KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Bezpieczeństwo aplikacji mobilnych [S1Cybez1>BAM]

Przedmiot

Kierunek studiów
Cyberbezpieczeństwo

Rok/Semestr
3/6

Studia w zakresie (specjalność)
–

Profil studiów
ogólnoakademicki

Poziom studiów
pierwszego stopnia

Język oferowanego przedmiotu
polski

Forma studiów
stacjonarne

Wymagalność
obligatoryjny

Liczba godzin

Wykład
24

Laboratorium
24

Inne
0

Ćwiczenia
0

Projekty/seminaria
0

Liczba punktów ECTS

3,00

Koordynatorzy

dr inż. Marcin Rodziewicz
marcin.rodziewicz@put.poznan.pl

Wykładowcy

Wymagania wstępne

Studenci rozpoczynający ten przedmiot powinni posiadać: 1. Podstawową znajomość programowania - znajomość języków programowania takich jak Java, Kotlin (Android) lub Swift (iOS), oraz umiejętność pracy z odpowiednimi narzędziami deweloperskimi 2. Podstawową znajomość mobilnych systemów operacyjnych 3. Podstawową wiedzę z zakresu bezpieczeństwa IT - wiedza o zagrożeniach bezpieczeństwa aplikacji, kryptografi oraz uwierzytelnianiu 4. Podstawą wiedzę na temat sieci komputerowych - zrozumienie działania sieci komputerowych i protokołów komunikacyjnych

Cel przedmiotu

Celem przedmiotu jest zapoznanie studentów z kluczowymi zagadnieniami związanymi z bezpieczeństwem aplikacji mobilnych, w tym z zagrożeniami specyficznymi dla platform Android i iOS oraz metodami ich minimalizacji. Uczestnicy nauczą się projektować i implementować bezpieczne aplikacje, chronić dane użytkowników, zapewniać bezpieczną komunikację oraz wykrywać i eliminować podatności aplikacji mobilnych.

Przedmiotowe efekty uczenia się

Wiedza:

1. Posiada uporządkowaną wiedzę w zakresie bezpieczeństwa aplikacji mobilnych [K1_W09]

Umiejętności:
1. Potrafi korzystać z bogatych zasobów dostępnych w Internecie (W tym w języku angielskim) w celu zapewnienia bezpieczeństwa aplikacji mobilnych [K1_U01]
2. Potrafi zaimplementować mechanizmy bezpieczeństwa w aplikacjach mobilnych [K1_U02]

Kompetencje społeczne:
1. Zna ograniczenia własnej wiedzy i umiejętności, rozumie konieczność dalszego dokształcania się [K1_K01]
2. Posiada świadomość konieczności profesjonalnego podejścia do rozwiązywanych problemów technicznych i podejmowania odpowiedzialności za proponowane przez siebie rozwiązania techniczne [K1_K02]
3. Ma poczucie odpowiedzialności za zaprojektowane systemy i zdaje sobie sprawę z zagrożeń dla ludzi i dla społeczeństwa w wypadku ich nieodpowiedniego zaprojektowania lub wykonania [K1_K05]

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:
Wiedza nabyta w ramach wykładu jest weryfikowana przez kolokwium lub zaliczenie ustne realizowane na ostatnim wykładzie.
Umiejętności nabyte w ramach zajęć laboratoryjnych weryfikowane są podstawie wykonania zadań przydzielanych podczas zajęć lub projektu.
W obu formach dydaktycznych przyjmuje się próg zaliczeniowy wynoszący 50% możliwych do zdobycia punktów. Stosuje się następującą skalę ocen: < 50% 2.0; 50%-59% 3.0; 60%-69% 3.5; 70%-79% 4.0; 80%-89% 4.5; 90%-100% 5.0.
Zasady zaliczania przedmiotu i dokładne progi zaliczeniowe zostaną przekazane studentom na początku semestru z wykorzystaniem uczelnianych systemów elektronicznych oraz na pierwszych zajęciach (w każdej formie zajęć).

Treści programowe

Program modułu obejmuje następujące zagadnienia:
• Wprowadzenie do bezpieczeństwa aplikacji mobilnych
• Zarządzanie tożsamością i dostępem
• Bezpieczne przechowywanie danych
• Bezpieczeństwo komunikacji
• Bezpieczeństwo kodu aplikacji
• Bezpieczeństwo interfejsu użytkownika
• Zabezpieczenia specyficzne dla platform

Tematyka zajęć

Program wykładu obejmuje:
1. Wprowadzenie do bezpieczeństwa aplikacji mobilnych
2. Architektura bezpieczeństwa systemów mobilnych
3. Bezpieczeństwo przechowywania danych
4. Bezpieczna komunikacja w aplikacjach mobilnych
5. Uwierzytelnianie i autoryzacja w aplikacjach mobilnych
6. Bezpieczeństwo kodu aplikacji mobilnych
7. Zarządzanie uprawnieniami i zasobami w aplikacjach
8. Bezpieczeństwo interfejsu użytkownika
9. Typowe podatności aplikacji mobilnych
10. Testowanie bezpieczeństwa aplikacji mobilnych
11. Zabezpieczenia specyficzne dla platform Android i iOS
12. Przyszłość bezpieczeństwa aplikacji mobilnych

Program laboratorium obejmuje:
1. Analiza i zarządzanie uprawnieniami aplikacji
2. Szyfrowanie danych lokalnych

3. Implementacja bezpiecznej komunikacji
4. Zabezpieczenie danych uwierzytelniających

Metody dydaktyczne

1. Wykład online: Instruktaż wraz z prezentacją multimedialną
2. Ćwiczenia laboratoryjne: Wykonywanie zadań z instrukcji dostarczanych przez prowadzącego lub projekt

Literatura

Podstawowa:
Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse, "Bezpieczeństwo aplikacji mobilnych. Podręcznik hakera"
Dokumentacja platform mobilnych
https://developer.android.com/topic/security
https://developer.apple.com/documentation/security

Uzupełniająca:
Uzupełniająca

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	90	3,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	48	1,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)	42	1,50