KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Bezpieczeństwo Systemów IoT

Przedmiot

Kierunek studiów
Informatyka

Rok/semestr
1/2

Studia w zakresie (specjalność)
Cyberbezpieczeństwo

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład	Laboratoria	Inne (np. online)
30	30	
Ćwiczenia	Projekty/seminaria	
	15	

Liczba punktów ECTS

6

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:
dr hab. inż. Paweł Śniatała
email: pawel.sniatala@put.poznan.pl
tel: 61 665 23 99
Wydział Informatyki i Telekomunikacji
Instytut Informatyki

Odpowiedzialny za przedmiot/wykładowca:
prof. dr hab. inż. Mariusz Głąbowski
email: mariusz.glabowski@put.poznan.pl
tel: 61 665 3904
Wydział Informatyki i Telekomunikacji
Instytut Sieci Teleinformatycznych

Wymagania wstępne

Student rozpoczynający ten przedmiot powinien posiadać podstawową wiedzę z zakresu elektroniki cyfrowej, mikrokontrolerów i mikroprocesorów. Powinien posiadać wiedzę pozwalającą mu na projektowanie i implementację programów komputerowych w wybranych językach programowania (np. C, Python). Powinien również posiadać umiejętność pozyskiwania informacji ze wskazanych źródeł oraz być gotowy do współpracy w zespole. W obszarze kompetencji społecznych musi prezentować postawy takie jak: uczciwość, odpowiedzialność, wytrwałość, ciekawość poznawcza, kreatywność, kultura osobista, szacunek dla innych ludzi.

Cel przedmiotu

Przekazanie studentom wiedzy z zakresu szeroko rozumianego bezpieczeństwa IoT oraz metod i narzędzi służących do szacowania i kontroli ryzyka naruszenia poufności, integralności i dostępności danych.

Kluczowe koncepcje bezpieczeństwa: poufność, uwierzytelnienie, integralność, kontrola dostępu, niezaprzeczalność i dostępność oraz najnowocześniejsze rozwiązania w zakresie bezpieczeństwa będą wzmacniane i badane.

Zapoznanie studentów z zaawansowanymi metodami, technikami i narzędziami stosowanymi w rozwiązywaniu złożonych zadań inżynierskich w zakresie projektowania i utrzymania systemów i urządzeń IoT z naciskiem na bezpieczeństwo systemów i danych.

Przedmiotowe efekty uczenia się

Wiedza

Student jest w stanie zrozumieć lub opanować bezpieczeństwo IoT związane ze sprzętem, systemem i siecią.

Student ma uporządkowaną i teoretycznie uzasadnioną wiedzę ogólną związaną z kluczowymi zagadnieniami w dziedzinie bezpieczeństwa IoT. Omówiony zostanie zarówno poziom urządzenia jak i systemu.

Student posiada zaawansowaną, szczegółową wiedzę z zakresu integracji wybranych czujników z platformami sprzętowymi (Raspberry Pi, Arduino) oraz posiada wiedzę na temat luk bezpieczeństwa związanych z analizowanymi systemami.

Student posiada wiedzę na temat trendów rozwojowych i najważniejszych nowych osiągnięć informatyki i telekomunikacji w zakresie bezpieczeństwa IoT.

Umiejętności

Student może uzyskać informacje na temat doboru sensorów do realizacji założonych funkcji systemów IoT oraz urządzeń IoT z punktu widzenia bezpieczeństwa. Uzyskane informacje, student potrafi zintegrować, a następnie poddać krytycznej ocenie.

Student potrafi zaplanować i przeprowadzić badania w zakresie pomiaru i testowania bezpieczeństwa urządzeń i systemów IoT, zinterpretować uzyskane wyniki i wyciągnąć wnioski.

Student potrafi zaimplementować lekkie algorytmy kryptograficzne na platfromach IoT.

Student potrafi wykorzystywać metody eksperymentalne do formułowania i rozwiązywania zadań inżynierskich oraz prostych problemów badawczych w obszarze bezpieczeństwa IoT.

Student potrafi integrować wiedzę z różnych dziedzin informatyki i telekomunikacji przy formułowaniu i rozwiązywaniu zadań inżynierskich związanych z projektowaniem i implementacją systemów IoT z uwzględnieniem wymagań bezpieczeństwa.

Student potrafi ocenić przydatność wykorzystania nowych rozwiązań sprzętowych i programowych do rozwiązywania zadań inżynierskich, polegających na budowie wydajnych, bezpiecznych systemów IoT.

Kompetencje społeczne

Student rozumie, że systemy IoT integrują wiele technologii, a wiedza i umiejętności z zakresu bezpieczeństwa IoT bardzo szybko się dezaktualizują.

Student rozumie znaczenie wykorzystania najnowszej wiedzy z zakresu IoT w rozwiązywaniu problemów badawczych i praktycznych.

Student ma świadomość konieczności profesjonalnego podejścia do rozwiązywania problemów z zakresu IoT i ponoszenia odpowiedzialności za proponowane przez siebie projekty.

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Wiedza zdobyta podczas wykładu jest weryfikowana poprzez test ustny i/lub pisemny.

Zagadnienia testowe, na podstawie których opracowywane są pytania, przesyłane są do studentów drogą elektroniczną za pomocą uczelnianego systemu poczty elektronicznej.

Egzamin ustny i/lub pisemny składa się z 3 do 5 pytań, na które oczekuje się odpowiedzi opisowej. Każda odpowiedź na pytanie jest oceniana w skali od 0 do 5 punktów. Każde pytanie jest jednakowo punktowane. Próg zaliczenia: 50% punktów.

W przypadku egzaminu ustnego studenci losują pytania z zestawu 30 pytań. W przypadku sprawdzianu pisemnego pytania zadaje wykładowca.

Umiejętności nabyte podczas zajęć laboratoryjnych są weryfikowane na bieżąco. Na każdych zajęciach laboratoryjnych poprawność wykonania ćwiczeń oceniana jest w skali od 2 do 5. Ocena końcowa jest średnią ocen uzyskanych z poszczególnych zajęć laboratoryjnych. Ocena końcowa jest średnią ocen uzyskanych z poszczególnych zajęć laboratoryjnych.

Treści programowe

Tematyka wykładów:

- Internet Rzeczy (IoT) - aplikacje, systemy, urządzenia, sensory.

- Zasady bezpieczeństwa IoT.

- Studia przypadków cyberataków na systemy IoT.

- Przegląd wybranych platform sprzętowych IoT i środowiska programistycznego (Raspberry Pi, Tizen) .

- Łączność / komunikacja urządzeń IoT (lekkie protokoły komunikacyjne IoT).

- Lekkie algorytmy kryptograficzne.

- Bezpieczeństwo systemów IoT i TustZone, Wykrywanie i zapobieganie włamaniom w IoT, Złośliwe oprogramowanie w IoT

- Cyfrowa kryminalistyka w IoT.

Zagadnienia laboratoryjne:

- Wykorzystanie Arduino do pozyskiwania informacji o parametrach środowiskowych (czujniki temperatury, fororezystory itp.)

- Awaryjne zatrzymanie procesu produkcyjnego w odpowiedzi na alarmy środowiskowe (Raspberry PI, JSON, MongoDB).

- Wykorzystanie Packet Tracer do testowania rozwiązań w dziedzinie inteligentnych miast i sieci (smart grids).

- Prototypowanie i testowanie instalacji inteligentnego domu przy użyciu Packet Tracer (Python, komputer jednopłytkowy, smartfon / tablet, router, czujnik otwarcia drzwi, itp.)

- Inteligentna kamera wrażliwa na uśmiech (Raspberry PI, kamera Raspberry PI, Python, uczenie maszynowe)

- Konfiguracja systemu zapobiegania włamaniom (Intrusion Prevention System - IPS).

- Testowanie podatności prostych rozwiązań IoT (Sensor-Actuator System, IFTTT) w zakresie bezpieczeństwa teleinformatycznego

- Implementacja wybranych lekkich algorytmów kryptograficznych (C, python).

Projekt:

Przygotowanie pracy naukowej w wybranej tematyce.

Metody dydaktyczne

Wykłady: prezentacje multimedialne, ilustrowane przykładami podawanymi na tablicy.

Ćwiczenia laboratoryjne: ćwiczenia praktyczne w grupach z wykorzystaniem platform sprzętowych.

Literatura

Podstawowa

1. Paweł Śniatała, Sitharama S Iyengar, Sanjeev Kaushik Ramani: Evolution of Smart Sensing Ecosystems and the need for Tamper Evident Security: Theory to Practice. Springer 2021

2. William Stallings, Lawrie Brown: Computer Security, Principles and Practice, Pearson 2015. ISBN: 0-13□377392□2.

3. Gaston C. Hillar, Internet of Things with Python Paperback, Packt Publishing, 2016.

Uzupełniająca

1. Marcin Sikorski, Adam Roman: Internet Rzeczy, Wydawnictwo Naukowe PWN 2020. ISBN: 9788301208400

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	150	6,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	75	3,0
Praca własna studenta (studia literaturowe, przygotowanie projektu, przygotowanie do egzaminu)[1]	75	3,0

[1] niepotrzebne skreślić lub dopisać inne czynności