FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Václav Švec
Oponent práce:	Ing. Tomáš Čejka, Ph.D.
Název práce:	Modernizace podpory protokolů SSL/TLS v Privoxy
Obor:	Počítačová bezpečnost

Datum vytvoření: 4. 6. 2020

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. 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 dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Komentář:
Práce se zabývá analýzou HTTP proxy (Privoxy), průzkumem aktuálního stavu a podpory kryptografických protokolů ve webových prohlížečích v posledních letech, nakonec práce řeší v rámci praktické části rozšíření existující HTTP proxy o podporu TLS. Odevzdané řešení splňuje zadání a naplánované cíle.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*75 (C)*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále 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. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Komentář:
Text práce obsahuje drobné nedostatky (např. překlepy), logická struktura práce by se dala vylepšit:
Na konci odstavce v Sekci 1.4 str. 5 se autor odkazuje na tabulku, která ale na sousedních stránkách není, možná se jedná až o Tabulku 1.1 na str. 20;
Na str. 36 autor zmiňuje a popisuje "Hlavní cíle" - popis cílů by ale asi měl být čtenáři znám již dříve.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*95 (A)*

Popis kritéria:
Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů

Komentář:
Výsledkem práce je funkční použitelné rozšíření nástroje Privoxy, tzn. HTTP proxy. Autor přidává podporu aktuálně používaných kryptografických protokolů pomocí linkované moderní knihovny, čímž významně vylepšil funkcionalitu celého systému a umožnil použití zabezpečené komunikace v rámci sítě s nasazenou aplikací Privoxy.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*95 (A)*

Popis kritéria:
Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Komentář:

Nepísemnou část práce hodnotím velice pozitivně. Podle verzovacího systému lze jasně vidět, že se jednalo o poměrně rozsáhlou a náročnou vývojářskou úlohu.
Na základě autorovy osobní ukázky funkčního prototypu jsem se navíc dozvěděl, že autor jedná s vývojáři upstream verze Privoxy o začlenění vytvořených úprav. Podle prvních zjištění se zdá, že úpravy a vylepšení (např. sdílení soketů) budou přijaty jako užitečné pro komunitu.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*

5. Otázky k obhajobě

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

Otázky:

1) Na str. 18 autor prezentuje graf využití různých verzí TLS (Obr. 1.4). Kde a jak bylo měření prováděno?
2) Z pohledu síťového provozu (na úrovni paketů) přináší upravená verze Privoxy a nově implementované chování sdílení síťových soketů významnou změnu v chování HTTP komunikace. Dokážete odhadnout, zda je kvůli těmto vylepšením na síťové úrovni snadnější rozpoznat provoz vytvořený proxy serverem od "normální" komunikace, kterou by generovaly samotné webové prohlížeče?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*

6. Celkové hodnocení

95 (A)

Popis kritéria:
Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

Text hodnocení:

Písemná část práce má sice nedostatky, ale vzhledem k tomu, že je psána v češtině, není tolik významná pro mezinárodní spolupráci jako nepísemná část práce. Nepísemná část vypadá jako dobře vypracovaná a podle autorova prohlášení je velká šance, že bude začleněna do oficiálně zveřejněných zdrojových kódů Privoxy. Tyto zdrojové kódy jsou spravovány zahraniční komunitou. Proto práci celkově hodnotím kladně.

Podpis oponenta práce: