



Hodnocení vedoucího závěrečné práce

Student: Bc. Petr Socha
Vedoucí práce: Ing. Vojtěch Miškovský
Název práce: Software toolkit for side-channel attacks
Obor: Návrh a programování vestavných systémů

Datum vytvoření: 10. 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: Student bez výhrad splnil všechny body zadání. Nad rámec zadání navíc implementoval možnost vyhodnocování spotřeby pomocí TVLA.	
Hodnotící kritérium:	Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):
2. Písemná část práce	98 (A)
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: Rozsah písemné zprávy je více než dostatečný. Informační hustota textu je velmi vysoká. Práce je logicky velmi dobře uspořádaná. K formálním zápisům v práci nemám výhrady. Typografická i jazyková stránka je na vysoké úrovni, oceňuji především použití angličtiny. Student využívá velké množství relevantních zdrojů, úroveň práce s citacemi je mimořádná. Jedinou výtka bych měl k tomu, že se autor příliš nehlasí k tomu, že některé citované zdroje jsou jeho vlastními (kvalitními) publikacemi.	
Hodnotící kritérium:	Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):
3. Nepísemná část, přílohy	99 (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: Kvalita a rozsah programové části jsou mimořádné. Student pro splnění požadavku rozšiřitelnosti a univerzálnosti zvolil možnost využití plug-inů, k čemuž využil framework Qt, což považuji za dobrou volbu. Zdrojové kódy jsou velice přehledné, místy možná trochu méně komentované. Dokumentace je kvalitně zpracovaná.	
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:

Realizovaný toolkit bude již v následujícím semestru využíván pro výzkumné i výukové účely. Dílčí výsledky práce byly již úspěšně publikovány ve formě dvou příspěvků na mezinárodních konferencích, jeden byl dokonce vyzván k rozšíření na časopiseckou publikaci (ta nyní prochází recenzními řízeními). Toolkit bude dále prezentován na tematických workshopech, kde má potenciál oslovit vědeckou komunitu hardwarové bezpečnosti.

Hodnotící kritérium:

Způsob hodnocení – následující škálou 1 až 5:

5. Aktivita a samostatnost studenta

5a:

1=výborná aktivita,
2=velmi dobrá aktivita,
3=průměrná aktivita,
4=slabší, ale ještě dostatečná aktivita,
5=nedostatečná aktivita

5b:

1=výborná samostatnost,
2=velmi dobrá samostatnost,
3=průměrná samostatnost,
4=slabší, ale ještě dostatečná samostatnost,
5=nedostatečná samostatnost

Popis kritéria:

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 (5a). Posuďte schopnost studenta samostatně tvůrčí práce (5b).

Komentář:

Student prokázal výbornou samostatnost, která byla bohužel srážena jeho prokrastinací. Na kvalitu řešení však studentova (ne)aktivita neměla negativní vliv. Všechny důležité kroky konzultoval student s vedoucím práce.

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 této práce bylo mimořádně náročné. Student musel prokázat velice široké spektrum znalostí od softwarového návrhu přes hardwarovou bezpečnost až po pokročilou statistiku. Studentovi se všechny tyto znalosti povedlo zdárně skloubit a vytvořil velice kvalitní nástrojovou sadu, kterou v textu práce kvalitně zdokumentoval. Jeho práce bude využívána pro výzkum a výuku. Dílčí výsledky práce již prošly recenzními řízeními a byly publikovány na mezinárodních konferencích. Na základě těchto faktů mi nezbývá než doporučit práci nejen k obhajobě se známkou A, ale také na cenu děkana.

Podpis vedoucího práce: