UNIWERSYTET IM. ADAMA MICKIEWICZA W POZNANIU

Bezpieczeństwo systemów mobilnych

Sylabus zajęć

Informacje podstawowe

Kierunek studiów
Informatyka

Specjalność
-

Jednostka organizacyjna
Wydział Matematyki i Informatyki

Poziom studiów
studia inżynierskie pierwszego stopnia

Forma studiów
studia niestacjonarne

Profil studiów
profil ogólnoakademicki

Cykl dydaktyczny
2023/24

Kod zajęć
06INFN.320S.03131.23

Języki wykładowe
polski

Obligatoryjność
Fakultatywny

Blok zajęciowy
Przedmioty specjalnościowe

Koordynator zajęć	Michał Ren
Prowadzący zajęcia	Michał Ren

Okres	Forma zajęć / liczba godzin / forma zaliczenia	Liczba punktów ECTS
Semestr 6	• Wykład: 15, Egzamin • Laboratorium: 15, Zaliczenie z oceną	5

Cele kształcenia dla zajęć

Kod	Cel
C1	Przedmiot uczy studentów zasad bezpiecznego programowania na platformach mobilnych – każdy napisze kilka prostych aplikacji, których celem będzie nauka mechanizmów bezpieczeństwa na wybranej przez studenta platformie mobilnej. Celem ogólnym przedmiotu jest nauczenie odpowiedniego podejścia i myślenia o bezpieczeństwie w projektowaniu, implementacji i wdrażaniu aplikacji mobilnych, zapewniając wiedzę ogólną o najpopularniejszych platformach mobilnych, ale bez wymuszania użycia którejkolwiek z nich.

Wymagania wstępne

Umiejętności programowania na dowolnej platformie mobilnej (szczególnie na Android lub iOS) są przydatne, ale przedmiot jest tak zorganizowany, by nie były one niezbędne; większość studentów przystępujących do przedmiotu ich nie posiada.

Efekty uczenia się dla zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
Wiedzy – Student/ka:			
W1	Rozumie model bezpieczeństwa AIC, wie na czym polega bezpieczeństwo w systemach teleinformatycznych.	INF_K3_W07	Egzamin pisemny
W2	Posługuje się podstawowymi pojęciami kryptologii, zna proste metody służące zapewnieniu poufności danych.	INF_K3_W01, INF_K3_W02, INF_K3_W07	Egzamin pisemny
W3	Orientuje się w metodach przechowywania haseł. Zna zasady przechowywania haseł w systemach teleinformatycznych.	INF_K3_W07	Egzamin pisemny
W4	Rozumie wady i zalety uwierzytelniania wieloskładnikowego, zna podstawowe metody jego realizacji.	INF_K3_W07	Egzamin pisemny
W5	Potrafi ocenić skuteczność testów biometrycznych, zna ich słabe i silne strony a także podstawy teorii stojącej za najpopularniejszymi ich rodzajami. Jest świadom problemów implementacyjnych testów biometrycznych.	INF_K3_W07	Egzamin pisemny
W6	Zna architekturę systemu GSM, jego cele i środki użyte w nim do zapewnienia bezpieczeństwa, a także najbardziej znane ataki.	INF_K3_W07	Egzamin pisemny
W7	Wie w jaki sposób niedoskonałości sprzętowe umożliwiają ataki i jak te ataki przekładają się na stworzenie podatności. Zna najpopularniejsze z nich.	INF_K3_W07	Egzamin pisemny
W8	Zna fizyczne podstawy działania systemów wykorzystujących fale elektromagnetyczne, podstawowe ataki na nie i metody przeciwdziałania im.	INF_K3_W07	Egzamin pisemny
W9	Rozumie założenia architektoniczne platformy mobilnej Android, jej budowę i komponenty oraz metody użyte do jej zabezpieczenia.	INF_K3_W03, INF_K3_W04_inz, INF_K3_W06_inz, INF_K3_W07	Egzamin pisemny
W10	Zna różnice między najpopularniejszymi platformami mobilnymi i rozumie jak różne podejścia do kwestii bezpieczeństwa doprowadziły do stosowania różnych architektur.	INF_K3_W06_inz, INF_K3_W07	Egzamin pisemny
W11	Rozumie technologie stosowane do zabezpieczania na poziomie fizycznym.	INF_K3_W07	Egzamin pisemny
Umiejętności – Student/ka:			
U1	Potrafi dostrzec w systemie elementy wymagające zabezpieczenia.	INF_K3_U07_inz	Zadania wykonywane podczas zajęć

