UNIVERSITAS MATARAM
(University of Mataram)
FAKULTAS TEKNIK
(Faculty of Engineering)
PROGRAM STUDI TEKNIK INFORMATIKA
(Department of Informatics Engineering)

MODULE HANDBOOK DESCRIPTION

Mobile Security (P22B09)

Module designation	Mobile Security
Semester(s) in which the module is taught	*8 / fourth year*
Person responsible for the module	*Raphael Bianco Huwae, S.T., M.T.*
Language	*Indonesian*
Relation to curriculum	*Electives*
Teaching methods	*Lectures, Discussions, Project*
Workload (incl. contact hours, self- study hours)	Contact Hours every week, each week of the 16 weeks/semester including Evaluation ● 2 x 50 minutes lecturer/week ● 120 minutes class exercise/week ● Self Study hours = 150 minutes/week ● Midterm Exam = 60 minutes ● Final Exam = 60 minutes Total workload 88,58 hours/semester
Credit points	*2 (~ 3,54 ECTS)*
Required and recommended prerequisites for joining the module	-

Module objectives/intended learning outcomes	The primary goal of this course is to provide students with an understanding of mobile security concepts, threats, and protection mechanisms. Upon completing the course, students should be able to: 1. Identify security vulnerabilities in mobile operating systems and applications. 2. Understand encryption and authentication techniques used in mobile security. 3. Implement security measures for mobile networks and communications. 4. Analyze malware and cyber threats targeting mobile platforms. 5. Assess risks and develop strategies to enhance mobile security. 6. Design and implement secure mobile applications.

Content	This course covers fundamental and advanced topics related to mobile security, including: 1. Introduction to Mobile Security: Threats, challenges, and importance. 2. Mobile Operating System Security: Android, iOS, and other platforms. 3. Authentication and Encryption: Techniques and best practices. 4. Mobile Application Security: Common vulnerabilities and countermeasures. 5. Mobile Malware Analysis: Types, detection, and prevention. 6. Secure Mobile Communications: Wireless security protocols and network protection. 7. Privacy and Data Protection in Mobile Environments. 8. Case Studies and Real-World Mobile Security Challenges.
Examination forms	*Assignments, Quiz, Simulation, Project (Oral Presentation)*
Study and examination requirements	*Assignments 10%,* *Quiz 25%,* *Simulation 25%,* *Project 40%*

Reading list	**1.** Stahl, F. (2021). Mobile Security and Privacy: Advances, Challenges, and Future Research Directions. Springer. **2.** Burns, J. (2012). Mobile Security for Dummies. John Wiley & Sons. **3.** Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A Survey of Mobile Malware in the Wild. IEEE Security & Privacy. **4.** Gupta, P. K., Agrawal, D., & Yamaguchi, S. (2020). Handbook of Mobile Security: Strategies and Implementations. CRC Press. **5.** Enck, W., & Octeau, D. (2016). Mobile Security: Technologies and Challenges. IEEE Computer Society.