Posudek oponenta bakalářské práce

Student: Balvín David
Téma: Šifrování nad textovými zprávami pro Android (id 19727)
Oponent: Švéda Petr, Mgr., UITS FIT VUT

1. Náročnost zadání **obtížnější zadání**

Cílem zadání práce byla zřejmě vyšší náročnost práce - nastudovat více protokolů a na základě této znalosti navrhnout možné optimální způsoby šifrování pro různé protokoly. Předložená práce se omezila na textové zprávy.

2. Splnění požadavků zadání **zadání splněno pouze částečně**

V bodu č. 1 se práce omezuje pouze na textové zprávy. Ostatní protokoly jsou pomíjeny - např. jediná zmínka XMPP je v odstavci 7.1. závěru práce, protokoly TOX, ZNS nebo jiné nejsou v práci zmíněny vůbec. Očekával bych přehled protokolů, jejich popis a charakteristiku výhod a nevýhod jako součást kapitoly 2 textu práce. Minimálně z pohledu zdali obsahují podporu šifrování mezi koncovými uživateli. Ohledně dalších částí práce lze polemizovat o míře splnění na hranici nezbytného minima.

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

Z hlediska číslovaných 35 normostran včetně příloh je zpráva v obvyklém rozsahu, celkově však budí dojem zbytečně nadhodnoceného rozsahu. Obrázky jsou zbytečně prezentovány na celou stranu - např. 3.1 na straně 15. Prázdné části stran - např. kapitola 4, strana 19 atp.

4. Prezentační úroveň předložené práce **50 b. (E)**

Logické členění práce je z hlediska struktury bez výhrad, problém ve srozumitelnosti je zejména z důvodu obsahu. Formulace ve zprávě zakládají důvodné pochybnosti o pochopení problematiky, kterou se práce měla zabývat. V implementaci v kapitole 5.5. je popsáno Huffmanovo kódování, nikoliv však šifrování. Z vlastního popisu implementace není patrné, které části kódu jsou převzaté a které jsou vlastní práce.

5. Formální úprava technické zprávy **50 b. (E)**

Typograficky práce obsahuje nešťastné prvky - nesouvislý tučný text (strana 3), nejednoznačný význam užívání kurzívy (odstavec strana 4 x jednotlivé samostatné věty strana 10 a 11, které nejsou sázeny ani jako samostatný odstavec), jednotlivé řádky odrážek na různých stranách (strana 7 a 8). V textu práce jsou nešťastně užívány počeštěné anglické termíny - např. scrollování (strana 22), defaultní (strana 22), Broadcasty (strana 22), Intent-em (strana 23).

6. Práce s literaturou **25 b. (F)**

Z textu práce není zřejmé, které části jsou převzaté. Citace jsou pouze na WWW stránky, nikoliv na původní díla. Například v odstavci 5.5 bych očekával citaci původního díla D. A. Huffman, "A Method for the Construction of Minimum-Redundancy Codes," in Proceedings of the IRE, vol. 40, no. 9, pp. 1098-1101, Sept. 1952. doi: 10.1109/JRPROC.1952.273898

7. Realizační výstup **25 b. (F)**

Z popisu implementace v textu zprávy ani z vlastního zdrojového kódu není patrné co je vlastní dílo a co je převzato. Navíc formulace v textu zprávy je v rozporu obsahem kódu. V závěru na straně 30 je konstatováno od upuštění od asymetrické šifry. V kódu Cryptic.java je volání Cipher.getInstance("AES/ECB/PKCS7Padding", "BC"). Pravděpodobně byl převzat buď cizí kód anebo nebyla pochopena problematika. Nápadná podobnost s kódem org.opensourcephysics.controls.Cryptic není nikde vysvětlena.

8. Využitelnost výsledků

Ve stávající podobě je aplikace spíše nepoužitelná. Obsahuje řadu chyb již v oblasti návrhu - viditelné znaky při zadání hesla bez možnosti volby, užití Huffmanova kódování výrazně zjednodušuje slovníkový útok, ...

9. Otázky k obhajobě

1. Prokažte pochopení problematiky šifrování. Kterou šifru lze chápat jako absolutně bezpečnou? Kde jsou její slabiny a výhody?

2. Vysvětlete, které části práce jsou vlastní dílo a které části jsou převzaté.

3. Je vzorek 5 respondentů (statisticky nepravděpodobný případ 5 žen) opravdu reálným a dostatečným testem?

4. Vysvětlete příčiny pádu Vaší aplikace při spuštění v simulátoru KO Player 1.4.1055.

10. Souhrnné hodnocení

49 b. nevyhovující (F)

Práci jako celek vnímám jako nevyhovující a doporučuji k přepracování. Její obsah neprezentuje zvládnutí problematiky a není jasné co je vlastní dílo. Případnou možnost obhajoby přímo nevylučuji. Jako stěžejní pro možnou obhajobu práce vnímám odpovědi na první dvě otázky.

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

V Brně dne: 1. června 2017

.....
podpis