KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo w sieciach bezprzewodowych [S2EiT1-TMiB>BwSB]

Przedmiot

Kierunek studiów
Elektronika i telekomunikacja

Rok/Semestr
2/3

Studia w zakresie (specjalność)
Technologie mobilne i bezprzewodowe

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
30

Laboratorium
0

Inne (np. online)
0

Ćwiczenia
0

Projekty/seminaria
15

Liczba punktów ECTS

4,00

Koordynatorzy

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

Wykładowcy

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z zakresu sieci komputerowych, systemów operacyjnych, systemów łączności bezprzewodowej, języków programowania oraz matematyki. Powinien również posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł oraz mieć gotowość do podjęcia współpracy w ramach zespołu.

Cel przedmiotu

Celem przedmiotu jest przekazanie studentom wiedzy i umiętności z zakresu ochrony danych i kryptografii. Zaprezentowanie zagadnień bezpieczeństwa i ochrony danych w systemach łączności bezprzewodowej obecnych na rynku lub będących w fazie standaryzacji.

Przedmiotowe efekty uczenia się

Wiedza:
Student ma praktyczną wiedzę na temat systemów bezpieczeństwa lub metod umożliwiających zapewnienie bezpieczeństwa informacji przesyłanych w sieciach komputerowych i radiokomunikacji. Ma podstawową wiedzę o trendach rozwojowych w zakresie bezpieczeństwa w systemach bezprzewodowych.

Umiejętności:
Student potrafi zaprojektować wybrane elementy systemów bezpieczeństwa lub potrafi zabezpieczać urządzenia sieciowe przed nieautoryzowanym dostępem i innymi zagrożeniami. Orientuje się w zasadach działalności w zakresie normalizacji rozwiązań technicznych związanych z bezpieczeństwem systemów telekomunikacyjnych, zna międzynarodowe i krajowe organizacje standaryzacyjne (ITU, ISO, ETSI, 3GPP, itp.). Potrafi pozyskiwać informacje z literatury i baz danych oraz innych źródeł w języku polskim lub angielskim; potrafi integrować uzyskane informacje, dokonywać ich interpretacji, wyciągać wnioski i uzasadniać opinie.

Kompetencje społeczne:
Student rozumie konieczność poznawania pojawiających się nowych rozwiązań z zakresu bezpieczeństwa systemów radiokomunikacyjnych. Rozumie, że rozmieszczanie coraz nowszych sieci i systemów radiokomunikacyjnych wymaga współpracy różnorodnych zespołów inżynierów. Rozumie wyzwania stojące przed radiokomunikacją spowodowane rosnącym zapotrzebowaniem na ich bezpieczeństwo.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza nabyta w ramach wykładu jest weryfikowana poprzez egzamin ustny. Egzamin składa się z odpowiedzi na przynajmniej 3 pytania. Pytania są zadawane przez prowadzącego. Pytania dotyczą zagadnień ze zbioru kilkudziesięciu zagadnień znanych studentom (przekazanych na wykładzie oraz drogą elektroniczną - mailową. Każda odpowiedź na zadane pytanie oceniana jest w skali od 2 do 5. Ocena końcowa z egzaminu ustnego stanowi średnią z ocen za poszczególne odpowiedzi. Egzamin jest zdany, gdy średnia ocena jest wyższa niż 2,75.
Umiejętności nabyte w ramach zajęć projektowych weryfikowane są podstawie ocen uzyskanych z przygotowywanych przez studenta raportów do zadań, które otrzymuje do realizacji w trakcie zajęć. Jest ich około pięciu, siedmiu w czasie semestru. Ocena końcwa uwzględnia zarówno zaangażowanie i postawę studenta w czasie zajęć jak i oceny ze wspomnianych raportów. Przygotowanie weryfikowane jest ustną odpowiedzią na każdych zajęciach Warunkiem koniecznym do zaliczenia jest uzyskanie pozytywnych ocen dla większości z realizowanych zagadnień.

Treści programowe

Zasady polityki bezpieczeństwa. Podstawowe pojęcia kryptografii, przykłady klasycznych systemów kryptograficznych. Metody łamania szyfrów, analiza statystyczna, liniowa, różnicowa kryptogramu. Przykłady innych systemów kryptograficznych DES, AES. Szyfry z kluczem publicznym. Szyfr plecakowy. Szyfr RSA. Zagadnienie bezpieczeństwa szyfru RSA. Szyfry Diffiego-Hellmana, El Gamala i Masseya - Omury. Funkcje skrótu MD5, SHA. Systemy detekcji intruzów.
Sposoby ochrony danych stosowane w systemach łączności bezprzewodowej: DECT, GSM, UMTS, LTE, 5G, IoT, TETRA, sieciach WLAN-802.11, WiMAX, Bluetooth, ZigBee.
W ramach projektu studenci realizują zadania w oparciu o oprogramowanie dydaktyczne Cryptool, piszą programy w C/C++ realizujące podstawowe algorytmu szyfrujące i deszyfrujące, rozwiązują problemy bezpieczeństwa sieci bezprzewodowych 802.11 wykorzystując urządzenia będące w laboratorium sieci bezprzewodowych.

Metody dydaktyczne

1. Wykład: prezentacja multimedialna przygotowana przez prowadzącego zajęcia, ilustrowana przykładami podawanymi na tablicy. Wykład prowadzony przeważnie w sposób tradycyjny, ale także częściowo w postaci wykładu konwersatoryjnego i/lub problemowego
2. Projekt: wykonanie zadań podanych przez prowadzącego i opisanych w postaci zadań problemowych, ćwiczenia praktyczne z wykorzystaniem dostępnego w laboratorium sprzętu. Projekt może być uzupełniony poprzez prezentacje multimedialne lub przykłady podawane na tablicy.

Literatura

Podstawowa
1. Ocena bezpieczeństwa sieciowego / Kevin Lam, David LeBlanc, Ben Smith ; [przekł. Marek Włodarz] ; Microsoft.,Warszawa : APN PROMISE, 2005.

2. Kryptografia i bezpieczeństwo sieci komputerowych : matematyka szyfrów i techniki kryptologii / William Stallings ; [tł. Andrzej Grażyński].,Gliwice : Helion, cop. 2012.
3. Systemy radiokomunikacji ruchomej, Krzysztof Wesołowski, WKiŁ, Warszawa, 2003.
4. Ochrona danych w sieci i intersieci – w teorii i praktyce, W. Stallings, WNT, Warszawa, 1997.
Kali Linux : audyt bezpieczeństwa sieci Wi-Fi dla każdego / Vivek Ramachandran, Cameron Buchanan ; [tłumaczenie: Grzegorz Kowalczyk]. Gliwice : Helion, cop. 2016.
Uzupełniająca
1. Wybrane fragmenty standardów systemów bezprzewodowych dostępnych w bibliotece cyfrowej IEEE.
2. Dowolny podręcznik dotyczący sieci Wi Fi (802.11) dostępny w j. polskim lub angielskim.
3. Dowolny podręcznik dotyczący standardów Bluetooth, Z-Wave, ZigBee, LoRA, TETRA.
4. Cryptography in C and C++, M. Welschenbach, APress, 2001.
5. UMTS system telefonii komórkowej trzeciej generacji, J. Kołakowski, J. Cichocki, WKiŁ, Warszawa, 2003.

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	100	4,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	55	2,00
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	45	2,00