Posudek oponenta bakalářské práce

Student: Letavay Viliam
Téma: Rekonstrukce zachycené komunikace na platformě iOS (id 18557)
Oponent: Kmeť Martin, Ing., UIFS FIT VUT

1. Náročnost zadání **obtížnější zadání**

Obtiažnosť zadania spočíva v analýze proprietárnych protokolov ku ktorým neexistuje existujúca dokumentácia. Implementácia je naviac zvolená ako rozšírenie nástroja Netfox Detective, čo pre študenta znamenalo zoznámenie sa s jeho pomerne zložitou architektúrou. Platforma Netfox Detective je naviac sama vo vývoji, a preto sa študent musel vyrovnať aj so zmenami v samotnej platforme počas riešenia zadania.

2. Splnění požadavků zadání **zadání splněno s podstatným rozšířením**

Všetky body zadania boli splnené. Študent naviac v rámci riešenia rozšíril funkčnosť nižšie položených vrstiev samotnej platformy Netfox Detective.

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

4. Prezentační úroveň předložené práce **65 b. (D)**

Študent by mal zapracovať na schopnosti štruktúrovať text. Úvod je pomerne krátky a neuvádza čitateľa do celej problematiky. Názvy kapitol sú nepresné a členenie práce je nejasné. Napríklad obsah kapitoly 2 úplne nekorešponduje s názvom a kapitola 3 by mala byť rozdelená do viacerých kapitol, čim by sa znížila potreba nadpisov 3. a 4. úrovne, a teda sa značne zvýšila "stráviteľnosť" tejto kapitoly pre čitateľa. Na druhú stranu popis samotných parametrov komunikácie je pomerne precízny.

5. Formální úprava technické zprávy **70 b. (C)**

Práca je vysádzaná v systéme LaTeX, a teda sa v nej nevyskytujú výrazné typografické nepresnosti. Objavujú sa však pomerne zbytočné chyby v podobe pretekajúcich obrázkov a podobne, ktoré ukazujú na dokončovanie práce v poslednej chvíli.

6. Práce s literaturou **80 b. (B)**

Študent pracoval s pomerne úzkou množinou literatúry. Táto však bola použitá a citovaná správne.

7. Realizační výstup **80 b. (B)**

V rámci práce na zadaní študent vytvoril pomerne veľké množstvo rekonštrukčných modulov a zároveň upravil aj existujúce. Z tohto dôvodu by som množstvo práce, ktoré študent musel venovať analýze protokolov a implementácii označil až masívnym. Na druhú stranu fáza testovania je podľa môjho názoru nedostatočná, čomu zodpovedá aj jej popis pozostávajúci z dvoch pomerne krátkych odstavcov. Pri testovaní bola použitá len jedna dátová sada, ktorá bola vytvorená študentom a bola pravdepodobne použitá aj ako referenčné dáta pri vývoji. Bolo by vhodné použiť viacero dátových sád, ktoré vznikli nezávisle na sebe a ideálne aj od iných užívateľov.

8. Využitelnost výsledků

Práca rozširuje existujúci nástroj a jej výsledky sú pripravené na aplikáciu v sieťovej forenznej analýze.

9. Otázky k obhajobě

1. V rámci práce ste spracoval modul na rekonštrukciu protokolu SPDY. Vývoj tohoto protokolu bol však zastavený v prospech protokolu HTTP/2. Aká je aktuálna a predpokladaná budúca využívanosť tohto protokolu?
2. V práci ste popisoval podvrhnutie certifikátov v systéme iOS po Jailbreaku. Skúmal ste možnosti podvrhnutia aj v systéme bez týchto úprav?
3. Vaše zadanie hovorí o rekonštrukcii komunikačných nástrojov na platforme iOS. Prečo ste sa teda v práci vôbec nevenoval komunikačnému nástroju iMessage, ktorý je pre túto platformu špecifický?

10. Souhrnné hodnocení **80 b. velmi dobře (B)**

Aj keď práca samotná nemá príliš vysokú úroveň a fáza testovania výsledkov bola značne podcenená, je potrebné prihliadnuť na pomerne vysokú obtiažnosť zadania. Študent naviac vykonal pomerne veľké množstvo práce pri realizácií výstupu, z ktorého časti boli nad rámec samotného zadania. Z tohoto dôvodu navrhujem hodnotenie stupňom B.

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

V Brně dne: 30. května 2016

.....
podpis