

POLITECHNIKA KRAKOWSKA IM. TADEUSZA KOŚCIUSZKI

KARTA PRZEDMIOTU

obowiązuje studentów rozpoczynających studia w roku akademickim 2019/2020

Wydział Informatyki i Telekomunikacji

Kierunek studiów: Informatyka

Profil: Ogólnoakademicki

Forma studiów: niestacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo dla inżynierów

1 INFORMACJE O PRZEDMIOCIE

NAZWA PRZEDMIOTU	Bezpieczeństwo aplikacji mobilnych
NAZWA PRZEDMIOTU W JĘZYKU ANGIELSKIM	Mobile application security
KOD PRZEDMIOTU	WiT I oIIN D8 19/20
KATEGORIA PRZEDMIOTU	Przedmioty specjalnościowe
LICZBA PUNKTÓW ECTS	2.00
SEMESTRY	3

2 RODZAJ ZAJĘĆ, LICZBA GODZIN W PLANIE STUDIÓW

SEMESTR	WYKŁAD	ĆWICZENIA	LABORATORIUM	LABORATORIUM KOMPUTERO- WE	SEMINARIUM	PROJEKT
3	9	0	18	0	0	0

3 CELE PRZEDMIOTU

Cel 1 Opanowanie przez studentów metod klasyfikacji i wykrywania podstawowych ataków i zagrożeń komponentów systemów i aplikacji mobilnych na platformę Android (i opcjonalnie iOS).

Cel 2 Zrozumienie przez studentów 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 przez studentów podstawowych narzędzi używanych w projektowaniu i implementacji bezpiecznych aplikacji mobilnych na platformie Android (i opcjonalnie iOS), umiejętność pracy z tymi mobilnymi narzędziami i implementacja własnych modyfikacji znanych algorytmów.

Cel 4 Przedstawienie studentom współczesnych kierunków rozwoju metod zabezpieczeń komponentów systemu i aplikacji mobilnych, umiejętność wyciągania wniosków przez studentów 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 Podstawowa wiedza z zakresu kryptografii

5 EFEKTY KSZTAŁCENIA

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

EK2 Wiedza Student ma zaawansowaną i pogłębioną wiedzę z zakresu bezpieczeństwa komponentów systemów i aplikacji mobilnych na platformy Android i iOS.

EK3 Umiejętności Student umie 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 Student posiada umiejętność pracy indywidualnej i w grupie, samokształcenia, umiejętność komunikacji z nauczycielem i środowiskiem pozauczelnianym w celu popularyzacji przedstawiania uzyskanych rezultatów w zrozumiały sposób.

6 TREŚCI PROGRAMOWE

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

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	Symulacje rzeczywistych ataków na czynności i komponenty aplikacji (zmiana kodu PIN, błędy podczas kompilacji własnych klas Javy).	2
L3	Omówienie podstawowych mechanizmów obronnych w systemie i aplikacjach na platformę Android).	4
L4	Projekty autorskich aplikacji studentów z implementacją wybranych metod zabezpieczania przechowywania plików na urządzeniu mobilnym i bezpiecznego udostępniania plików innym aplikacjom.	8
L5	Podsumowanie zajęć, ocena projektów studentów.	2

7 NARZĘDZIA DYDAKTYCZNE

N1 Wykłady

N2 Ćwiczenia laboratoryjne

N3 Dyskusje

N4 Konsultacje

8 OBCIĄŻENIE PRACĄ STUDENTA

FORMA AKTYWNOŚCI	ŚREDNIA LICZBA GODZIN NA ZREALIZOWANIE AKTYWNOŚCI
Godziny kontaktowe z nauczycielem akademickim, w tym:	
Godziny wynikające z planu studiów	27
Konsultacje przedmiotowe	2
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	4
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	2
SUMARYCZNA LICZBA GODZIN DLA PRZEDMIOTU WYNIKAJĄCA Z CAŁEGO NAKŁADU PRACY STUDENTA	36
SUMARYCZNA LICZBA PUNKTÓW ECTS DLA PRZEDMIOTU	2.00

9 SPOSOBY OCENY

Nie przeprowadza się testu wstępnego.

OCENA FORMUJĄCA

F1 Sprawozdania z wykonanych ćwiczeń laboratoryjnych.

F2 Egzamin pisemny

OCENA PODSUMOWUJĄCA

P1 Średnia ważona ocen formujących (70%, 30%).

WARUNKI ZALICZENIA PRZEDMIOTU

W1 Pozytywna ocena z ćwiczeń laboratoryjnych - zaliczenie wszystkich elementów.

W2 Pozytywna ocena z egzaminu

OCENA AKTYWNOŚCI BEZ UDZIAŁU NAUCZYCIELA

B1 Udział studentów w konsultacjach zdalnych, aktywność na platformie e-learningowej.

KRYTERIA OCENY

EFEKT KSZTAŁCENIA 1

NA OCENĘ 2.0	Student nie przyswoił sobie wiedzy na temat rodzajów ataków w systemach mobilnych i mechanizmów wykrywania anomalii i fałszywych danych w aplikacjach na platformę Android.
NA OCENĘ 3.0	Student ma podstawową wiedzę na temat rodzajów ataków w systemach mobilnych i mechanizmów wykrywania anomalii i fałszywych danych w aplikacjach na platformę Android
NA OCENĘ 3.5	Student ma podstawową wiedzę na temat rodzajów ataków w systemach mobilnych i mechanizmów wykrywania zagrożeń dla aplikacji dedykowanych platformie Android, potrafi przeprowadzić analizę krytyczną istniejących modeli i wyciągnąć odpowiednie wnioski.
NA OCENĘ 4.0	Student ma poszerzoną wiedzę na temat rodzajów ataków w systemach mobilnych i mechanizmów wykrywania zagrożeń dla aplikacji dedykowanych platformie Android, potrafi przedstawić zaawansowaną charakterystykę wybranych metod i przeprowadzić analizę porównawczą.
NA OCENĘ 4.5	Student potrafi opracować prostą klasyfikację ataków i taksonomię metod wykrywania zagrożeń sprzętowych, konfiguracyjnych, komunikacyjnych i dla aplikacji na platformę Android, potrafi dokonać analizy krytycznej metod ujętych w taksonomii i wyciągnąć z niej odpowiednie wnioski.
NA OCENĘ 5.0	Student ma bardzo zaawansowaną wiedzę na temat zagrożeń i ataków w środowisku Android z punktu widzenia użytkownika i dewelopera, potrafi odpowiednio poklasyfikować zarówno ataki i jak i metody ich detekcji, zwracając szczególną uwagę na metody inteligentne (np. uczenia maszynowego).
EFEKT KSZTAŁCENIA 2	
NA OCENĘ 2.0	Student nie zna podstawowych metod zabezpieczeń komponentów aplikacji mobilnych i systemu na platformie Android.
NA OCENĘ 3.0	Student potrafi przeprowadzić prostą klasyfikację metod zabezpieczeń komponentów aplikacji mobilnych i systemu na platformie Android.
NA OCENĘ 3.5	Student potrafi przeprowadzić prostą klasyfikację metod zabezpieczeń komponentów aplikacji mobilnych i systemu na platformach Android i iOS.
NA OCENĘ 4.0	Student ma poszerzoną wiedzę na temat charakterystyki i własności metod zabezpieczeń komponentów aplikacji mobilnych i systemu na platformach Android i iOS, potrafi przeprowadzić ich analizę porównawczą i wyciągnąć odpowiednie wnioski.
NA OCENĘ 4.5	Student potrafi zdefiniować własną taksonomię metod zabezpieczeń komponentów aplikacji mobilnych i systemu na platformach Android i iOS, potrafi przeprowadzić ich analizę porównawczą i wyciągnąć odpowiednie wnioski.
NA OCENĘ 5.0	Student potrafi zdefiniować własną taksonomię metod zabezpieczeń komponentów aplikacji mobilnych, metod bezpiecznej transmisji danych i komunikacji na platformach Android i iOS, potrafi przeprowadzić ich analizę porównawczą i wyciągnąć odpowiednie wnioski.
EFEKT KSZTAŁCENIA 3	

NA OCENĘ 2.0	Student nie potrafi zaimplementować prostych metod zabezpieczających komponenty aplikacji mobilnych na platformę Android , nie wie, jak przygotować narzędzia do symulacji ataków.
NA OCENĘ 3.0	Student potrafi opracować koncepcje prostych ataków, zna narzędzia do implementacji algorytmów zabezpieczających podstawowe komponenty aplikacji mobilnych i potrafi je zaimplementować.
NA OCENĘ 3.5	Student potrafi opracować koncepcje prostych ataków, zna narzędzia do implementacji algorytmów zabezpieczających podstawowe komponenty aplikacji mobilnych i potrafi je zaimplementować, potrafi wykonać proste testy i opracować wyniki.
NA OCENĘ 4.0	Student ma poszerzoną wiedzę na temat narzędzi do implementacji modeli bezpieczeństwa dla aplikacji mobilnych, potrafi przeprowadzić symulację ataku, opracować wyniki i wyciągnąć odpowiednie wnioski.
NA OCENĘ 4.5	Student ma poszerzoną wiedzę na temat narzędzi do implementacji modeli bezpieczeństwa dla aplikacji mobilnych, potrafi opracować bezpieczne metody udostępniania danych i pobierania danych dla aplikacji ze źródeł zewnętrznych, potrafi przeprowadzić symulację ataku, opracować wyniki i wyciągnąć odpowiednie wnioski.
NA OCENĘ 5.0	Student ma bardzo zaawansowaną wiedzę i potrafi zaimplementować oraz przeprowadzić eksperymenty z wykorzystaniem autorskich modyfikacji algorytmów do zabezpieczania komponentów aplikacji mobilnych, potrafi opracować metody bezpiecznej komunikacji pomiędzy komponentami aplikacji i platformy mobilnej, potrafi opracować bezpieczne metody udostępniania danych i pobierania danych dla aplikacji ze źródeł zewnętrznych, potrafi przeprowadzić symulację ataku, opracować wyniki i wyciągnąć odpowiednie wnioski.
EFEKT KSZTAŁCENIA 4	
NA OCENĘ 2.0	Student nie radzi sobie z pracą indywidualną nad postawionymi zadaniami, nie wykonuje zaleceń nauczyciela.
NA OCENĘ 3.0	Student w miarę sumiennie uczęszcza na zajęcia, radzi sobie z pracą indywidualną.
NA OCENĘ 3.5	Student jest aktywny na zajęciach, demonstruje stosowane metody rozwiązywania postawionych zadań, bierze udział w dyskusji.
NA OCENĘ 4.0	Student jest aktywny na zajęciach, potrafi objaśniać w sposób zrozumiały zastosowane metody rozwiązywania postawionych zadań, potrafi pracować nad problemem w małej grupie.
NA OCENĘ 4.5	Student jest aktywny na zajęciach, potrafi objaśniać w sposób zrozumiały zastosowane metody rozwiązywania postawionych zadań, potrafi pracować nad problemem w małej grupie, potrafi pokierować pracą tej grupy.
NA OCENĘ 5.0	Student jest bardzo aktywny na zajęciach, potrafi objaśniać w sposób zrozumiały zastosowane metody rozwiązywania postawionych zadań, potrafi pracować nad problemem w małej grupie, potrafi kreować pracę tej grupy i przedstawiać w sposób zrozumiały wyniki pracy.

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_W04 I2_W06	Cel 1 Cel 4	W2 W3 W4 W5 L2 L3	N1 N2 N4	F1 F2 P1
EK2	I2_W02 I2_W04 I2_W06	Cel 2 Cel 3 Cel 4	W2 W3 L2 L4	N1 N2 N4	F1 F2 P1
EK3	I2_U01b I2_U02b I2_U07 I2_U11 I2_U12	Cel 2 Cel 3 Cel 4	W5 L3 L5	N1 N2 N3 N4	F1 F2 P1
EK4	I2_K02	Cel 1 Cel 2 Cel 3	L2 L3 L5	N3 N4	F2 P1

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

LITERATURA UZUPEŁNIAJĄCA

- [1] 530514, 102199, 2, 1, <https://sekurak.pl/>, , , 0, ,
- [2] **K. Beaver** — *Hacking for Dummies*, , 2018, Wiley & Sons

LITERATURA DODATKOWA

- [1] 530516, 102199, 3, 1, <https://www.sonarqube.org/features/security/>, , , 0, ,
- [2] **H. Dwivedi, C. Clark, D. Thiel** — *Mobile Application Security: Protecting Mobile Devices and their Applications*, , 2010, McGraw Hill Professional

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 dr hab., prof. PK Joanna Kołodziej (kontakt: jokolodziej@pk.edu.pl)

2 mgr inż. Andrzej Wilczyński (kontakt: and.wilczynski@gmail.com)

13 ZATWIERDZENIE KARTY PRZEDMIOTU DO REALIZACJI

(miejscowość, data)

(odpowiedzialny za przedmiot)

(dziekan)

PRZYJMUJĘ DO REALIZACJI (data i podpisy osób prowadzących przedmiot)

.....
.....