Kod	Efekty uczenia się dla zajęć w zakresie	Efekty uczenia się dla kierunku	Metody weryfikacji osiągnięcia efektów uczenia się dla zajęć
U2	Potrafi konstruować politykę doboru haseł.	INF_K3_U07_inz	Zadania wykonywane podczas zajęć
U3	Umie zastosować zabezpieczenia biometryczne w platformie mobilnej.	INF_K3_U05_inz, INF_K3_U07_inz	Zadania wykonywane podczas zajęć
U4	Potrafi dokonać prostego ataku side channel.	INF_K3_U06_inz, INF_K3_U07_inz	Zadania wykonywane podczas zajęć
U5	Potrafi stosować techniki bezpieczeństwa zgodnie z dokumentacją deweloperską.	INF_K3_U06_inz, INF_K3_U07_inz	Zadania wykonywane podczas zajęć
U6	Potrafi posługiwać się interfejsami do zabezpieczeń fizycznych.	INF_K3_U05_inz, INF_K3_U06_inz, INF_K3_U07_inz	Zadania wykonywane podczas zajęć
U7	Potrafi stosować uwierzytelnianie wieloskładnikowe.	INF_K3_U06_inz	Zadania wykonywane podczas zajęć

Treści programowe dla zajęć

Lp.	Treści programowe dla zajęć	Efekty uczenia się dla zajęć	Formy zajęć
1.	Podstawowe pojęcia bezpieczeństwa, modelowanie bezpieczeństwa, triada AIC.	W1, U1	Wykład, Laboratorium
2.	Podstawowe pojęcia kryptologii, poufność danych, terminologia, proste szyfry.	W2	Wykład, Laboratorium
3.	Przechowywanie haseł, haszowanie, key stretching, tęczowe tablice i podstawowe ataki.	W3, U2	Wykład, Laboratorium
4.	Uwierzytelnianie wieloskładnikowe – S/KEY, HOTP, TOTP, FIDO U2F.	W4, U7	Wykład, Laboratorium
5.	Biometria – testy biometryczne, krzywe ROC, badanie odcisków palców, skanery tęczówek, rozpoznawanie twarzy, najpopularniejsze ataki.	W5, U3	Wykład, Laboratorium
6.	System GSM i jego bezpieczeństwo – podatności SS7, ataki man-in-the-middle, "jaskółki", szyfr A5/1.	W6	Wykład
7.	Ataki sprzętowe – side channel, Drammer.	W7, U4	Wykład, Laboratorium
8.	Podstawy bezpieczeństwa radiowego – atak TEMPEST i metody przeciwdziałania mu, TEMPEST optyczny.	W8	Wykład
9.	Cechy bezpieczeństwa platformy Android.	W9, U5	Wykład, Laboratorium
10.	Porównanie cech bezpieczeństwa platform mobilnych.	W10	Wykład, Laboratorium
11.	Zabezpieczenia sprzętowe na współczesnych urządzeniach abonenckich – TEE/REE, secure/authenticated boot, system KeyStore, standard Global Platform, TPM.	W11, U6	Wykład

Informacje dodatkowe

Forma zajęć	Metody i formy prowadzenia zajęć
Wykład	Wykład z prezentacją multimedialną wybranych zagadnień, Wykład konwersatoryjny, Dyskusja, Pokaz i obserwacja, Demonstracje dźwiękowe i/lub video, Metoda aktywizująca - "burza mózgów"
Laboratorium	Rozwiązywanie zadań (np.: obliczeniowych, artystycznych, praktycznych), Metoda laboratoryjna

Forma zajęć	Warunki zaliczenia zajęć
Wykład	Końcowa ocena składa się z wyniku uzyskanego na egzaminie pisemnym. Skala ocen: 1. bardzo dobry (bdb; 5,0) – co najmniej 80% punktów, 2. dobry plus (db plus; 4,5) – co najmniej 70% punktów, 3. dobry (db; 4,0) – co najmniej 60% punktów, 4. dostateczny plus (dst plus; 3,5) – co najmniej 50% punktów, 5. dostateczny (dst; 3,0) – co najmniej 40% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 40% punktów.
Laboratorium	Końcowa ocena składa się z wyniku uzyskanego z zadań wykonywanych podczas zajęć. Skala ocen: 1. bardzo dobry (bdb; 5,0) – co najmniej 80% punktów, 2. dobry plus (db plus; 4,5) – co najmniej 70% punktów, 3. dobry (db; 4,0) – co najmniej 60% punktów, 4. dostateczny plus (dst plus; 3,5) – co najmniej 50% punktów, 5. dostateczny (dst; 3,0) – co najmniej 40% punktów, 6. niedostateczny (ndst; 2,0) – poniżej 40% punktów.

Literatura

Obowiązkowa

1. Mobile Platform Security. Synthesis Lectures on Information Security, Privacy, and Trust. N. Asokan, Lucas Davi, Alexandra Dmitrienko, Stephan Heuser, Kari Kostiainen, Elena Reshetova, Ahmad-Reza Sadeghi. https://www.morganclaypool.com/doi/abs/10.2200/S00555ED1V01Y201312SPT009
2. Wireless and Mobile Device Security. Jim Doherty. https://www.jblearning.com/catalog/productdetails/9781284059274
3. Security Engineering. Ross Anderson. https://www.cl.cam.ac.uk/~rja14/book.html
4. Android Security Cookbook. Keith Makan, Scott Alexander-Bown. https://www.packtpub.com/application-development/android-security-cookbook
5. Android Developer Documentation https://developer.android.com/docs
6. Apple Developer Documentation. https://developer.apple.com/documentation/

Dodatkowa

1. Dokumentacja wybranej platformy mobilnej

Nakład pracy studenta i punkty ECTS

Rodzaje zajęć studenta	Średnia liczba godzin* przeznaczonych na zrealizowane rodzaje zajęć
Wykład	15
Laboratorium	15
Przygotowanie do zajęć	40

Czytanie wskazanej literatury	30
Przygotowanie do egzaminu	25
Łączny nakład pracy studenta	**Liczba godzin** 125
Liczba punktów ECTS	**ECTS** 5

* godzina (lekcyjna) oznacza 45 minut

Efekty uczenia się dla kierunku

Kod	Treść
INF_K3_U05_inz	Absolwent/ka potrafi pisać, uruchamiać i testować programy w wybranym środowisku programistycznym
INF_K3_U06_inz	Absolwent/ka potrafi ocenić, na podstawowym poziomie, przydatność metod i narzędzi informatycznych oraz wybrać i zastosować właściwą metodę i narzędzia do typowych zadań informatycznych
INF_K3_U07_inz	Absolwent/ka potrafi zastosować wybrane metody wykorzystywane w wiodących kierunkach badań informatyki
INF_K3_W01	Absolwent/ka zna i rozumie zaawansowane pojęcia z działów matematyki służące do modelowania i rozwiązywania problemów w informatyce
INF_K3_W02	Absolwent/ka zna i rozumie zaawansowane pojęcia i problemy formujące kanon dyscypliny informatyka
INF_K3_W03	Absolwent/ka zna i rozumie narzędzia, technologie i urządzenia informatyczne właściwe dla wybranych obszarów zastosowań oraz podstawy ich działania
INF_K3_W04_inz	Absolwent/ka zna i rozumie zaawansowane pojęcia, konstrukcje i procesy związane z językami programowania i inżynierią programowania
INF_K3_W06_inz	Absolwent/ka zna i rozumie zaawansowane pojęcia związane z informatyczną architekturą sprzętowo-programową
INF_K3_W07	Absolwent/ka zna i rozumie zaawansowane pojęcia związane z technologiami sieciowymi, bezpieczeństwem i protokołami kryptograficznymi