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: V súčasnosti mnohé hardvérové zariadenia obsahujú viacero integrovaných obvodov, ktoré sú vzájomne prepojené komunikačnými zbernicami, ako napríklad UART alebo SPI. Z bezpečnostného hľadiska je nevyhnutné analyzovať komunikáciu prebiehajúcu na týchto zberniciach, keďže môže dochádzať k úniku citlivých údajov, ako sú heslá či šifrovacie kľúče. Osobitnú pozornosť si vyžaduje aj aktívne zasahovanie do komunikácie, ktoré môže viesť k zmene konfiguračných parametrov alebo iným bezpečnostným incidentom.

Cieľom práce je preskúmať možnosti implementácie hardvérového útoku typu „Man-in-the-Middle“ (MITM) na báze FPGA v kontexte komunikačných zberníc prepájajúcich rôzne integrované obvody, napríklad modul TPM a procesor. Práca sa zameria na návrh a implementáciu takéhoto útoku na platformách iCEstick alebo iCE40-HX8K FPGA. Implementované riešenie by malo umožňovať aktívne zasahovanie do prebiehajúcej komunikácie v reálnom čase, pričom dôraz bude kladený na jeho univerzálnosť, aby bolo možné jednoduchým spôsobom podporovať rôzne protokoly a typy útokov. Záverečná fáza práce bude zahŕňať experimentálne overenie použiteľnosti riešenia prostredníctvom demonštrácie aspoň dvoch útokov typu MITM.

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

Spôsob sprístupnenia 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