Posudek oponenta bakalářské práce

Student: Šumšal František
Téma: Průběžné testování interoperability knihoven TLS/SSL (id 19513)
Oponent: Fiedor Tomáš, Ing., UITS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

Náročnost zadání považuji mezi průměrně obtížným a obtížným zadání. Jedná se spíše o práci implementačního charakteru, nicméně vyžadující důkladné pochopení protokolu TLS/SSL a jeho implementací.

2. Splnění požadavků zadání **zadání splněno**

Může se zdát, že bod 4. nebyl splněn, protože práce nepojednává o demonstraci funkčnosti na příkladech s uměle vytvořenými chybami, ale namísto toho práce nalezla reálné chyby. Toto považuji za více než uspokojující demonstraci užitečnosti i funkcionality vytvořené implementace.

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

Práce je v obvyklém rozmezí, sestává z 29 vysázených stran (tzn. cca 43 normostran). Kapitoly jsou informačně bohaté a všechny jsou nezbytně nutné pro pochopení práce. Zpráva navíc obsahuje cca 9 stránek příloh, které přináší užitečné detaily o metodologii a průběhu testování interoperability TLS/SSL knihoven.

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

Struktura práce je logická (prvně jsou představeny protokoly a testované knihovny; pak je rovnou diskutováno řešení, s veškerou analýzou možností a problémy, které bylo nutné řešit; nakonec je funkcionalita experimentálně vyhodnocena výčtem nalezených chyb). Menší výhradu mám k podkapitole ohledně CI Jenkins, kde je v textu zmiňován Beaker, OpenStack a Docker, které jsou blíže popsány až na konci podkapitoly, což může být matoucí. Jinak je práce dobře pochopitelná.

5. Formální úprava technické zprávy **90 b. (A)**

Obsahuje mírné množství typografických chyb (např. jednopísmenná slova na konci odstavce), přesahů (např. str. 12, 17), překlepů (např. v závěru stared -> started), několik chybných dělení slov (např. SSL/TLS v úvodu) a několik nevhodných formulací. Na druhou stranu je práce psána angličtinou na vysoké úrovni, minimalizuje vatu a vyjadřuje se technicky a precizně.

6. Práce s literaturou **80 b. (B)**

Práce cituje 20 zdrojů, z toho jde většinou o RFC a manuály nástrojů. Vzhledem k implementační a síťové podstatě zadání toto považuji za OK. Není mi známo, že by byla porušena citační technika.

7. Realizační výstup **100 b. (A)**

Práce je veřejně dostupná na githubu. Jedním z výstupů práce je integrace v Travis CI, což vysoce oceňuji, protože tím lze lehce ověřit reprodukovatelnost výstupu práce. Hlavní jádrem práce je pak sada shell skriptů, které podstatně rozšířily počáteční množinu testovacích případů. Rovněž si velmi cením, že práce má reálné výsledky---během experimentálního vyhodnocení a řešení práce bylo nalezeno cca 8 chyb v různých knihovnách implementujících TLS/SSL.

8. Využitelnost výsledků

Práce je šířena pod GNU/GPL licencí. Výsledky jsou již schváleny a sloučeny v upstreamu souvisejícího projektu, práce má reálné využití a bude zajisté velice užitečná pro vývojáře TLS/SSL knihoven. Během experimentálního vyhodnocení a vývoje byly nalezeny a vývojářům nahlášeny reálné chyby.

9. Otázky k obhajobě

1. Předpokládejte, že jsem autorem nové implementace TLS/SSL (nebo např. zmiňovaného BoringSSL). Jaké kroky je třeba podniknout, aby tato implementace byla podporována Vaším řešením?
2. Je Vaše řešení multiplatformní? Bylo by možné testovat interoperabilitu knihoven např. na MacOS X?

10. Souhrnné hodnocení **90 b. výborně (A)**

Student navrhl a realizoval fungující řešení testování interoperability implementací TLS/SSL knihovne. Velice pozitivně hodnotím, že práce byla napsaná v dobré angličtině a je tímto dostupná širší skupině vývojařů. Dále oceňuji její reálné výsledky (8 nalezených chyb), použitelnost do budoucna a fakt, že je již schválena a sloučena v upstreamu projektu. Práci pana Šumšala proto hodnotím **90 (A)**.

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

V Brně dne: 31. května 2017

.....
podpis