Obuda University John von Neumann Faculty of Informatics			*Institute of Biomatics and Applied Artificial Intelligence*	
Name and code: Automotive Cybersecurity *NBVAC1EBNE* **Credits*: 3*** *Computer Science Engineering BSc* *2022/23 year I. semester*				
Responsible person of subject: Dr. Bánáti Anna				
Subject lecturers: Dr. Csilling Ákos, Mera Abbassi				
Prerequisites (with code):	Informatikai biztonság (NIEIB0HBNE)			
Weekly hours:	Lecture: 2	Seminar: 0	Lab. hours: 1	Consultation: 0
Way of assessment (exam or midterm grade):	Midterm grade			
Course description:				
Goal: The goal of this course is to introduce students to the basics of cybersecurity within the automotive industry. Students will get an overview about cybersecurity management, ethical hacking, system, software, and hardware security – using practical examples and case-studies from the automotive industry.				
Course description: Introduction to automotive cybersecurity and its management. Introduction to automotive networks and their security, basics of penetration testing. Application of cryptography within vehicles. Security of low-level languages (C, C++), secure coding. Security of operating systems and firmware. Introduction to hardware-level security, analysis of programmable circuit boards (PCB), reverse engineering, case studies.				

Lecture schedule	
Education week	*Topic*
1.	Introduction to automotive cybersecurity, case studies.
2.	Cybersecurity management. Threat analysis and risk assessment. Post development cybersecurity tasks.
3.	Introduction to ethical hacking, regulations, approaches. Port scanning, fuzzing, other information gathering techniques. Understanding vulnerabilities, vulnerability scanning.
4.	Ethical hacking tools. Installation and configuration of Kali Linux. Useful tools in Kali Linux, Metasploit Framework.
5.	Security of automotive networks I. Internal communication protocols (Ethernet, CAN, LIN, FlexRay), weaknesses and security measures.
6.	Security of automotive networks II. Wireless technologies (V2X, 5G, GPS, Wi-Fi, Bluetooth), attack surfaces.
7.	Applied cryptography. Cryptographic primitives, in-vehicle use cases. Restrictions and limitations of the environment. Security trade-offs.
8.	Security of low-level programming languages, C and C++. Memory layout and architecture. Understanding the basics of buffer overflow, control flow hijacking, remote code execution. Security measures, secure coding.
9.	OS & firmware security. Malware, ransomware, spyware. Protecting access with HSM. Malicious flashing and flashware tampering.
10.	Hardware security I. Analysing a PCB (UART, SPI, I2C, JTAG).
11.	Hardware security II. Structure of a firmware. Encryption, decryption, hardcoded secrets.
12.	Hardware security III. Reverse engineering, understanding a binary.
13.	Midterm

14.	Midterm (re-take)

Midterm requirements

Assessments schedule		
Education week	*Topic*	
13.	Theoretical test	
14.	Theoretical test (first re-take)	
1. exam week	Theoretical test (second re-take)	

Final grade calculation methods

Achieved result	Grade
89%-100%	excellent (5)
76%-88<%	good (4)
63%-75<%	average (3)
51%-62<%	satisfactory (2)
0%-50<%	failed (1)

The final grade will be calculated based on the theoretical midterm test.
Students will be offered optional quizzes and practical homeworks during the semester, by completing these quizzes and homeworks, extra points can be collected to raise the final grade (only applicable if the satisfactory grade is reached by the midterm test).
Presence is required up to 70% both at the lectures and at the lab sessions.

Type of midterm test

Multiple choice theoretical test, in a written form.

Type of replacement

First retake of the midterm on the last week.
Second retake of the midterm on the first week of the exam period (only if the student attempted the midterm or the first retake but failed).

References

Obligatory: The slides presented at the lectures.

Recommended: Optional materials and useful WEB links shared at the lectures.