Posudek oponenta závěrečné práce

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

Student: Bc. Marek Švepeš
Oponent práce: Ing. Pavel Benáček, Ph.D.
Název práce: Rozšíření systému NEMEA pro nasazení v distribuovaném prostředí
Obor: Systémové programování

Datum vytvoření: 29. 5. 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:
Práce se zabývá návrhem paralelizace open-source systému NEMEA tak, aby byl schopen v reálném čase detekovat větší množství hrozeb. Student musel nastudovat aktuální stav projektu NEMEA, provést návrh a realizaci samotné paralelizace. Celý projekt je navíc velmi rozsáhlý a implementuje různé detekční moduly. Navíc musí celý paralelizovaný systém vykazovat ekvivalentní chování s jeho neupravenou variantou. Z těchto důvodů hodnotím zadání 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:
Student splnil zadání diplomové práce. Výsledky této závěrečné práce budou také publikovány na mezinárodní konferenci Autonomous Infrastructure, Management and Security (AIMS) 2017 v Zurichu, Švýcarsko.

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:
Text plně odpovídá požadavkům 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 po faktické části zcela v pořádku. Student zcela jasně a objektivně vysvětlil všechna architektonická rozhodnutí, která posléze potvrdil experimenty. Po této stránce nemám k práci připomínky. Text práce je přehledný a jeho strukturu hodnotím také velmi kladně.

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. 14/2015, článek 3.

Komentář:
Po formální stránce je text naprosto v pořádku.

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 zdroje hodnotím jako relevantní. Všechny převzaté části jsou správně citovány a student je velmi jasně oddělil od svých výsledků, které jsou velmi dobré.

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:
Student navrhl a implementoval možný způsob paralelizace detekce v open-source systému NEMEA. K tomuto účelu použil různé metody distribuování požadavků na detekční uzly. Odhadnuté chování poté experimentálně ověřil. Výsledný systém byl schopen detekovat stejné incidenty, jako jeho ne-paralelní verze. Výsledky poté byly prezentovány v v článku, který byl přijat na mezinárodní konferenci Autonomous Infrastructure, Management and Security (AIMS) 2017 v Zurichu, Švýcarsko.

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:
Autoři open-source systému NEMEA rozhodli o začlenění implementované funkcionality do produkčního kódu. Jeho využití v praxi je tedy vysoké.

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:
i) V závěru práce autor uvedl, že způsob paralelizace zpracování a použité metody jsou aplikovatelné i na jiné detekční systémy. Znamená to tedy, že použité metody jsou dostatečně obecné na to, aby byly použity i pro jiné detekční moduly systému NEMEA (tzn., dají se použít i na jiné metody než jsou uvedeny ve studii)? Případně, mohou se aplikovat i na jiné systémy než je NEMEA?

ii) Tato otázka přímo nesouvisí s touto diplomovou prací, ale chtěl bych se zeptat na možnost šifrování komunikace mezi uzly distribuovaného systému NEMEA, protože se kvůli detekci mohou přenášet citlivé informace. Můžete toto nějak okomentovat?

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 nastudoval systém NEMEA a provedl implementaci paralelního zpracování detekce událostí. Všechna architektonická rozhodnutí byla jasně vysvětlena a dokázána experimenty. Navíc byly výsledky uvedeny v publikaci, které byla přijata na mezinárodní konferenci Autonomous Infrastructure, Management and Security (AIMS) 2017 v Zurichu, Švýcarsko. Text tedy prošel i recenzemi jiných odborníků, což zvyšuje význam a korektnost uvedených faktů. Navíc se správci projektu NEMEA rozhodli začlenit všechny uvedené úpravy do produkčního kódu. Z těchto důvodů doporučuji práci k obhajobě a hodnotím ji stupněm A (výborně).

Podpis oponenta práce: