Posudek oponenta diplomové práce

Student: Grofčík Peter, Bc.
Téma: Emulace útoků na řídicí komunikaci SCADA/ICS (id 24420)
Oponent: Grégr Matěj, Ing., Ph.D., UIFS FIT VUT

1. Náročnost zadání **obtížnější zadání**

Práci považuji za lehce obtížnější. Síťové protokoly používané v průmyslových sítích nejsou tak rozšířené a není k dispozici tolik nástrojů a informaci jako u standardních protokolů.

2. Splnění požadavků zadání **zadání splněno s drobnými výhradami**

Práce splnila zadání. Očekával bych ale širší diskuzi k dosaženým vysledkům experimentů a jednotlivých metod, které byly v práci testovány.

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

4. Prezentační úroveň předložené práce **75 b. (C)**

Práce má logickou strukturu. Jednotlivé kapitoly na sebe navazují. Text by mohl nicméně obsahovat i popis a vybrané charakteristiky protokolu IEC104. Pak by mohl být popis útoků pro čtenáře pochopitelnější.

5. Formální úprava technické zprávy **65 b. (D)**

Typograficky považuji práci za vcelku kvalitní. Práce je psaná slovensky. I s mou znalostí slovenštiny lze ale nalézt řadu překlepů a chyb, které by v práci být nemusely.

6. Práce s literaturou **75 b. (C)**

Práce cituje relevantní zdroje. Porušení citačních zvyklostí a etiky jsem nezaznamenal. Pro ověření a volbu detekčních algoritmů by ale mohl student zvolit širší rozsah publikací, které jsou k danému tématu dostupné.

7. Realizační výstup **55 b. (E)**

Realizační výstup se krom datové sady a pcap souborů skládá z python skriptu pro testování detekčních metod a kódu pro modifikaci provozu protokolu IEC104. Kód považuji za vcelku čitelný, ale prakticky příliš nepoužitelný, jelikož jednotlivé parametry jsou natvrdo napsány přímo v kódu a musí se před kompilaci, či spuštěním modifikovat. Funkčnost je také závislá na topologii, která byla použita v práci a je tak obtížněji přenositelná. U rozšíření nástroje ettercap pro modifikaci provozu IEC104 také není příliš jasné, co je převzatý kód a co vlastní práce studenta a měla by zde být doplněna licence.

8. Využitelnost výsledků

Datová sada je využitelná pro další projekty zkoumající útoky na průmyslové sítě.

9. Otázky k obhajobě

-

10. Souhrnné hodnocení **65 b. uspokojivě (D)**

Práce si klade za cíl zmapovat útoky na průmyslové sítě, vytvořit datasety a otestovat metody pro detekci anomálií. Datové sady bude možné využít i v navazujících pracích. U detekčních metod mi v práci chybí nějaké podrobnější vyhodnocení a diskuze k výsledkům. Celkově hodnotím práci jako uspokojivou (D).

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

V Brně dne: 2. června 2022

Grégr Matěj, Ing., Ph.D.
oponent