Politechnika Krakowska im. Tadeusza Kościuszki

Karta przedmiotu

obowiązuje studentów rozpoczynających studia w roku akademickim 2021/2022

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma sudiów: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo

1 Informacje o przedmiocie

Nazwa przedmiotu	Bezpieczeństwo aplikacji mobilnych
Nazwa przedmiotu w języku angielskim	Security of mobile applications
Kod przedmiotu	WIiT I oIIS D8 21/22
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	2.00
Semestry	3

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
3	15	0	30	0	0	0

3 Cele przedmiotu

Cel 1 Opanowanie metod klasyfikacji i wykrywania podstawowych ataków i zagrożeń komponentów systemów i aplikacji mobilnych na platformy Android i iOS.

Cel 2 Zrozumienie problemu zabezpieczenia komponentów systemów, komunikacji w tych systemach, danych generowanych i przechowywanych na urządzeniach mobilnych wykorzystywanych w aplikacjach oraz samych aplikacji mobilnych.

Cel 3 Opanowanie podstawowych narzędzi używanych w projektowaniu i implementacji bezpiecznych aplikacji mobilnych na platformy Android i iOS, umiejętność pracy z tymi mobilnych narzędziami i implementacja własnych modyfikacji znanych algorytmów.

Cel 4 Zapoznanie się ze współczesnymi kierunkami rozwoju metod zabezpieczeń komponentów systemu i aplikacji mobilnych, nabycie umiejętności wyciągania wniosków i formułowania własnych tez.

4 Wymagania wstępne w zakresie wiedzy, umiejętności i innych kompetencji

1 Podstawowa wiedza z zakresu programowania, w tym programowania aplikacji mobilnych i internetowych, umiejętność projektowania i implementacji algorytmów i prostych struktur danych.

2 Podstawowa wiedza z zakresu systemów operacyjnych (w tym platform mobilnych).

3 Znajomość co najmniej jednego języka programowania obiektowego.

4 Podstawowa wiedza z zakresu kryptografii.

5 Efekty kształcenia

EK1 Wiedza Zna zaawansowane metody, techniki i narzędzia informatyczne stosowane do wykrywania zagrożeń i ataków w aplikacjach mobilnych dedykowanych głównie platformie Android.

EK2 Wiedza Posiada zaawansowaną i pogłębioną wiedzę z zakresu mechanizmów bezpieczeństwa danych, komunikacji oraz komponentów systemów i aplikacji mobilnych na platformy Android i iOS.

EK3 Umiejętności Potrafi posługiwać się zaawansowanymi metodami, technikami i narzędziami informatycznymi do rozwiązywania złożonych problemów z zakresu bezpieczeństwa komponentów systemów mobilnych i aplikacji mobilnych oraz planować i wykonywać eksperymenty w zakresie symulowania ataków i podniesienia bezpieczeństwa aplikacji mobilnych.

EK4 Kompetencje społeczne Umie pracować indywidualnie i w grupie, potrafi komunikować się z nauczycielem i środowiskiem pozauczelnianym w celu prezentacji uzyskanych przez siebie rezultatów w zrozumiały sposób.

6 Treści programowe

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L1	Organizacja zajęć, omówienie programu ćwiczeń laboratoryjnych, konfiguracja sprzętu, omówienie (na przykładzie) komponentów aplikacji na system Android i podstawowych modułów (warstw) systemu operacyjnego.	2
L2	Zapoznanie się z projektem OWASP Mobile Security.	2
L3	Symulacje rzeczywistych ataków na czynności i komponenty aplikacji (zmiana kodu PIN, błędy podczas kompilacji własnych klas Javy).	4
L4	Omówienie podstawowych mechanizmów obronnych w systemie i aplikacjach na platformę Android).	10

Laboratorium		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
L5	Projekty autorskich aplikacji studentów z implementacją wybranych metod zabezpieczania przechowywania plików na urządzeniu mobilnym i bezpiecznego udostępniania plików innym aplikacjom.	10
L6	Podsumowanie zajęć, ocena projektów studentów.	2

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Architektury mobilnych systemów operacyjnych (Android iOS) i rodzaje aplikacji mobilnych.	1
W2	Aspekty bezpieczeństwa z perspektywy użytkowników urządzeń mobilnych (domyślne systemy zabezpieczeń urządzeń mobilnych, data wiping)	2
W3	Mechanizmy bezpieczeństwa dostarczane developerom (system uprawnień w Androidzie, Data Protection i Keychain w iOS).	2
W4	Zagadnienia inżynierii odwrotnej w systemach Android.	2
W5	Rodzaje ataków, ataki typu jailbreak, ataki typu injection (iOS) SQL injection (Android), ataki na komponenty aplikacji (Android), ataki na dane użytkowników i dane szyfrowane (ogólnie).	2
W6	Bezpieczeństwo danych w systemach mobilnych.	2
W7	Bezpieczeństwo komunikacji w systemach mobilnych.	2
W8	Tworzenie bezpiecznych aplikacji na platformę Android.	2

7 Narzędzia dydaktyczne

N1 Wykłady (w przypadku realizacji zajęć w trybie zdalnym z wykorzystaniem stosownych narzędzi teleinformatycznych)

N2 Ćwiczenia laboratoryjne (w przypadku realizacji zajęć w trybie zdalnym z wykorzystaniem stosownych narzędzi teleinformatycznych)

N3 Prezentacje multimedialne (w przypadku realizacji zajęć w trybie zdalnym z wykorzystaniem stosownych narzędzi teleinformatycznych)

N4 Konsultacje (w przypadku realizacji zajęć w trybie zdalnym z wykorzystaniem stosownych narzędzi teleinformatycznych)

8 Obciążenie pracą studenta

Forma aktywności	Średnia liczba godzin na zrealizowanie aktywności
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	45
Konsultacje przedmiotowe	4
Egzaminy i zaliczenia w sesji	1
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	0
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	10
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**60**
Sumaryczna liczba punktów ECTS dla przedmiotu	2.00

9 Sposoby oceny

Ocena formująca

F1 Egzamin pisemny sprawdzający wiedzę z wykładów

F2 Sprawozdania z wykonanych ćwiczeń laboratoryjnych

F3 Kolokwia na laboratoriach

F4 Projekt indywidualny

Ocena podsumowująca

P1 Średnia ważona ocen formujących

Warunki zaliczenia przedmiotu

W1 Pozytywna ocena z egzaminu pisemnego z wykładu

W2 Pozytywna ocena z zajęć laboratoryjnych (kolokwia, projekt indywidualny)

W3 Obecność na co najmniej 50% zajęć laboratoryjnych

Kryteria oceny

Efekt kształcenia 1	
Na ocenę 2.0	Student nie spełnia warunków określonych dla oceny 3.0.

Na ocenę 3.0	Student opanował co najmniej 50% materiału.
Na ocenę 3.5	Student opanował więcej niż 60% materiału.
Na ocenę 4.0	Student opanował więcej niż 70% materiału.
Na ocenę 4.5	Student opanował więcej niż 80% materiału.
Na ocenę 5.0	Student opanował więcej niż 90% materiału.
Efekt kształcenia 2	
Na ocenę 2.0	Student nie spełnia warunków określonych dla oceny 3.0.
Na ocenę 3.0	Student opanował co najmniej 50% materiału.
Na ocenę 3.5	Student opanował więcej niż 60% materiału.
Na ocenę 4.0	Student opanował więcej niż 70% materiału.
Na ocenę 4.5	Student opanował więcej niż 80% materiału.
Na ocenę 5.0	Student opanował więcej niż 90% materiału.
Efekt kształcenia 3	
Na ocenę 2.0	Student nie spełnia warunków określonych dla oceny 3.0.
Na ocenę 3.0	Student opanował co najmniej 50% materiału.
Na ocenę 3.5	Student opanował więcej niż 60% materiału.
Na ocenę 4.0	Student opanował więcej niż 70% materiału.
Na ocenę 4.5	Student opanował więcej niż 80% materiału.
Na ocenę 5.0	Student opanował więcej niż 90% materiału.
Efekt kształcenia 4	
Na ocenę 2.0	Student nie spełnia warunków określonych dla oceny 3.0.
Na ocenę 3.0	Student opanował co najmniej 50% materiału.
Na ocenę 3.5	Student opanował więcej niż 60% materiału.
Na ocenę 4.0	Student opanował więcej niż 70% materiału.
Na ocenę 4.5	Student opanował więcej niż 80% materiału.
Na ocenę 5.0	Student opanował więcej niż 90% materiału.

10 Macierz realizacji przedmiotu

Efekt kształcenia	Odniesienie danego efektu do szczegółowych efektów zdefiniowanych dla programu	Cele przedmiotu	Treści programowe	Narzędzia dydaktyczne	Sposoby oceny
EK1	I2_W02 I2_W08 I2_U01b I2_U04b I2_U12 I2_K02 I2_K04	Cel 1 Cel 4	L2 L3 W2 W3 W4 W5	N1 N2 N3 N4	F1 F2 F3 F4
EK2	I2_W05 I2_W06 I2_W08 I2_U01b I2_U11 I2_K02 I2_K03	Cel 2 Cel 3 Cel 4	L2 L4 W2 W3 W6 W7	N1 N2 N3 N4	F1 F2 F3 F4
EK3	I2_W01 I2_W02 I2_W05 I2_W08 I2_U01b I2_U02b I2_U03b I2_U08 I2_K02 I2_K04	Cel 2 Cel 3 Cel 4	L3 L5 W8	N1 N2 N3 N4	F1 F2 F3 F4
EK4	I2_W05 I2_W06 I2_W08 I2_U01b I2_U05 I2_U07 I2_U08 I2_K02 I2_K04	Cel 1 Cel 2 Cel 3	L2 L3 L5	N2 N3 N4	F2 F3 F4

11 Wykaz literatury

Literatura podstawowa

[1] D. Chell, T. Erasmus, S. Colley, O. Whitehouse — *Bezpieczeństwo aplikacji mobilnych. Podręcznik hackera*, , 2017, Helion

[2] V. Prashant, D. Akshay — *Bezpieczeństwo urządzeń mobilnych. Receptury*, , 2017, Helion

[3] Źródło internetowe — *https://sekurak.pl/*, , 0,

Literatura uzupełniająca

[1] K. Beaver — *Hacking for Dummies*, , 2018, Wiley &Sons

[2] 3H. Dwivedi, C. Clark, D. Thiel — *Mobile Application Security: Protecting Mobile Devices and their Applications*, , 2010, McGraw Hill Professional

[3] Źródło internetowe — *https://www.sonarqube.org/features/security/*, , 0,

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr inż. Andrzej Wilczyński (kontakt: `andrzej.wilczynski@pk.edu.pl`)

13 Zatwierdzenie karty przedmiotu do realizacji

(miejscowość, data) (odpowiedzialny za przedmiot) (dziekan)