



KARTA OPISU PRZEDMIOTU - SYLABUS

Nazwa przedmiotu

Ataki typu Side-channel [S2Inf1E-CYB>SCHA]

Przedmiot

Kierunek studiów

Informatyka/Computing

Rok/Semestr

1/2

Studia w zakresie (specjalność)

Cyberbezpieczeństwo

Profil studiów

ogólnoakademicki

Poziom studiów

drugiego stopnia

Język oferowanego przedmiotu

angielski

Forma studiów

stacjonarne

Wymagalność

obligatoryjny

Liczba godzin

Wykład

15

Laboratorium

15

Inne

0

Ćwiczenia

0

Projekty/seminaria

0

Liczba punktów ECTS

2,00

Koordynatorzy

dr inż. Marek Michalski

marek.michalski@put.poznan.pl

Wykładowcy

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 (Tabela MITRE)

Mechanizmy ataków typu do Side Channel

Analiza - wybrane przykłady urządzeń, Kto popełnił błąd, czy można było go uniknąć, jak zrobić to lepiej

Analiza mocy (podstawowa, różnicowa korelacyjna - SPA, DPA/CPA)

Fizyczność a programowalność urządzeń (FPGA)

Trojany sprzętowe, Szyfrowanie logiki, piractwo, fałszerstwa układów scalonych

Funkcje bezpieczeństwa (Physical Unclonable Functions)

Obszary podatności SCA – urządzenia powszechnego użytku, znane CVE

Fault Injection, Glitching

Sposoby realizacji funkcjonalności urządzeń a podatności bezpieczeństwa

Automatyzacja analizy podatności na etapie projektu, prototypu, produktu

Testowanie (elementy Design for Testing - DFT)

Bezpieczny firmware - jak przygotować

Konsekwencje kompatybilności wstecznej

Sposoby i narzędzia zapobiegania SCA

Analiza przykładowych ataków na sprzęt - konsola XBOX, FPGA ZYNQ, Starlink

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, debugger realnych przykładowych systemów,

przykładowe wykorzystanie Xilinx ISE do przygotowania kompletnego układu sprzętowego i jego analiza

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

Glitching + fault injection

Analiza mocy w celu wymuszenia wycieku danych

Analiza pasma radiowego wokół pracującego urządzenia

Pomiary realnych urządzeń testowych, przykładowe ataki

Projektowanie bezpiecznych urządzeń, analiza poziomu ich bezpieczeństwa

Tematyka zajęć

brak

Metody dydaktyczne

Wykład konwersatoryjny z udziałem studentów,

Laboratorium z samodzielną pracą i analizą omawianych przykładów

Literatura

Podstawowa

Side-Channel Analysis of Embedded Systems; Maamar Ouladj. Sylvain Guilley Springer 2021 (open access)

Power Analysis attacks; Mangard, Oswald, Popp, Springer 2007 (open access)

Uzupełniająca

Bilans nakładu pracy przeciętnego studenta

	Godzin	ECTS
Łączny nakład pracy	50	2,00
Zajęcia wymagające bezpośredniego kontaktu z nauczycielem	30	1,50
Praca własna studenta (studia literaturowe, przygotowanie do zajęć laboratoryjnych/ćwiczeń, przygotowanie do kolokwium/egzaminu, wykonanie projektu)	20	0,50