Hodnocení vedoucího závěrečné práce

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

Student: Jiří Havránek
Vedoucí práce: Ing. Tomáš Čejka
Název práce: Exportér síťových toků s podporou aplikačních informací
Obor: Teoretická informatika

Datum vytvoření: 8. 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 hodnotím jako náročnější, protože staví na původním předchozím řešení, které nesplňovalo požadavky a bylo potřeba jej upravit a rozšířit. Vedle toho, že samotné zpracování aplikačních informací ze síťových paketů není lehký úkol, ukázalo se, že původní řešení bylo potřeba z velké části předělat.

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:
Zadání bylo splněno ve všech bodech, výsledkem je funkční a používaný exportér síťových toků.

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:
Práce má přiměřený rozsah, práce neobsahuje zbytečné části, všechny části jsou informačně bohaté.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*90 (A)*

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:
Práce má logickou strukturu, a po věcné stránce je v pořádku. V sekci testování by bylo užitečné přidat porovnání počtu toků, které je exportér schopen zpracovat, s průměrným objemem provozu běžných malých sítí. Z tohoto porovnání by jasně vyplývalo, že optimalizovaná verze exportéru je použitelná pro reálné nasazení v malých sítích, což je i cíl tohoto nástroje.

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. 14/2015, článek 3.

Komentář:
Práce obsahuje drobné typografické chyby a překlepy.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*95 (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 obsahuje dostatečné množství relevantních zdrojů, které jsou dobře citované.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*100 (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:
Výsledek této práce hodnotím jako vynikající. Nejen že se studentovi podařilo různými optimalizacemi zvýšit výkon exportéru, rozšíření o možnost exportovat informace z aplikační vrstvy znamená, že se z exportéru stal výjimečný nástroj mezi existujícími open source řešeními. Zároveň je potřeba zmínit, že před touto bakalářskou prací předcházely jiné úspěšně obhájené závěrečné práce, které významně těžily z výsledků této bakalářské práce v době jejího vznikání. Konkrétně se používala možnost sběru testovacích dat s aplikačními položkami z reálného síťového provozu. Získaná data byla základem pro výzkum a vývoj detekčních metod, přičemž některé vyvinuté detekční metody byly dokonce publikovány v článcích na konferencích.

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:
Výsledný exportér síťových toků je součástí open source projektu NEMEA a je dostupný na github.com pro mezinárodní vědeckou komunitu z oblasti síťové bezpečnosti. Exportér byl v minulosti již mnohokrát použit k získání dat pro různé experimenty, návrh a testování vyvíjených detekčních algoritmů. Portování na platformu OpenWrt, které se studentovi podařilo, umožňuje použít vzniklý nástroj v levných nevýkonných domácích směrovačích a umožnit tak získání přehledu o provozu na síti a detekování potenciálně škodlivého provozu.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
9. Aktivita a samostatnost studenta v průběhu řešení	9a: ***1=výborná aktivita,*** *2=velmi dobrá aktivita,* *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 9b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (9a). Posuďte schopnost studenta samostatné tvůrčí práce (9b).

Komentář:
Student pracoval aktivně, samostatně a průběžně během posledních 2 let. Během této doby byl důležitou součástí týmu studentů, kteří se na FITu zabývají monitorováním síťového provozu a výzkumem a vývojem metod pro detekci škodlivého provozu. Student byl vždy ochotný pomoci ostatním členům týmu a jeho práce na rozšiřitelném exportéru umožnila dosáhnout skvělých výsledků v minulých závěrečných pracích studentů, kteří ke své práci potřebovali zdroj dat.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*100 (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:
Předložená práce je kvalitně zpracovaná, je použitelná v praxi a již v průběhu vývoje byla aktivně používána ostatními členy týmu. Přes drobné nedostatky zmíněné výše (formálního rázu) hodnotím práci jako vynikající.

Podpis vedoucího práce: