

Posudek oponenta bakalářské práce

Student: Zuzelka Jozef
Téma: Nástroj pro zachycení síťového provozu s aplikačním tagem (id 20013)
Oponent: Lichtner Ondrej, Ing., UIFS FIT VUT

1. Náročnosť zadání **obtížnější zadání**

Práca vyžadovala komplexné naštudovanie technológií zachytávania sieťovej komunikácie, identifikácie aplikácií ako aj optimalizácií potrebných pre bezstratové zachytávanie. Keďže zadanie bolo riešené multiplatformovo bolo potrebné štúdium veľkého množstva technológií, ktoré boli využité vo finálnom riešení. Zadanie preto považujem za náročnejšie.

2. Splnění požadavků zadání **zadání splněno**

Zadanie splnené bez výhrad. Nad rámec zadania študent vypracoval článok pre konferenciu Excel@FIT, na ktorú bol prijatý.

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

Práca je vysádzaná LaTeXovou šablónou na 37 strán textu vhodne dopĺňaného obrázkami prípadne ukázkami kódu. Je teda v obvyklom rozsahu.

4. Prezentční úroveň předložené práce **85 b. (B)**

Prvé tri kapitoly (okrem úvodu), sa zaoberajú problematikami zachytávania sieťových komunikácií, rôznymi formátmi súborov vhodných pre uloženie zachytených dát a možnosťami identifikácie aplikácií. Kapitoly sú logicky členené podľa technológie, ktorej sa venujú alebo operačného systému, pre ktorý sú relevantné. Na predchádzajúce kapitoly potom naväzuje kapitola, ktorá dopodrobna popisuje návrh a implementáciu odovzdanej aplikácie. Samostatne je vyčlenená kapitola popisujúca formát výstupného súboru. V poslednej obsahovej kapitole sa autor venuje výkonnostnému testovaniu aplikácie na oboch podporovaných operačných systémoch.

Ako plus hodnotím, že dlhšie kapitoly, venujúce sa väčšiemu počtu tém, sú zakončené sekciou, ktorá stručne zhrnie a zopakuje dôležité informácie.

Kapitola 4, o možnostiach identifikácie aplikácií, má ale iba dve sekcie na dvoch stranách a túto zhrňujúcu sekciu nepotrebuje.

5. Formální úprava technické zprávy **85 b. (B)**

Po typografickej stránke je práca v poriadku. Práca je písaná v anglickom jazyku. Miestami obsahuje vety s nesprávnym slovosledom alebo inými štylistickými chybami, celková čitateľnosť textu je ovplyvnená iba mierne.

6. Práce s literaturou **95 b. (A)**

Študent v práci cituje z množstva relevantných zdrojov, zoznam literatúry obsahuje 33 položiek. V texte sú riadne odkazované.

7. Realizační výstup **95 b. (A)**

Vytvorená aplikácia spĺňa všetky požiadavky na funkčnosť a je jednoducho použiteľná. Podporuje operačné systémy Windows a Linux, a je pripravená na rozšírenie o ďalšie OS. Aplikácia je naprogramovaná v C++ a rozumne organizovaná do modulov a tried, všetky zdrojové kódy sú dokumentované pre nástroj doxygen.

8. Využitelnost výsledků

Práca prináša koncept zahrnutia identifikácie aplikácií priamo do zachytenej sieťovej komunikácie a implementuje jeho riešenie funkčne na dvoch operačných systémoch. Možnosť použitia v praxi si viem predstaviť ako zjednodušenie administrácie systémov, prípadne analýzy možných bezpečnostných problémov.

9. Otázky k obhajobě

1. Premýšľali ste o rozšírení dostupných multiplatformových nástrojov pre zachytávanie komunikácie (napríklad Wireshark), o schopnosti identifikácie aplikácií?

2. Dátový blok obsahujúci identifikáciu aplikácii, ktorý pripájate k zachyteným dátam, mapuje meno aplikácie na identifikáciu paketov, ktoré aplikácii patria. Keďže chcete ale priradiť meno aplikácie k paketu nebolo by lepšie mať dáta mapované opačným spôsobom? Teda ak mám paket identifikovaný portom, protokolom, adresou a časovou značkou, podľa týchto údajov budem vyhľadávať aplikáciu, ku ktorej patrí.

10. Souhrnné hodnocení **95 b. výborně (A)**

Odovzdaná práca je kvalitným riešením náročnejšieho zadania. Hlavným dôvodom náročnosti je zameranie na

podporu viacerých operačných systémov a z toho vyplývajúca celková rozsiahlosť riešeného problému. Okrem vytvorenia kvalitného riešenia študent vytvoril aj článok pre konferenciu Excel@FIT.

Celkovo teda prácu hodnotím na A.

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

V Brně dne: 31. května 2017

.....
podpis