Hodnocení vedoucího závěrečné práce

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

Student: Bc. Juraj Horňák
Vedoucí práce: Ing. Josef Kokeš
Název práce: Bezpečnostní analýza programu BestCrypt Volume Encryption
Obor: Počítačová bezpečnost

Datum vytvoření: 5. 5. 2016

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:
Student měl provést bezpečnostní analýzu bootovacího kódu programu BestCrypt Volume Encryption technikou reverzního inženýrství. V tomto případě existovaly pro obecně velmi obtížné reverzní inženýrství usnadňující faktory (analýza 16bitového kódu), které ale byly více než kompenzovány požadavkem na provedení bezpečnostní analýzy nalezeného kódu: to totiž vyžaduje nejen důkladné porozumění neznámému kódu, ale také správné vyhodnocení bezpečnostních implikací jednotlivých instrukcí. Celkově tak lze zadání stále hodnotit jako mimořádně obtížné.

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 splněno, včetně volitelného úkolu na ověření správnosti použití kryptografických primitiv.

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:
Práce svou délkou vyhovuje požadavkům. Obsahuje sice větší množství obrázků nebo algoritmů, ty jsou však vždy relevantní k analyzovaným tématům a obsahové stránce práce jednoznačně prospívají.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*90 (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:
Po věcné stránce je práce výborná, chyby ani nepřesnosti téměř neobsahuje. Na jediný závažnější problém jsem narazil u algoritmu 3.3, jehož popis v práci neodpovídá přesně prováděnému kódu; rozdíly padají na vrub snaze usnadnit čtenáři pochopení algoritmu, což lze jistě chápat, v bezpečnostní analýze však i drobný rozdíl může vést k chybným závěrům a bylo by proto vhodnější dodržet přesnou shodu s kódem i za cenu prodloužení a zesložitění popisu algoritmu. Menší nedostatek lze spatřovat v programu pro dešifrování sektorů, který heslo přijímá na příkazové řádce a z paměti ho nemaže, což je potenciálně rizikové; protože však jde jen o ověřovací aplikaci, nejde o podstatnou závadu.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*99 (A)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 12/2014, článek 3.

Komentář:
Moje znalost slovenštiny není tak dobrá, abych byl schopen vyhodnotit jazykovou stránku práce stoprocentně, ale až na jednu čárku a jednu dvojtečku jsem nenarazil na nic, co by mě v jazyku práce zarazilo. Typografické stránce není co vytknout, formální zápisy zejm. algoritmů jsou vynikající.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*90 (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:
Práce používá nadprůměrné množství pramenů, i když mnoho z nich jen v roli odkazu na použitý produkt. Citelně chybí literatura zabývající se teorií reverzního inženýrství (např. Eilam, Chikofsky: Reversing: Secrets of reverse engineering), lze však pochopit, že v práci tohoto druhu bude praktické použití známých technik důležitější. Podstatné je, že převzaté myšlenky jsou důsledně citovány. U zdrojů 24-26 mám výhradu k nekonzistentnímu zápisu jména firmy Microsoft.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*98 (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 vynikající. Studentovi se podařilo dosti detailně pochopit kód aplikace a na základě toho vyvodit závěry o bezpečnosti programu. To je velmi cenné pro uživatele software BestCrypt Volume Encryption, kteří tak dostávají do ruky nezávislé zhodnocení kvality kódu, které dosud nebylo veřejně k dispozici a nedalo se očekávat, že by se v dohledné době objevilo (k programu není k dispozici zdrojový kód).

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:
Výsledky ZP jsou zcela originální a velmi důležité pro praxi. Identifikovaná slabá místa budou nahlášena výrobci programu, čímž by se měla dále zvýšit kvalita programu a jeho užitečnost pro uživatele. I bez toho je ale pro uživatele důležité, že nebyly nalezeny žádné fatální chyby, protože tak získali nezávislé ujištění, že mohou program používat bez obav o svoji bezpečnost. Škoda jen, že jazykem práce není angličtina, která by využitelnost výsledků významně zvýšila.

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:
Pan Horňák řešil úlohu samostatně, možná až příliš - častější konzultace by neuškodily, i když z dosažených výsledků je zřejmé, že se student dobře obešel i bez nich. Rozhodně by pomohly vedoucímu k většímu klidu.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*95 (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:
Student se svého velmi náročného úkolu zhostil velmi dobře. Důkladně pronikl do kódu programu a dokázal z něj vyvodit závěry, kterým se dá důvěřovat. Nad rámec očekávání při zadávání práce dokázal ověřit kryptologická primitiva použitá v programu, což je u vstupu reprezentovaného pouze strojovým kódem mimořádně obtížné. Práci doporučuji k obhajobě a hodnotím známkou A.

Podpis vedoucího práce: