(pieczęć wydziału)

**SUBJECT INFORMATION**

| | | |
|---|---|---|
| **1. Subject name: COMPUTER SYSTEMS SECURITY** | **2. Subject code: CSS** | |
| **3. Subject information available since academic year:** 2012 | | |
| **4. Form of education:** second level study | | |
| **5. Form of study**: full-time studies | | |
| **6. Field of study**: COMPUTER SCIENCE; INSTITUTE AEII | | |
| **7. Profile of study:** academic | | |
| **8. Specialty:** | | |
| **9. Semester: 9** | | |
| **10. Object providing unit:** Institute of Computer Science, RAu2 | | |
| **11. Subject leader**: Jacek Lach, PhD | | |
| **12. Belonging to a group of subjects:** common subjects | | |
| **13. Subject status:** mandatory | | |
| **14. Subject language:** English | | |
| **15. Intorductory courses and prerequisities:** Computer programming, Operating Systems, Computer Networks.. | | |
| **16. Subject goal:** Information being processed in computer systems became invaluable. To protect this information we have to use qualified tools and algorithms. Most of the mechanisms that are widely used today are secure. Most problems with security today stems from improper usage of strong security. The aim of the course is not only to present common security solutions but also to demonstrate some background knowledge which would help using proper tools for proper tasks and allow for building secure solutions. | | |

**17. Education effects:**

| Nr | Description of the effect of education | The method of checking education effect | Teaching form | The reference to the effects |
|---|---|---|---|---|
| W1 | Knowledge of the essential elements of computer systems security | | | K_W15 |
| W2 | Knowledge of new aspects of information protection | | | K_W16 |
| U1 | Ability to use and understand existing security specification | | | K_U03 |
| U2 | Ability to use standard tools for evaluation of system security | | | K_U01 |
| U3 | Ability to use cryptographic operations in implemented software | | | K_U14, K_U18 |

**18. Education forms a number of hours**
**Lectures : 15 Laboratory: 15**

**19. The content of education:**

**Lectures**

Introduction to computer security. History, terms, basic components, threats, trust. Overview of security areas: computer networks, operating systems, transactional systems, telecommunication, e-voting, e-documents.

Implementing security: cryptography I. Definition of cryptography. Classial cryposystems: transposition and substitution. Symmetric cryptosystems. Public key cryptosystems. Key management: key generation, key exchange, key storage, key revocation. Key infrastructures: X.509, PGP.

Implementing security: cryptography II. Stream and block ciphers. Algorithms: DES, AES, RSA. Block cipher modes of operation.Randomness in computer system, how random is random(). Pseudo Random Number Generators. Stream ciphers. Hash functions. Digital signatures. Weakening strong ciphers – common problems. Strenghtening weak solutions – common solutions.

Security of data: storage systems. Encrypted filesystems, encrypted directories, encrypted containers. Whole-Disk encryption. Problems with disk encryption. Secure deletion of data.

Operating system security: access control, Bell-LaPadula model, security policies, capabilities, access control lists. Authentication: something you know, something you have, something you are: passwords, tokens and biometrics. One time passwords. Dictionary attacks. System security evaluation – Common Criteria.

Network security: secure comunication, secure services. Security at different levels: application layer – mail security, spam, transport layer: SSL, network layer: IPSec.

Modern aspects of security: biocryptography, steganography, digital watermarking, visual cryptography.

**Laboratory**

The laboratory consists of three practical aspects of computer security. Each excersise should be finalized within 4 hours.

1. Security evaluation. Penetration tests.
2. Data encryption.
3. Steganography.

**20. Exam:** no

**21. Basic literature:**

M. Bishop: Computer security. Art and science. Addison-Wesley. 2003

J. Pieprzyk, T. Hardjono, J. Seberry: Fundamentals of Computer Security, Springer-Verlag, 2003

A. J. Menezes, P. C. Van Oorschot, S.A. Vanstone: Handbook of applied cryptography, CRC Press, 1997

**22. Literatura uzupełniająca:**

Bruce Schneier. Applied Cryptography, John Wiley & Sons, 1996

**23. Student workload required to achieve the effects of education**

| Lp. | Type of course | Number of contact hours / students workload |
|---|---|---|
| 1 | Lecture | 15/15 |
| 2 | Exercise | 0/0 |
| 3 | Laboratory | 15/15 |
| 4 | Project | 0/0 |
| 5 | Seminar | 0/0 |
| 6 | Other | 0/0 |
| | Total hours | 30/30 |

**24. The sum of all hours: 60**

**25. ECTS:[1] points 2**

**26. Number of ECTS credits gained in the classroom with the direct participation of an academic teacher: 2**

**27. Number of ECTS credits gained in the class of practical (laboratories, projects): 2**

**26. Comments:**

Approval:

…… ……

*(date and signature of leading)* *(data and signature of the director of the institute / head of the department / Director of the College of Foreign Languages / manager or inter-unit director)*

[1] 1 punkt ECTS – 25-30 godzin.