FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

# Posudek oponenta závěrečné práce

| | |
|---|---|
| **Oponent práce:** | Ing. Filip Kodýtek, Ph.D. |
| **Student:** | Marek Bizík |
| **Název práce:** | Demonstrace metod analýzy postranních kanálů |
| **Obor / specializace:** | Bezpečnost a informační technologie |
| **Vytvořeno dne:** | 12. června 2023 |

## Hodnotící kritéria

### 1. Splnění zadání

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

Základní podobu zadání student splnil, práce však obsahuje řadu nedostatků souvisejících právě s kvalitou splnění zadání.

### 2. Písemná část práce 60 / 100 (D)

Práce je velmi stručná a krátká, což nemusí nutně být problém, zde je ale vynechána spousta podstatných věcí. Šifra AES (na kterou je prováděn útok) je popsána velmi krátce, je zde jen náznak jejího popisu. Podstatné by zde měly být ale především 3 různé metody útoku, které byly prováděny - i ty jsou nevysvětlené. Např. u útoků pomocí šablon nebo náhodného lesa jsou popisy jen textové bez detailnějšího vysvětlení a tudíž velmi nepřehledné a pro čtenáře nepochopitelné. Chybí jejich matematický popis, neuškodil by také předcházející popis notace. Problém nepřehlednosti a nejasnosti popisu různých metodik, volby parametrů, provedení experimentů atd. provází práci po celou dobu.

### 3. Nepísemná část, přílohy 70 / 100 (C)

Chybí zde lepší popis/komentáře popisující jednotlivé skripty (resp. Jupyter notebooky), popřípadě sjednocující text popisující co jednotlivé části SW dělají pro snadnější orientaci. V experimentální části není řečeno na kolika různých deskách byla měření prováděna, předpokládám, že pouze na jednom CW Lite (resp. Nano, které pak ale bylo nahrazeno). Z pohledu toho, že byly prováděny profilovací útoky, jejichž výhoda je právě v tom, že útočník může "trénovat" na jednom zařízení pod vlastní kontrolou a následně útočit na jiné se stejným HW, jako podstatný nedostatek. Mělo by zde být demonstrováno,

že profilovací útok je použitelný nejen na zařízení, na kterém byla samotná profilace provedena.

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

Práci lze využít jako základ pro vytvoření úlohy ve výuce hardwarové bezpečnosti nebo pro další experimenty a výzkum v oblasti útoků postranními kanály.

## Celkové hodnocení 65 /100 (D)

Práci doporučují k obhajobě, ale kvůli výše zmíněným nedostatkům hodnotím stupněm D.

## Otázky k obhajobě

Můžete více popsat proč byl nutný přechod na CW Lite kvůli útoku pomocí náhodného lesa, když u ostatních postačilo CW Nano?
Proč nebyl útok proveden na více zařízeních (zejména v případě profilovaných útoků)?

# 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.

## 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.