FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Jiří Havránek
Oponent práce:	Ing. Pavel Benáček, Ph.D.
Název práce:	Využití jazyka P4 pro generování síťových bezpečnostních aplikací
Obor:	Počítačová bezpečnost

Datum vytvoření: 29. 5. 2019

Hodnotící kritérium:	*Způsob hodnocení – následující škálou 1 až 4:*
1. 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 dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Komentář:
Práce se zabývá využitím jazyka P4 pro popis exportéru síťových toků schopného exportovat informace z aplikačních vrstvev (L7). Student musel nastudovat standard jazyka P4, aktuálně dostupné nástroje a existující implementaci exportéru. Dále musel student vytvořit popis exportéru v jazyce P4 a celý návrh implementovat. Pro implementaci překladače byl využit volně dostupný frontend P4C, který zpracovává gramatiku a poskytuje základní třídy pro vývoj. Navrhnuté řešení je poměrně unikátní, protože jsem v publikacích nenalezl podobné využití jazyka P4 pro flexibilní rozšiřování exportéru síťových toků. Zadání práce bylo splněno a hodnotím ji jako náročnější.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*85 (B)*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále 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. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3. Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Komentář:
Práce splňuje požadavky na diplomovou práci. Jednotlivé části jsou dobře členěny a zpracovány. Text práce je dobře čitelný a zcela pochopitelný. Určitou část bodů strhávám za překlepy v textu. Všechny převzaté prvky jsou řádně odlišeny a citovány, ale některé citace neodpovídají citační normě ČSN ISO 690. Nicméně tyto nedostatky nemají vliv na kvalitu samotné práce. Z pohledu licenčních podmínek převzatého SW neshledávám žádné nedostatky.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*100 (A)*

Popis kritéria:
Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce
– opakovatelnost experimentů

Komentář:
Pro vývoj překladače z P4 do C byl využit standardní frontend P4C, který je vytvářen standardizační skupinou pro jazyk P4. Zdrojový kód je přehledný a dobře členěn. Jednotlivé použité technologie jsou z mého pohledu vhodně zvoleny. Vytvořený software byl podroben testům a bylo dosaženo funkcionality původního exportéru síťových toků. Přidanou hodnotou je pak flexibilita a jednoduchá rozšiřitelnost na základě popisu chováni v jazyce P4.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*

4. Hodnocení výsledků, jejich využitelnost	*100 (A)*

Popis kritéria:
Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Komentář:

Výsledkém této práce je funkční překladač exportéru síťových toků z popisu v jazyce P4 do zdrojových kódů v C, které se pak mohou přeložit a výsledek překladu se může ihned nasadit. Celé řešení je poměrně unikátní a autor plánuje jeho nasazení v rámci projektu NEMEA (software pro distribuovanou bezpečnostní analýzu síťových dat), což dále zvyšuje jeho užitnou hodnotu. Využitelnost v praxi je tedy poměrně vysoká a samotná možnost jednoduše rozšiřovat měření i na L7 vrstvách dělá z toho projektu výborný výsledek. Komisi také doporučuji zvážit nominaci této práce o cenu děkana za vynikající DP.

Hodnotící kritérium:	*Způsob hodnocení – nehodnotí se*

5. Otázky k obhajobě

Popis kritéria:
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

Otázky:

- Plánujete práci rozšířit o export do jiných formátů než je IPFIX? Pokud ano, do jakých?
- Plánujete práci uvolnit P4 komunitě? Výsledky práce jsou totiž velmi dobré a pro komunitu by tento projekt mohl být velmi zajímavý.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*

6. Celkové hodnocení	*95 (A)*

Popis kritéria:
Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.

Text hodnocení:

Výsledkem práce je funkční implementace generátoru flexibilního exportéru síťových toků z popisu v jazyce P4. Při vývoji byly využity standardní nástroje vytvořené v rámci P4 komunity. Student musel nejdříve nastudovat jazyk P4, identifikovat jednotlivé části exportéru síťových toků a popsat je pomocí prostředků jazyka P4. Další přidanou hodnotou je unikátnost této práce, protože doposud jsem v dostupné literatuře nenašel podobné řešení. Vytvořený zdrojový kód nástroje je přehledný, řádně členěn a dokumentován. Výsledek je dále v plánu nasadit i v rámci projektu NEMEA, což dále zvyšuje využitelnost výsledků v praxi. Práci proto doporučuji k obhajobě a hodnotím ji známkou A - výborně. Vážené komisi také doporučuji zvážit případnou nominaci této práce na cenu děkana za vynikající BP/DP.

Podpis oponenta práce: