FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Student:	Bc. Peter Páleník
Vedoucí: práce:	Ing. Tomáš Čejka, Ph.D.
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:

Student ve své práci nastudoval specifikaci několika vybraných protokolů pro průmyslové a IoT sítě a zaměřil se detekci chyb a bezpečnostních hrozeb, které je možné odhalit v síťovém provozu. Výsledkem práce je důkladná analýza protokolů popsaná v práci a následně návrh a sestrojení množiny diagnostických pravidel pro diagnostický systém. Díky těmto diagnostickým pravidlům je možné provést automatickou analýzu zachyceného síťového provozu s cílem identifikovat potenciální problémy. Zadání práce bylo splněno.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
2. Písemná část práce	*89 (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:

Text práce je dobře členěný, ale obsahuje typografické chyby (např. přesahy). Teoretická část obsahuje detailní analýzu vybraných průmyslových protokolů. Tato analýza je nezbytným předpokladem pro vytvoření diagnostických pravidel. Kapitola realizace popisuje funkcionalitu systému Distance pomocí příkladů nově vytvořených pravidel a soustředí se na konkrétní konstrukce použité při diagnostice nastudovaných průmyslových protokolů.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
3. Nepísemná část, přílohy	*85 (B)*

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:

Výsledkem práce je sada diagnostických pravidel pro protokoly CoAP, MMS a GOOSE. Tato diagnostická pravidla se skládají z popisu událostí, které mohou v komunikaci nastat, a testovaných předpokladů - charakteristik komunikace. Konkrétní reprezentace je ve formátu Yaml doplněném o úseky python skriptů. Student dokázal pokrýt většinu identifikovaných stavů komunikace. Protokol DTLS zatím v práci nebyl řešen, protože nebyl součástí původně plánované množiny protokolů. V průběhu řešení se však ukázalo, že by i tento protokol byl užitečný k prohloubení schopností diagnostiky protokolu CoAP.

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:

Diagnostika problémů v síťovém provozu a interpretace zachycené komunikace patří k důležitým úlohám síťových operátorů. V mnoha případech tato činnost vyžaduje hluboké expertní znalosti. Specifikace protokolů pro řízení průmyslových systémů bývají často dlouhé a komplikované. Proto jakákoliv automatická diagnostika poslouží jako užitečná pomoc při řešení chybových stavů, které není snadné rozpoznat na uživatelské úrovni. Výsledky této práce jsou využitelné v praxi.

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

Popis kritéria:
V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (5a). Posuďte schopnost studenta samostatné tvůrčí práce (5b).

Komentář:

Student byl velmi aktivní a pečlivý po celou dobu práce na tématu. Během krátké doby byl schopen nastudovat rozsáhlé specifikace vybraných protokolů a získané poznatky využít k návrhu diagnostických pravidel. Vytváření podobných diagnostických pravidel pro automatickou analýzu zachyceného provozu je netriviální úloha, se kterou si student dokázal velice dobře poradit.

Hodnotící kritérium:	*Způsob hodnocení – bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Celkové hodnocení	*90 (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:

Zadání práce bylo náročné především kvůli rozsahu a komplexitě vybraných ICS protokolů. Studentovi se podařilo pokrýt většinu problémových stavů provozu pomocí vytvořených diagnostických pravidel. Výsledky práce jsou důležitým doplňkem standardním síťovým analyzátorům a díky automatickému vyhodnocení mohou pomoci operátorům průmyslových sítí s vyhodnocením provozu. Práce sice neobsahuje pokrytí protokolu DTLS, ale přesto jsou vytvořené výsledky již nyní využitelné v praxi.

Podpis vedoucího práce: