COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security of wireless systems [S1Cybez1>BSB]

Course

Field of study
Cybersecurity

Year/Semester
3/6

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
elective

Number of hours

Lecture
24

Laboratory classes
24

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

3,00

Coordinators

prof. dr hab. inż. Hanna Bogucka
hanna.bogucka@put.poznan.pl

Lecturers

Prerequisites

The student starting this course should have a basic understanding of computer system security. Additionally, they should possess foundational knowledge of computer networks and wireless technologies. Basic knowledge of cryptography and security protocols is also required.

Course objective

The objective of the course is to introduce students to the security challenges associated with wireless systems. It covers 5G/6G technologies and open systems (e.g., OpenWiFi, OpenRAN, Open5GS) from a security perspective, including their application in enhancing security through artificial intelligence. The course takes a practical approach to analyzing vulnerabilities in wireless networks, including cellular systems, WLAN, TETRA, and WiMAX. It focuses on understanding the principles of designing and implementing secure wireless systems.

Course-related learning outcomes

Knowledge:
The student has a comprehensive understanding of key wireless technologies (Wi-Fi, LTE, 5G, 6G, TETRA) and their architectures, considering the specific security threats associated with each. They are

familiar with security standards and protocols used in wireless systems, including WPA3, IPsec, TLS, DTLS, and privacy protection mechanisms. They have knowledge of common attacks on wireless systems, such as sniffing, spoofing, man-in-the-middle (MITM), denial-of-service (DoS), and methods for detecting and mitigating these threats. The student is skilled in designing and implementing secure wireless communication systems, including virtual network slices for 5G (network slicing). They are aware of the latest trends in wireless network security, such as edge computing, artificial intelligence in threat detection, and the challenges associated with 5G/6G technologies. [K1_W07][K1_W10][K1_W14]

Skills:
The student can analyze threats and identify vulnerabilities in wireless networks, including 5G/6G systems. They are skilled in configuring and testing security mechanisms in Wi-Fi and cellular networks, such as WPA3. The student can utilize tools for analyzing and monitoring traffic in wireless networks, such as Wireshark and Aircrack-ng, to detect and mitigate threats. They are capable of designing and implementing basic security systems in wireless networks and virtual 5G infrastructures. Additionally, the student can implement risk management procedures and evaluate the effectiveness of security measures in wireless systems. [K1_U02][K1_U03][K1_U04][K1_U06]

Social competences:
The student is capable of critically analyzing and evaluating the security of wireless systems in evolving technological and threat landscapes. They are prepared to make responsible decisions regarding the design, implementation, and management of wireless systems, while considering ethical aspects and privacy protection. The student can collaborate effectively within interdisciplinary teams on projects related to wireless network security. They strive for continuous knowledge improvement in the field of wireless technologies and their security, in the context of the dynamic development of 5G/6G technologies. [K1_K01][K1_K02][K1_K05]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lecture:
Knowledge is assessed through an examination conducted either in written or oral form, or via a test. The passing grade is 51% of the total points, and no auxiliary materials are allowed during the exam.
Laboratory:
Knowledge and skills are assessed based on ongoing progress in the completion of tasks; the evaluation of intended learning outcomes is carried out through an evaluation process. Written reports on individual laboratory topics, and potentially tests assessing the ability to design, configure, and apply security principles in wireless systems, including cellular networks, are required.
In each form of the course assessment, the grade depends on the number of points the student earns relative to the maximum number of required points. Earning at least 51% of the possible points is a prerequisite for passing. The relationship between the grade and the number of points is defined by the Study Regulations. Additionally, the course completion rules and the exact passing thresholds will be communicated to students at the beginning of the semester through the university’s electronic systems and during the first class meeting (in each form of classes).

Programme content

The curriculum covers key wireless technologies, such as Wi-Fi, LTE, 5G/6G, and TETRA, with a focus on their security architectures and associated threats. Particular emphasis is placed on the use of artificial intelligence and machine learning for network traffic analysis, anomaly detection, and addressing advanced threats such as sniffing and DDoS attacks in mobile networks and WLAN systems. Students will learn protective mechanisms, including intrusion detection and prevention systems leveraging AI solutions. The program also includes the design and implementation of secure wireless systems, addressing challenges related to network virtualization (Network Slicing) and edge computing. The practical part of the course focuses on developing skills in risk identification, security configuration, and the implementation of protection strategies using AI technologies in open and modern 5G/6G networks.

Course topics

Lecture Content:
1. Introduction to Wireless System Security

Overview of basic wireless system security (802.11).
Security principles in TETRA systems.
2. Introduction to Security in Cellular Systems
Overview of the security architecture of GSM, UMTS, LTE, 5G/6G systems.
Implementation of integrity, confidentiality, and authentication principles.
3. Open Systems in Wireless Networks
Characteristics of open systems: open interfaces, standards, and platforms.
Open-source projects in wireless networks: OpenWiFi, OpenRAN, OpenAirInterface.
Advantages and disadvantages of open systems: interoperability, flexibility vs. vulnerability to attacks.
Security management in open systems.
4. Specific Threats in Wireless Networks
Basic attacks on access networks and core systems of wireless networks.
Attacks on wireless system applications.
5. 802.11i and WPA3 Security Standards
Ensuring confidentiality in wireless systems, end-to-end security.
6. Wi-Fi Security
Open Wi-Fi networks: threats and protection techniques.
Tools for security analysis in WLAN networks, e.g., Wireshark, Aircrack-ng.
Principles for configuring secure Wi-Fi networks.
7. 5G Security
Security architecture of 5G/6G: Radio Access Network (RAN), Core Network, and Network Slicing.
Threats in 5G networks: attacks on virtualization, Edge Computing, API security.
8. 6G Security Mechanisms
Challenges and potential threats in security through artificial intelligence and quantum technologies.
Security mechanisms: SEPP (Security Edge Protection Proxy), Network Function Virtualization (NFV).
9. Practical Examples and Projects
Analysis of real security incidents in Wi-Fi, 5G systems.
Designing and configuring secure Wi-Fi networks in open environments.
Implementing Network Slicing in 5G, with security mechanisms.
Assessing vulnerabilities and implementing security in open systems (e.g., OpenWiFi, OpenRAN).
10. Artificial Intelligence in Threat Detection in 5G/6G and WLAN Networks
Utilizing machine learning algorithms for anomaly detection.
Attacks on such solutions and countermeasures.
11. Risk Management in Wireless Systems
Risk analysis methodologies (e.g., NIST, ISO/IEC 27005).
Creating security policies for wireless systems.
Incident response procedures.
Security audits and penetration testing of wireless systems.
12. Future of Security in Wireless Networks
Quantum networks.
New security technologies.
Laboratory Content:
1. Introduction and Overview of Laboratory Exercises
Use of Cryptool tool.
2. Analysis of IEEE 802.11 Frame Structure Using Wireshark.
3. Security Analysis and Cracking of WEP, WPA/WPA2, and WPS Mechanisms
Using rainbow tables.
4. Creation and Configuration of Virtual WLAN Networks.
5. Analysis of IEEE 802.1X and RADIUS/EAP Protocols.
6. Different Types of Attacks on IEEE 802.11 Networks
Using tools like Aircrack-ng, Kismet.
7. Open Systems: OpenWiFi Security
Installation and configuration of OpenWiFi.
Risk analysis and mitigation for open standards.
8. Machine Learning Algorithms for Anomaly Detection
Classifying normal and suspicious traffic using Python libraries (e.g., Scikit-learn).
9. Threat Detection in 5G Networks
Analysis of 5G protocols: SEPP, NAS, NGAP.
AI usage for predicting potential threats in 5G environments.
10. Application of AI in Intrusion Detection Systems (IDS)

Creating a simple machine learning-based IDS system.
Analyzing the effectiveness of threat detection in Wi-Fi and 5G networks.
11. Penetration Testing in Wireless Networks
Introduction to penetration testing tools (Aircrack-ng, Metasploit).
Simulating attacks on open systems (e.g., OpenRAN).
Examples of open-source projects (e.g., OpenAirInterface, srsRAN).
12. Conclusion Session. Final exam review.

Teaching methods

Lecture:
1. Multimedia presentation supplemented with real-life examples to illustrate key concepts.
Laboratory Exercises:
2. Performing assigned tasks by the instructor - practical exercises, teamwork, and use of network devices and simulation environments.

Bibliography

Basic:
1. William Stallings, Wireless Communications & Networks, Pearson, 2021.
2. Mazin Alshamrani, Security and Privacy in 5G and Beyond Networks: Challenges and Solutions, Wiley, 2021.
3. Matthew S. Gast, 802.11 Wireless Networks: The Definitive Guide, O'Reilly Media, 2022.
4. Geert Leus, Danilo Mandic (red.), Machine Learning for Wireless Communications, Academic Press, 2022.
5. Literatura z uznanych czasopism naukowych, dokumenty normalizacyjne.

Additional:
1. Haipeng Yao, Mugen Peng, AI for 5G: Core Technologies and Applications, Springer, 2021.
2. Jie Gao, Artificial Intelligence for Wireless Communication and Networking, Wiley-IEEE Press, 2021.
3. nwar Al-Dulaimi, Syed Rizvi, Qiang Ni (red.), 5G Networks: Fundamentals, Techniques, and Applications, Wiley, 2020.

Breakdown of average student's workload

	Hours	ECTS
Total workload	78	3,00
Classes requiring direct contact with the teacher	48	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	30	1,00