FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Dr.-Ing. Martin Novotný
Student:	Lukáš Daněk
Název práce:	Implementace Paillierova kryptosystému a útok injekcí chyb na procesoru CEC 1702
Obor / specializace:	Počítačové inženýrství
Vytvořeno dne:	1. června 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 zpráva reprezentuje obrovské množství práce provedené za cca 21 měsíců. Předtím, než bylo vůbec možné přistoupit k samotné práci, bylo nutné objevit a obejít chyby ve vývojovém prostředí mikroC pro for ARM, které, bohužel, je v současné době jediným prostředím pro vývoj firmware pro procesor CEC1702.
Následně autor provedl doladění kryptografické knihovny bigi a úpravu programu pro Paillierův algoritmus. Všechny funkcionality byly ověřeny proti skriptům v Ruby, které byly dodány třetí stranou.
V další části práce se autor zabývá útokem na RSA-CRT. Vzhledem k tomu, že se mu podařilo úspěšně zaútočit i na vestavěný hardwarový akcelerátor RSA, můžeme očekávat i úspěšný útok na Paillierův algoritmus ve verzích založených na CRT (tj. jak čistě softwarové, tak využívající hardwarový akcelerátor).

2. Písemná část práce 98 / 100 (A)

Práce je přehledně členěná, text je srozumitelný a je obsahově velmi bohatý. Vzhledem k množství odvedené práce (v podstatě se jedná o dvě samostatné práce) text přesahuje horní doporučenou mez.

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

Přiložené paměťové médium obsahuje jak původní verzi knihovny bigi a Paillierova algoritmu, tak aktuální verzi obou. Čtenář může snadno provést diferenci, aby zjistil rozsah provedených prací (a to včetně úprav nutných vzhledem k chybovosti překladače

mikroC - kód obahuje příslušná varování). Podobné je to v případě dalšího vyvinutého firmware a software pro prováděné útoky injekcí chyb.

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

Práce se skládá ze dvou částí:
1) Knihovna bigi a Paillierův algoritmus byly dotaženy do funkční podoby. Knihovna a program byly upraveny tak, aby byly použitelné i na procesoru CEC1702 za použití vývojového prostředí mikroC pro for ARM. Knihovnu lze nyní publikovat.
2) Byly provedeny útoky injekcí chyb na procesory STM32 a CEC1702. Útoky na RSA, variantu využívající CRT, byly úspěšné i tehdy, kdy byl na CEC1702 použit vestavěný kryptografický akcelerátor. Zdá se tedy, že návrháři akcelerátoru RSA nevěnovali řádnou pozornost ochraně proti tomuto typu útoku. Tato skutečnost nebyla zřejmě zatím nikde publikována.

5. Aktivita studenta

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

Scházeli jsme se na pravidelných týdenních schůzkách.

6. Samostatnost studenta

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

Bez výhrad.

Celkové hodnocení 99 /100 (A)

Práce se skládá ze dvou částí:
1) Knihovna bigi a Paillierův algoritmus byly dotaženy do funkční podoby. Knihovna a program byly upraveny tak, aby byly použitelné i na procesoru CEC1702 za použití vývojového prostředí mikroC pro for ARM. Knihovnu lze nyní publikovat.
2) Byly provedeny útoky injekcí chyb na procesory STM32 a CEC1702. Útoky na RSA, variantu využívající CRT, byly úspěšné i tehdy, kdy byl na CEC1702 použit vestavěný kryptografický akcelerátor. Zdá se tedy, že návrháři akcelerátoru RSA nevěnovali řádnou pozornost ochraně proti tomuto typu útoku. Tato skutečnost nebyla zřejmě zatím nikde publikována.
Vzhledem k rozsahu, novátorství a kvalitě práce si dovoluji komisi doporučit, aby zvážila navržení předložené práce na cenu děkana.

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.