



Hodnocení vedoucího závěrečné práce

Student: Bc. Václav Švec
Vedoucí práce: Ing. Josef Kokeš
Název práce: Modernizace podpory protokolů SSL/TLS v Privoxy
Obor: Počítačová bezpečnost

Datum vytvoření: 26. 5. 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: Odevzdaná práce splňuje zadání a v některých ohledech jde i výrazně nad jeho rámec. Analýza vývoje v prohlížečích je například velmi pěkně zpracovaná.	
Hodnotící kritérium:	Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):
2. Písemná část práce	98 (A)
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: Textová stránka práce je na velmi vysoké úrovni. Student systematicky a přehledně postupuje od analýzy vývoje problémové oblasti přes analýzu silných a slabých stránek stávající implementace po návrh řešení jednotlivých oblastí. Po obsahové stránce nemám co vytknout, také jazyková je vysoce nadprůměrná. Rozsah je naprosto vyhovující. Všiml jsem si jediné skutečné chyby v příkladu na konci strany 82, zřejmě v důsledku chybně použitého search&replace.	
Hodnotící kritérium:	Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):
3. Nepísemná část, přílohy	89 (B)
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: Programová část práce je také velmi kvalitní. Student vyřešil takřka všechny nedostatky, které měla předchozí implementace, a navíc dodal práci správnou "štábní kulturu" tak, aby mohla být skutečně používána - zdrojové kódy zpracoval v Gitu, zajistil uživatelsky přívětivou kompilaci a připravil potřebnou dokumentaci. Umožnil také snadné rozšiřování programu o použití dalších kryptografických knihoven, pokud by to bylo potřeba. Mrzí mě pouze dva aspekty, oba plynoucí z nedostatku času: 1) Nepodařilo se odhalit důvody, proč někdy program zablokuje víc přenosů, než by měl. Děje se to jen v některých instalacích a jen na některých webech, podle vnějších znaků možná v souvislosti s generováním certifikátů na straně proxy serveru a s cachováním obsahu na straně prohlížeče. Vzhledem k velmi specifické konfiguraci, na které se chyba projevuje, nejde o příliš závažný nedostatek. 2) Vytvořená úprava nebyla zatím předána autorovi Privoxy pro zařazení do oficiální verze projektu.	

<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</i>
4. Hodnocení výsledků, jejich využitelnost	92 (A)
<i>Popis kritéria:</i> 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.	
<i>Komentář:</i> Úpravu Privoxy vytvořenou v rámci této práce považuji za velice praktickou už s ohledem na stále silnější tlak výrobců prohlížečů na úplné opuštění nešifrovaného HTTP. Za těchto okolností je nezbytné, aby filtrovací proxy server umožnil pomocí MITM filtrovat i šifrovanou komunikaci, a toho se v rámci práce podařilo dosáhnout. Implementace je navíc přehledná a dobře strukturovaná, nebude obtížné ji udržovat a např. rozšiřovat o další šifrovací knihovny, pokud to uživatel bude potřebovat.	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení – následující škálou 1 až 5:</i>
5. Aktivita a samostatnost studenta	5a: 1=výborná aktivita, 2=velmi dobrá aktivita, 3=průměrná aktivita, 4=slabší, ale ještě dostatečná aktivita, 5=nedostatečná aktivita 5b: 1=výborná samostatnost, 2=velmi dobrá samostatnost, 3=průměrná samostatnost, 4=slabší, ale ještě dostatečná samostatnost, 5=nedostatečná samostatnost
<i>Popis kritéria:</i> V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (5a). Posuďte schopnost studenta samostatně tvůrčí práce (5b).	
<i>Komentář:</i> Student byl velice aktivní a také naprosto samostatný, nemám k jeho práci žádné připomínky.	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):</i>
6. Celkové hodnocení	92 (A)
<i>Popis kritéria:</i> 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.	
<i>Text hodnocení:</i> Student provedl důkladnou analýzu aktuálního vývoje ve světě prohlížečů i aktuální stav filtrovacího proxy serveru Privoxy a navrhl a implementoval taková rozšíření jeho podpory pro filtrování SSL komunikace, která ho činí velmi praktickým i v aktuální době a s výhledem do budoucnosti. Kód je dobře napsaný i organizovaný a demonstruje, že je student schopen samostatné inženýrské práce na vysoké úrovni.	

Podpis vedoucího práce: