Hodnocení vedoucího závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Jan Vojtěšek
Vedoucí práce: Ing. Josef Kokeš
Název práce: Analysis of the Rescue File of BestCrypt Volume Encryption
Obor: Informační technologie

Datum vytvoření: 21. 5. 2017

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	***1=mimořádně náročné zadání,*** *2=náročnější zadání, 3=průměrně náročné zadání, 4=lehčí, ale ještě dostatečně náročné zadání, 5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Zadání vyžadovalo, aby student porozuměl programu ve strojovém kódu tak dobře, aby dokázal zdokumentovat formát neznámého binárního souboru a vyhodnotit bezpečnostní rizika z toho vyplývající. U diplomových prací toto hodnotíme jako mimořádně náročné; že by si téma zvolil student bakalářského programu, to rozhodně nebylo předpokládáno.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. 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 splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Zadání bylo výrazně překročeno. Student se nespokojil se splněním všech bodů ze zadání, ale provedl i bezpečnostní analýzu dalších částí programu BestCrypt Volume Encryption. Už to by samo o sobě stačilo na novou diplomovou práci - je třeba si uvědomit, že než vůbec bylo možné přistoupit k jejich bezpečnostní analýze, musel student detailně porozumět strojovému kódu programu, a to nejen v jednotlivých funkcích, ale i v jejich vztahu k celku.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	***1=splňuje požadavky,*** *2=splňuje požadavky s menšími výhradami, 3=splňuje požadavky s většími výhradami, 4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Rozsah bakalářské práce a hustota informací v ní odpovídají požadavkům.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*100 (A)*

Popis kritéria:
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.

Komentář:
Věcná úroveň práce je perfektní. K logické struktuře nemám výhrady.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*100 (A)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3.

Komentář:
Práce je napsána v anglickém jazyce a její úroveň je výborná. Nenarazil jsem na prakticky žádné chyby. Ani po formální stránce nemám co vytknout.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*

6. Práce se zdroji — *95 (A)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Také práce se zdroji je výborná. Student využívá značné množství materiálů, relevantních a vhodně použitých.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*100 (A)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Dosažené výsledky jsou nejlepší, jaké jsem v českých ZP viděl. Student provedl fantastickou bezpečnostní analýzu aplikace, a to na naprosto profesionální úrovni srovnatelné s Open Crypto Audit Project pro TrueCrypt. Zdokumentoval dosud neznámý formát Rescue souboru pro BestCrypt Volume Encryption a popsal v něm nedostatky, které mohou vést ke ztrátě dat nebo k porušení jejich důvěrnosti. Navíc provedl analýzu dalších kritických komponent programu BCVE a nalezl další vážné nedostatky. Získané informace mohou být bez problémů publikovány na konferenci DEFCON nebo podobné.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
ZP představuje zatím nejdůkladnější analýzu bezpečnosti programu BestCrypt Volume Encryption. Byly nalezeny zranitelnosti, které jsou pro uživatele velmi významné. Tyto byly v souladu s principem responsible disclosure nahlášeny výrobci, který je uznal a opravil*). Uživatelé tak získají bezpečnější produkt. Zároveň jim práce poskytuje návod, jak program používat bezpečně, tím, že varuje před potenciálními citlivými operacemi, které dosud nebyly uživatelům známy. Třetím významným přínosem jsou vytvořené aplikace, které dovolují například on-line přístup k zašifrovaným svazkům z jiného počítače s využitím Rescue souboru, což dosud nebylo možné. Díky důslednému použití angličtiny v celé DP jsou všechny tyto výsledky dostupné uživatelům z celého světa.

*) Výjimkou je zranitelnost, která si vyžádá komplikovanější opravu. Kvůli tomu není přímou součástí ZP, ale nachází se v samostatném dokumentu, aby mohla být zveřejněna samostatně, až se podaří chybu opravit.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
9. Aktivita a samostatnost studenta v průběhu řešení	9a: *1=výborná aktivita,* *2=velmi dobrá aktivita,* *3=průměrná aktivita,* ***4=slabší, ale ještě dostatečná aktivita,*** *5=nedostatečná aktivita* 9b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (9a). Posuďte schopnost studenta samostatné tvůrčí práce (9b).

Komentář:
Student pracoval naprosto samostatně, z pohledu vedoucího až příliš - konzultací bylo jen poměrně málo. Nemohu říci, že by tím kvalita práce nějak utrpěla, uvítal bych ovšem pravidelnější setkání.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*100 (A)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Absolutní hodnocení je vždy podezřelé, zde však nemám na výběr. Student odvedl prakticky dokonalou práci na mimořádně těžkém tématu a jeho dílo může směle konkurovat podobným analýzám profesionálních skupin kolem známých osobností oboru bezpečnosti (např. Matthew Green a jeho Open Crypto Audit Project). Že dokázal totéž jako jediná osoba, navíc nad programem, ke kterému není k dispozici zdrojový kód, je obdivuhodné. Neznám lépe provedenou závěrečnou práci.

Podpis vedoucího práce: