

# Posudek oponenta závěrečné práce

České vysoké učení technické v Praze

Fakulta informačních technologií

**Student:** Tomáš Šmíd  
**Oponent práce:** Ing. Tomáš Kadlec  
**Název práce:** Zabezpečení komunikace s učebnovými PC  
**Obor:** Softwarové inženýrství

**Datum vytvoření:** 2. 6. 2017

<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení - následující škálou 1 až 5:</b>
<b>1. Náročnost a další komentář k zadání</b>	<b>1=mimořádně náročné zadání, 2=náročnější zadání, 3=průměrně náročné zadání, 4=lehčí, ale ještě dostatečně náročné zadání, 5=nedostatečně náročné zadání</b>
<b>Popis kritéria:</b> 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.)	
<b>Komentář:</b> Hlavní důvody k hodnocení zadání jako náročnější jsou: Výstupem má být aplikace, která bude použita v provozu. Samotná zadaná problematika je netriviální tím, že vyžaduje znalost řady standardů - protokolů, kryptografických formátů apod.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení - následující škálou 1 až 4:</b>
<b>2. Splnění zadání</b>	<b>1=zadání splněno, 2=zadání splněno s menšími výhradami, 3=zadání splněno s většími výhradami, 4=zadání nesplněno</b>
<b>Popis kritéria:</b> 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.	
<b>Komentář:</b> Zadání považuji za splněné. I přesto, že proxy server není integrován do ProgtestEnv, jak bylo požadováno. Doplnění považuji za triviální (jelikož jsem autorem ProgtestEnv).	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení - následující škálou 1 až 4:</b>
<b>3. Rozsah písemné zprávy</b>	<b>1=splňuje požadavky, 2=splňuje požadavky s menšími výhradami, 3=splňuje požadavky s většími výhradami, 4=nesplňuje požadavky</b>
<b>Popis kritéria:</b> Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.	
<b>Komentář:</b> Písemná zpráva splňuje kladené požadavky. Zpráva dokumentuje celý proces vývoje aplikace od analýzy problémové domény, návrh, implementaci až po testování.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):</b>
<b>4. Věcná a logická úroveň práce</b>	<b>90 (A)</b>
<b>Popis kritéria:</b> 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.	
<b>Komentář:</b> Práce je vhodně strukturovaná. Čtenář je postupně prováděn řešenou problematikou a jsou mu představovány dílčí závěry (ať už se jedná např. o specifikaci požadavků, způsob zpracování souběžných spojení či scénáře akceptačního testu). Na několika místech je však čtenář zahlcen detaily natolik, že se v textu může snadno ztratit. Text je doplněn diagramy, které usnadňují pochopení řešené problematiky.	
<b>Hodnotící kritérium:</b>	<b>Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):</b>
<b>5. Formální úroveň práce</b>	<b>90 (A)</b>
<b>Popis kritéria:</b> Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3.	
<b>Komentář:</b> Práce je celkově na velmi dobré úrovni. Neobsahuje překlepy, pravopisné a gramatické chyby (do míry, kterou jsem schopen posoudit). Po stylistické stránce se autor v některých částech odchyluje od odborného stylu. Sazba byla provedena systémem LaTeX a odpovídá požadavkům.	

<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):</i>
<b>6. Práce se zdroji</b>	<b>100 (A)</b>
<i>Popis kritéria:</i> 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.	
<i>Komentář:</i> Autor se zdroji aktivně pracuje, jsou řádně uvedeny a citovány.	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):</i>
<b>7. Hodnocení výsledků, publikační výstupy a ocenění</b>	<b>89 (B)</b>
<i>Popis kritéria:</i> 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.	
<i>Komentář:</i> V rámci práce vznikla aplikace, která splňuje požadavky a lze ji použít jako ssl-to-ssl proxy. Analýza a návrh aplikace jsou provedeny odpovídajícím způsobem. Implementaci nemohu posoudit, jelikož se vývoji v C++ více než 10 let nevěnuji. U aplikace postrádám: * state of the art - alespoň základní analýzu stavu řešené problematiky, zejména zhodnocení stávajících aplikací, které stejnou/obdobnou funkcionalitu nabízí, * využití existujících knihoven i pro zpracování HTTP, * automatické testování jejich částí (alespoň jednotkové testování, které by bránilo regresi při dalším vývoji).	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení - nehodnotí se</i>
<b>8. Komentář o využitelnosti výsledků</b>	
<i>Popis kritéria:</i> Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.	
<i>Komentář:</i> Z písemné zprávy lze usuzovat, že aplikaci lze nasadit do provozu. V práci však postrádám ověření funkce aplikace v reálném prostředí.	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení - nehodnotí se</i>
<b>9. Otázky k obhajobě</b>	
<i>Popis kritéria:</i> Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).	
<i>Otázky:</i> * Je možné realizovat ssl-to-ssl proxy jiným způsobem než vaší aplikací? Lze k tomu využít např. HAproxy či některý z běžných webserverů - httpd, nginx? * Je v rámci TLS handshake podporováno dojednání šifer nebo musí být použity nějaké konkrétní? Je možné používané šifry v konfiguraci nastavit (tj. nepovolit klientovi použít slabé šifry)? * Jaký důvod vás vedl k vlastní implementaci obsluhy HTTP požadavků? Proč jste nepoužil některou z existujících knihoven (např. Apache APR)? Není důsledkem tohoto rozhodnutí i fakt, že vaše aplikace nepodporuje HTTP/2.0? * Je oprava nutná low-level implementace (C++)? Nezvažoval jste použití jiné technologie (Go, Python), které by díky rozsáhlé nabídce dalších knihoven nejspíš usnadnilo implementaci? Pokud ano, zjišťoval jste případné výhody a nevýhody?	
<i>Hodnotící kritérium:</i>	<i>Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):</i>
<b>10. Celkové hodnocení</b>	<b>90 (A)</b>
<i>Popis kritéria:</i> Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení <b>nesmí</b> být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.	
<i>Text hodnocení:</i> Písemná zpráva i aplikace samotná ukazují, že se autor dokáže samostatně vypořádat s netriviálním problémem. Práci doporučuji k obhajobě a navrhuji ji klasifikovat známkou i přes výše uvedené výhrady, které nejsou závažného charakteru, zvláště uvážíme-li, že se jedná o bakalářskou práci.	

Podpis oponenta práce: