mobile Applications	2		
Dynamic Reverse Engineering on Mobile Applications	2		
Anti-analysis Techniques	2		
Mobile Malware	2		
Privacy Issues in Mobile Environments	2		
Privilege Escalation	2		
The Security of GSM Networks	2		
The Security in Internet of Things	2		
Summary, Recap and Exam Preparation	2		

Bibliography

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

8.2. Seminar / Laboratory / Project	Number of 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

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

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 Attendance and active participation during lectures	Written exam, including online quiz tests (e.g. on Moodle platform) and presentation(s) of different subjects / paper in the course's field during semester time.	70%
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%

Minimum standard of performance

***Lecture*.** Attending **minimum 50%** of lecture classes, to be allowed to take the final examination. Students must be able to define and describe fundamental aspects regarding mobile devices and their security mechanisms. Minimum final grade must be 5 for the exam to be considered passed.

***Lab*.** Attending **all lab classes** (one lab could be recovered during the semester, and one more during re-examination sessions). Students must be able to identify fundamental vulnerabilities in given programs specific to mobile platforms, in particular Android. This kind of assessment could happen in relation to assignments given during semester or subjects given during the final lab evaluation. Minimum lab grade must be 5 for being allowed at final exam.

Date of filling in:		**Title Surname Name**	**Signature**
	Lecturer	Assoc. Prof. Dr. Eng. Ciprian Oprisa	
	Teachers in charge of application	Assoc. Prof. Dr. Eng. Ciprian Oprisa	

Date of approval in the Computer Science Department 20.02.2024	Head of department Prof.dr.ing. Rodica Potolea
Date of approval in the faculty of Automation and Computer Science 22.02.2024	Dean Prof.dr.ing. Mihaela Dinsoreanu