Posudek oponenta bakalářské práce

Student: Lysoněk Milan
Téma: Existující útoky na SSL/TLS (id 20047)
Oponent: Smrčka Aleš, Ing., Ph.D., UITS FIT VUT

1. Náročnost zadání **obtížnější zadání**

Téma zadání vyžaduje hlubší pochopení problematiky protokolů SSL/TLS, jejich bezpečnosti a fuzzy testování.

2. Splnění požadavků zadání **zadání splněno**

3. Rozsah technické zprávy **přesahuje obvyklé rozmezí**

Bakalářská práce má cca 60 normostran, všechny části dávají smysl.

4. Prezentační úroveň předložené práce **80 b. (B)**

Technická zpráva rozebírá současný stav implementace SSL/TLS, bezpečnostní rizika a pro vybrané bezpečnostní chyby popisuje způsob jejich reprodukce a integraci do fuzzeru Tlsfuzzer. Celkově je práce pochopitelná pro čtenáře. Mám jen pár drobných výhrad: např. kostrbatý popis inicializační fáze handshake, přítomnost popisu Tlslite-ng (podkap. 2.3.4) moc nezapadá mezi ostatní implementace (není dostatečně zdůvodněna), klíčový popis architektury projektu Tlsfuzzer by měl být podrobnější. V příloze by měl být lépe popsán obsah přiložených dat včetně vyčlenění vlastního přínosu.

5. Formální úprava technické zprávy **80 b. (B)**

Jazyková a typografická úroveň je nadprůměrná. Nelibé je skloňování cizích výrazů "handshaku", "warning alerty", "payloadu", nebo citace v názvu podkapitoly.

6. Práce s literaturou **70 b. (C)**

V technické zprávě jsou řádně odlišeny vlastní a cizí výsledky včetně citací. Mám výhradu k nadměrnému využití Wikipedie.

7. Realizační výstup **85 b. (B)**

Kvalita realizačního výstupu nespočívá v množství, ale ve správné integraci a čitelnosti. Výsledkem jsou části kódu, které rozšiřují stávající nástroj Tlsfuzzer o testy dalších druhů zranitelnosti. Kódy jsou dostatečně zdokumentovány a experimentálně ověřeny.

8. Využitelnost výsledků

Výsledek práce je cílen právě na využitelnost v praxi a to se studentovi podařilo. Implementované testy budou používány v praxi.

9. Otázky k obhajobě

- Řekněme, že se test zaměřuje na existující zranitelnost. Co, s ohledem na vámi zvolenou terminologii, znamená, že výsledek testu je chyba?

10. Souhrnné hodnocení **85 b. velmi dobře (B)**

Student se věnoval aktuální problematice, seznámil se s právě vyvíjeným produktem Tlsfuzzer a úspěšně se mu podařilo do něj integrovat podporu o detekci dalších zranitelností.

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

V Brně dne: 30. května 2017

.....
podpis