Posudek oponenta bakalářské práce

Student: Pristaš Ján
Téma: Generování provozu IoT sítí a detekce bezpečnostních incidentů (id 21299)
Oponent: Ryšavý Ondřej, doc. Ing., Ph.D., UIFS FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

2. Splnění požadavků zadání **zadání splněno**

Student v textové části uvedl dostatečné informace ke všem bodům zadání. Z textu a na přiloženém médiu je zřejmé, že zadání bylo splněno.

3. Rozsah technické zprávy **je v obvyklém rozmezí**

Práce obsahuje relevantní informace k řešené oblasti čemuž odpovídá i její rozsah.

4. Prezentační úroveň předložené práce **80 b. (B)**

Práce má dobrou strukturu a uvedené informace jsou vesměs pro čtenáře srozumitelné. Některé části jsou převzaty pouze z jednoho zdroje, například popis útoků, které byly na SCADA systémy zaznamenány. Tento text je informačně méně bohatý, respektive uvedené informace jsou spíše povrchní.

5. Formální úprava technické zprávy **80 b. (B)**

Text je čistý bez výrazných typografických prohřešků. V některých částech práce je text méně srozumitelný. Celkově je práce na dobré jazykové úrovní.

6. Práce s literaturou **70 b. (C)**

Student se v práci odkazuje na relevantní zdroje a uvedené informace jsou v textu řádně odlišeny od převzatých. Množství informačních zdrojů je vzhledem k obsahu práce dostačující.

7. Realizační výstup **70 b. (C)**

Realizačním výstupem je implementace klienta komunikující protokoly DLMS/COSEM a IEC104 vytvořená na základě dostupného příkladu. Přestože se nejedná o nikterak komplikovanou implementaci, je výstup funkční a byl použit k provedení experimentů.

8. Využitelnost výsledků

Práce má z velké části kompilační charakter. Student shromáždil relevantní informace k problematice bezpečnosti SCADA prostředí. Vytvořené PCAP soubory je možné dále využít pro demonstraci vybraných protokolů průmyslové komunikace a testování nástrojů pro jejich zpracování.

9. Otázky k obhajobě

- Při testování používáte zachycený provoz, který modifikujete a posíláte na server. Z jakého důvodu nešlo použít již existující nástroje, například tcpreplay?
- Jaký bezpečnostní problém demonstrují testy č.4 a č.7? Zdá se, že se jedná o legitimní komunikaci.

10. Souhrnné hodnocení **80 b. velmi dobře (B)**

Celkově je práce na dobré úrovni. Zadání bylo splněno a vytvořené výsledky je možné dále použít pro studium zranitelnosti SCADA systémů. Realizační výstup nepředstavuje komplikovaný systém, ale je funkční a použitelný při experimentech se SCADA komunikací. Student shromáždil zajímavé a dále použitelné informace a nástroje pro experimenty s komunikací ve SCADA prostředí.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 28. května 2018

.....
podpis