FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student: Radek Smejkal
Oponent práce: Ing. Jiří Buček, Ph.D.
Název práce: Bezpečnostní analýza programu Passbolt
Obor: Bezpečnost a informační technologie

Datum vytvoření: 11. 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 splněno v plném rozsahu.

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:
Práce je členěna logicky a jednotlivé části jsou přiměřeně obsáhlé. Student postupoval systematicky a pečlivě. Po obsahové ani formální stránce nemám závažnější výhrady. Práce je psána spisovnou češtinou s malým počtem překlepů (např. "standart", "strovnání") .

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 práce jsou binární verze použitého prohlížeče (Firefox), binární a zdrojové kódy klientské i serverové části analyzovaného software (Passbolt), a soubory se záznamy studentovy analýzy (zejména síťové komunikace). Příloha obsahuje vše potřebné pro zajištění opakovatelnosti experimentů, s výjimkou obrazů virtuálních strojů, jejichž přiložení by bylo nepraktické.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*90 (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:
Teoretická část práce poslouží jako základní přehled o existujících aplikacích pro správu hesel. Analytická část přináší nezávislé zhodnocení bezpečnosti aplikace Passbolt a může být užitečná při výběru aplikace pro správu hesel.

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: Na str. 28 uvádíte vzorec pro odhad entropie hesla. Myslíte si, že je takto sestavený vzorec dostatečný jako podklad pro zpětnou vazbu uživateli? Byl by rozdíl v odhadu entropie např. hesel "9<7vNj+c@`N=" a "Aaaaaaaaaa.1"? Jaký vliv může mít případné úspěšné nasazení kvantových počítačů s dostatečnou kapacitou s ohledem na kryptografické algoritmy použité v aplikaci Passbolt?	
Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*90 (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: Práce je zdařilá, student pracoval systematicky a pečlivě. Rovněž navázal komunikaci s autory aplikace a zaslal jim výsledky své analýzy. Práci hodnotím jako výbornou.	

Podpis oponenta práce: