Hodnocení vedoucího závěrečné práce

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

Student: Petr Mück
Vedoucí práce: Ing. Josef Kokeš
Název práce: Knihovna pro off-line práci se šifrovanými kontejnery TrueCryptu
Obor: Informační technologie (bakalářský)

Datum vytvoření: 16. 5. 2015

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 patří mezi spíš jednodušší, největší část práce spočívá ve vhodném propojení knihoven, které vytvořil někdo jiný. Nalézt tyto knihovny, naučit se s nimi pracovat a navrhnout toto "vhodné propojení" ale může být pro studenta, který dosud nemá rozsáhlejší praktické zkušenosti, komplikované. Druhým zesložiťujícím faktorem je, že se práce zabývá bezpečnostním produktem a tudíž by měla být napsána tak, aby pracovala bezpečně.

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. Nad rámec zadání student zajistil multiplatformnost svého řešení (ověřeno na platformě Windows).

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:
Porovnejte rozsah předložené písemné zprávy s požadovaným rozsahem, viz Směrnice děkana č. 9/2011, článek 3. Pro hodnocení ZP je také důležité, zda všechny části písemné zprávy jsou informačně bohaté a pro práci nezbytné. Text ZP by neměl obsahovat zbytečné části.

Komentář:
Požadovaný rozsah zprávy je splněn, zohledníme-li ale prázdné stránky na koncích kapitol, pohybuje se délka jen mírně nad jeho spodní hranicí. Toto se projevuje zejména v kapitole 3, která by si zasloužila podstatně podrobnější provedení.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*85 (B)*

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:
Práce je logicky strukturována a ve své drtivé většině je i věcně správná, nesprávná tvrzení jsou spíš jen detaily: Není pravda, že SubBytes provádí permutaci bitů (poznámka 10 na str. 11). NTFS není preferovaný na všech Windows od NT 3.1 dále (str. 19) - řada Windows 9X NTFS nepodporovala. Tvrzení, že "Struktura file_info obsahuje většinu běžných atributů" (str. 26), je možná formálně správné, ale srovnání obsahu file_info s WIN32_FIND_DATA (pracujeme FAT, tak využijme Microsoftí standardizaci) a s výstupem ls -l (knihovna byla vyvíjena na Linuxu, tak s ním autor zřejmě je obeznámen) dopadá pro file_info dost nepříznivě - očekával bych, že struktura bude obsahovat sjednocení vlastností, ne jejich průnik; mimo jiné to zesložiťuje budoucí přidání dalších souborových systémů.

Větší výhrady mám jen ke kapitole 3, která je příliš stručná a jako zdroj informací pro další rozvoj vytvářené knihovny ne zcela použitelná. Vinu za to musím bohužel dávat sám sobě, že jsem studenta nechal v raných fázích zpracování práce soustředit se na implementaci a nenutil ho do pořádné rešerše.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*80 (B)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 9/2011, článek 3.

Komentář:
Jazyková úroveň práce je vesměs velmi dobrá. Napočítal jsem 19 překlepů, chybějících čárek a neshod mezi podmětem a přísudkem, což se může zdát hodně, ale ve srovnání s tím, co se můžeme dočíst v jiných pracech, to vůbec není špatné.

Formální úroveň je výborná, chválím obvyklý zápis algoritmů. Škoda špatných přetečení na straně 3 a chybného zápisu Galoisova tělesa a jeho ireducibilního algoritmu v legendě k algoritmu 2 (str. 13).

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*100 (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:
Student pečlivě cituje cizí myšlenky, množství citací je na bakalářskou práci nadprůměrné. Kvalita zdrojů je odpovídající; že jejich těžiště leží v online zdrojích, lze vzhledem k povaze TrueCryptu očekávat.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*80 (B)*

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:
Výstupem BP je knihovna, která umožňuje přistupovat k TrueCryptovskému kontejneru off-line, bez připojení tohoto kontejneru jako virtuálního disku. To je velmi užitečné v mnoha situacích, kdy potřebujeme kontejner použít v prostředí, nad nímž nemáme stoprocentní kontrolu. Knihovna není dokonalá, požadované úkoly však plní. Jako významné pozitivum vnímám, že se student snažil myslet i na bezpečnost svého programu a citlivé údaje po použití maže. Hlavní nedostatky svého řešení student sám správně rozpoznal (kap. 4.4) a zdá se, že se z nich dokáže poučit. Určité rezervy spatřuji v jeho pojetí "snadné rozšiřitelnosti", ale to je hlavně otázka praktických zkušeností, v rámci BP je použité řešení odpovídající. Několik dalších poznámek:
1) Bývá zvykem k programu připravit makefile a nespoléhat se na sestavovací skript v SH.
2) Pokud funkce EVP_Decrypt* v tclib-aes.c selžou, nedojde k přemazání připraveného klíče.
3) Je vhodné likvidovat citlivé údaje hned, jak přestanou být potřeba. Například klíč pro AES by tak bylo vhodné přemazat hned po skončení EVP_DecryptInit_ex, bez ohledu na to, jestli tato funkce skončila úspěšně.

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:
Knihovna nepřináší žádné zásadně nové poznatky, ale i tak je přínosem:

1) Už teď umožňuje základní offline práci s kontejnery a po rozšíření o další šifry a souborové systémy se stane skutečně velmi užitečnou.

2) Tím, že úspěšně re-implementujte funkce TrueCryptu jinými prostředky, vlastně dokazuje, že původní implementace v TrueCryptu je v souladu s dokumentovanými specifikacemi. To je velmi důležitý poznatek, protože ačkoliv TrueCrypt sám už se nevyvíjí, má několik následníků vycházejících z jeho kódu a tato knihovna tak slouží jako nezávislé ověření správnosti jejich implementace.

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 samostatně a řešil požadované dílčí úkoly.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*90 (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:
Práce plní zadané požadavky a ve své většině je na velmi dobré úrovni. Významné plus spatřuji v tom, že knihovnu i dodané demo aplikace lze bez úprav použít i pod Windows. Kvituji také schopnost studenta zhodnotit, kde jsou v jeho práci nedostatky, a navrhnout způsoby, jak se s nimi vypořádat. Kvůli horší použitelnosti kapitoly 3 by práce nejspíš zasloužila B, nemohu však studentovi příliš vyčítat, že na důležitost této kapitoly nepřišel sám - měl jsem mu to včas říci já. Proto navrhuji komisi, aby práci hodnotila stupněm A.

Podpis vedoucího práce: