FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student: Josef Hušek
Oponent práce: Ing. Jiří Dostál, Ph.D.
Název práce: The use of cryptography in 7-zip
Obor: Bezpečnost a informační technologie

Datum vytvoření: 10. 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:
Zadání bylo sice splněno, ale práce na mě působí, jako by byla psána na poslední chvíli, důležitá kapitola o útoku na archiv by zasloužila lepší zpracování.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*55 (E)*

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:
Velkou výtku mám ke struktuře práce, jsou zde 2 kapitoly "Theoretical Backgroung" a "Analysis of 7-zip," kdy analýzy je zahrnut i vlastní útok na archiv (důležitý bod zadání). Chybí mi zde podrobnější postup útoku a hlavně přehledné výsledky, 7 obrázků (které jsou ve skutečnosti výpisy kódu) a žádná tabulka k tomu nepřispívá. V práci se od kapitoly 2.4 velice špatně orientuje. Vlastní praktický úkol ze zadání je pak v kapitole 2.4 nedostatečně popsán, čekal bych postup krok za krokem s výsledky testování, ideálně v příloze. Takto není úplně zřejmé jaké útoky byly provedeny, s jakými parametry apod.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*60 (D)*

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:
K práci jsou přiloženy zdrojové soubory použité v práci, bohužel bez podrobné dokumentace, což ztěžuje reprodukci testování a posouzení práce.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*60 (D)*

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:
Bohužel autor nevyužil plný potenciál jinak velice zajímavého tématu - např. mě zaujal problém chybějícího salt u KDF.

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: Jakým způsobem ovlivňuje chybějící salt KDF a celkové zabezpečení archivu?	

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*65 (D)*
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: Zadání bylo sice splněno, ale práce na mě působí, jako by byla psána na poslední chvíli, důležitá kapitola o útoku na archiv by zasloužila lepší zpracování. Chybí mi zde podrobnější postup útoku a hlavně přehledné výsledky. V práci se od kapitoly 2.4 velice špatně orientuje. Vlastní praktický úkol ze zadání je pak v kapitole 2.4 nedostatečně popsán, čekal bych postup krok za krokem s výsledky testování, ideálně v příloze. Zajímavá zranitelnost ve formě chybějícího salt je velice špatně zdokumentována.	

Podpis oponenta práce: