AN APPROPRIATE STRATEGY FOR DETECTING SECURITY INCIDENTS IN INDUSTRIAL NETWORKS

Karel Kuchař, Eva Holasová
Master Degree Programme (2), FEEC BUT
E-mail: xkucha24@vutbr.cz, xholas08@vutbr.cz

Supervised by: Radek Fujdiak
E-mail: fujdiak@feec.vutbr.cz

Abstract:

This paper is focused on environment of critical infrastructure and inadequate security problem. Industrial network typically works with old devices and a potential update may cause delay in the production and costs a lot of money. That is the reason why additional devices improving security of all system must be introduced. Tools like IDS/IPS (Intrusion Detection System/Intrusion Prevention System) are great for detecting anomalies and defining signatures in the network traffic. For such types of the network it is critical proper handling of security issues and generated alerts.

Keywords: ICS, Critical Infrastructure, Security, IDS, IPS, Modbus

1 ÚVOD

Oblast průmyslových sítí je stále více přístupná prostřednictvím internetu. V této oblasti také zaostává tlak na zvyšování úrovně zabezpečení s následnou implementací bezpečnostních opatření. Použité zařízení a aplikovaná bezpečnostní opatření v průmyslových sítích jsou mnohdy na nedostatečné úrovni. Tato práce si dává za cíl vytvoření metodik detekce bezpečnostních incidentů v oblasti průmyslových sítích za použití IDS/IPS systémů Snort a Zeek.

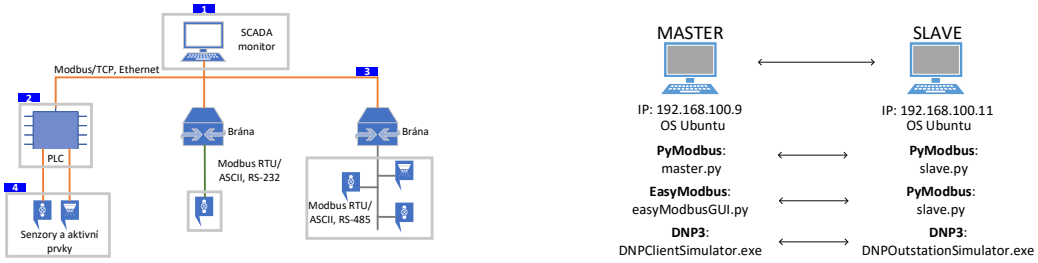
2 PRŮMYSLOVÉ SÍTĚ

Mezi hlavní prvky prostředí průmyslových sítí patří PLC (Programmable Logic Controller), které komunikují se senzory a aktivními prvky (např. senzor tlaku, nebo ventil). Ke komunikaci s obsluhou se využívá HMI (Human Machine Interface). K umožnění komunikace mezi jednotlivými prvky průmyslové sítě je využíván průmyslový protokol. Mezi nejznámější protokoly patří Modbus, Profinet, PROFIsafe, DNP3, EtherCAT a další. Tyto protokoly poskytují omezený, nebo žádný stupeň zabezpečení. K nasazení adekvátního dodatečného zabezpečení je nutné nejprve identifikovat jednotlivé vektory útoku. Obrázek 1 zobrazuje jednotlivé vektory zaměřené na často využívaný protokol Modbus. Tento protokol má dvě implementace, Serial Modbus (RTU/ASCII) a Modbus/TCP. Vektory útoku tvoří: HMI (1), řídící prvek PLC (2), přenosové médium (3), senzory a aktivní prvky (4).

Nejen u protokolu Modbus, ale u velké části protokolů průmyslových sítí není implementována autentizace. K navázání spojení postačuje znalost cílové IP adresy, portu a kódu funkce (k definování prováděné operace). Tyto informace mohou být snadno odposlechnuty a následně zneužity útočníkem, protože není implementováno šifrování přenášených paketů. Důvodem nedostatečného zabezpečení je předpoklad využívání jen v oddělených a vysoce kontrolovaných částech sítě. Dále bylo zamýšleno, že zabezpečení bude implementováno pomocí jiných technik. Samotné protokoly tak často postrádají bezpečnostní mechanismy, čerpáno z [1, 2].

3 EXPERIMENTÁLNÍ TESTOVÁNÍ

Pro simulaci prostředí průmyslových sítí byla vytvořena virtualizovaná experimentální síť, realizující protokol Modbus pomocí knihovny PyModbus a knihovny EasyModbus. Jako hostovaný OS byl vybrán OS Ubuntu. Pro realizaci protokolu DNP3 byla využita aplikace pro testování DNP komunikace DNPClientSimulator (DNPOustationSimulator), viz obrázek 1. Vybrané protokoly využívají model master-slave (klient-server). V rámci komunikace Modbus protokolu byl k otestování komunikace proveden příkaz Write Single Register (provedení jednobitové změny v registru slave zařízení), obdobně u protokolu DNP3.



(a) (b)

Obrázek 1: Vektory útoku, protokol Modbus (a), zapojení Experimentální sítě (b) [3].

3.1 DETEKCE BEZPEČNOSTNÍHO INCIDENTU – SNORT

Za účelem zvýšení bezpečnosti sítě bylo využito IDS/IPS (Intrusion Detection System/Intrusion Prevention System) nástroje Snort [4]. Nástroj provádí detekci anomálií a signatur v síťovém provozu a vytvořená pravidla jsou zaměřena na protokol Modbus/TCP (cílový port je pozměněn na port 5020). Výpis 1 představuje pravidlo, které provádí filtraci zdrojových adres zařízení, které se pokouší navázat spojení se slave zařízením. V případě, že došlo k navázání spojení z jiné, než definované adresy master zařízení (white-list), je vygenerován alert, viz výpis 2.

Výpis 1: Pravidlo pro detekci neautorizovaného přístupu.

```
alert tcp !$MODBUS_CLIENT any -> $MODBUS_SERVER 5020 (content:"|00 00|"; msg:"SCADA_IDS:
    Modbus/TCP: Unauthorized request"; sid:10000002; priority:1;)
```

Výpis 2: Alert vygenerovaný pravidlem při pokusu o změnu hodnoty.

```
12/02-11:59:20.782511 [**] [1:10000002:0] SCADA_IDS: Modbus/TCP: Unauthorized request [**]
    [Priority: 1] {TCP} 192.168.100.7:58669 -> 192.168.100.11:5020
```

Dále bylo vytvořeno pravidlo, které provádí kontrolu délky paketu, viz výpis 3. Pokud je maximální povolená délka paketu překročena, je vygenerován alert upozorňující na možný pokus o odepření služby, viz výpis 4.

Výpis 3: Pravidlo pro detekci příliš velkého paketu.

```
alert tcp any any <> $MODBUS_SERVER 5020 (content:"|00 00|"; dsize:>300; msg:"SCADA_IDS:
    Modbus/TCP: Illegal Packet Size, Possible DoS"; sid:1000004; priority:1;)
```

Výpis 4: Alert při překročení maximálního limitu délky paketu.

```
12/03-06:43:17.499610  [**] [1:1000004:0] SCADA_IDS: Modbus/TCP: Illegal Packet Size,
    Possible DoS [**] [Priority: 1] {TCP} 192.168.100.7:58669 -> 192.168.100.11:5020
```

3.2 DETEKCE BEZPEČNOSTNÍHO INCIDENTU – ZEEK (BRO)

V rámci demonstrace detekce anomálií byl také využit IDS systém ZEEK (BRO) [4], který mimo jiné podporuje práci s protokolem Modbus. Nejprve byla provedena instalace závislostí následovaná instalací systému ZEEK. V konfiguračních souborech byly pozměněny některé parametry k práci na experimentální síti, jako jsou zvolené rozhraní pro zachytávání síťového provozu, definování adresy sítě apod. Pro práci s protokolem Modbus je zapotřebí definovat cestu ke zvoleným skriptům. Pro detekci anomálií byl vybrán skript „track-memmap.zeek“, který byl doplněn o událost detekce operace Write Single Register (WSR). Na této operaci lze demonstrovat, že realizace DoS (Denial of Service) útoku na tuto operaci, může způsobit odepření služby.

Útok DoS na operaci WSR lze provádět zasíláním hodnoty z master zařízení na jeden vybraný registr v cyklu, dokud nedojde u slave zařízení k překročení výpočetních kapacit a odepření služby. Slave zařízení musí při této operaci odpovědět téměř stejnou zprávou, která byla odeslána z master zařízení. Tento útok může být dále prováděn z více master zařízení (DDoS, Distributed DoS), tím dochází k vyčerpání výpočetních kapacit dříve. Útok lze obdobně provádět zápisem hodnoty na jednotlivé registry v cyklu (zápis není prováděn pouze do jednoho vybraného registru). Tento typ útoku je hůře detekovatelný.

V rámci experimentálního testování byla zaměřena pozornost na operaci WSR a možnosti detekce zmíněných útoků na slave zařízení. K určení, zda se jedná o nestandardní provoz, je využit odestup (δ) mezi jednotlivými WSR operacemi realizovanými na jeden registr v paměti slave zařízení. K vytvoření rozhodovací prahové hodnoty (Δ) je využito několik (x) předcházejících operací, viz rovnice 1. V době "učení"je nutné zajistit kontrolu, zda se v síti nevyskytuje útočník. Z každé následující zprávy je získán odestup od předchozí zprávy (δ) a porovnán s prahovou hodnotou (Δ), viz rovnice 2. V případě splnění podmínky je vyhlášen poplach oznamující potenciální DoS útok. Aby bylo možné detekovat i potenciální DoS útok pomocí operace WSR i na více registrů (zápis je prováděn cyklicky na jednotlivé registry) je porovnáván odestup (δ) jednotlivého registru s předchozím odstupem stejného registru, viz rovnice 3. Pokud jsou tyto hodnoty s určitou odchylkou (r [%]) totožné, je vyhlášen poplach s upozorněním na možný DoS útok.

$$\Delta = \frac{\sum_{n=1}^{x} \delta}{x} \quad [\mathrm{s}] \qquad (1)$$

$$\delta < \Delta \quad [-] \qquad (2)$$

$$\delta_{k-1} - r * \delta_k \leq \delta_k \leq \delta_{k-1} + r * \delta_k \quad [-] \qquad (3)$$

V rámci vytvořeného skriptu jsou jednotlivé rovnice implementovány. Pokud je některá z podmínek splněna je proveden záznam v rámci logu, viz výpis 5. V rámci experimentálního testování byla hodnota x natavena na hodnotu 10 a hodnota r byla nastavena na hodnotu 3 %. Nejprve dochází k vytvoření (naučení) prahové hodnoty (Δ) z prvních x (x=10) WSR operací, reprezentováno výpisem „ucim se“. Během fáze učení však nastalo splnění podmínky definované rovnicí 3 (řádek 14). Ve sloupci „text“ je proveden výpis „treshold se opakuje“, který upozorňuje na potenciální zápis hodnot v cyklu. Po ukončení fáze „učení“ (do řádku 15 včetně) dochází ke stanovení prahové hodnoty (viz sloupec treshold od řádku 16) a dochází tak k aplikaci rovnice 2, její splnění je reprezentováno výpisem „treshold prekrocen“, který upozorňuje na zápis v neobvyklém intervalu. Zpráva, která nesplňuje ani jednu vytvořenou podmínku je reprezentována textem „zprava prijata“.

Výpis 5: Zeek, zjednodušený log.

```
#path modbus_register_change
#open 2020-02-29-07-07-55
#fields ts         id.orig_p id.resp_p new_val delta     src_addr      dst_addr        text                treshold
#types  time       port      port      count   interval  addr          addr            string              interval
1582988875.499218 44373     5020      10      -         192.168.100.9 192.168.100.11  Navazano spojeni    -
1582988878.137259 59707     5020      10      2.638041  192.168.100.9 192.168.100.11  Ucim se             0.000000
1582988879.238013 40747     5020      10      1.100754  192.168.100.9 192.168.100.11  Ucim se             0.000000
1582988880.182552 47265     5020      10      0.944539  192.168.100.9 192.168.100.11  Ucim se             0.000000
1582988881.004920 47805     5020      10      0.822368  192.168.100.9 192.168.100.11  Ucim se             0.000000
1582988881.771920 38581     5020      10      0.767000  192.168.100.9 192.168.100.11  Ucim se             0.000000
1582988882.433527 53953     5020      10      0.661607  192.168.100.9 192.168.100.11  Ucim se             0.000000
1582988883.068828 37633     5020      10      0.635301  192.168.100.9 192.168.100.11  Ucim se             0.000000
1582988883.724617 49305     5020      10      0.655789  192.168.100.9 192.168.100.11  Ucim se             0.000000
1582988884.397594 42075     5020      10      0.672977  192.168.100.9 192.168.100.11  TRESHOLD SE OPAKUJE 0.000000
1582988884.972997 50889     5020      10      0.575403  192.168.100.9 192.168.100.11  Ucim se             0.000000
1582988885.625668 40575     5020      10      0.652671  192.168.100.9 192.168.100.11  TRESHOLD PREKROCEN  0.947378
1582988886.141697 49753     5020      10      0.516029  192.168.100.9 192.168.100.11  TRESHOLD PREKROCEN  0.947378
1582988888.328261 46409     5020      10      2.186564  192.168.100.9 192.168.100.11  Zprava prijata      0.947378
1582988889.939448 57977     5020      10      1.611187  192.168.100.9 192.168.100.11  Zprava prijata      0.947378
```

Vytvořený systém pravidel pomocí IDS Zeek je schopen detekovat DoS útok zaměřený na operaci WSR. Hlavní výhodou je vytvoření prahové hodnoty Δ, pro každý registr odlišně, pomocí které lze detekovat vyskytující se anomálie v síti. Vytvořený systém pravidel detekce DoS na operaci WSR je možné dále rozšířit o možnosti detekce pravidelně prováděných operací v rámci průmyslové sítě. V případě plánovaných a pravidelně prováděných operací lze detekovat, zda se daná operace skutečně provedla a nedošlo ke zpoždění nebo odstranění zprávy ze sítě.

4 ZÁVĚR

K zajištění bezpečnosti průmyslových sítí je zapotřebí využit různých mechanismů. Pro detekci signatur byl využít nástroj Snort, ve kterém byly definovány pravidla pro detekci určených IP adres master zařízení a pro detekci paketů přesahující maximální povolenou velikost. Za účelem demonstrace využití metod anomálií byl využit systém ZEEK, ve kterém byla vytvořena metoda pro detekci Write Single Register operace. Pro detekci anomálie je využit odestup přicházejících zpráv. Vytvořené metodiky detekce jsou schopny provádět detekci anomálií a bezpečnostních incidentů na základě získaných parametrů. Každý vygenerovaný alert je nutné prověřit a popřípadě definovat následná opatření, jak bude s detekovaným případem zacházeno. K zabezpečení průmyslových sítí je nutné použít více dostupných systémů, které zajišťují/doplňují bezpečnost spolu s kombinací systémů detekující signatury a anomálie v síti. Včasná detekce může útoku efektivně zabránit, popřípadě provést bezpečné a řízené vypnutí systému a předejít tak ztrátě kontroly nad systémem.

REFERENCE

[1] COLLANTES, Miguel Herrero a Antonio López PADILLA. Protocols and Network Security in ICS Infrastructures. *The Spanish National Institute for Cyber-security*. 2015.

[2] SCADA MODBUS Protocol Vulnerabilities. *Cyberbit.com* [online]. 2017 [cit. 2019-10-29]. Dostupné z: https://www.cyberbit.com/blog/ot-security/scada-modbus-protocol-vulnerabilities/

[3] KUCHAŘ, Karel. Vhodná strategie pro detekci bezpečnostních incidentů v průmyslových sítích [online]. Brno, 2019 [cit. 2020-02-14]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/123145. Semestrální práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Radek Fujdiak.

[4] FACHKHA, Claude. Cyber Threat Investigation of SCADA Modbus Activities. *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* [online]. IEEE, 2019, 2019, , 1-7 [cit. 2020-03-02]. DOI: 10.1109/NTMS.2019.8763817. ISBN 978-1-7281-1542-9. Dostupné z: https://ieeexplore.ieee.org/document/8763817/