FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student: Bc. Jonatan Matějka
Vedoucí: práce: Ing. Josef Kokeš
Název práce: Odhalení klíče AES sledováním běhu programu
Obor: Počítačová bezpečnost

Datum vytvoření: 19. 5. 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:

Perfektní práce! Značně komplikované zadání, vyžadující detailní porozumění implementační stránky šifry AES a porozumění tomu, jak fungují debuggery, bylo splněno úplně a bez nejmenších výhrad.

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

Práce systematicky a logicky vede čtenáře celou problematikou. Všechny části jsou informačně bohaté a přitom přehledné a srozumitelné, jejich logické uspořádání je dokonalé. Také technická a gramatická stránka je na výši, narazil jsem na jedinou chybějící čárku. Použitá literatura je rozsáhlá, relevantní a vhodně odkazovaná.

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:

Student vypracoval program, který jako debugger spustí cílový proces, sleduje v něm prováděné šifrovací operace a průběžně vypisuje detekované klíče a šifrované otevřené texty. Kód programu je stručný a přehledný a vhodně strukturovaný na dvě části - platformově závislý kód sbírající informace (čtení a zápis paměti procesu, řešení rozšířeného paměťového breakpointu) a nezávislá knihovna provádějící veškerá vyhodnocení.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*100 (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:
Vytvořený program perfektně řeší předmětnou oblast - detekce použití AESu v ryze softwarové implementaci. Jeho použití je velmi jednoduché a přímočaré, přitom funkční, řešeny jsou i velmi obtížné mezní situace. Proběhly také praktické testy nad řadou běžně používaných kryptografických knihoven i nad aplikacemi, které mají vlastní implementaci AESu.

Implementována je pouze samostatná verze, úprava do podoby pluginu pro debugger by ale měla být vzhledem k výborně navržené struktuře jednoduchou záležitostí. Hardwarově asistované šifrování (instrukce AES-NI, využití vektorové jednotky a bitslicingu) řešeno není, ale ani nebylo součástí zadání a náročnost by řádově narostla; student nicméně přesto uvádí aspoň teoretické postupy, jak tyto varianty řešit. Zdánlivě malý výkon programu není problémem, alternativní řešení mají výkon ještě horší a optimalizace (např. asynchronním zpracováním událostí, jak student navrhuje) není náročná.

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 pracoval velmi samostatně, konzultací bylo jen minimální množství. Výsledek ale mluví sám za sebe, student se zjevně věnoval spíš zpracování práce než konzultacím, které by byly jen formální.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*100 (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:
Vždy se s podezřením dívám na stoprocentní hodnocení, zde ale nemám na výběr. Práce je perfektní, jak její textová stránka, tak vytvořený program, který je velmi snadno použitelný a přitom skvěle plní požadovanou funkci - spustit aplikaci třetí strany a v ní detekovat a vypisovat případy použití šifry AES. Jde o skvělou ukázku inženýrské práce, které není co vytknout - snad jen škoda, že text není psán v angličtině a že pro vytvořené dílo nebyla zvolena nějaká permisivnější licence.

Podpis vedoucího práce: