FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Student:	Bc. Peter Páleník
Oponent práce:	Ing. Simona Buchovecká
Název práce:	Diagnosis of traffic of ICS protocols
Obor:	Počítačová bezpečnost

Datum vytvoření: 7. 6. 2020

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:
Formálně byly všechny aspekty zadání splněny, avšak poslední částí testování je věnováno jenom málo prostoru - vzhledem k jeho povaze by výsledný produkt zasloužil formálnější testování a shrnutí výsledku, zejména s ohledem na poměr pozitivních a falešně pozitivních detekcí, falešně negativních výsledků ale i třeba zpoždění s jakým se dostane diagnostická zpráva k správci sítě, jelikož student zmiňuje, že se nejedná o real-time monitoring.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*70 (C)*

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:
Písemná část práce by ještě zasloužila revizi. Jazyk je místy velice neformální a formulace jako např. "rozširuje sa ich funkcionalita a pridáva sa im (zařízením) schopnosť ”rozmýšľať“", ""prehluší“ legitímnu odpoveď" či "obídenie firewallu" do diplomové práce nepatří.

Teoretický úvod (kapitola 2.1) je velmi povrchní, srovnání ICS a IoT je velmi zjednodušené, a zejména podkapitola 2.1.2 velmi neformálně popsaná. Cílové použití vybraných protokolů je velmi odlišné, jak i student v práci sam konstatuje, a pro další analýzu vybírá jak sadu protokolů ICS, tak CoAP protokol, který nachází uplatnění spíše ve světě IoT - z pohledu diagnostiky a bezpečnosti jsou priority v monitorování ICS a IoT odlišné, plynoucí z jejich odlišné kritičnosti, architektury a účelu použití, a tato diskuse v práci chybí.

Celou prací se prolíná téma spolehlivosti a bezpečnosti ICS/IoT systémů, avšak to není v textu odlišeno a zavadeno. I autor v závěru píše, že jedním z hlavních cílů práce bylo připravit nástroj, který bude "slúžiť správcom sietí na automatizovanú diagnostiku problémov v konfigurácií ICS a IoT zariadení", tomu odpovídá i implementační část, avšak v teoretické části se student věnuje zejména kybernetickým hrozbám, chybí diskuse možných provozních problémů a chybových stavů.

V části testování, jak jsem již zmínila v předchozím bodě, mi chybí formálnější vyhodnocení výsledků.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*90 (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:

V rámci nepísemných částí práce mi student nasdílel konfigurační protokoly pro nástroj Distance, to považuji vzhledem k zadání práce za adekvátní.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Hodnocení výsledků, jejich využitelnost	*90 (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:

Jelikož primárním cílem práce bylo rozšíření funkcionality již existujícího nástroje Distance, věřím, že výsledky práce najdou praktické uplatnění.

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:

Jak vnímáte rozdílné priority v monitorování ICS a IoT systémů?
Jaká další rizika, kromě kybernetických hrozeb, je nutné při monitorování ICS zohlednit?

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*80 (B)*

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:

Vzhledem k rozsahu odvedené práce studentem a praktického přínosu k nástroji Distance, práci doporučuji k obhajobě. Kvalita textové části však neodpovídá odvedené práci, a proto se kloním k hodnocení B.

Podpis oponenta práce: