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 sudiów: stacjonarne

Kod kierunku: I

Stopień studiów: II

Specjalności: Cyberbezpieczeństwo dla licencjatów

1 Informacje o przedmiocie

Nazwa przedmiotu	Bezpieczeństwo aplikacji mobilnych
Nazwa przedmiotu w języku angielskim	Mobile application security
Kod przedmiotu	WIiT I oIIS D9 19/20
Kategoria przedmiotu	Przedmioty specjalnościowe
Liczba punktów ECTS	2.00
Semestry	4

2 Rodzaj zajęć, liczba godzin w planie studiów

Semestr	Wykład	Ćwiczenia	Laboratorium	Laboratorium komputerowe	Seminarium	Projekt
4	30	0	15	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 mobilnych 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 rozwiązywania złożonych problemów informatycznych - w zakresie systemów mobilnych i cyberbezpieczeństwa.

EK2 Wiedza Student ma zaawansowaną i pogłębioną wiedzę z zakresu szeroko rozumianych systemów informatycznych- w tym systemów mobilnych, podstaw teoretycznych ich budowania oraz metod, narzędzi i środowisk programistycznych wykorzystywanych do ich implementacji.

EK3 Umiejętności Student umie posługiwać się zaawansowanymi metodami, technikami i narzędziami informatycznymi do rozwiązywania złożonych problemów informatycznych oraz planować i wykonywać eksperymenty w zakresie bezpieczeństwa aplikacji mobilnych.

EK4 Kompetencje społeczne Student potrafi pracować w zespole interdyscyplinarnym, określać priorytety realizowanych zadań, kierować tym zespołem i odpowiadać za efekty jego pracy.

6 Treści programowe

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W1	Architektury mobilnych systemów operacyjnych (Android iOS) i rodzaje aplikacji mobilnych	2
W2	Aspekty bezpieczeństwa z perspektywy użytkowników urządzeń mobilnych (domyślne systemy zabezpieczeń urządzeń mobilnych, data wiping)	2
W3	TMechanizmy bezpieczeństwa dostarczane developerom (system uprawnień w Androidzie, data [rotection i Keychain w iOS)	2
W4	Zagadnienia Inżynierii odwrotnej w systemach Android i iOS	4
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)	6

Wykład		
Lp	Tematyka zajęć Opis szczegółowy bloków tematycznych	Liczba godzin
W6	Bezpieczeństwo danych w systemach mobilnych	2
W7	Bezpieczeństwo komunikacji w systemach mobilnych	2
W8	Identyfikowanie problemów w implementacji aplikacji mobilnych przykłady dla platformy Android	4
W9	Tworzenie bezpiecznych aplikacji na platformę Android	4
W10	Podsumowanie i problemy otwarte	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	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)	2
L4	Omówienie podstawowych mechanizmów obronnych w systemie i aplikacjach na platformę Android)	4
L5	Projekt autorskiej aplikacji studenta z implementacją wybranych metod zabezpieczania przechowywania plików na urządzeniu mobilnym i bezpiecznego udostępniania plików innym aplikacjom	4
L6	Podsumowanie zajęć, ocena projektów studentów	1

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	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	5
Opracowanie wyników	0
Przygotowanie raportu, projektu, prezentacji, dyskusji	5
Sumaryczna liczba godzin dla przedmiotu wynikająca z całego nakładu pracy studenta	**60**
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 (80%, 20%).

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 porównawcza 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. 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 porównawcza 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 W6 W7 L2 L4	N1 N2	F1 F2 P1
EK3	I2_U01b I2_U02b I2_U07 I2_U11 I2_U12	Cel 2 Cel 3 Cel 4	W8 L3 L5	N1 N2 N3 N4	F1 F2 P1
EK4	I2_U03b 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

[3] 529182, 101938, 1, 3, https://sekurak.pl/, , , 0, ,

Literatura uzupełniająca

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

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

Literatura dodatkowa

[1] 529183, 101938, 3, 1, https://www.sonarqube.org/features/security/, , , 0, ,

12 Informacje o nauczycielach akademickich

Osoba odpowiedzialna za kartę

dr hab. prof.PK Joanna Kołodziej (kontakt: `jokolodziej@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)

. . . . . .

. . . . . .