Module name:	Number of hours:	Lecturer:
Digital Forensics	10	Michał Weissenberg, PhD

Module Descriptions:

The module introduces students to the foundations and advanced concepts of Identity and Access Management (IAM), covering identity lifecycle management, authentication and authorization methods, federated identity, and accounting mechanisms. Students learn about modern authentication techniques, including passwordless solutions, biometric verification, and identity proofing. The module covers key standards used in contemporary IAM systems such as OAuth, OpenID Connect, and SAML, as well as governance, compliance, privileged access management (PAM), and identity challenges in cloud and hybrid environments. The course provides both theoretical knowledge and practical understanding of IAM technologies that are foundational to cybersecurity in modern, interconnected digital ecosystems.

Purpose of the support under Module:

The overall objective of the Innovative International Education Program in Cybersecurity within the IMPACT project is to raise the competencies of international students in key digital technologies and to support personalized, flexible, and modern education aligned with current global needs in the area of cybersecurity.

The specific purpose of this module is to equip students with competencies in identity and access management, including:

- understanding authentication, authorization, and accounting mechanisms;
- learning identity lifecycle management processes and governance models;
- applying IAM standards in modern systems (OAuth, OIDC, SAML);
- implementing and evaluating federated identity and Single Sign-On (SSO) solutions;
- understanding IAM challenges in cloud, hybrid, and distributed environments;
- recognizing the importance of PAM, auditability, and compliance in secure operations;
- developing awareness of privacy, legal, and ethical considerations in identity systems.

Method of support under Module:

Support within the module is provided with the participation of the instructor and divided into the following elements:

- 6-week self-study program using teaching materials provided by the instructor on the e-learning platform;

POZNAN UNIVERSITY OF TECHNOLOGY

- 6 weeks of support from the instructor in the form of online consultations using tools that enable meetings to be held;
- a test to verify the acquisition of competences.

Module-related learning outcomes:

Descriptions of the new competences:

Participants gain new competencies in identity and access management, including the ability to understand and compare authentication methods, implement authorization models, work with IAM standards, evaluate identity lifecycle processes, and recognize IAM risks and governance requirements in cloud and hybrid environments. Students also develop awareness of ethical, legal, and compliance implications related to identity management.

Knowledge:

1. Student has structured and theoretically grounded knowledge of identity management fundamentals, authentication mechanisms (passwords, MFA, biometrics), authorization models (RBAC, ABAC), and accounting/audit processes.
2. Student understands modern IAM standards and technologies, including federated identity, SSO, OAuth, OpenID Connect, SAML, API security, and identity verification techniques.
3. Student knows current trends and challenges in IAM, including passwordless authentication, PAM, cloud and hybrid IAM strategies, compliance requirements, and identity governance frameworks.

Skills:

1. Student can assess and apply authentication and authorization methods appropriately to different security contexts, understanding their advantages and limitations.
2. Student is able to evaluate and implement IAM standards (OAuth, OIDC, SAML) and configure federated identity and SSO mechanisms.
3. Student can analyse IAM risks, interpret audit logs, assess identity governance processes, and propose solutions to strengthen access control and identity assurance.
4. Student is able to independently continue learning in the field of IAM and support others in acquiring new competencies in identity management and governance.

Social competences:

1. Student understands the rapidly evolving nature of IAM technologies and practices, recognizing the need for continuous learning and professional development.
2. Student demonstrates responsible and ethical behaviour when working with identity data, user credentials, and audit information, and adheres to legal, compliance, and governance standards.

Criteria for verifying learning outcomes

earning outcomes are verified through an online single-choice test assessing the student's knowledge of identity management principles, authentication and authorization methods,

POZNAN UNIVERSITY OF TECHNOLOGY

IAM standards, federated identity, governance processes, and cloud IAM challenges. The test evaluates both theoretical understanding and the ability to interpret and apply IAM concepts. A minimum of 51% of correct answers is required to pass.

Method of verification/validation of learning outcomes

Verification is carried out using an online single-choice test delivered on the dedicated e-learning platform. The test is conducted individually, without access to supporting materials, and evaluates the extent to which the student has achieved the intended knowledge, skills, and social competences. The results are automatically recorded and validated according to predefined assessment criteria.

Workload

 25 h (including work with teaching materials provided by the lecturer, consultation, and the student's own work) – 1 ECTS point

Level of the European Qualifications Framework