# Posudek oponenta závěrečné práce

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

**Student:** Bc. Jan Karafiát
**Oponent práce:** Ing. Tomáš Čejka
**Název práce:** Generátor síťového provozu na úrovni aplikačních protokolů
**Obor:** Počítačová bezpečnost

**Datum vytvoření:** 8. 6. 2016

| *Hodnotící kritérium:* | *Způsob hodnocení - následující škálou 1 až 5:* |
|---|---|
| **1. Náročnost a další komentář k zadání** | ***1=mimořádně náročné zadání,***<br>*2=náročnější zadání,*<br>*3=průměrně náročné zadání,*<br>*4=lehčí, ale ještě dostatečně náročné zadání,*<br>*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:*
Práce se zabývá netriviální oblastí modelování a generování síťového provozu, což je problematika, které se zabývá současný celosvětový výzkum.

| *Hodnotící kritérium:* | *Způsob hodnocení - následující škálou 1 až 4:* |
|---|---|
| **2. Splnění zadání** | *1=zadání splněno,*<br>***2=zadání splněno s menšími výhradami,***<br>*3=zadání splněno s většími výhradami,*<br>*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:*
Zadání obsahuje požadavek na vytvoření tzv. knihovny vzorků provozu datové sítě na úrovni vybraných aplikačních protokolů. V práci jsem si splnění tohoto bodu nevšiml. Na druhou stranu je práce informačně bohatá a vybraná (nemalá) podmnožina zadání je zpracovaná důkladně a pečlivě. Proto hodnotím práci jako splněnou.

| *Hodnotící kritérium:* | *Způsob hodnocení - následující škálou 1 až 4:* |
|---|---|
| **3. Rozsah písemné zprávy** | ***1=splňuje požadavky,***<br>*2=splňuje požadavky s menšími výhradami,*<br>*3=splňuje požadavky s většími výhradami,*<br>*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:*
Nemám žádné výhrady.

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **4. Věcná a logická úroveň práce** | *89 (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:*
Na straně 11 je zřejmě omylem uveden typ obsahu u signatury application/gif.
Na straně 34 je diskutován výpočet času parsování obsahu, který může v určitých případech vyjít záporně, což se nezdá být odpovídající realitě (viz otázka).

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **5. Formální úroveň práce** | *89 (B)* |

*Popis kritéria:*
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 12/2014, článek 3.

*Komentář:*
Předložená práce obsahuje drobné chyby - špatné uvozovky, popisky výpisů.

| *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:*
Nemám žádné výhrady.

| *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:*
Autor v textu na několika místech naznačuje, že výsledné softwarové řešení vykazuje drobné vady/nepřesnosti, např. chybějící data v PCAP souborech, nepřesné časové značky přeposlaného provozu, neparsovatelná přeposlaná data (výstup nástroje Wireshark pro některé obrázky). Přesto hodnotím práci jako velice zdařilou.

| *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:*
Na základě textu soudím, že hlavním přínosem práce je modifikace existujícího modelu pro generování HTTP provozu s realistickými statistickými vlastnostmi. V textu mi však chybí důkladné porovnání nově navrženého modelu s původním. Pokud by se dalšími experimenty ověřilo zlepšení vlastností generátoru, soudím, že by bylo velice vhodné výsledky práce publikovat např. na některé vědecké konferenci. Podle mého názoru jsou výsledky práce využitelné v praxi v oblasti verifikace síťových nástrojů a síťové bezpečnosti.

| *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:*
* Čas parsování se v práci počítá jako rozdíl ukončení přenosu hlavního objektu a začátku přenosu prvního vestavěného objektu. Tento způsob neodpovídá realitě v případě, že se parsování začne provádět "za běhu" před dokončením přenosu hlavního objektu. Mělo by smysl (nějaké praktické výhody pro generátor) změnit výpočet tak, aby to lépe odpovídalo realitě (tj. nevycházel záporný výsledek)?
* Na straně 35 je uvedena informace o nezachycených či poškozených paketech. Čím je tento jev způsoben? (předpoklad: u korektní komunikace by měl být TCP paket přeposlán, což by v PCAP souboru mělo být vidět)
* V sekci 2.1.3.3 není zcela jasné, jestli se EM alg. používá nad paketovými nebo tokovými daty. Podle sekce 2.1.3.2 se používají jen toky. Jak je tedy ze základních záznamů o tocích možné zjistit typ obrázkových objektů?

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **10. Celkové hodnocení** | *95 (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:*
Práce splňuje všechny požadavky a po zodpovězení uvedených otázek navrhuji hodnocení práce známkou A.

Podpis oponenta práce: