Hodnocení vedoucího závěrečné práce

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

Student: Bc. Jakub Souček
Vedoucí práce: Ing. Josef Kokeš
Název práce: Security Analysis of BestCrypt
Obor: Počítačová bezpečnost

Datum vytvoření: 7. 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:
Zatímco implementační části zadání jsou spíše jednodušší (když odhlédneme od nekompletní dokumentace), je nutno brát v úvahu, že složitost zadání spočívá v nutnosti vyhodnotit bezpečnostní aspekty jednotlivých komponent programu BestCrypt. I jediná strojová instrukce může snadno znamenat rozdíl mezi kvalitní implementací a fatálním selháním. Od studenta to vyžaduje značný rozhled v počítačové bezpečnosti, velkou pozornost a také schopnost hledat neočekávané vztahy ve zdánlivě nesouvisejících částech programu.

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:
Student zadání splnil a podařilo se mu dokonce najít dosud neznámé bezpečnostní slabiny v programu BestCrypt.

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 práce splňuje stanovené požadavky, i když po odstranění ilustračních obrázků jen těsně.

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:
Věcná stránka práce je v pořádku. Lze si představit, že některé bezpečnostní aspekty softwaru mohly být řešeny detailněji, ale odvedené množství práce je zcela odpovídající. Výhrady mám k příliš optimistickým závěrům, doporučoval bych větší opatrnost (řešení chyb navržené výrobcem podle mě nemusí nutně vést k nápravě, záleží na konkrétní implementaci; že aplikace neprováděla během testů zjistitelnou síťovou aktivitu není dokladem toho, že ji zaručeně nikdy neprovádí).

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*70 (C)*

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:
Formální zápisy jsou v pořádku, typografická stránka vesměs také (jeden zapomenutý spojovník místo pomlčky, špatné uvozovky apod.). Nejsem nadšen z použití bitmapových obrázků i tam, kde se dal snadno vytvořit obrázek vektorový. Angličtina práce není zcela ideální, z textu je zcela zřejmé, že ho nepsal rodilý mluvčí ani člověk s větší praxí (časté neshody časů, problémy s členy a čárkami, místy chybné předložky nebo podivný slovosled), ale nepřekáží v porozumění textu. Doporučuji však v hodnocení přihlédnout k tomu, že student angličtinu zvolil primárně proto, aby umožnil uživatelům i výrobci programu využít nalezená zjištění, tedy s úmyslem jim prospět.

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:
Citované zdroje jsou použity vhodným způsobem a jsou k práci relevantní. Jejich počet je nadprůměrný.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*95 (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:
Studentovi se podařilo nalézt dvě dosud neznámé bezpečnostní slabiny v programu BestCrypt. Zejména prolomení vlastnosti důvěryhodného popření (Plausible Deniability) považuji za mimořádně závažné, i s ohledem na okruh uživatelů programu BC (jak ho deklaruje výrobce) - nesprávná implementace této vlastnosti může pro uživatele znamenat velmi závažné následky. Také možnost oslabení hlavního klíče kontejneru pomocí předčasného zastavení generování seedu není zanedbatelný detail.

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:
Práce přináší úplně nová zjištění, protože analýza programu BestCrypt nebyla dosud veřejně publikována. Práce zdokumentovala dosud jen problematicky popsanou knihovnu BDK a ověřila, že BestCrypt implementuje kryptologická primitiva správně, navíc se nepodařilo najít žádná zadní vrátka. To má velký přínos pro uživatele, kteří dosud neměli objektivní důvod programu věřit.

Byly nalezeny dvě bezpečnostní chyby, z toho slabina v Plausible Deniability je podle mého názoru naprosto fatální a její odhalení je studentův veliký úspěch. Obě nalezené chyby byly předány výrobci programu, který je jako chyby uznal a přislíbil nápravu, což povede k zlepšení kvality šifrovacího programu a zvýšení bezpečnosti pro uživatele.

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 byl velmi aktivní i samostatný, nemám, co bych mu v této oblasti mohl vytknout.

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 se svým úkolem vypořádal velmi zodpovědně a kvalitně. Nalezení kritické slabiny v Plausible Deniability nelze zhodnotit jinak než jako vynikající úspěch, který by si sám o sobě zasloužil ohodnocení práce stupněm A - student tím nepochybně prokázal, že je schopen inženýrské práce v oboru počítačové bezpečnosti. Problematická angličtina jakožto nejhůře zpracovaný aspekt práce nesnižuje výrazně její hodnotu, naopak je třeba ocenit, že tím, že student zvolil obtížnější psaní v cizím jazyce, výrazně zvýšil hodnotu práce pro uživatele.

Podpis vedoucího práce: