Posudek oponenta bakalářské práce

Student: Ambrož Tomáš
Téma: Rekonstrukce zachyceného provozu komunikačních nástrojů (id 18833)
Oponent: Matoušek Petr, Ing., Ph.D., M.A., UIFS FIT VUT

1. Náročnost zadání **obtížnější zadání**

Zadání považuji za obtížnější, neboť se týká rekonstrukce provozu aplikací WhatsApp a Viber, což jsou proprietární systémy využívající šifrování. Zpracování a analýza dat je založena na reverzním inženýrství a studiu odborných článků.

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

Popis protokolů Viber a WhatsApp (bod č.2) je proveden velmi stručně. U protokolů Viber jde o popis dvou zpráv HTTP Get a Post, ostatní text tvoří popis HTTP a SSL. Popis WhatsApp víceméně kopíruje výsledky článku [11] včetně obrázků. Taktéž implementace je provedena značně minimalisticky. Analyzátor protokolu Viber nebyl implementován vůbec, u protokolu WhatsApp se analýza týká protokolu verze 1.5, která se již nepoužívá. Proto je demonstrace ukázána pouze na jedné zachycené komunikaci. U testování aplikace (str. 30-31) není jasné, zda aplikace správně funguje. Z výpisu exportu dat aplikace toto není zřejmé.

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

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

Technická zpráva z větší části popisuje implementační detaily zvoleného prostředí, volání funkcí a závislosti tříd. Toto není z mého pohledu pro čtenáře přínosné. Zajímavější by byl detailní rozbor komunikace, popis analýzy dat a zpracování výsledků. Například obecný popis symetrických šifrovacích algoritmů na str. 13 - 14 není vzhledem k tématu práci nutný. Podobně popisy návrhového vzoru MVVM (str. 19) či volání funkcí a implmentace tříd (str. 23-28) nejsou pro čtenáře přínosné. Popis testování je z mého pohledu nedostatečný, protože z textu není jasné, na jakém datovém vzorku testování probíhalo, kolik tam bylo paketů a konverzací WhatsApp apod.

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

Práce obsahuje překlepy, které bylo možné odstranit automatickou kontrolou pravopisu (např. ispell pro LaTeX). Tabulky 5.1 a 5.2 na str. 30 a 31 nemají velkou vypovídací hodnotu.

6. Práce s literaturou **80 b. (B)**

Použitá literatura je relevantní. U článků z konferencí či časopisů se v Literatuře neuvádí odkaz URL na jejich elektronickou verzi. Také u standardů IETF RFC není potřeba odkazy URL uvádět.

7. Realizační výstup **55 b. (E)**

Součástí realizačního výstupu byl modul do nástroje NetFox Detective. Zmíněný model WhatsApp umí zpracovat komunikaci protokolem WhatsApp při zadání klíče a hesla. Aplikace zobrazí základní přehled rozpoznaných konverzací WhatsApp. Funkčnost lze vyzkoušet pouze na jednom dodaném souboru, kde aplikace rozpozná pět konverzací, ale pouze dvě jsou blíže specifikované. U zbývajících tří chybí v exportu jakékoliv informace o tom, o jaká data se jedná. Ani v textu zprávy toto není vysvětleno.

8. Využitelnost výsledků

Implementace se týká verze protokolu, který se v praxi nepodporuje. Použitelnost je tedy minimální.

9. Otázky k obhajobě

1. Proč jste neimplementoval analýzu protokolu Viber?
2. Proč jsou tři exportované konverzace z testovacího souboru wh.pcap prázdné, tj. co to znamená?
3. V čem vidíte vlastní přínos práce?

10. Souhrnné hodnocení **55 b. dostatečně (E)**

Přestože se jednalo o náročnější zadání, výsledek i přínos práce je podle mého názoru minimalistický.

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

V Brně dne: 27. května 2016

.....

podpis