FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Jonatan Matějka
Oponent práce:	Ing. Tomáš Zahradnický, Ph.D.
Název práce:	Odhalení klíče AES sledováním běhu programu
Obor:	Počítačová bezpečnost

Datum vytvoření: 2. 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:
Cílem diplomové práce bylo nastudovat algoritmus AES a jeho implementace. Dále student měl navrhnout a implementovat algoritmus odhalující použití AES klíčů jako součást programu pro cílový procesor. Konstatuji, že tyto body byly splněny, a proto považuji zadání za splněné.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*90 (A)*

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:
Po popisu šifry Rijndael/AES a jejích implementací následují metody detekce implementace šifry AES v programu. Dále následuje návrh detekčních algoritmů založených na paměťových bodech přerušení (angl. breakpoints) spolu s rekonstrukcí klíče a dat. Následuje implementační kapitola, která pipsuje ladící rozhraní, nalezení substitučních boxů šifry AES, opět pomocí bodů přerušení a dále pomocí nastavení pčístupových příznaků paměťových stránek. Následuje popis testování a dosažených výsledků.

Logická struktura práce je bezproblémová. Snad jen připomínka, že v případě 6.1.3 chybí obdobný výpis jako v ostatních případech. Bezproblémovost spatřuji i po stránce typografické i jazykové.

Jako drobný nedostatek vidím, to, že na platormě Windows nebyla uvažována knihovna Cryptography API Next Generation (bcrypt.dll) [1]. Knihovna je dostupná již od Windows Vista a nahrazuje zastaralou knihovnu Crypto API (crypt32.dll). Dále je také škoda, že je podporována jen 32bitová architektura. Aplikaci PuTTY.EXE nevnímám jako typický zástupce Windows aplikace. Podle mého názoru by bylo vhodnější zkusit odhalit klíč například při připojení k VPN anebo v internetovém prohlížeči Edge anebo Chrome při navazování TLS spojení.

[1] Microsoft Corp. Cryptography API: Next Generation. https://docs.microsoft.com/en-us/windows/desktop/seccng/cng-portal.

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

Příloha k práci na disku DVD obsahuje program a text diplomové práce. Ten je možné použít.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*95 (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:

Práce demonstruje, jak „snadné“ je získání AES klíče z běžícího procesu. Pokud proces běží pod stejným uživatelským účtem, je pravděpodobné, že se podaří klíč získat. Pro tyto důvody se kryptografické funkce vyvíjejí směrem k použití identifikátorů klíčů (handles) namísto aktuálních klíčů a přesunem kryptografie a operací s klíči mimo proces, například do kernelu. Kryptografická volání pak probíhají prostřednictvím interprocesové komunikace.

Jako drobný nedostatek vnímám chybějící 64bitovou variantu.

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:

1. Jaké jsou výsledky pro aplikaci linkovanou s Crypt Next Generation na Windows?
2. Jak by bylo nutné program upravit tak, aby fungoval i v případě kernelové kryptografie?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*95 (A)*

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:

Diplomovou práci pana Bc. Jonatana Matějky doporučuji k obhajobě a hodnotím ji stupněm A (výborně).

Podpis oponenta práce: