COURSE DESCRIPTION CARD - SYLLABUS

Course name
Biometric Identity Authentication [S1Cybez1>BUT]

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
16

Number of credit points

4,00

Coordinators

dr inż. Sławomir Maćkowiak
slawomir.mackowiak@put.poznan.pl

Lecturers

Prerequisites

The student should have a basic understanding of mathematics and computer science, particularly in the areas of data processing and algorithms. Familiarity with Python programming and basic skills in analyzing multimedia data, such as images and audio, are recommended. Prior knowledge of digital security and data protection is also beneficial for a better understanding of biometric authentication challenges. Students should be able to work with analytical tools and demonstrate openness to applying modern technologies in practical laboratory tasks.

Course objective

The aim of the course is to familiarize students with modern biometric techniques used for identity verification and protection in the digital environment. The course provides both theoretical knowledge and practical skills in analyzing biometric data, such as images, audio, and user behavior. Students will learn methods for implementing authentication algorithms, techniques for protecting biometric data against forgery, and the applications of biometrics in various fields, ranging from transaction security to advanced identification systems. Upon completing the course, students will be able to design, test, and evaluate biometric systems in terms of their effectiveness and security.

Course-related learning outcomes

Knowledge:
• K1_W05 - Possesses advanced knowledge of complex data structures; understands the basics of theory, principles of data management, and related standards; understands cybersecurity and privacy principles used for managing risks related to the utilization, processing, storage, and transmission of information or data.
• K1_W12 - Has in-depth knowledge of authentication, authorization, and access control principles for computer systems; is aware of the necessity of implementing access control policies and adapting them to risk levels; understands biometric authentication principles.
• K1_W13 - Understands data hiding principles, such as cryptography and steganography; possesses advanced knowledge of cryptography, cryptographic algorithms, their limitations, and their role in cybersecurity.
• K1_W17 - Has in-depth knowledge of legal regulations, principles, and ethics concerning cybersecurity and privacy; is aware of the operational implications of cybersecurity breaches; possesses comprehensive knowledge of cybersecurity principles, privacy protection, and organizational requirements (relating to confidentiality, integrity, availability, authentication, and non-repudiation).
• K1_W16 - Has fundamental knowledge of machine learning systems and artificial neural networks; possesses structured knowledge of principles and methods for solving decision-making and optimization problems using heuristic and non-heuristic state-space search algorithms.

Skills:
• K1_U02 - Is able to apply appropriately selected methods and tools, including advanced information and communication techniques, and to develop simple applications or configure basic systems for conducting simulations, analyses, and designing systems or applications relevant to the field of study.
• K1_U03 - Can plan and conduct tests of software, computer systems, and networks to identify vulnerabilities to attacks; is able to propose solutions to improve operational security.
• K1_U09 - Can critically analyze and evaluate the performance of existing solutions used in software, data processing, and computer systems and networks using appropriately selected methods and tools.
• K1_U04 - Is capable of planning and performing computer simulations and measurements, including those related to the operation of telecommunication systems; can present the obtained results in numerical and graphical form, interpret them, and draw appropriate conclusions.
• K1_U07 - Is able to recognize both systemic and non-technical aspects, including ethical, economic, and legal considerations, when formulating and solving cybersecurity-related tasks.

Social competences:
• K1_K01 - Understands the importance of enhancing professional, personal, and social competencies; is aware that knowledge and skills in the field of cybersecurity evolve rapidly.
• K1_K02 - Recognizes the value of knowledge in solving cybersecurity problems; is aware of the necessity of utilizing expert knowledge when addressing engineering tasks that go beyond their own competencies.
• K1_K03 - Understands the need to formulate and communicate information and opinions to society regarding the positive and negative aspects of cybersecurity and is ready to act in the public interest.
• K1_K05 - Is aware of the significance of personal work and the need to adhere to professional ethics; is ready to comply with teamwork principles, take responsibility for jointly completed tasks, and care for the achievements and traditions of the profession.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

1. Lecture
Problem-solving task: Case studies requiring teamwork to analyze and resolve problems. Assessment of collaboration skills, setting priorities, and proposing effective solutions. Evaluation of critical thinking, problem-solving abilities, and team dynamics. Written or oral exam.
The passing threshold is 50% of the total points.
In the case of written and oral assessments, points are combined.
Grading scale:
• <50% - 2.0 (fail);
• 50% to 59% - 3.0 (pass);
• 60% to 69% - 3.5 (satisfactory+);
• 70% to 79% - 4.0 (good);
• 80% to 89% - 4.5 (good+);

• 90% to 100% - 5.0 (very good).
2. Laboratory
Skills acquired in the laboratory are assessed based on reports (documentation) of completed laboratory exercises (OL) and a final assessment (ZK), which takes the form of an independently executed exercise or project.
Social competencies (KS) are evaluated based on the ability to actively listen, collaborate, and effectively participate in team discussions, as well as the level of engagement in problem-solving processes.
A weighted average is calculated:
OK = 0.5 x OL + 0.3 x ZK + 0.2 x KS, and grades are assigned as follows:
• 5.0 for OK > 4.75;
• 4.5 for 4.75 > OK > 4.25;
• 4.0 for 4.25 > OK > 3.75;
• 3.5 for 3.75 > OK > 3.25;
• 3.0 for 3.25 > OK > 2.75;
• 2.0 for OK < 2.75.
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 course program covers both theoretical and practical aspects of applying biometrics in user identity verification. The classes discuss biometric methods based on physical features, such as face recognition, iris analysis, fingerprints, and voice, as well as techniques utilizing behavioral features, including typing rhythm analysis, mouse movement patterns, and other user behavior traits. Students learn the basics of image and audio processing, applying algorithms for data analysis, and methods related to machine learning. The course also addresses issues related to securing biometric systems against attacks, protecting data from manipulation, and techniques for encrypting and storing it. During practical sessions, students develop skills in implementing and testing biometric systems in terms of their effectiveness and security, as well as analyzing challenges associated with their use in real-world scenarios.

Course topics

The course begins with biometric techniques based on physical features, such as face and voice analysis. Students learn how face recognition technology, rooted in morphological patterns, is applied to identity verification. The course also covers voice biometrics, where features like tone, melody, and speech tempo, unique to each user, are analyzed. Algorithms for image and audio signal processing, as well as security aspects related to their implementation, are discussed. Students will learn how these systems can be secured against various attacks, such as fake faces and voice recordings.
The next module focuses on behavioral analysis, a modern approach to authentication based on unique user behavior patterns. Students will explore behavioral analysis techniques, such as typing rhythm, mouse movement habits, and text input patterns. The course explains how collected behavioral data can be processed and compared for user authentication, as well as how these methods can complement traditional biometric techniques to enhance security. Threats like impersonation and behavioral data interception attacks, along with strategies for securing such systems, will also be covered.
The course further introduces topics related to digital multimedia signatures, which provide an additional layer of security for transactions. Students will study techniques for digitally signing documents, videos, and audio to ensure data authenticity and integrity. Algorithms such as RSA and ECDSA and hashing techniques like SHA-256, essential in the authentication process, will be discussed.
To broaden their knowledge of biometrics, the course also includes other types of multimedia data used in biometric authentication. Students will learn methods for fingerprint recognition using images, iris analysis, and gait recognition technologies based on video recordings. Methods for storing and encrypting biometric data, as well as techniques for detecting and defending against spoofing-attempts to impersonate legitimate users using fake biometric patterns-will be presented.
Practical laboratory sessions:
• Secure authentication using voice and face biometrics
• Behavioral analysis as an authentication method
• Techniques for securing transactions with digital multimedia signatures
• Advanced biometric techniques using multimedia data

Teaching methods

• Active Learning Techniques: Strategies such as group discussions, problem-solving, and case studies to actively engage students in the learning process. Encouraging collaborative learning and interaction to foster critical thinking and the practical application of knowledge.
• Technology Integration: Utilizing technological tools and platforms to enhance learning quality. Leveraging online collaboration tools during brainstorming sessions, virtual simulations for problem-solving, and multimedia presentations to deliver engaging content. Additionally, using online discussion forums or learning management systems for asynchronous learning and resource sharing.
• Case-Based Learning: Incorporating real-world case studies into lectures and labs to demonstrate the practical application of creative thinking in solving technical problems. This approach encourages students to analyze and discuss cases, identify creative solutions, and reflect on decision-making processes.
• Feedback and Peer Teaching: Introducing mechanisms for student feedback, where learners provide constructive critiques of their peers' problem-solving approaches or project solutions. Encouraging peer-teaching sessions where students can share their knowledge and creative techniques with classmates.
• Project-Based Learning: Embedding project-based learning into the curriculum, where students tackle real-world problems or design challenges requiring creative thinking. This approach enables them to apply their skills, conduct in-depth research, and develop innovative solutions through hands-on, experiential learning.
• Online lectures

Bibliography

Basic:
• Anil K. Jain, Patrick Flynn, Arun A. Ross, Handbook of Biometrics, Springer, 2007.
• David D. Zhang, Automated Biometrics: Technologies and Systems, Kluwer Academic Publishers, 2000.
• James Wayman, Anil K. Jain, Davide Maltoni, Dario Maio, Biometric Systems: Technology, Design and Performance Evaluation, Springer, 2005.

Additional:
• Anil K. Jain, Ruud M. Bolle, Sharath Pankanti, Biometrics: Personal Identification in Networked Society, Springer, 1999.
• Julian Ashbourn, Practical Biometrics: From Aspiration to Implementation, Springer, 2004.
• John Chirillo, Scott Blaul, Implementing Biometric Security, Wiley, 2003.

Breakdown of average student's workload

	Hours	ECTS
Total workload	119	4,00
Classes requiring direct contact with the teacher	64	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	55	2,00