FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Jiří Buček, Ph.D.
Student:	Jakub Kučera
Název práce:	Aktivní neinvazivní útok na mikrokontroler vkládáním poruch
Obor / specializace:	Informační bezpečnost 2021
Vytvořeno dne:	10. června 2024

Hodnotící kritéria

1. Splnění zadání

- ▸ [1] **zadání splněno**
  [2] zadání splněno s menšími výhradami
  [3] zadání splněno s většími výhradami
  [4] zadání nesplněno

Student splnil zadání bez výhrad.

2. Písemná část práce 94 /100 (A)

Studentova práce je psána čtivou angličtinou, struktura práce je přehledná a logicky členěná. Po věcné stránce nemám výraznější připomínky, student postupoval systematicky a pečlivě. Relevantní zdroje student z velké části nastudoval samostatně a cituje je korektně.

3. Nepísemná část, přílohy 98 /100 (A)

Student vytvořil jednak HW architekturu v použité FPGA desce včetně periferie pro generování pulzů (ve Verilogu), a také SW pro vložený soft-procesor Microblaze (v C). Dále vytvořil řídicí program pro PC (v Pythonu) a několik Jupyter notebooků realizujících různé druhy útoku vkládáním poruch a analýzu pořízených dat pro zjištění klíče.

4. Hodnocení výsledků, jejich využitelnost 98 /100 (A)

Studentova práce je velice užitečná pro výuku a experimenty v hardwarové bezpečnosti. Díky studentově řešení můžeme využít existující FPGA desky Digilent CMOD S7 pro řízení vkládání poruch, přičemž máme detailní kontrolu nad časováním pulzů a řízením celého útoku. Student svou práci již testoval při výuce předmětu NI-HWB Hardwarová bezpečnost (i když zatím v omezeném rozsahu). Po výrobě odpovídajícího počtu desek s cílem (obětí)

útoku bude možno tento typ útoku demonstrovat při výuce s aktivnější participací studentů.

5. Aktivita studenta

- [1] **výborná aktivita**
- [2] velmi dobrá aktivita
- [3] průměrná aktivita
- [4] slabší, ale ještě dostatečná aktivita
- [5] nedostatečná aktivita

6. Samostatnost studenta

- [1] výborná samostatnost
- [2] **velmi dobrá samostatnost**
- [3] průměrná samostatnost
- [4] slabší, ale ještě dostatečná samostatnost
- [5] nedostatečná samostatnost

Celkové hodnocení

98 /100 (A)

Student prokázal schopnost samostatné tvůrčí práce a zvládl poměrně náročnou kombinaci návrhu SW, HW (v FPGA) a kryptoanalýzy. Jeho práci hodnotím jako výbornou.

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.