FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Petr Socha
Oponent práce:	Dr.-Ing. Martin Novotný
Název práce:	Software toolkit for side-channel attacks
Obor:	Návrh a programování vestavných systémů

Datum vytvoření: 18. 1. 2019

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
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.

Komentář:
Autor beze zbytku splnil zadání. Do statistické analýzy začlenil mj. nástroj, který publikoval v [26], a tak samotný výpočet běhá svizně. Vyhodnocení matice korelačních koeficientů provádí mj. nástrojem, který publikoval v [19] a který výrazně zvyšuje úspěšnost útoku i v zarušeném prostředí. Další publikace se připravují.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*85 (B)*

Popis kritéria:
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. 26/2017, 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.

Komentář:
Práce je logicky členěná a dobře čitelná. Úroveň angličtiny je vysoká. Práce obsahuje pouze drobné překlepy - například se domnívám, že se nepíše "it's", ale "its", pokud se jedná o přivlastňovací zájmeno ("it's" znamená "it is" a ve formálním textu by i toto mělo být rozepsáno). V práci jsem ale nenašel zmínku o provedených testech jím vytvořeného díla, přestože je autor jistě provedl.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*100 (A)*

Popis kritéria:
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

Komentář:
Vytvořený programový balík je značně rozsáhlý. Dobrým rozhodnutím bylo zvolení modulární koncepce celého programového balíku formou plug-inů.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*100 (A)*

Popis kritéria:
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.

Komentář:
Dílo (nebo jeho některé moduly) bude nasazeno ve výuce předmětu MI-BHW.16 Bezpečnost a technické prostředky. Dále se bude používat při experimentech ve výzkumu Katedry číslicového návrhu. Některé moduly byly již použity, například kolegou Brejníkem při tvorbě jeho diplomové práce.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*

5. Otázky k obhajobě

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
Jaké testy jste provedl?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*

6. Celkové hodnocení

100 (A)

Popis kritéria:
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.

Text hodnocení:
Zadání práce vyžadovalo od studenta hluboké znalosti z několika oblastí - číslicového návrhu, kryptografie, kryptoanalýzy, statistiky a softwarového inženýrství. Dílčí výsledky práce byly přijaty k publikaci na prestižních mezinárodních konferencích. V současné době probíhá recenzní řízení časopisecké publikace. Přestože v textu práce chybí pasáž o provedených testech, nezbývá mi nežli hodnotit práci nejvyšší známkou. Zároveň si dovoluji komisi doporučit, aby práci nominovala na cenu děkana.

Podpis oponenta práce: