KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu
Ataki typu Side-channel

Przedmiot

Kierunek studiów
Informatyka

Rok/semestr
1/2

Studia w zakresie (specjalność)
Cyberbezpieczeństwo

Profil studiów
ogólnoakademicki

Poziom studiów
drugiego stopnia

Język oferowanego przedmiotu
angielski

Forma studiów
stacjonarne

Wymagalność
obieralny

Liczba godzin

Wykład	Laboratoria	Inne (np. online)
15	15	
Ćwiczenia	Projekty/seminaria	

Liczba punktów ECTS

2

Wykładowcy

Odpowiedzialny za przedmiot/wykładowca:
dr inż. Marek Michalski
marek.michalski@put.poznan.pl
tel: 61 665 39 06
Wydział Informatyki i Telekomunikacji
Instytut Sieci Teleinformatycznych

Odpowiedzialny za przedmiot/wykładowca:

Wymagania wstępne

Student ma podstawy elektroniki, sieci komputerowych, programowania i systemów operacyjnych

Student posiada umiejętność samodzielnego znajdowania źródeł informacji i oceny ich przydatności

Student posiada umiejętność samodzielnego pozyskiwania wiedzy ze wskazanych oraz samodzielnie znalezionych źródeł

Cel przedmiotu

Przedstawienie studentom natury systemów przetwarzania informacji, sposobów komunikacji i wykorzystywanych mechanizmów w aspekcie bezpieczeństwa

Omówienie możliwych do realizacji ataków, ich skutków, zakresów i sposobów zabezpieczenia na praktycznych przykładach

Przedmiotowe efekty uczenia się

Wiedza

Student zna mechanizmy, na bazie których funkcjonują omawiane systemy

Umiejętności

Student umie analizować przedstawione mechanizmy, rozumie ich działanie, potrafi znaleźć i poprawić słabości

Kompetencje społeczne

Student ma świadomość postępu i potrzeby kształcenia się i uaktualniania wiedzy w zakresie bezpieczeństwa

Metody weryfikacji efektów uczenia się i kryteria oceny

Efekty uczenia się przedstawione wyżej weryfikowane są w następujący sposób:

Pisemny test, próg do zaliczenia konieczny to 51% zdobytych punktów

Treści programowe

Kategoryzacja ataków i naruszeń bezpieczeństwa

Mechanizmy ataków (ograniczone ataków typu do Side Channel)

Analiza - wybrane przykłady urządzeń

Kto popełnił błąd, czy można było go uniknąć, jak zrobić to lepiej

Fizyczność a programowalność urządzeń

Obszary podatności SCA – urządzenia powszechnego użytku

Sposoby realizacji funkcjonalności urządzeń a podatności bezpieczeństwa

Podatności sieci (telekomunikacyjnych, energetycznych, bankowych, trakcyjnych, różnych mediów)

Sposoby analizy urządzeń i odkrywanie ich podatności

Automatyzacja analizy podatności na etapie projektu, prototypu, produktu

Konsekwencje kompatybilności wstecznej

Uwarunkowania historyczne, prawne, społeczne

Sposoby i narzędzia zapobiegania SCA

Sposoby i narzędzia monitorowania podatności na i wykrywanie SCA

W ramach wykładu będzie spotkanie z profesjonalnymi konstruktorami urządzeń i rozmowa na tematy analizy i zapewnienia bezpieczeństwa ich produktów

Laboratorium

Zapoznanie się z platformą laboratoryjną do badania i analizy ataków typu Side Channel.

Działania na systemie Linux, debuger realnych przykładowych systemów,

Analiza sprzętu na poziomie elektrycznym, użycie programowych i sprzętowych analizatorów urządzeń

Analiza pasma radiowego

Pomiary realnych urządzeń testowych

Projektowanie bezpiecznych urządzeń, analiza poziomu ich bezpieczeństwa

Metody dydaktyczne

Wykład konwersatoryjny z udziałem studentów,

Laboratorium z samodzielną i analizą omawianych przykładów

Literatura

Podstawowa

Omar Santos, CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide, Cisco Press, Hoboken, NJ, 2021

Uzupełniająca

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	50	2,0
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	30	1,5
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwiów/egzaminu, wykonanie projektu)[1]	20	0,5

[1] niepotrzebne skreślić lub dopisać inne czynności