STU

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE

MATERIÁLOVOTECHNOLOGICKÁ FAKULTA SO SÍDLOM V TRNAVE

Ing. Tibor Horák

Autoreferát dizertačnej práce

Nové metódy zvýšenia bezpečnosti Internetu vecí v rámci konceptu Industry 4.0

na získanie akademického titulu: doktor (philosophiae doctor, PhD.)

v doktorandskom študijnom programe: Automatizácia a informatizácia procesov

v študijnom odbore: Kybernetika

Forma štúdia: denná

Miesto a dátum: Trnava, 31.5.2021

STU

Dizertačná práca bola vypracovaná na Katedre aplikovanej informatiky a automatizácie a Ústave aplikovanej informatiky, automatizácie a matematiky

Predkladateľ: Ing. Tibor Horák
Ústav aplikovanej informatiky, automatizácie a matematiky
Materiálovotechnologická fakulta so sídlom v Trnave,
Slovenská technická univerzita v Bratislave
Jána Bottu 2781/25
917 24 Trnava

Školiteľ: doc. RNDr. PaedDr. Ladislav Huraj, PhD.
Katedra aplikovanej informatiky
Fakulta prírodných vied
Univerzita sv. Cyrila a Metoda v Trnave
Nám. J. Herdu 2, 917 01 Trnava

Oponenti:

Autoreferát bol rozoslaný: .....

Obhajoba dizertačnej práce sa bude konať dňa ...... **o** .....**h**.

Na Materiálovotechnologickej fakulte fakulte STU so sídlom v Trnave, J. Bottu 25, 917 24, Trnava

.....

prof. Ing. Miloš Čambál, CSc.
dekan MTF STU

Obsah

Úvod

Internet vecí predstavuje komunikačnú sieť spájajúcu rôzne typy zariadení v priemysle (industrial IoT networks) alebo v domácnosti (home IoT networks). Internet vecí je rozvíjajúca sa oblasť s exponovaným technickým, sociálnym a ekonomickým významom. Spotrebný tovar, osobné a nákladné automobily, priemyselné a úžitkové zariadenia, snímače a ďalšie rôzne zariadenia sú v rámci Internetu vecí pripojené k sieti a je vykonávaná analýza ich údajov. Predpokladá sa viac ako 100 miliárd pripojených zariadení internetu vecí v roku 2025. Väčšina týchto zariadeniach obsahuje len malé alebo žiadne zabezpečenie proti útokom z lokálnej siete či z Internetu. Väčšina bezpečnostných prostriedkov založená na tradičných centrálne orientovaných autentifikačných protokoloch využívaných pre komunikačné siete v rámci Internetu nie je pre Internet vecí prakticky použiteľná. Heterogénny a často distribuovaný charakter IoT sietí, využívajúci end-to-end dôveru medzi zariadeniami, môže často viesť k rôznym zneužitiam. Škody spôsobené zneužitím IoT zariadení môžu byť veľmi vážne. Nejde iba o zámerný útok, ale aj chybné nastavenie či výpadok riadiacej jednotky.

Cieľom dizertačnej práce je analyzovať a kategorizovať bezpečnostnú problematiku IoT zariadení. Budú preskúmané a kategorizované sieťové protokoly, ktoré sú používané pre integráciu IoT a na základe zistených skutočností bude navrhnutý spôsob analýz a kontroly uplatniteľné pre IoT zariadenia, ktoré budú nápomocné pre otestovanie zraniteľnosti a umožnia predikovať dopady integrácie IoT z pohľadu bezpečnosti do priemyselného prostredia a výrobnej linky. Na základe analýz a vykonaných testov budú identifikované priame a nepriame dopady a podozrivé vzory správanie. Na základe výsledkov budú klasifikované zistené fakty a vytvorené základné odporúčané pravidlá a spôsoby ochrany IoT zariadení. Výsledkom budú komplexné ale jasné prístupy a metódy, ktoré napomôžu plánovať systém integrácie a spôsobu ochrany IoT zariadení a zároveň umožnia nastaviť efektívne a jasné pravidlá integrácie IoT zariadení do produkčného prostredia.

1 Analýza a problematika súčasného stavu

Výrobné linky sú jedným zo základných prvkov priemyselnej výroby a umožňujú efektívne riadenie výrobného procesu a tým zníženie nákladov. Na zlepšovanie výkonnosti výroby a efektívneho prepojenia výrobných celkov je potrebné klásť dôraz na monitorovanie a údržbu jednotlivých komponentov zapojených do výrobného procesu. Monitorovanie a údržba výrobnej linky je v súčasnosti robená pomocou tabletov alebo operátorských panelov, kde operátori môžu na diaľku nastaviť rôzne parametre výrobnej linky alebo skontrolovať stav linky. Pri tejto činnosti nachádza svoje uplatnenie práve priemyselný Internet vecí (IIoT). IIoT sa už bežne využíva na monitorovanie rozsiahlych výrobných systémov a na diagnostiku porúch, ale aj na identifikáciu strojov napr. cez RFID a na mnohé ďalšie využitia pre rôzne odvetvia priemyslu, ako elektrárne, dodávky vody, alebo ropné a plynové rafinérie [1,2].

Rapídny rozvoj komunikačných sietí umožnil aplikovanie sieťových riadiacich systémov do výroby, pričom je umožnené, aby kľúčové komponenty výroby boli distribuované a riadené prostredníctvom komunikačnej siete. Integrácia IIoT technológie do priemyselného prostredia prináša lepšiu flexibilnosť a efektívnosť výrobného systému a nové služby. Údaje získavané pomocou IIoT sú presnejšia a ich zber je možné robiť nepretržite. Presnejšie a nepretržité údaje umožnia lepší monitorovací systém, ktorý zabráni vzniku nebezpečných situácií a je jedno, či ide o jadrovú elektráreň alebo iný výrobný závod. Okrem toho sa implementácia IIoT vo výrobných linkách alebo iných priemyselných projektoch zameriava na zníženie výrobných nákladov alebo nákladov na údržbu a zlepšenie efektívnosti, stability, bezpečnosti atď. [3]. Integrácia IIoT technológie do priemyselného prostredia na druhej strane prináša aj nové výzvy, ktorým je potrebné čeliť. Výrobcovia kladú pri IoT zariadeniach dôraz predovšetkým na nízku cenu a je zanedbávané zabezpečenie IoT zariadení. Typické IoT zariadenie obsahuje procesor s relatívne nízkym výkonom, nízku kapacitu operačnej pamäte a schopnosť pripojenia sa k Internetu. Snaha o implementáciu bezpečnostného prvku priamo v IoT zariadení zväčša rapídne zníži výkon IoT zariadenia a navýši jeho cenu. Práve bezpečnosť internetu vecí predstavuje jedno z najväčších slabých miest brzdiacich prijatie IIoT v masovom rozsahu.

Útoky typu DoS spôsobujú vyčerpanie zdrojov systému a následné pomalé spracovanie, až kým sa systém nezablokuje alebo nevypne. Distribuovaný DoS (DDoS) je navrhnutý tak, aby využíval na útok veľa útočiacich zariadení, ktoré odosielajú vysoký objem prenosu do siete a spotrebúvajú tak počítačové zdroje. Útok DDoS môže tiež znížiť funkčnosť internetu vecí, pretože IoT zariadenia nie sú navrhnuté na zvládnutie DDoS útokov. V mnohých prípadoch môže útok spôsobiť prerušenie výrobnej linky a opätovné zavedenie správneho chodu systému je možné len pomocou ľudskej asistencie. Implementácia IoT zariadení do výrobného systému môže zvýšiť zraniteľnosť systému a umožniť útočníkovi realizovať útok spôsobom, ktorý by predtým nebol možný. Príkladom môže byť využitie implementovaného IoT zariadenia ako reflektora pre reflektovaný DDoS útok. Mnohé publikácie sa odvolávajú na zraniteľnosť výroby a výrobnej linky prepojenej s IoT zariadeniami práve DDoS útokom, napr. [4,5,6], ale konkrétne dopady na výrobnú linku nie sú nikde detailnejšie opísané alebo testované.

2 Ciele a východiská dizertačnej práce

Dizertačná práca sa venuje problematike zabezpečenia IoT zariadení v koncepte Industry 4.0. Väčšina bezpečnostných prostriedkov založená na tradičných centrálne orientovaných autentifikačných protokoloch využívaných pre komunikačné siete v rámci Internetu nie je pre Internet vecí prakticky použiteľná. Spoliehať sa len na izolovanosť prostredia nie je v koncepte Industry 4.0 bezpečným riešením. Koncept Industry 4.0 využíva vzdialený prístup k strojom, čo prináša jasné výhody pre výrobu. Priemyselné riadiace a kontrolné systémy SCADA ICS/DCS tvoria z pohľadu kybernetickej bezpečnosti rozsiahlu a donedávna nezávislú oblasť [7].

Kybernetické útoky zacielené na priemyselné zariadenia sú však vážnou hrozbou. Priemyselné IoT zariadenia prinášajú rôzne zmeny vo výrobnom systéme. Pridávajú však tiež rôzne bezpečnostné výzvy do životného cyklu produktu výrobného systému.

Dizertačná práca sa zaoberá zabezpečením výrobných sieťových infraštruktúr, do ktorých sú do výrobného procesu integrované IoT zariadenia. Je potrebné poznamenať, že hoci zraniteľnosť IoT zariadení je vo všeobecnosti známa, aplikovanie problému na výrobnú linku je v literatúre často len predpokladané, ale nie otestované, či dokumentované.

Pre komplexnosť tejto problematiky a na základe získaných poznatkov sme sa rozhodli v dizertačnej práci venovať komunikácii priemyselných IoT zariadení s výrobnou linkou riadenou PLC zariadeniami a dôkladnej analýze a testovaniu súčasného zabezpečenia a odolnosti voči kybernetickým DDoS a reflektovaným DRDoS útokom počas výrobného procesu. Útoky DDoS a DRDoS sú založené na protokoloch TCP, UDP a ICMP. DDoS útoky sú jednou z najzávažnejších hrozieb, s ktorými sa firmy dnes stretávajú.

Hlavným cieľom dizertačnej práce je analyzovať, navrhnúť, implementovať, otestovať a zhodnotiť možné bezpečnostné opatrenia a riešenia proti zvoleným kybernetickým DDoS a reflektovaným DRDoS typom útokov s prihliadnutím na kompromis medzi pripojením a bezpečnosťou, ktorý je dôležitou výzvou pri integrácií priemyselných IoT zariadení do výroby.

Splnenie hlavného cieľa dizertačnej práce je podmienené naplnením stanovených čiastkových cieľov, ktoré sú sformulované nasledovným spôsobom:

1. **Analýza a spracovanie teoretických východísk a poznatkov zo skúmanej problematiky z domácej a zahraničnej literatúry a vedeckých štúdii.** Vytvoriť prehľad, štatistiku využívania a súčasný stav problematiky kybernetickej bezpečnosti z pohľadu integrácie IoT zariadení do výrobných procesov s výrobnou linkou.
2. **Stanovenie cieľov a výskumných okruhov.** Na základe vypracovania analýzy a orientovaní sa v problematike stanoviť ciele a smerovanie skúmanej problematiky.
3. **Analýza a testovanie možných spôsobov útokov na priemyselné IoT zariadenia.** Zraniteľnosť výrobnej linky s integráciou priemyselných IoT zariadení je zväčša len predpokladaná, ale nie reálne potvrdená. Snahou je ukázať reálne experimenty útokov a s

nimi spojene aj dopady na výrobnú linku a výrobné procesy integrované s priemyselnými IoT zariadeniami.

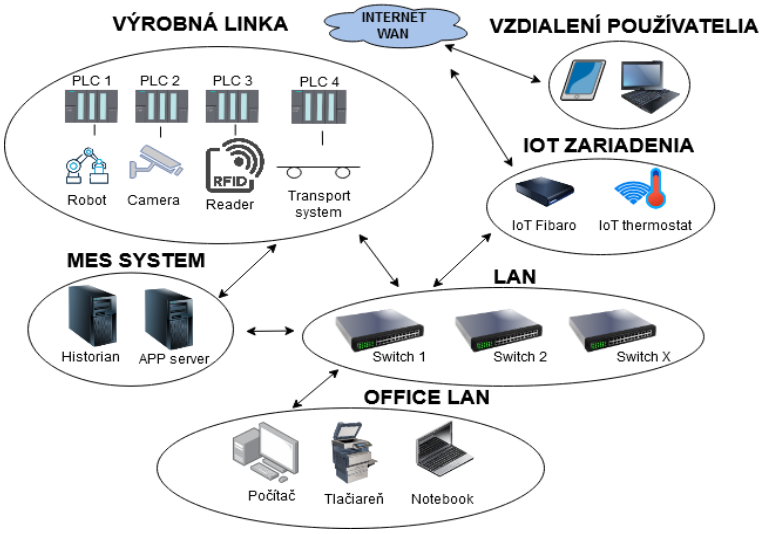
4. **Návrh a implementácia bezpečnostných riešení.** Na základe analýzy reálnych experimentov útokov a s nimi spojených dopadov na výrobné procesy integrovanými IoT zariadeniami preskúmať rôzne metódy bezpečnostných autorizačných protokolov heterogénnych IoT sietí a navrhnúť, vylepšiť a implementovať spôsoby ochrany zamerané priamo na priemyselné IoT zariadenia, ako aj definovať možnosti ochrany zariadení či podsietí využívajúce dané IoT zariadenia proti zvoleným typom útokov.
5. **Overenie a zhodnotenie navrhnutých riešení.** Po implementácii navrhnutých riešení pomocou penetračného testovania overiť ich účinnosť v reálnej výrobnej infraštruktúre s integrovanými IoT zariadeniami. Na základe výsledkov zhodnotiť efektivitu navrhnutých a implementovaných riešení.
6. **Posúdenie prínosov dizertačnej práce pre špecifikovanú oblasť.** Na základe analýzy návrhu, implementácie, overenia a zhodnotenia riešení špecifikovať prínosy dizertačnej práce.

3 Testovanie bezpečnosti reálnej výrobnej infraštruktúry s integrovanými IoT zariadeniami.

Pre overenie bezpečnosti v podobe implementácií DDoS a reflektovaných DDoS (DRDoS) útokov sa používa reálna výrobná sieťová infraštruktúra, do ktorej boli integrované IoT zariadenia. Túto sieťovú infraštruktúru spájajú dva switche značky TP-Link. Switche spájajú výrobnú linku so serverom, IoT zariadeniami a podsieťou Office LAN. Server je vybavený operačným systémom Windows 2008 server. Tento server obsahuje Mes systém, cez ktorý je možné riadiť a kontrolovať výrobné procesy. Obsahuje podsystém Historian, kde sa ukladajú všetky historické údaje o výrobe a výrobných procesoch.

Pre modernizáciu a priblíženiu sa ku konceptu Industry 4.0 bola výrobná linka rozšírená v sieťovej infraštruktúre aj o IoT zariadenia. Tieto pridané zariadenia majú za úlohu chrániť výrobnú linku aj procesy a zároveň umožňujú prístup z vonkajšej siete WAN pre ich jednoduché ovládanie a informovanie operátorov na diaľku cez mobilné aplikácie. Pri tomto prístupe zo siete WAN vznikajú riziká útokov z vonkajšej siete a tým sa celá infraštruktúra vrátane výrobnej linky stáva oveľa zraniteľnejšou a náchylnou na DDoS a DRDoS útoky smerované cez IoT zariadenia.

Prvým IoT zariadením, o ktoré bola linka rozšírená, je IoT termostat. Úlohou IoT termostatu je zabezpečiť reguláciu teploty na diaľku v miestnosti, kde sa výrobná linka nachádza. Toto zariadenie je do sieťovej infraštruktúry pripojené bezdrôtovo cez technológiu Wi-Fi a maximálnu rýchlosť dátového prenosu dosahuje 54Mbps. Ďalším pridaným IoT zariadením je Fibaro. Toto IoT zariadenie svojimi IoT senzormi má za úlohu chrániť výrobnú linku z bezpečnostného hľadiska pred požiarmi, záplavami a pomocou pohybového senzora kontrolovať prítomnosť operátorov na pracovisku.



Obr.1. Reálna sieťová infraštruktúra použitá pri testovaní

Všetky zariadenia sú v sieťovej infraštruktúre pripojené cez LAN pevnú sieť dosahujúcu výšku dátového prenosu až 1Gbps. Ako znázorňuje obrázok č.1, vo výrobnej linke, ktorá je súčasťou sieťovej infraštruktúry sa nachádzajú stroje, ktoré komunikujú so svojim PLC zariadením. PLC zariadenia sú značky Siemens S7-300 typ 314. Každé PLC je prepojené káblom LAN so switchom

aj so strojom. Stroje sú naprogramované cez PLC zariadenia, ktoré riadia výrobný proces. Súčasťou testovacieho prostredia je aj pridaný počítač cez LAN kábel a ten slúžil ako paket generátor na vykonávanie DDoS útokov na výrobnú linku a IoT zariadenia.

Hlavným zariadením, ktoré tvorí fundamentálnu súčasť výrobného procesu je výrobná linka. Na výrobnej linke, ako môžeme vidieť na obrázku č. 2, bežia reálne výrobne procesy, ktoré používajú poprední priemyselní výrobcovia nápojov, potravín a aj chemický priemysel.

Obr.2. Reálna výrobná linka.

Výrobná linka pozostáva z piatich zón. Každá z nich vytvára časť výrobného procesu. Väčšina týchto zón je ovládaná PLC kontrolérmi od výrobcu Siemens a tie majú za úlohu vykonávať operácie od tých najjednoduchších až po tie najzložitejšie. V prvej zóne prebieha zber a dávkovanie materiálov. V druhej zóne po zmiešaní a dávkovaní materiálov pokračuje výrobný proces tým že sa daný materiál plní do fliaš, ktoré sú uzatvárané uzáverom na otočnom stole. Fľaše sú triedené pomocou RFID snímača a sú expedované transportným systémom. Transportný systém nakladá naplnené fľaše do prepraviek. Správne naplnenie prepraviek fľašami kontroluje vysokorýchlostná kamera. Zóna 3 slúži na dávkovanie polotovarov na výrobu uzáverov. Zóna 4 slúži na prepravovanie prepraviek medzi jednotlivými stanicami pomocou dopravného pásu. Zóna 5 slúži na vykladanie fliaš z prepraviek a ich následný transport do rozbaľovacej stanice. Ide o recyklačnú stanicu v ktorej sa nachádza Robot a čerpadlo pomocou nich prebieha vyprázdňovanie nepotrebného tekutého obsahu fliaš. Jednotlivé zóny komunikujú pomocou siete Ethernet.

Výrobná linka pre efektívnu výrobu je vybavená MES systémom založenom na platforme Wondervare. Tento systém sleduje a dokumentuje výrobný proces. Na základe získaných informácii dokážu výrobcovia nastaviť výrobne podmienky tak, aby sa zlepšila efektivita výrobného procesu. Súčasťou je aj podsystém Historian Server a ten slúži ako vysoko rýchlostná databáza historizovaných informácii v reálnom čase [8].

