

Posudek oponenta bakalářské práce

Student: Oškera Jan

Téma: Využití druhého SIM slotu telefonu jako bezpečnostního modulu (id 21230)

Oponent: Peringer Petr, Dr. Ing., UIT FIT VUT

- 1. Náročnost zadání** **obtížnější zadání**
Zadání je poněkud problematické, protože mimo jiné vyžaduje rozsáhlé znalosti a experimentování podobně jako při klonování SIM karet, což je náročné.
- 2. Splnění požadavků zadání** **zadání splněno pouze částečně**
Mám výhrady ke splnění bodu 3 zadání - návrh API nakonec skončil pouze použitím existujícího rozhraní pro čtení/zápis kontaktů do SIM karty. To je ale dáno především tím, že experimenty s Java kartami nebyly úspěšné. Proto nehodnotím tento nedostatek přísně. Další problém je v bodu 4, který požaduje vytvoření *podrobné dokumentace řešení*, ale v textu práce ani na přiloženém DVD nic takového není.
- 3. Rozsah technické zprávy** **je v obvyklém rozmezí**
Rozsah textu je vyhovující (46 vysazených stran textu a 5 stran příloh).
- 4. Prezentační úroveň předložené práce** **50 b. (E)**
Struktura textu je nevyhovující - autor na úvodních 29 stranách popisuje převážně formou výčtů a tabulek řadu technických informací převzatých z odpovídajících standardů, takže text připomíná spíše manuál. Vlastnímu přínosu jsou věnovány pouhé 3 strany kapitoly 4 "*Návrh řešení*" a 9 stran kapitoly 5 "*Způsob implementace*", což je jen stěží dostačující. Navíc je text psán nepříliš srozumitelně, je špatně strukturovaný a obsahuje řadu zbytečně podrobných informací, které by mohly být přesunuty do přílohy nebo vynechány. Názvy některých kapitol jsou přinejmenším podivné (viz str. 34 dole). Popis (nakonec neúspěšných) pokusů s Java kartami je nevhodný - viz např. seznam funkcí na str. 37. Popis aplikace v kapitole 5.2. patří většinou do kapitoly 4. Specifikace autorem použitého šifrovacího algoritmu na straně 42 je zcela nedostačující. V textu je příliš mnoho podobných nedostatků.
- 5. Formální úprava technické zprávy** **55 b. (E)**
Typograficky je text práce podprůměrný - řada obrázků není centrována (viz například strana 10), velké množství tabulek narušuje strukturu textu (str. 25), některé kapitoly a odstavce jsou příliš krátké (str. 44), seznam klíčových slov je nesmyslně podrobný.
Po jazykové stránce je práce také slabá - v textu je řada podivných formulací a několik hrubých chyb. Některé chyby souvisí s překladem z angličtiny, např. slovo "*optional*" je přeloženo jako "optimální" (viz strana 10, obr. 3.2 nebo poslední věta na straně 36), atd.
- 6. Práce s literaturou** **75 b. (C)**
Z přehledu použité literatury (46 položek z nichž některé jsou ale zbytečné - například odkazy na Wikipedii) a úvodních kapitol je patrné, že autor musel věnovat studijní části velké množství času.
- 7. Realizační výstup** **50 b. (E)**
Výsledkem této práce je několik zdrojových kódů v Javě, které jsou rozděleny do dvou částí. První část (cca 3000 řádků) je pro experimentování s Java kartami a obsahuje nepříliš dobře strukturovaný kód. Druhá část (cca 250 řádků) je jednoduchá aplikace pro Android. Funkčnost obou částí jsem neověřoval, protože nemám potřebné vybavení a student na můj e-mail se žádostí o předvedení nereagoval.
- 8. Využitelnost výsledků**
Nejsem přesvědčen o vhodnosti používání vytvořené aplikace v praxi.
- 9. Otázky k obhajobě**
 - Vysvětlíte smysl obrázku 5.3 "*Použitý šifrovací algoritmus*" na str. 42.
 - Proč nepoužíváte ověřený šifrovací algoritmus a například *Base64* pro vytvoření textové podoby zašifrovaných dat?
 - Vyjádřete se k možnosti použití speciálních testovacích SIM karet.

10. Souhrnné hodnocení

50 b. dostatečně (E)

Zadání nebylo podle mého názoru zcela splněno (což ale nemusí být u takto experimentálního charakteru zadání jen chyba studenta). Text práce je celkově velmi slabý, především část s popisem řešení. Také výsledná aplikace pro Android je až příliš jednoduchá. Přes uvedené výhrady autor prokázal jisté schopnosti v oblasti experimentování s Java kartami a vytváření aplikací pro OS Android. Také musel prostudovat poměrně rozsáhlou literaturu. Proto navrhuji celkové hodnocení **E**.

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

V Brně dne: 31. května 2018

.....
podpis