FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Ing. Jiří Buček, Ph.D.
Student:	Bc. František Kovář
Název práce:	Útoky postranními kanály na Supersingular Isogeny Diffie–Hellman Key Exchange
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	22. srpna 2022

Hodnotící kritéria

1. Splnění zadání

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

Zadání bylo splněno s výhradou, že do odevzdání práce student neodstranil všechny chyby, a v důsledku toho byl vlastní útok neúspěšný. V době psaní posudku však student již podstatné chyby v kódu opravil a ukázal úspěšný útok.

2. Písemná část práce 70/100 (C)

Písemná část práce je stručná ale přehledná. Stručnost práce je bohužel občas na úkor srozumitelnosti a úplnosti popisu jak principu samotného algoritmu, tak i útoků. Zvolené téma je značně komplexní a student si v závěru práce nenechal dost času, a tím utrpěla kvalita textu.

3. Nepísemná část, přílohy 80/100 (B)

Přílohou jsou zejména výsledky experimentů ve formě měření a analytických programů pro výpočet hypotéz a vyhodnocení klíče z měření. Přiložena jsou rovněž měřená data.

4. Hodnocení výsledků, jejich využitelnost 80/100 (B)

Výsledky práce jsou využitelné jako základ pro další výzkum a vývoj v této oblasti.

5. Aktivita studenta

[1] výborná aktivita

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

Student začal s tématem pracovat relativně pozdě. S tím, jak se blížil termín odevzdání a zbývající čas klesal k nule, rostla opět studentova aktivita nade všechny meze.

6. Samostatnost studenta

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

Student pracoval zcela samostatně, v případě potřeby svoji práci konzultoval.

Celkové hodnocení 80 /100 (B)

Student prokázal schopnost samostatné tvůrčí práce. Nedostatek času se projevil sníženou kvalitou textové části práce a tím, že první verze jeho útoku nefungovala. Od té doby student opravil chyby ve svém kódu a předvedl funkční útok. Vzhledem k tomu a ke značné obtížnosti tématu hodnotím ještě známkou velmi dobře.

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.