FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Jakub Klemsa
Student:	Tereza Horníčková
Název práce:	Odběrová analýza kryptografického procesoru CEC 1702
Obor / specializace:	Počítačové inženýrství
Vytvořeno dne:	25. května 2022

Hodnotící kritéria

1. Splnění zadání

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

Cíle práce byly jasně formulovány a také bez výhrad splněny. Pozitivně hodnotím vymezení i následné provedení průzkumné činnosti na "bojišti": tak se o práci s některými nedotaženými vývojovými přípravky rozhodně dá mluvit.

2. Písemná část práce 65 /100 (D)

Rozsah ZP je informačně přiměřený obsahu, bez věcných nepřesností. Tok myšlenek je logický, strukturování je však místy poněkud nešťastné: hlavně jednostránková kapitola 4, celkově hodně nadpisů, dále prohozené pořadí obrázků 2.6 a 2.7, apod. Text je převážně srozumitelný, avšak dosti strohý, místy také pokulhává gramatika/stylistika: obzvláště věty bez přísudku v páté kapitole, dále kvalitě textu ubírají některé těžkopádné větné konstrukce, chybějící čárky, apod. Po typografické stránce vesměs v pořádku, až na některé přetečené řádky, zápis citací, písmenko X místo odpovídajícího znaku, apod. Citace a použití softwaru jsou provedeny v souladu s pravidly a zvyklostmi.

3. Nepísemná část, přílohy 90 /100 (A)

Pilířem této ZP je právě experimentální práce, která se sestává ze dvou částí: (i) výběr vhodného prostředí a "rozdýchání" vybraných mikrokontrolérů, a (ii) provedení a zpracování útoků postranním kanálem.

Díky výsledkům práce provedené v kroku (i) je možné podobné experimenty s vybranou platformou o mnoho snadněji reprodukovat. Na základě popisu některých vyvstanuvších překážek měl však tento krok blíže k detektivní, než k inženýrské činnosti: některé

objevené nedostatky ve zkoumaných technologiích se dají označit až za amatérské. Přesto tyto překážky nezanechaly znatelný vliv na množství odvedené práce.

Obsahem přiložené SD karty jsou použité skripty včetně zachycených powertraců v kroku (ii), díky kterým je možné tyto experimenty zopakovat a případně i rozšířit. Slabší stránkou je struktura přiložených dat pro případné pokračování třetí stranou.

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

Výsledky práce přinášejí potenciál budoucího využití, především k výzkumu útoků postranním kanálem na mikrokontroléru CEC1702, který byl poněkud těžko uchopitelný.

Celkové hodnocení 75 /100 (C)

Na celkovém hodnocení se nejvíce podepisují dvě stránky věci: (i) provedená experimentální činnost, a (ii) text samotné práce.

Ad (i) experimentální činnost:
+ průzkum "bojiště" (např. problémy s EFUSE potvrzeny i ze strany NewAE, objevení až neuvěřitelných záludností/chyb v jednom z vývojových prostředí),
+ volná licence díla,
+ množství otestovaných kombinací (2 mikrokontroléry, 2 měřicí soupravy),
- některá rozhodnutí nedostatečně okomentovaná.

Ad (ii) text práce:
+ logická návaznost,
- strohý text a další dříve popsané formální nedostatky.

Celkově navrhuji hodnocení C.

Otázky k obhajobě

1) Kap. 1.2: Popište v jednoduchosti rozdíl mezi DPA a CPA. Je jedno podmnožinou druhého?
2) Kap. 5.2.2: Jaké rozhodnutí stálo za použitím 13 000 powertraců v případě (jen částečně úspěšného) útoku pomocí Chip Whispereru na naivní implementaci AES spuštěné na CEC1702? Pro HW variantu máte přitom naměřené desítky/stovky milionů traců.
3) Kap. 5.3.3: Pokud je pravděpodobnost správného uhodnutí jednoho bitu klíče 50% (tedy zcela náhodné hádání), dostaneme ve střední hodnotě 64 bitů ze 128 špatně. Jaká by musela být tato pravděpodobnost, aby byl střední počet špatně uhodnutých bitů 55, tak jako ve Vašich výsledcích? Dotaz nijak nerozporuje tvrzení o neúspěchu tohoto útoku.

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.