



Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Bc. Dennis Vita
Študijný program: informatika (Jednoodborové štúdium, magisterský II. st., denná forma)
Študijný odbor: informatika
Typ záverečnej práce: diplomová
Jazyk záverečnej práce: slovenský
Sekundárny jazyk: anglický

Názov: Hardvérové MITM útoky na komunikáciu po zberniciach
Hardware MITM attacks on communication buses

Anotácia: Mnohé dnešné hardvérové zariadenia pozostávajú z viacerých integrovaných obvodov, ktoré sú navzájom prepojené komunikačnými zbernicami (napríklad I²C alebo SPI). Z bezpečnostného hľadiska je dôležité vedieť, aká komunikácia na týchto zberniciach prebieha. Podľa toho je možné posúdiť, napríklad či je takýmto spôsobom možné odpočúvať dôverné dáta (napríklad heslá, šifrovacie kľúče). Ďalším zaujímavým aspektom je aktívne zasahovanie do komunikácie, napríklad za účelom zmeny konfiguračných parametrov.

Preto je cieľom práce preskúmať možnosti implementácie hardvérového FPGA „Man-in-the-middle“ (MITM) útoku na komunikačné zbernice prepájajúce rôzne integrované obvody (napríklad EEPROM). Ďalším krokom je implementácia na FPGA, ktorá by po pripojení na zbernicu dokázala v reálnom čase zaznamenávať komunikáciu oboch strán a takisto v reálnom čase aktívne zasahovať do prebiehajúcej komunikácie. Po implementácii je ďalším cieľom práce experimentálne overenie, ako výpočtovo zložité zásahy do komunikácie a jej sledovanie sa budú dať realizovať v reálnom čase na implementovanom riešení.

Vedúci: RNDr. Richard Ostertág, PhD.
Katedra: FMFI.KI - Katedra informatiky
Vedúci katedry: prof. RNDr. Martin Škoviera, PhD.

Spôsob prístupnosti elektronickej verzie práce:
bez obmedzenia

Dátum zadania: 05.12.2023

Dátum schválenia: 03.01.2024

prof. RNDr. Rastislav Kráľovič, PhD.
garant študijného programu

.....
študent

.....
vedúci práce