COURSE DESCRIPTION CARD - SYLLABUS

Course name
Authentication and authorization algorithms in wireless systems [S1MiKC1E>AUiAwSB]

Course

Field of study
Microelectronics and Digital Communication

Year/Semester
3/5

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
English

Form of study
full-time

Requirements
elective

Number of hours

Lecture
15

Laboratory classes
0

Other
0

Tutorials
0

Projects/seminars
15

Number of credit points

2,00

Coordinators

dr hab. inż. Piotr Remlein
piotr.remlein@put.poznan.pl

Lecturers

Prerequisites

The student starting this course should have basic knowledge of telecommunications systems. Additionally, the student should have basic knowledge of telecommunication networks, basic skills in configuring network devices, and an understanding of the communication process between network devices. The student should also have basic programming skills and the ability to gather information from specified sources.

Course objective

The aim of the course is to familiarize students with the basic methods of authentication and authorization of users, devices, and systems in various technological environments. The course covers both theoretical aspects of security and authentication, as well as practical applications in the context of contemporary security threats in various telecommunication systems, including mobile networks and other wireless systems.

Course-related learning outcomes

Knowledge:
The student knows basic concepts and definitions related to authentication and authorization. They

understand the difference between identification, authentication, and authorization. They can explain the role of authentication in security systems.
The student is familiar with various authentication methods. They can characterize static, biometric, token-based, and multi-factor authentication methods. They understand authentication mechanisms based on protocols, such as OAuth, Kerberos, SAML, and 802.1X.
The student knows the threats associated with authentication systems. They understand attacks such as brute force, phishing, and credential stuffing, and are aware of countermeasures to prevent them. They recognize the importance of protecting authentication data through encryption and other security measures.
The student understands the applications of authentication systems in different environments and systems. They grasp the specifics of authentication in wired and wireless systems, mobile applications, cloud environments, sensor networks, and IoT.

Skills:
The student is able to select appropriate authentication methods for specific applications. They analyze security requirements and the application environment to design an appropriate authentication system.
The student knows how to design and configure systems using authentication methods.
They can solve practical problems related to authentication. The student is capable of simulating attacks on authentication systems and evaluating their resilience. They can prepare a report assessing the effectiveness of the implemented authentication mechanisms and key management.

Social competences:
The student understands the responsibility of designing secure authentication systems. They recognize the importance of protecting personal data and confidentiality in the context of authentication. The student makes decisions that take into account the security of end users. They can work effectively in a project team and communicate the results of analyses and proposed improvements regarding authentication. The student strives for continuous expansion of knowledge in the field of information system security, keeping up with current threats and new authentication methods in a dynamically changing technological environment.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

The knowledge acquired during the lecture is assessed through a written exam, typically consisting of several open-ended questions (usually five) selected from a provided list of topics, with varying point values. The passing threshold is set at 51% of the total points.
The project is also assessed based on achieving at least 50% of the possible points.
Grading scale: <50% - 2.0 (fail); 50% to 59% - 3.0 (satisfactory); 60% to 69% - 3.5 (fairly good); 70% to 79% - 4.0 (good); 80% to 89% - 4.5 (very good); 90% to 100% - 5.0 (excellent).

Programme content

The course covers topics related to user identification, authentication, and authorization, access control, and data protection in information systems and both wired and wireless networks. Various authentication methods are discussed, including the use of passwords, tokens, biometrics, and multi-factor authentication (MFA) mechanisms. The course also addresses key protocols such as 802.1X, Kerberos, OAuth 2.0, and OpenID Connect, as well as their application in ensuring security.
In the area of key management, students learn about the processes of generating, storing, distributing, and rotating cryptographic keys, with particular emphasis on Public Key Infrastructure (PKI). An important part of the course is the analysis of communication security, including the authentication methods used in practical systems, such as GSM, UMTS, LTE, 5G, sensor networks, and IoT. Authentication in the TETRA system is also discussed.
Additionally, the course covers threats such as brute-force attacks, man-in-the-middle attacks, and phishing, as well as methods for detecting and preventing them. The course also explores the application of authentication systems in IoT environments, wireless networks (WPA2, WPA3), the cloud, and web solutions, considering the latest trends such as passwordless authentication and quantum cryptography.
As part of the project, students carry out tasks using selected software to implement specific authentication algorithms. They evaluate and analyze the results and may use selected simulation programs such as Tamari or Scyther.

Course topics

Lecture:
1. (1h) Introduction to security in wireless systems.
2. (2h) Introduction to authentication and key management in networks.
Basic concepts: identification, authentication, authorization.
The role of key management in protecting data transmitted in networks.
The role of centralization of authentication in large IT systems.
Connection of authentication processes with key management systems (KMS).
3. (2h) Authentication methods in wired networks and web applications.
Mechanisms 802.1X and EAP (Extensible Authentication Protocol).
The role of RADIUS server in user authentication.
4. (2h) Authentication in wireless networks.
Authentication mechanisms in WLAN standards (WPA2, WPA3).
Authentication at the level of cellular networks (GSM, UMTS, LTE, 5G).
Authentication in TETRA system.
Lightweight authentication algorithms for sensor networks and IoT.
5. (2h) Authentication protocols in corporate and public networks.
Kerberos: principles of operation and application.
Key management in wired, wireless, cloud, and IoT environments:
Examples of solutions (e.g., AWS KMS, Google Cloud KMS).
Challenges in key management in decentralized environments.
Methods of generating, distributing, and storing keys. Key rotation and data leak protection.
6. (2h) Public Key Infrastructure (PKI).
Digital certificates and the chain of trust.
Processes related to PKI: registration, revocation, and renewal of certificates.
PKI components: digital certificates, the chain of trust, Certification Authorities (CA).
Processes in PKI: issuance, renewal, and revocation of certificates.
Role of PKI in authentication systems, e.g., TLS/SSL, principles of these protocols.
7. (2h) Attacks on authentication systems and countermeasures.
Protection against attacks such as jamming, eavesdropping, or spoofing.
Typical threats: brute force, man-in-the-middle, replay attack.
Defense mechanisms, e.g., account timeouts, behavioral analysis.
8. (2h) Modern approaches to authentication and key management.
The development of passwordless authentication systems.
Potential use of quantum cryptography in key management.
Project: As part of the project, students should design and implement selected authentication algorithms that use key management mechanisms. They must analyze their functionality and complexity. They should assess the system's resilience to attacks by simulating in a selected test environment, such as Scyther.
Expected project results: documentation containing: project assumptions and adopted technical solutions, system architecture diagrams, risk analysis and security proposals, implementation description, tests, authentication test scenarios, and a report on the effectiveness of the system in terms of security.

Teaching methods

1. Lecture: Multimedia presentation illustrated with examples.
2. Project: Performing tasks assigned by the instructor - practical exercises, teamwork, using software and simulation environments.

Bibliography

Basic:
1. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 2020.
2. Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security Essentials: Applications and Standards, Pearson, 2020.
3. RFC 5246 - The Transport Layer Security (TLS) Protocol.
4. Literature from recognized scientific journals, standardization documents, and manufacturers' websites, provided by the instructor on the e-learning platform.

Additional:
1. Jonathan Katz, Yehuda Lindell, Introduction to Modern Cryptography, CRC Press, 2020.
2. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, Cengage Learning, 2021.
3. RFC 4120 - The Kerberos Network Authentication Service (V5), 2005.
4. Roger Grimes, Hacking Multifactor Authentication, Wiley, 2020.

Breakdown of average student's workload

	Hours	ECTS
Total workload	57	2,00
Classes requiring direct contact with the teacher	32	1,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	25	1,00