

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2023/2024

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: 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	WiT I oIIS D11 23/24
KATEGORIA PRZEDMIOTU	Przedmioty specjalnościowe
LICZBA PUNKTÓW ECTS	3.00
SEMESTRY	3

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁAD	ĆWICZENIA	LABORATORIUM	LABORATORIUM KOMPUTERO- WE	SEMINARIUM	PROJEKT
3	15	0	0	30	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.

Kod archiwizacji:

Cel 3 Opanowanie podstawowych narzędzi używanych w projektowaniu i implementacji bezpiecznych aplikacji mobilnych na platformy Android i iOS, umiejętność pracy z tymi mobilnymi 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 Znajomość języka angielskiego w stopniu umożliwiającym studiowanie literatury

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 pozauczełnianym w celu prezentacji uzyskanych przez siebie rezultatów w zrozumiały sposób.

6 TREŚCI PROGRAMOWE

LABORATORIUM KOMPUTEROWE		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
K1	Organizacja zajęć, omówienie programu ćwiczeń laboratoryjnych, konfiguracja sprzętu, omówienie (na przykładzie) komponentów aplikacji na system Android i podstawowych modułów (warstw) systemu operacyjnego.	2
K2	Zapoznanie się z projektem OWASP Mobile Security.	2
K3	Symulacje rzeczywistych ataków na czynności i komponenty aplikacji (zmiana kodu PIN, błędy podczas kompilacji własnych klas Javy).	4
K4	Omówienie podstawowych mechanizmów obronnych w systemie i aplikacjach na platformę Android).	10

LABORATORIUM KOMPUTEROWE		
LP	TEMATYKA ZAJĘĆ OPIS SZCZEGÓŁOWY BLOKÓW TEMATYCZNYCH	LICZBA GODZIN
K5	Projekty autorskich aplikacji studentów z implementacją wybranych metod zabezpieczania przechowywania plików na urządzeniu mobilnym i bezpiecznego udostępniania plików innym aplikacjom.	10
K6	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)
- N5** MS Teams - ogłoszenia, wykład w formie zdalnej, kontakt prowadzącego ze studentami poza zajęciami stacjonarnymi
- N6** Delta - oceny cząstkowe, archiwum projektów

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	0
Godziny bez udziału nauczyciela akademickiego wynikające z nakładu pracy studenta, w tym:	
Przygotowanie się do zajęć, w tym studiowanie zalecanej literatury	10
Opracowanie wyników	10
Przygotowanie raportu, projektu, prezentacji, dyskusji	10
SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA	79
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	3.00

9 SPOSOBY OCENY

OCENA FORMUJĄCA

F1 Sprawozdania z wykonanych ćwiczeń laboratoryjnych

F2 Kolokwia na laboratoriach

F3 Projekt indywidualny

OCENA PODSUMOWUJĄCA

P1 Średnia ważona ocen formujących

WARUNKI ZALICZENIA PRZEDMIOTU

W1 Pozytywna ocena z zajęć laboratoryjnych (kolokwia, projekt indywidualny)

W2 Wymaganie obecności minimum na 70% zajęć

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	K2 K3 W2 W3 W4 W5	N1 N2 N3 N4	F1 F2 F3
EK2	I2_W05 I2_W06 I2_W08 I2_U11 I2_K02 I2_K03	Cel 2 Cel 3 Cel 4	K2 K4 W2 W3 W6 W7	N1 N2 N3 N4	F1 F2 F3
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	K3 K5 W8	N1 N2 N3 N4	F1 F2 F3
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	K2 K3 K5	N2 N3 N4	F1 F2 F3

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 hab. prof.PK Joanna Kołodziej (kontakt: joanna.kolodziej@pk.edu.pl)

OSOBY PROWADZĄCE PRZEDMIOT

1 mgr inż. Michał Niedźwiecki (kontakt: michal.niedzwiecki@pk.edu.pl)

13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejscowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....