

Posudek oponenta diplomové práce

Student: Slivka Miroslav, Ing.
Téma: Rekonstrukce webmailového provozu (id 17546)
Oponent: Ryšavý Ondřej, doc. Ing., Ph.D., UIFS FIT VUT

1. **Náročnost zadání** průměrně obtížné zadání
2. **Splnění požadavků zadání** zadání splněno
3. **Rozsah technické zprávy** je v obvyklém rozmezí
4. **Prezentační úroveň předložené práce** 70 b. (C)

Technická zpráva obsahuje motivaci, rozbor problému, návrh jeho řešení a zhodnocení dosažených výsledků včetně jejich otestování. Návrh je logický, přestože jednotlivé kapitoly nejsou příliš vyvážené. Jako největší nedostatek vidím poměrně mělký rozbor problematiky zabezpečeného přenosu, kde se uvádí informace o SSL/TLS, které jsou obecně dostupné.
5. **Formální úprava technické zprávy** 80 b. (B)

Práce obsahuje drobné typografické a jazykové nedostatky (například časté zvláštní skloňování cizích slov "Handshake-u", cypher->cipher). Nicméně text je dobře srozumitelný a výstižně popisuje řešenou problematiku. Text je doplněn obrázky a schémata, které přináší užitečné informace.
6. **Práce s literaturou** 75 b. (C)

Literatura odpovídá řešené problematice. Často se jedná spíše o obecné zdroje informací. Při výběru zdrojů se autor mohl více zaměřit na zdroje, které poskytují specifické informace k řešené problematice.
7. **Realizační výstup** 90 b. (A)

Realizační výstup je funkční a byl otestován jak pomocí unit testů tak na předem připravených datech. Výstupem jsou softwarové komponenty napsány v jazyce C#. Tyto komponenty jsou integrovány do existující prostředí Netfox Detective, ve kterém byly také důkladně otestovány.
8. **Využitelnost výsledků**

Výsledky budou integrovány do prostředí pro analýzu síťové komunikace Netfox Detective. Vytvořené výsledky tak naleznou praktického uplatnění.
9. **Otázky k obhajobě**
 - Při analýze jednotlivých webmail systémů (na straně 6) uvádíte také způsob předávání parametrů. Jedná se o metodu GET či POST?
 - Vysvětlíte prosím obrázek 4.1. Jak je to tedy s výkonností implementace? Co ji ovlivňuje?
 - Uvádíte, že SSL Decrypter provádí analýzu SSL/TLS handshake komunikace. Je nutné mít veškerou tuto komunikaci k dispozici?
10. **Souhrnné hodnocení** 80 b. velmi dobře (B)

Předložená práce je kvalitní. Realizační výstup je na výborné úrovni, je plně použitelný a integrovatelný do existujícího systému. Předložená technická zpráva neobsahuje vážné nedostatky, ale by mohla jít do větší hloubky zejména v rozboru problému.

V Brně dne: 12. června 2015

.....
podpis