Posudek oponenta závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Václav Švec
Oponent práce: Ing. Tomáš Zahradnický, Ph.D.
Název práce: Podpora pro filtrování SSL/TLS komunikace v Privoxy
Obor: Informační technologie

Datum vytvoření: 14. 6. 2017

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	*1=mimořádně náročné zadání,* ***2=náročnější zadání,*** *3=průměrně náročné zadání,* *4=lehčí, ale ještě dostatečně náročné zadání,* *5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Zadání práce hodnotím jako náročnější vzhledem k tomu, že student se musel seznámit a pochopit zdrojové kódy produktu Privoxy a následně na nich stavět dále.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Konstatuji, že zadání práce bylo splněno.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	***1=splňuje požadavky,*** *2=splňuje požadavky s menšími výhradami,* *3=splňuje požadavky s většími výhradami,* *4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Zadání svým rozsahem splňuje požadavky na bakalářskou práci.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*85 (B)*

Popis kritéria:
Posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře.

Komentář:
Věcná úroveň práce je velmi dobrá. Student v některých případech nezabíhá do detailů, které by si práce na toto téma zasloužila. Např. ze sekce 3.2.1 není patrné, že je možné certifikát od serveru vůbec nedostat (obrázek na str. 25 má zprávu Certificate v závorkách, což znamená její nepovinnost), avšak text se o této eventualitě nezmiňuje. Stejně tak šifrování. Teoreticky je možné navázat TLS spojení, které nebude ani šifrovat, ani používat MAC a dokonce bude i bez jakéhokoliv certifikátu. Jako další příklad uvádím nedostatečnou analýzu příčiny selhání při importu certifikátu v sekci 4.4.1 a že pro prohlížeč Mozilla Firefox je třeba řešit věc jinak - jak, to už práce nezmiňuje. Dalším příkladem je mělké řešení nekompatibility licencí knihovny OpenSSL s licencí Privoxy - student zvolí nějakou knihovnu, aniž by patřičně zdůvodnil proč. Stejně dobře se mohl rozhodnout například pro GnuTLS, anebo požádat autory Privoxy o výjimku. Dále student píše o kontrole revokovaných certifikátů, avšak nezmiňuje se vůbec o možnosti použití OCSP Stapling, které by mohlo věc značně urychlit. Další věcí, kterou považuji za nevhodnou je způsob synchronizace na str. 37. Vytvořit pole 65536 mutexů je podle mého názoru naivní, když by stačilo použít bitové pole s RMW (atomickými) operacemi, čímž by se velmi silně ušetřilo na přepínání kontextu i paměti. Alternativně by šly použít zámky v souborovém systému (man flock, man fcntl).

Logickou úroveň práce považuji za výbornou.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*90 (A)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3.

Komentář:
Formální úroveň práce považuji za výbornou.
Jazykovou stránky práce považuji za velmi dobrou. Nacházím občas nějaký anglicismus typu handshake (navazování spojení), mutex (zámek), atd., pro který existuje ustálený český překlad.
Typografická stránka práce je výborná; nacházím jen 2 vytékající slova ze zrcadla stránky (str. 13 sekce 1.6.2 odst. 2 řádek 2, str. 39).

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*100 (A)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Práce cituje celkem 22 zdrojů. Webové a knižní zdroje. Pro tuto práci považuji jejich množství a kompozici za bezproblémovou.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*90 (A)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
Student navrhl, implementoval a otestoval rozšíření nástroje třetí strany Privoxy. K tomu, aby mohl student tuto činnost provést, musel vynaložit značné množství úsilí. Je trochu škoda, že některé záležitosti nezkoumal hlouběji (například použití TLS) anebo efektivitu zamykání.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Výsledky práce považuji zatím za použitelné pro testovací prostředí. Pokud by student pokračoval na této práci jako na své diplomové práci, dala by se dotáhnout a zoptimalizovat pro nasazení v produkčním prostředí.

Je velká škoda, že práce je psána v českém jazyce, protože mohla sloužit jako dokumentace pro uživatele.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
9. Otázky k obhajobě	

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:
1. Proč zvolil student knihovnu mbed TLS a nepřenesl možnost volby knihovny pro TLS na uživatele, případně nepožádal autory Privoxy o výjimku?
2. Jaké nacházíte rozdíly mezi komerčními kořenovými certifikáty a certifikátem generovaným na str. 35? Proč Firefox certifikát neakceptuje?
3. Privoxy je pod licencí GNU GPLv2 licencí. Nemělo se zvolit proto prohlášení č. 4, aby se volnost licence zachovala, když se uvádí např. část zdrojových kódů v příloze?

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*90 (A)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
I přes značné množství výhrad považuji bakalářskou práci pana Václava Švece velmi rozsáhlou a složitou. Práci doporučuji k obhajobě a hodnotím ji stupněm A (výborně).

Podpis oponenta práce: