FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Jakub Klemsa
Student:	Lukáš Daněk
Název práce:	Implementace Paillierova kryptosystému a útok injekcí chyb na procesoru CEC 1702
Obor / specializace:	Počítačové inženýrství
Vytvořeno dne:	27. 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

Předložená ZP jasně vymezuje cíle a také je bez výhrad naplňuje. Množství odvedené práce a provedených experimentů hodnotím jako práci nad rámec zadání, týká se též řešení vyvstanuvších komplikací.

2. Písemná část práce 90/100 (A)

I přes velký rozsah práce (72 stran textu!) je její obsah informačně nabitý a celou dobu velmi poutavý. Po věcné stránce je práce z mé strany bez výhrad (když nepočítám jeden překlep na str. 8, $r < n$ namísto $r < m$). Také členění práce do kapitol odpovídá logickým celkům odvedené práce. Po jazykové stránce je práce též v pořádku (jen pár drobností), typograficky je práce také na velmi dobré úrovni (vytknout by se daly tečky za popisky obrázků). Za nedostatek práce považuji chybějící číslování rovnic, na které tak nejde odkazovat. Citace a použití softwaru jsou provedeny v souladu s pravidly a zvyklostmi.

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

Prvním krokem studenta bylo seznámení se s existujícím SW a HW, a naučit se s ním pracovat. Vzhledem k některým až amatérským výtvorům nejmenovaných firem byl tento krok podle všeho velmi náročný, student si s ním přesto velmi elegantně poradil (např. část 2.3.4 věnující se vlastnímu způsobu naflashování). V dalších krocích se věnoval jednak dotažení existujících implementací, tak útokům na ně, oboje se objevuje ve velmi dobré a znovupoužitelné kvalitě na přiloženém elektronickém nosiči.

4. Hodnocení výsledků, jejich využitelnost 100 /100 (A)

Vedle zprovoznění a dotažení existujících implementací představuje práce úspěšný útok na RSA pomocí Fault Injection: a to jak na SW variantu na dvou mikrokontrolérech, tak na HW variantu na mikrokontroléru CEC1702. Přestože se jedná o velmi dobře popsaný a známý útok, podle poznatků této práce se před ním HW akcelerátor použitý na CEC1702 nijak nechrání. Díky popisu celého toolchainu a zdrojovým kódům k útokům je možné na útoku dále stavět a zdokonalovat ho, případně ho přidat mezi oficiální existující příklady útoku, nebo ho převzít do laboratorních cvičení.

Celkové hodnocení 95 /100 (A)

Tato práce zaujme hlavně nebývalým rozsahem a množstvím dílčích netriviálních problémů, které bylo potřeba vyřešit k úspěšnému splnění zadání. I přes velký rozsah zadání si s ním student skvěle poradil a odevzdal velmi obsáhlou a poutavou práci.

Celkově navrhuji hodnocení A.

Otázky k obhajobě

1) V práci zmiňujete RSA padding. Velmi stručně okomentujte jeho důležitost.
2) Kap. 1.2.1.1, poslední rovnice: vysvětlete, co znamená v této rovnici operace dělení následovaná modulem? (Tady by se hodily ty číslované rovnice...)
3) Str. 36: "Autor předpokládá, že je funkce (rsa_encrypt(), pozn. JK) zabezpečená proti útokům postranními kanály (oproti funkci rsa_modular_exp())". Na základě čeho byl vytvořen tento předpoklad? Funkce rsa_encrypt() přeci pracuje s veřejným klíčem. (V experimentální části už útočíte logicky na rsa_crt_decrypt(), která by být zabezpečená měla, protože pracuje se soukromým klíčem.)
4) Našel jste v literatuře FI útok na RSA akcelerátor na CEC1702?

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.