Posudek oponenta bakalářské práce

Student: Klemens Jakub
Téma: Platformově nezávislé úložiště citlivých dat (id 18471)
Oponent: Herout Adam, prof. Ing., Ph.D., UPGM FIT VUT

1. Náročnost zadání **jednoduché zadání**

Samo znění zadání umožňuje naplnění hodně komplexním způsobem a nebo i jednoduše.
Řešitel k zadání přistoupil až naivním způsobem a vytvořil knihovnu, která je triviálním a pomýleným řešením zadaného problému.

2. Splnění požadavků zadání **zadání nesplněno**

Knihovna umožňuje ukládat pouze řetězce a nabízí funkce, které do řetězce převedou (a následně uloží) hodnoty typu double, float, int a bool. Rozhodně tedy nedošlo k naplnění bodu 2. zadání.
V textu ani na CD není k nalezení žádná zmíňka o demonstrační aplikaci podle bodu 4. zadání (asi za ni nelze počítat prográmky přetištěné na straně 34 textu).
Vyhodnocení řešení (bod 5. zadání) proběhlo pouze změřením informativních časů uložení (tabulka 8.1 na str. 35) a ověřením triviálního faktu, že když alespoň jedna ze tří kopií dat uložených v systému existuje, knihovna uložené hodnoty přečte, zatímco když jsou všechny smazány, knihovna hodnoty již nepřečte (kap. 8.2). U kryptografického systému by bylo daleko zajímavější analyzovat možnosti útoků, zálohování, kompatibility, atp.

3. Rozsah technické zprávy **je v obvyklém rozmezí**

4. Prezentační úroveň předložené práce **30 b. (F)**

Kapitoly 2 a 3 popisují pozadí kryptologie a kryptografie, historii a matematickou podstatu jednotlivých šifer. Pro řešenou knihovnu jsou to však poznatky prakticky irelevantní - řešitel jednotlivé šifry používá jako černé skříňky schované v knihovně Crypto++.
Co relevantní je, technická zpráva ani nezmiňuje: architektura souborových systémů, druhy útoků na kryptografické systémy a obrany proti nim, správa paměti počítače, atp.
Analýza řešeného problému a návrh řešení jsou naprosto nedostatečné. Zde je nejvíc relevantní kapitola 5.1 "Cílová skupina", která je ohromně stručná a nejasná (na to, že má identifikovat proč a co řešitel vlastně řeší). Z ní pak vyplývají požadavky sepsané v kapitole 5.2.
Nedostatečné je také vyhodnocení (kap. 8), jak již bylo zmíněno.

5. Formální úprava technické zprávy **65 b. (D)**

Po jazykové stránce je práce přijatelná - obsahuje nevelký počet jazykových chyb a o něco větší množství chyb typografických. Zejména vadí občasné přesáhnutí šířky řádku (str. 18, 33, 34, 35), mizerná kvalita obrázků (obr. 2.2, 5.1, 5.2, 8.1) a notorická absence mezery před levou závorkou.

6. Práce s literaturou **65 b. (D)**

Text cituje nadstandardní množství kvalitních pramenů z oblasti kryptografie. Nezdá se, že by zdroje řešitel pro svou práci potřeboval a že by je opravdu všechny musel nastudovat.
Podstatné zdroje (a práce s informacemi z nich) v textu chybí (jak bylo uvedeno v bodě 2. tohoto posudku).

7. Realizační výstup **20 b. (F)**

Knihovna je obsažena ve dvou souborech (.cpp, .hpp), doplněných o krátký soubor (.cpp) s unit testy.
Jak bylo uvedeno výše, navržená a vytvořená knihovna je triviálním a degenerovaným řešením zadaného problému.
Zdrojový kód (PISSD.cpp) je příkladem špatného softwarového inženýrství. Celá knihovna je tvořena jednou třídou s jediným atributem (mutex). Vše je uloženo v izolovaných funkcích, které vesměs netestují korektnost svých vstupů (z řetězců se dělají názvy adresářů a souborů bez kontroly na výskyt nepřijatelných znaků, atp.). Chyby nejsou řešeny mechanismem výjimek, ale vypisováním střídavě pomocí "_tprintf" a "std::cerr <<".
Kryptograficky a bezpečnostně je návrh hodně podivný. Názvy modulů a uložených položek jsou pro uživatele (a nebo jiného útočníka) viditelné jako názvy adresářů a souborů. Každý jednotlivý záznam (hodnota float, bool, string, ...) je uložen zvlášť do svého souboru pojmenovaného podle jména položky. Soubory jsou ztrojeny a uloženy s příznakem "skrytý", aby bylo dosaženo "security by obscurity".

8. Využitelnost výsledků

NE

9. Otázky k obhajobě

-

10. Souhrnné hodnocení

20 b. nevyhovující (F)

Zadání nebylo splněno - vytvořená knihovna nemá s bezpečností a kryptografií (a s dobrým softwarovým inženýrstvím) co společného. Nebyla dodána demonstrační aplikace.
Rozsah vytvořeného díla je velice malý (dva soubory s knihovnou, 2044 a 87 řádků).
Technická zpráva popisuje obšírně irelevantní věci (historii a matematickou podstatu šifer) a nevěnuje se věcem podstatným (rysy operačních systémů, bezpečnost a útoky, případy užití knihovny, analýza potenciálně ukládaných dat, návrh demonstrátoru, atp.).

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

V Brně dne: 28. května 2018

.....
podpis