FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Martin Heinrich
Oponent práce:	Ing. Josef Kokeš
Název práce:	Útok postranním kanálem na šifru ChaCha
Obor:	Bezpečnost a informační technologie

Datum vytvoření: 3. 6. 2018

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
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.

Komentář:
Zadání bylo splněno - student naimplementoval šifru ChaCha na čipu AVR a zaútočil na ni technikou diferenciální odběrové analýzy. Provedl sadu experimentů zaměřených na odhalení klíče a tyto experimenty interpretoval. Na bakalářské úrovni jde o velmi pěkný výsledek.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*80 (B)*

Popis kritéria:
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. 26/2017, 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.

Komentář:
Písemná část práce je přiměřeně rozsáhlá a bez gramatických chyb. Posloupnost kroků je logicky zdůvodněna a práce se snadno čte. Dobrý dojem kazí několik zbytečných technických nedostatků, jako je nesouhlasící značení v listingu 1 a 2, neseřazený seznam zkratek nebo nevhodné odkazy na jiné části textu (vesměs v podobě "viz X", kde 1) není jasné, jaký typ objektu je "X", a 2) práce by neměla čtenáři nic přikazovat). Bylo by také vhodné rozšířit seznam literatury, sedm zdrojů je poměrně málo (a to ještě položky 2, 6 a 7 nejsou moc relevantní).
Po věcné stránce nenacházím v práci vyslovené chyby, ale některé formulace jsou přinejmenším podezřelé a potřebovaly by lepší zdůvodnění:
1) Na obrázku 3.1 jsou vyznačena místa, na která může být prováděn útok. Není jasné, proč zrovna tato dvě místa - jako mnohem vhodnější by se jevil bod po sečtení c0 a k0, do kterého nezasahují další potenciálně neznámé hodnoty (práce sice předpokládá znalost "nonce", při použití navrhovaného bodu by ovšem tato znalost nebyla potřeba).
2) Zvolená technika "komprese" (průměrování dvou nebo více po sobě jdoucích hodnot) výrazně zhoršuje přesnost analýzy. Student to zdůvodňuje výpočetními nároky pro zpracování dat, tento argument se však zdá být přinejmenším pro variantu "jen první čtvrtrunda" slabý. Očekával bych, že aspoň jeden test proběhne nad nekomprimovanými daty.
3) Hypotézy v sekci 3.3.2 jsou buď nepřesně popsané, nebo nesprávné. Formulace v textu vzbuzuje dojem, že přičítání konstanty ke klíči probíhá po bajtech, ve skutečnosti probíhá po 32bitových slovech.
4) Model spotřeby používající Hammingovu vzdálenost nepotřeboval znalost poloviny klíče, pokud by bylo použito měřící místo dle připomínky 1 výše - pak by šlo pro každou konkrétní vstupní hodnotu klíče dopočítat očekávanou hodnotu po výpočtu a z rozdílu mezi nimi dovodit Hammingovu vzdálenost.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*75 (C)*

Popis kritéria:
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

Komentář:

V softwarové části práce se poměrně obtížně orientuje kvůli nevhodné a nedostatečně popsané struktuře adresářů - šifrovací program pro čipovou kartu se jmenuje "driver", v adresáři "measure" se nachází směsice materiálů od dokumentace k osciloskopu přes vyhodnocovací skripty až po samotnou měřící aplikaci (která je dále rozložena do dvou podadresářů, jeden pro Cčkové zdrojáky a knihovny a druhý pro projektový soubor a binárky). Nalezl jsem nicméně tři místa, která vyvolávají pochybnosti o zformulovaných závěrech:
1) Šifra ChaCha je naimplementována v rozporu s její specifikací - všechny použité programy používají odlišné konstanty s mnohem menší entropií. Mimo jiné tak nelze použít standardní testovací vektory pro ověření správnosti implementace! Přitom nevidím žádný přínos této úpravy.
2) Pro všechny testy byl použit klíč s velmi nízkou entropií. Navíc dochází k velmi nežádoucím interakcím mezi entropií klíče a konstant výše, šifra se chová výrazně hůře, než je od ní očekáváno.
3) Plaintext pro zašifrování je vytvořen pomocí RNG funkce, která není kryptograficky bezpečná a které je předáván konstantní seed. Přitom není vůbec jasné, proč byla použita tato funkce, analýzu šlo zrovna tak dobře provádět na plaintextu tvořeném samými nulami. Vzbuzuje to zbytečné pochybnosti o kryptografických základech práce.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*75 (C)*

Popis kritéria:
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.

Komentář:

Dosažené výsledky by mohly být velice zajímavé - technika DPA je sice dobře známá, její použití na proudovou šifru však není běžné a zjištění tak mohla přinést něco skutečně nového. Nedostatky popsané v bodech 2 a 3 tohoto hodnocení však vzbuzují pochybnosti o tom, zda jsou výsledky uvedené v práci skutečně správné.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*
5. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

Můžete se vyjádřit k poznámkám 1 až 3 z hodnocení písemné části práce a poznámce 1 z hodnocení nepísemné části?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*79 (C)*

Popis kritéria:
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.

Text hodnocení:

Předložená bakalářská práce je rozporuplná. Pozitivně vnímám to, že si student zvolil dosti náročné téma a poměrně dobře ho zpracoval, a dále výbornou logickou a jazykovou stránku textové části. Naproti tomu některé klíčové body vlastního provedení práce by potřebovaly podrobnější zdůvodnění. Zcela nejasný je důvod, proč byla šifra ChaCha upravena v rozporu s její specifikací. Za těchto okolností hodnotím práci jen stupněm C-dobře, pokud se však dokáže uspokojivě vyjádřit k uvedeným námitkám, klidně by se mohlo hodnocení zlepšit až na A-výborně. Potenciál pro to práce určitě má.

Podpis oponenta práce: