KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo w sieciach bezprzewodowych [S2EiT1E-TIT>BwSB]

Przedmiot

Kierunek studiów
Elektronika i telekomunikacja/Electronics and Telecommunications

Rok/Semestr
2/3

Studia w zakresie (specjalność)
Technologie informacyjno-telekomunikacyjne

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład
15

Laboratorium
30

Inne
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

4,00

Koordynatorzy

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

Wykładowcy

Wymagania wstępne

brak

Cel przedmiotu

brak

Przedmiotowe efekty uczenia się

Wiedza:
-

Umiejętności:
-

Kompetencje społeczne:
-

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

brak

Treści programowe

Praktyczne wykorzystanie zasad polityki bezpieczeństwa. Użycie zasad klasycznej kryptografii w praktycznych zastosowaniach do uwierzytelnienia, realizacji poufności i integralności danych w bezprzewodowych systemach teleinformatycznych.
Wykorzystanie systemów detekcji intruzów, analizy statystycznej, liniowej, różnicowej.
Sposoby ochrony danych stosowane w systemach łączności bezprzewodowej: w sieciach WLAN-802.11, w systemach komórkowych (GSM,UMTS, LTE, 5G) w systemie TETRA, WiMAX, Bluetooth,
ZigBee, w rozwiązaniach IoT.
W ramach laboratorium studenci realizują zadania w oparciu o oprogramowanie dydaktyczne Cryptool, wykorzystują system Kali Linux i jego narzędzia.
Mogą stosować oprogramowanie Tamarin soft, piszą programy w C/C++ realizujące algorytmy zapewniające poufność, integralność
danych, lub mechanizmy uwierzytelnienia.

Tematyka zajęć

Mechanizmy detekcji intruzów i analiza zabezpieczeń.
Bezpieczeństwo w sieciach WLAN (802.11).
WEP, WPA, WPA2, WPA3 – mechanizmy zabezpieczeń i ich ewolucja.
Ataki na sieci WLAN: podsłuchiwanie, Evil Twin, ataki brute force.
Ochrona danych w sieciach korporacyjnych i domowych.
Bezpieczeństwo w systemach komórkowych (GSM, UMTS, LTE, 5G).
Mechanizmy szyfrowania i uwierzytelniania: A5/1, KASUMI, 5G-AKA.
Ochrona danych użytkownika i transmisji.
Zagrożenia i ataki: IMSI catchery, ataki na sygnalizację SS7.
TETRA: algorytmy TEA, uwierzytelnianie użytkowników.
WiMAX: mechanizmy szyfrowania i autoryzacji (PKMv2).
Bluetooth: zabezpieczenia w wersjach Bluetooth LE i Classic.
ZigBee: szyfrowanie na poziomie warstwy aplikacji (AES-128).
Bezpieczeństwo w rozwiązaniach IoT
Realizacja poufności i integralności danych w praktyce.
Implementacja VPN w sieciach bezprzewodowych.
Uwierzytelnianie dwuskładnikowe i certyfikaty cyfrowe.
Konfiguracja i zabezpieczenie sieci WLAN (WPA3).
Analiza protokołów zabezpieczeń WEP, WPA, WPA2, analiza ruchu sieciowego.
Wykrywanie ataków i analiza ruchu za pomocą narzędzi IDS.

Metody dydaktyczne

brak

Literatura

Podstawowa:
-

Uzupełniająca:
-

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