Posudek oponenta závěrečné práce

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

Student: Petr Mück
Oponent práce: Ing. Tomáš Zahradnický, Ph.D.
Název práce: Knihovna pro off-line práci se šifrovanými kontejnery TrueCryptu
Obor: Informační technologie (bakalářský)

Datum vytvoření: 8. 6. 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:
Student se při své práci musel seznámit s programem TrueCrypt a jeho implementací. Na základě pochopení interní funkcionality tohoto programu musel navrhnout a implementovat vlastní produkt, a to včetně implementace souborových systémů. Provo považuji zadání práce za náročnější.

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 práce požaduje provedení rešerše knihoven pro souborové systémy - tu práce obsahuje. Z nich má být, tak jak zadání rozumím, vybrán vždy jeden a ten má být zakomponován do studentovy knihovny. Děje se tak pouze pro souborový systém FAT. Ostatní souborové systémy nejsou v práci po implementační stránce řešeny. Mohu však konstatovat, že demonstračními programy tc-ls a tc-cp jsem byl schopen načíst soubor jak ze standardního, tak i ze skrytého oddílu v rámci kontejneru aplikace TrueCrypt se souborovým systémem FAT. Doplnění dalších souborových systémů bylo žádoucí, avšak nepovažuji ho za příliš dramatický nedostatek - jádro práce pracuje, a proto konstatuji, že zadání práce bylo splněno s malou výhradou.

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 co do rozsahu splňuje požadavky na bakalářskou práci.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*65 (D)*

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 členěna na úvod, 4 kapitoly a závěr. V úvodu a kapitole 1. student stručně popisuje aplikaci TrueCrypt a její historický vývoj. V kapitole 2., TrueCrypt - realizace, student popisuje strukturu kontejneru aplikace TrueCrypt, hlavičky, klíče, hašovací funkce a šifrovací metody. Podle mého názoru je tato kapitola nevyvážená. Část popisující hlavičky a kontejner aplikaci TrueCrypt je zcela bez obrázků a/nebo schémat, přitom ty jsou esenciální pro implementační část. Na druhou stranu algoritmy pro šifrování a hašovací funkce, které student sám neimplementuje, jsou zde popisovány až zbytečně detailněji. Dále následuje kapitola 3., Souborové systémy, ve které student provádí rešerši dostupných knihoven pro přístup k souborovým systémům FAT, NTFS a ext. Ač kapitola na konci obsahuje shrnující tabulku se srovnáním knihoven, chybí jí závěr stanovující, pro kterou knihovnu a proč se student rozhodl. Následuje kapitola 4., Realizace, ve které student popisuje implementaci. Kapitole nepředchází návrhová kapitola, což může poukazovat na jistou míru nesystematičnosti a nenásleduje ji testování. Poslední kapitola, Závěr, stručně rekapituluje obsah práce.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*65 (D)*

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:
Po typografické stránce vykazuje práce nedostatky, občas nacházím vytékající slova ze zrcadla stránky (např. str. 3, 31, 32, 41), spojovník je používán namísto pomlky.

Po jazykové stránce nacházím sem tam překlepy (např. str. 3 distrubuci) a řadu anglicismů (backdoor, brute-force, hidden, open-source, padding, ...), dělení u některých slov je nesprávné (str. 4 Tru-eCryptu, str. 12 Ci-pherText). Některé výrazy jsou psány nekonzistentně např. hashovací vs. hašovací.

Jednotky nejsou psány v souladu s normou ISO 80000:13, např. 128 kB jistě student nemyslel 128 000 B, ale mocninu dvou tj. 131 072 B značených jako 128 KiB!

Notace zápisu polynomu a Galoisova tělesa na str. 13 pod algoritmem 2 jsou špatně, horní a dolní indexy jsou prohozeny.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*80 (B)*

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 obsahuje odkazy na celkem 43 zdrojů, což považuji za množství přesahující běžný počet odkazů u bakalářské práce. Citace jsou umísťovány za věty, až za koncovou tečku - tento způsob nepovažuji za zcela standardní. Stejně jako považuji za nepříliš šťastné se odkazovat např. na algoritmus AES na stránku na serveru Wikipedia (odkaz č. 1). Také způsob řazení publikací, nikoliv podle abecedy, ale podle výskytu v práci, považuji za zmatečný.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*75 (C)*

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:
Jádro práce je funkční. Práce poskytuje funkční nástroje tc-ls pro vypsání obsahu kontejneru aplikace TrueCrypt a nástroj tc-cp pro zkopírování souboru z kontejneru mimo něj. Práce se zaměřuje pouze na souborové systémy z rodiny FAT, chybí však podpora pro souborové systémy z rodiny ext a NTFS.

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:
Pokud by byly nástroje používané se souborovým systémem FAT, který je v dnešní době stále méně a méně častý, stačily by. Tím, že nástroj nezvládá práci se souborovými systémy NTFS a ext, považuji jeho využití za omezené.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
9. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
1. V podsekci 2.1.2 student uvádí, že: "Ten [skrytý oddíl] je přístupný pomocí odlišného hesla a nesdílí s hlavním oddílem žádná data." Kde je tedy skrytý oddíl v souboru aplikace TrueCrypt umístěn, když s hlavním oddílem nesdílí žádná data?

2. V sekci 3.1 se uvádí, že do množiny souborových systémů patří i souborový systém exFAT. Dále se uvádí, že: "Hlavními problémy FAT jsou omezení co se týče velikosti jak celého souborového systému, tak jehoho souboru a celkového počtu souborů v systémů." Jak do tohoto tvrzení zapadá souborový systém exFAT?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*70 (C)*

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:
I přes množství výhrad k práci, které jsou spíše drobnějšího charakteru doporučuji bakalářskou práci pana Petra Mücka k obhajobě a hodnoním ji stupněm C (dobře).

Podpis oponenta práce: