Security engineering - opis przedmiotu

Informacje ogólne

Nazwa przedmiotu	Security engineering
Kod przedmiotu	11.9-WE-INFD-SecEng-Er
Wydział	Wydział Informatyki, Elektrotechniki i Automatyki
Kierunek	Informatyka
Profil	ogólnoakademicki
Rodzaj studiów	Program Erasmus
Semestr rozpoczęcia	semestr zimowy 2017/2018

Informacje o przedmiocie

Semestr	1
Liczba punktów ECTS do zdobycia	5
Typ przedmiotu	obowiązkowy
Język nauczania	angielski
Sylabus opracował	• dr hab. inż. Bartłomiej Sulikowski, prof. UZ

Formy zajęć

Forma zajęć	Liczba godzin w semestrze (stacjonarne)	Liczba godzin w tygodniu (stacjonarne)	Liczba godzin w semestrze (niestacjonarne)	Liczba godzin w tygodniu (niestacjonarne)	Forma zaliczenia
Wykład	30	2	-	-	Zaliczenie na ocenę
Laboratorium	30	2	-	-	Zaliczenie na ocenę

Cel przedmiotu

- familiarizing the student with cryptographic algorithms and protocols
- development of skills in the use of information security procedures
- familiarizing the student and shaping the skills of defining and applying security policy in company

Wymagania wstępne

Computer networks

Zakres tematyczny

Information Safety. Definitions. Infrastructure. Security models.
Access to the system. System access control. User access management. Range of the user responsibility. Risk estimation and management.
Security of teleinformatic systems and networks. Types of attacks. Firewalls (IDS and IPS). Physical security. Alarm systems. Protection against electro-magnetic eavesdropping - TEMPEST standard.
Security policies. The role and tasks of the security administrator.
Industrial safety.
Cryptography. Symmetric algorithms (DES, 3DES, AES, Twofish, RCx family, Serpent, Mars) and asymmetric (RSA, DH, ElGamal, EC). Cryptographic protocols. Public key cryptography. Hashing functions. Electronic signature and its verification. Certification of devices and users. PKI architecture. Other services using cryptography.

Metody kształcenia

lecture: conventional lecture, discussion

laboratory: laboratory exercises

Efekty uczenia się i metody weryfikacji osiągania efektów uczenia się

Opis efektu	Symbole efektów	Metody weryfikacji	Forma zajęć
Student knows the structure of the protection division in the organizational unit (enterprise), understands the tasks of employees of the protection division		• sprawdzian	• Wykład
knows the rules for protection of classified information, in particular physical protection and electromagnetic		• sprawdzian	• Wykład
understands the problems related to industrial security		• sprawdzian	• Wykład • Laboratorium

Opis efektu	Symboleefektów	Metody weryfikacji	Forma zajęć
knows the characteristics of cryptographic algorithms and protocols and hashing functions		• obserwacja i ocena aktywności na zajęciach • sprawdzian	• Wykład • Laboratorium
is capable of choosing cryptosystem parameters in order to mantain prescribed functions in data protection		• dyskusja • obserwacja i ocena aktywności na zajęciach • sprawdzian	• Wykład • Laboratorium
has knowledge of applications and threats of electronic signature		• obserwacja i ocena aktywności na zajęciach • sprawdzian	• Laboratorium

Warunki zaliczenia

Lecture - the condition for passing is to obtain positive grades from the knowledge tests in the written form, carried out at least once per semester
Laboratory - the condition to pass is the realization of at least 80% of the planned exercises
Components of the final grade = lecture: 50% + laboratory: 50%

Literatura podstawowa

1. W. Stallings, Cryptography and Network Security Principles and Practices, Prentice Hall, 2018
2. S. McClure et al., Hacking Exposed: Network Security Secrets and Solutions, 2012
3. B. Halton et al., Kali Linux 2: Windows Penetration Testing, Packt, 2016

Literatura uzupełniająca

1. Dudek A.: Jak pisać wirusy, Jelenia Góra 1993.
2. Kutyłowski M., Strothmann W.B.: Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych, Oficyna Wydawnicza Read ME, Warszawa, 1998.
3. Russell R. i in. : Hakerzy atakują. Jak przejąć kontrolę nad siecią, Helion, 2004.
4. Potter B., Fleck B.: 802.11. Bezpieczeństwo, Wyd. O'Reilly, 2005.
5. Balinsky A. i in.: Bezpieczeństwo sieci bezprzewodowych, PWN, CISCO Press, 2007.
6. Mochnacki W.: Kody korekcyjne i kryptografia. Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 1997.
7. Schneider B.: Kryptografia dla praktyków — protokoły, algorytmy i programy zródłowe w języku C. Wydawnictwa Naukowo-Techniczne, Warszawa 1995.

Uwagi

Zmodyfikowane przez dr hab. inż. Bartłomiej Sulikowski, prof. UZ (ostatnia modyfikacja: 04-04-2018 09:56)

Wygenerowano automatycznie z systemu SylabUZ