Posudek oponenta závěrečné práce

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

Student: Bc. Zdeněk Rosa
Oponent práce: Ing. Pavel Benáček
Název práce: Automatizovaný záchyt síťových dat k detekovaným událostem
Obor: Systémové programování

Datum vytvoření: 19. 1. 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:
Téma spadá do oblasti monitoringu počítačových sítí. Výsledek diplomové práce je programové vybavení pro záchyt historického a živého provozu k nahlášeným incidentům z distribuovaného detekčního systému NEMEA (System for network traffic analysis and anomaly detection), který je vytvářen v organizaci CESNET. Systém je schopný využít i síťových akcelerátorů s FPGA obvody, které umožňují odlehčit CPU od zpracování nezajímavých síťových toků. Celý systém je distribuovaný a je navržen tak, aby bylo možné zachytávat data na více sondách v síti. Student musel nastudovat detekční systém NEMEA, podklady nutné k integraci s síťovým akcelerátorem a navrhnout celý systém na propustnost vhodnou k monitorování na vysokorychlostních sítích. Z uvedených důvodů hodnotím práci jako náročnější.

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:
Všechny zadané úkoly autor práce splnil. Nastudoval problematiku monitorování vysokorychlostních sítí, propojil celý systém se síťovým akcelerátorem a vytvořil distribuovaný systém pro zachytávání historického a živého provozu k nahlášeným incidentům. Zachycený provoz je také následně analyzován detekčním systémem Bro a Tranalyzer. Celý soubor dat je následně komprimován a uložen pro případ pozdější analýzy. Záchyt historických dat může být navíc použit jako důkazní materiál, protože data ze začátku incidentu vetšinou poskytují mnoho informací. Celý monitorovací systém byl otestován a prezentován na mezinárodní konferenci v Kanadě.

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 splňuje požadavky na diplomovou práci.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*100 (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 je přehledná a dobře čitelná. Po věcné stránce v práci nic nechybí.

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

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:
Slohovou úroveň shledávám jako výbornou. Samotný text je jasný a naprosto srozumitelný.

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:
Všechny uvedené studijní materiály jsou relevantní. Všechny zdroje jsou řádně citovány, jsou úplné a v souladu s citačními zvyklostmi a normami.

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:
Výsledkem práce je funkční prototyp distribuovaného systému pro záchyt živých a historických dat. Data jsou zachytávána dle nahlášených událostí ze sytému NEMEA. Přínos práce spočívá v možnosti záchytu dat, které mohou být použity pro detailnější pochopení incidentu, jako důkazní materiál a podobně. Všechny vybrané postupy, algoritmy, datové struktury a řešení byly jasně vysvětleny a uvedeny v textu. Jejich výběr hodnotím jako velmi vhodný pro využití v páteřních vysokorychlostních sítích. Celé řešení bylo navíc publikováno na mezinárodní konferenci v Kanadě.

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:
Výsledek je funkční systém, který je integrován se systémem NEMEA. Základní myšlenka práce byla uvedena v článku od S. Kornexela - Building a time machine for efficient recording and retreival of high-volume network traffic. Autor diplomové práce byl však schopen dosáhnout záchytu na vysokorychlostní páteřní síti. O úrovní diplomové práce také vypovídá prezentace na mezinárodní konferenci v Kanadě. Využitelnost výsledku je tedy vysoká.

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:
1) Jak systém řeší delší výpadek Správce událostí, který je použit pro řízení záchytu na více sondách? Nedojde tak k ztrátě nachytaných dat na sondách?
2) Povedlo se systémem zachytit nějaké zajímavé síťové incidenty (např. DDoS, DNS amplifikační útok, atd.) ?

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:
Student navrhl, implementoval a otestoval distribuovaný systém pro záchyt historických a živých dat k nahlášeným událostem ze systému NEMEA. Výsledné řešení také může využít síťových akcelerátorů, které tak umožňují monitoring na vysokorychlostních páteřních sítích. Práce byla navíc prezentována na mezinárodní konferenci, což vypovídá o její kvalitě. Práci proto doporučuji k obhajobě a hodnotím ji známkou A - výborně.

Podpis oponenta práce: