FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student: Adam Zahumenský
Vedoucí: práce: Ing. Jiří Buček, Ph.D.
Název práce: Timing side-channel attack on AES
Obor: Bezpečnost a informační technologie

Datum vytvoření: 13. 6. 2019

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:
Student splnil zadání v plném rozsahu.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*75 (C)*

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 práce je příliš stručná, ale přesto obsahuje ty nejdůležitější potřebné části. Práci by prospěl detailnější popis a vysvětlení metody útoku a detailnější popis implementace.
Práce obsahuje některé formální chyby, které vznikly v časové tísni studenta před odevzdáním práce. Jedná se například o chybu v hierarchii číslování podkapitol v kapitole 5.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*90 (A)*

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:
Přílohou jsou zdrojové soubory implementace šifry AES pomocí T-boxů, zdrojové soubory analytického jádra útoku v jazyce C a spouštěcí a pomocné soubory (skripty v Pythonu, makefile).

Studentův kód je poměrně přehledný a je dobře komentován. Části psané v C by prospělo rozdělení na dva moduly, aby se oddělil kód počítající statistiky od měřicího kódu.

V souboru README.md je přehledný návod použití včetně pokynů pro překlad a běh na různých platformách a s různým cílem útoku (implementací AES).

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*99 (A)*

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:

Výsledkem práce je fungující útok časovým postranním kanálem na šifru AES implementovanou pomocí T-boxů. Metoda útoku vychází z publikace D. Bernsteina (2005). Útok byl otestován na několika různých implementacích AES a na různých platformách. Útok byl úspěšný jak na studentovu vlastní implementaci AES, tak i na implementaci obsaženou v knihovně OpenSSL 1.1.b, ovšem pouze pokud byly vypnuty optimalizace pro platformu x86 resp. x64 (konfigurační volbou no-asm). Podle očekávání útok nebyl úspěšný na implementaci využívající HW akceleraci v instrukční sadě AES-NI.

Úspěšnost útoku závisí i na konkrétní platformě a OS. Na mém notebooku s OS Windows 10 útok odhalil 11 z 16 bajtů klíče, přičemž odhalených 11 bajtů se nacházelo na prvních místech v příslušných skupinách kandidátů už po cca 5 minutách běhu programu. Celý klíč byl prolomen i s pomocí dopočítání hrubou silou za méně než hodinu.

V kódu jsou navržena místa pro vynechání (vymazání) části programu míněné jako úlohu pro studenty. V současné podobě kód funguje pod OS Linux a Windows, což dovoluje značnou flexibilitu při nasazení do výuky.

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 5:*
5. Aktivita a samostatnost studenta	5a: ***1=výborná aktivita,*** *2=velmi dobrá aktivita,* *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 5b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
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 (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:

Student postupoval převážně samostatně, a v případě problémů aktivně vyhledal konzultaci. Na konzultace byl řádně připraven a získané informace dokázal účinně zapracovat do svého řešení.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*88 (B)*

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:

Student prokázal schopnost samostatné tvůrčí práce. Vzhledem k náročnosti zadání je velkým úspěchem, že se studentovi podařilo dotáhnout řešení do funkčního stavu. V průběhu práce dlouho nebylo jasné, zda na současné generaci procesorů bude původní Bernsteinův útok fungovat. Nakonec se studentovi po značném úsilí podařilo útok vyladit do podoby, kdy je skutečně funkční a prolomí většinu bajtů klíče (a dopočítá dokonce celý klíč). Bohužel některé úpravy a experimenty student prováděl až těsně před odevzdáním práce, což se negativně projevilo na rozsahu a částečně i formální úpravě textové zprávy. Vzhledem k výše uvedeným skutečnostem navrhuji hodnocení velmi dobře.

Podpis vedoucího práce: