SYLLABUS

Securing Mobile and IoT Software

University year 2025-2026

1. **Information regarding the programme**

1.1. Higher education institution	Babeș-Bolyai University
1.2. Faculty	Faculty of Mathematics and Computer Science
1.3. Department	Department of Computer Science
1.4. Field of study	Computer Science
1.5. Study cycle	Master
1.6. Study programme/Qualification	Cybersecurity
1.7. Form of education	Full time

2. **Information regarding the discipline**

2.1. Name of the discipline	**Securing Mobile and IoT Software**					Discipline code	**MME8209**
2.2. Course coordinator	Dan Cojocar, PhD						
2.2. Seminar coordinator	Dan Cojocar, PhD						
2.4. Year of study	**2**	2.5. Semester	**1**	2.6. Type of evaluation	**E**	2.7. Discipline regime	**Mandatory**

3. **Total estimated time** (hours/semester of didactic activities)

3.1. Hours per week	**4**	Of which: 3.2 course	**2**	3.3. Seminar/laboratory/project	**2 lab/ seminar**
3.4. Total hours in the curriculum	**56**	Of which: 3.5 course	**28**	3.6. Seminar/laboratory/project	**28**
Time allotment for individual study (ID) and self-study activities(SA)					**hours**
Learning using manual, course support, bibliography, course notes (SA)					30
Additional documentation (in libraries, on electronic platforms, field documentation)					20
Preparation for seminars/labs, homework, papers, portfolios, and essays					24
Tutorship					10
Evaluations					10
Other activities					0
3.7. Total individual study hours				**94**	
3.8. Total hours per semester				**150**	
3.9. Number of ECTS credits				**6**	

4. **Prerequisites** (if necessary)

4.1. Curriculum	Mobile Application Programming, Programming Fundamentals (e.g., Java/Kotlin/Swift, Python), Object-Oriented Programming, Computer Networks, Operating Systems.
4.2. Competencies	Basic knowledge of programming, understanding of client-server architectures, familiarity with common operating systems (Linux, Windows, Android, iOS).

5. **Conditions** (if necessary)

4.1. For the course	Lecture hall with projector and internet access.
4.2. For the seminar/lab activities	• Lab with computers (Windows, Linux, or macOS). • Internet access for downloading tools and accessing resources. • Ability to install software (emulators, security tools, IDEs).

6.1. **Specific competencies acquired**[1]

Professional/ essential competencies	• Know and understand the main paradigms related to data protection: confidentiality, integrity and data availability. • Proficient use of verification, validation, and evaluation criteria and methods in order to ensure software security. • Demonstrate advanced skills to analysis, design, and construction of secure software systems, using a wide range of hardware / software platforms (especially mobile and IoT). • Acquiring a solid theoretical foundation in communication through unsafe medium, as well as the use of secure communication protocols on the Internet.

[1]One can choose either competences or learning outcomes, or both. If only one option is chosen, the row related to the other option will be deleted, and the kept one will be numbered 6.

	• Learning how the main forms of malware and the main forms of attacks on the Internet work, as well as the methods of protection against them. • Knows the basic concepts of programming applications for mobile devices and security models used in such applications.
Transversal Competencies	• Applying the norms of organized and efficient work, responsibility and reliability of the work performed both individually and within a team. • Ethic and fair behaviour, commitment to professional deontology. • Develops and promotes effective work strategies and practices, exemplary professional style and conduct, respecting the values and principles of professional ethics and deontology. • Uses efficient strategies, methods and techniques for lifelong education, in order to self educate and self develop his/her personal and professional skills. • Demonstrates teamwork capabilities and develops communication skills.

6.2. **Learning outcomes**

Knowledge	The student / graduate knows the basic concepts of programming applications for mobile devices and security models used in such applications. - The student / graduate has knowledge about the most popular types of malware applications, about their architecture and how they work. - The student / graduate acquires knowledge about the worst types of vulnerabilities in the field, as well as about measures to prevent these vulnerabilities. - The student / graduate has knowledge about Internet applied cryptography, especially knowledge related to the public and private key cryptography. - The student / graduate understands the fundamental aspects of organizations, human resources and management in the field of organizational security.
Skills	The student / graduate is able to develop secure software systems. - The student / graduate is able to identify possible security issues in software systems. - The student / graduate acquires skills to use various tools in the testing process to identify software vulnerabilities. - The student / graduate acquires the minimum basic skills needed to write a clean source code without vulnerabilities. - The student / graduate is able to assess the security risk using at least one of the established methods. - The student / graduate has the ability to evaluate the security features of software applications at the source code level.
Responsibility and autonomy	• The student / graduate knows how to approach from a legal and moral point of view various topics such as Internet crime and user privacy. • The student / graduate is able to elaborate a security procedure. • The student/graduate assumes responsibility for the product of his / her work, requests feedback and uses it constructively.

7. **Objectives of the discipline** (outcome of the acquired competencies)

7.1. **General objective of the discipline**	• To acquire theoretical and methodological knowledge related to mobile and IoT application security. • To develop practical skills in identifying, analyzing, and mitigating security vulnerabilities in mobile and IoT ecosystems.
7.2. **Specific objective of the discipline**	• Understanding the mobile/IoT threat landscape and risk assessment. • Analyzing the human element in mobile security (social engineering, user awareness). • Securing the mobile application lifecycle (vetting, secure coding, testing). • Implementing identity, access management, and cryptography on mobile devices. • Securing IoT systems controlled by mobile applications.

8. **Content**

8.1. **Course**	Teaching methods	Remarks
1. [The Mobile Security Landscape: Principles, Threats, and Risk Management] Introduction to Mobile Security Principles (CIA), Taxonomy of Mobile Threats (Malware, Phishing, Network Attacks), Mobile Vulnerabilities (OS, App, Net-	Exposure: description, examples, discussion of case studies, live demo.	

work), Risk Assessment Frameworks.		
2. [The Human Element: Social Engineering and User-Centric Security] Psychology of Social Engineering, User Behavior and Awareness, Managing Privacy Settings and Permissions, Situational Crime Prevention.		
3. [Securing the App Ecosystem: Application Stores, Vetting, and Sideloading] Security Architecture of Apple App Store vs. Google Play, Application Vetting Process (Static, Dynamic), Dangers of Sideloading, Permission Models (Android & iOS).		
4. [Practical Mobile Application Security: Identifying and Mitigating Common Vulnerabilities] OWASP Mobile Top 10, Vulnerability Discovery (SAST, DAST, IAST), Reverse Engineering (APK, IPA), Secure Coding Practices.		
5. [The Arms Race Against Mobile Malware] Modern Mobile Malware Landscape (Spyware, Ransomware, Trojans), Signature-based vs. Behavior-based Detection, Applying Machine Learning for Malware Detection, Effectiveness of Anti-Malware apps.		
6. [Identity and Access Management (IAM) in a Mobile World] Challenges in Mobile Identity, Authentication Factors (Biometrics), Mobile as an MFA Token, Federated Identity (OAuth 2.0, OpenID Connect), Performance of Cryptographic Operations.		
7. [Advanced Mobile Privacy: From Permissions to Formal Models] The Mobile Privacy Landscape (Trackers, Ad Networks), Deep Dive into Android/iOS Permissions, Privacy-Enhancing Technologies (PETs), Formal Privacy Models (k-Anonymity, Differential Privacy).		
8. [Developing a Corporate Mobile Security Strategy] Building a Mobile Security Strategy, BYOD vs. Corporate-Owned, Mobile Device Management (MDM/MAM/UEM), Implementing Technical Controls, Incident Response for Mobile.		
9. [Mobile Digital Forensics: Evidence Acquisition and Analysis] Principles of Digital Forensics (Preservation, Extraction), Challenges (Encryption, Cloud), Logi-		

cal vs. Physical Acquisition, Artifact Analysis (Logs, Location Data).		
10. [Applied Cryptography for Mobile and IoT Devices] Fundamentals of Symmetric/Asymmetric Cryptography, Performance Challenges on Mobile, Digital Signature Schemes (RSA, ECDSA), Securing Data-in-Transit (TLS) and Data-at-Rest.		
11. [The Mobile-IoT Security Nexus] Mobile Apps as IoT Control Plane, REST Foundations for IoT, Authentication and Security for RESTful IoT Protocols, REST Message Authentication Mechanisms.		
12. [Specialized Applications and the Future of Mobile Security] Case Studies (mHealth, Mobile Payments, Law Enforcement), Impact of 5G on Security, Future of Defense (AI/ML in Security), Post-Quantum Cryptography.		
13. [Project Work Session & Q&A] Dedicated session for consultation on the final project. Review of key concepts and difficult topics.		
14. [Final Review & Exam Preparation] Summary of the course, key topics, discussion of exam format and final project presentations.	Discussion of case studies, exam discussions.	

- "Dwivedi, H., Clark, C., & Thiel, D. V. (2010). Mobile application security (Vol. 275). New York: McGraw-Hill."
- "Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. International Journal of Information Management, 52, 102063."
- "Russell, B., & Van Duren, D. (2016). Practical internet of things security. Packt Publishing Ltd."
- "Alanda, A., Satria, D., Mooduto, H. A., & Kurniawan, B. (2020, May). Mobile application security penetration testing based on OWASP. In IOP Conference Series: Materials Science and Engineering (Vol. 846, No. 1, p. 012036). IOP Publishing"
- OWASP Internet of Things Top 10

8.2. Seminar/Laboratory	Teaching methods	Remarks
1. [Introduction & Project Setup] Discussion of course topics, brainstorming project ideas. Setup of development and security tools.	Exposure: description, discussion. Evaluation.	Seminar/Project sessions are held for 2 hours, once every two weeks.
2. [Project Proposal & Threat Modeling] Students present their project ideas, scope, and initial architecture. Conduct a threat modeling exercise (e.g., STRIDE).		
3. [Vulnerability Analysis 1] Practical lab on Static Analysis (SAST) and Reverse Engineering of Android/iOS apps.		
4. [Vulnerability Analysis 2] Practical lab on Dynamic Analysis (DAST) and Intercepting Network		

Traffic (e.g., Burp Suite, mitmproxy).		
5. [Secure Implementation] Project progress check. Focus on implementing security controls (e.g., secure storage, proper auth, input validation).		
6. [Project Pre-Presentations] Near-final project demonstrations and peer/instructor code review. Feedback session.		
7. [Final Project Presentations & Submissions] Final evaluation of the project. Demo and defense of the security measures implemented.		

- "Dwivedi, H., Clark, C., & Thiel, D. V. (2010). Mobile application security (Vol. 275). New York: McGraw-Hill."
- "Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. International Journal of Information Management, 52, 102063."
- "Russell, B., & Van Duren, D. (2016). Practical internet of things security. Packt Publishing Ltd."
- "Alanda, A., Satria, D., Mooduto, H. A., & Kurniawan, B. (2020, May). Mobile application security penetration testing based on OWASP. In IOP Conference Series: Materials Science and Engineering (Vol. 846, No. 1, p. 012036). IOP Publishing"
- OWASP Internet of Things Top 10

9. **Corroborating the content of the discipline with the expectations of the epistemic community, professional associations, and representative employers within the field of the program**

- The course aligns with the IEEE and ACM curriculum recommendations for Computer Science programs.
- It is included in the study programs of major universities both in Romania and internationally.
- The course content is considered essential by software companies for developing solid, industry-relevant programming skills.

10. **Evaluation**

Activity type	10.1. Evaluation criteria	10.2. Evaluation methods	10.3. Percentage of final grade
10.4 Course	• Final Written Exam.	• Written exam covering theoretical concepts from all lectures.	• 40%
10.5 Seminar/ laboratory	• Semester Project. • Practical lab activities and milestone checks.	• Evaluation of project milestones, final presentation, and submitted code/report. • Assessment of practical skills during lab sessions.	• 60%
10.6. Minimum standard of performance			
• Attendance at a minimum of 75% of seminar/project sessions. • A minimum grade of 5 (on a scale of 1 to 10) on the final written exam. • A minimum grade of 5 (on a scale of 1 to 10) on the semester project/seminar activities. • The final aggregated grade must be at least 5.			

11. **Labels ODD (Sustainable Development Goals)**[2]

Not applicable.

Date: Signature of course coordinator, Dan Cojocar, PhD Signature of seminar coordinator, Dan Cojocar, PhD

[2]Keep only the labels that, according to the Procedure for applying ODD labels in the academic process, suit the discipline and delete the others, including the general one for Sustainable Development – if not applicable. If no label describes the discipline, delete them all and write "Not applicable.".

Date of approval:

Signature of the head of department,
Adrian Sterca, PhD