Posudek oponenta diplomové práce

Student: Chromečka Jiří, Bc.
Téma: Analýza šifrovacích metod pro klonování disků (id 17976)
Oponent: Černý Martin, Ing., Fujitsu

1. Náročnost zadání **průměrně obtížné zadání**

Zadání bylo zvoleno tak, aby bylo prakticky využitelné při bitovém kopírování pevných disků - jedná se o standardní postup při multiplikaci akceptovaného řešení pro zákazníka. Vzhledem k požadavku na ochranu přenášených dat je někdy nutné tato data šifrovat.

2. Splnění požadavků zadání **zadání splněno**

Při praktické prezentaci bylo provedeno měření a srovnání dosažených výsledků. Výsledek splnil očekávání nejen s ohledem na zpracovanou písemnou část, ale i s ohledem na vytvořený software a měřitelné výsledky.

3. Rozsah technické zprávy **splňuje pouze minimální požadavky**

Popis je dostatečný, srovnání metod mohlo být více do detailu - zejména mohlo být zmíněno třeba skriptování nebo jiné programové využití, a mohlo být také rozpracováno předání sdíleného tajemství - použití asymetrického šifrování - šifrovaný email atd., zejména s ohledem na velmi rozsáhlé instalace po celém světě.

4. Prezentační úroveň předložené práce **92 b. (A)**

Struktura i provázání kapitol na sebe navazuje a práce je docela dobře členěna.

5. Formální úprava technické zprávy **82 b. (B)**

Typograficky dochází ke směšování fontů, kdy jednou je použita kurzíva pro označení metody, jindy u produktu v další kapitole je pro podobné účely použito tučné písmo atd. Jazykově se zdá být vše v pořádku - textu rozumím, ale např. formulace vstupu a požadavky heslo je možné zobrazí přejetím myši přes otazník."

6. Práce s literaturou **90 b. (A)**

Uvedené publikační zdroje jsou adekvátní předložené práci a výborným způsobem pokrývají danou problematiku. V uvedených neschází žádný stěžejní, navíc jsou zdroje aktuální.

7. Realizační výstup **92 b. (A)**

Vytvořené řešení splnilo očekávání a umožňuje přenášet šifrované informace podle zadání. V rámci možností došlo i k optimalizaci a otestování i na dalších platformách (které nebyly součástí zadání), čímž jsem ověřil, že student opravdu dílu rozumí a sám jej podstatnou měrou vytvořil.

8. Využitelnost výsledků

Výsledky a řešení jsou v praxi využitelné. S výsledky jsem seznámil kolegy a v případě požadavku zákazníka na přenos šifrovaných informací, budeme zvažovat i použití tohoto řešení. Každopádně využijeme i shrnutí komerčních produktů, které podobnou problematiku řeší.

9. Otázky k obhajobě

Vzhledem k tomu, že řešení splňuje požadavky, jsou otázky k obhajobě spíše doplnění nebo rozšíření práce. Např. by bylo vhodné promyslet, jak takový software certifikovat. Protože pro certifikaci by musel být software napsán takovým způsobem, aby splnil určitá kritéria a to jak metodická tak i formální. Doplněním by mohly být i určité skriptovací vlastnosti, aby bylo možné zařadit dešifrování automatizovaně třeba po startu. K tomu vede další zamyšlení jak přenášet sdílené tajemství, např. hesla. Dále by mohlo být zamyšlení nad vzdáleným použitím.

10. Souhrnné hodnocení **90 b. výborně (A)**

Pozitivně mne překvapila vysoká úroveň zpracování dané problematiky. Student rozumí a umí použít šifrovací nástroje a zároveň je implementovat do uceleného produktu. Práci tedy hodnotím nadmíru pozitivně.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 27. května 2016

.....
podpis