



ZADANIE ZÁVEREČNEJ PRÁCE

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

Názov: Útoky na hardvér pomocou indukovania chýb
Attacking hardware using fault injection

Anotácia: Pomocou externých faktorov je možné ovplyvniť správanie hardvéru až do takej miery, že nekorektne vykoná nejakú operáciu. Takýmto spôsobom je možné zmeniť hodnoty prečítaných príznakov alebo cieľovú adresu skokov, či výsledky iných operácií. Toto neštandardné správanie je potom možné využiť na cielený útok na zvolený hardvér. Medzi tieto externé vplyvy patria napríklad zmena napájania (obvykle podpätie) alebo elektromagnetické rušenie.

Cieľom práce je zozbierať, podrobne popísať (vrátane potrebných zapojení, nástrojov, ...) a prakticky vyskúšať rôzne útoky. Napríklad:

- prečítanie obsahu pamäte s firmvérom aj pri zapnutej ochrane pred čítaním (code read protection)
- rôzne možnosti ovplyvnenia vykonávanie algoritmov (napríklad ovplyvnenie podmienených skokov, výsledkov matematických a logických operácií)

Výsledkom práce by malo byť aj overenie ako veľmi záleží na presnosti a časovaní pri takýchto útokoch na rôzny hardvér (napríklad Arduino, STM32) a či treba pri implementácii využiť rýchlosť a presnosť FPGA.

Ďalším cieľom práce je príprava nových úloh do súťaží typu Capture The Flag (CTF). Úlohy by pozostávali zo zadania, vzorového riešenia (zapojenie, program, obrázky, prípadne aj video riešenie).

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: 30.09.2022

Dátum schválenia: 05.10.2022

doc. RNDr. Dana Pardubská, CSc.
garant študijného programu

.....
študent

.....
vedúci práce