Komponenty výrobnej linky komunikujú pomocou siete Ethernet. PLC, HMI panely majú pridelené statickú IP adresu a ich adresný priestor je pridelená IPv4 v adresnej triede C. PLC posielajú správu, ktorou do siete indikujú stav o ich dostupnosti. Táto aktivita beží periodicky

a opakovane overuje stav o dostupnosti iných PLC jednotiek. PLC sú vyrobené tak, aby odolali extrémnym teplotám, vibráciám a vlhkosti. PLC nie sú závislé od PC alebo pripojenia do sieťovej infraštruktúry a fungujú nezávisle bez nutnosti pripojenia k sieťovej infraštruktúre [9].

Ostatné prvky výrobnej linky sú prepojené aj inými protokolmi ale nie sú pripojené na switch infraštruktúry. Tieto boli vynechané z testovania vzhľadom na to, že ich protokoly nie sú priamo pripojené a predstavujú nezávislú časť výrobnej linky. PLC zariadenia mali otvorené porty 80, 443 a 8080 web, 23 telnet, 21 ftp, 111 rpc bind, 389 ldap a porty10001 až 10004 a port 10009. Robot mal dostupné porty 1200 a 10001 a používal UDP protokol.

Prvým integrovaným IoT zariadením je multizónový regulátor umožňujúci ovládanie teploty jednotlivých miestností s využitím individuálnych časových programov. Systém je určený pre vykurovanie radiátormi, podlahové vykurovanie a tiež pre riadenie zohrievania zásobníka vody.

Druhým integrovaným zariadením do výrobnej infraštruktúry je IoT bezpečnostný systém v podobe miniaturizovanej riadiacej jednotky, ktorá je centrálou systému Fibaro. Riadiaca jednotka počúva a riadi cez sieť technológiou Z-Wave všetky bezdrôtové moduly, ktorými sú detektory pohybu, dymu, zaplavenia, dverový senzor a bezdrôtová zásuvka a zároveň môže byť aj bránou do internetu a Wi-Fi siete. S jej pomocou je možné zaznamenávať vstupné parametre zvolených veličín z prostredia podniku dokáže spravovať všetky nastavenia na jednom mieste. Taktiež umožňuje sa pripojiť cez mobilnú aplikáciu alebo webové rozhranie odkiaľkoľvek a dokáže kontrolovať moderný podnik vzdialene a ušetrí čas aj peniaze.

3.1 Testovanie výrobnej infraštruktúry v podobe DDoS útokov

Testovacie pracovisko je založené na reálnom výrobnom prostredí v reálnom čase. Keďže výrobná linka za účelom priblíženia sa ku konceptu Industry 4.0 bola rozšírená o IoT zariadenia, ktoré umožňujú komunikáciu aj s vonkajším prostredím WAN, je zároveň zraniteľnejšia o možné útoky z vonkajšej siete. Ďalšou nevýhodou IoT zariadení Fibaro a termostat je, že zariadenia sú slabo zabezpečené, čo bolo preukázane aj v nedávnych výskumoch týchto IoT zariadení [10].

Za účelom vykonania testovacích scenárov v podobe kybernetických útokov bolo použité PC zariadenie ako útočník, ktorý preverí útokmi komunikáciu sieťovej infraštruktúry zloženej s IoT zariadeniami a výrobnej linky. PC zariadenie pre vykonanie útokov využíva operačný systém Kali Linux. Tento operačný systém je vybavený nástrojmi Hping3. Nástroj Hping3 dokáže pracovať so sieťovými protokolmi TCP, UDP, ICMP. Riadenie a ovládanie generovania paketov sa vykonáva pomocou príkazov cez príkazový riadok.

Bolo zrealizovaných päť typov scenárov útokov. Všetky scenáre útokov boli spustené za plnej funkčnosti výrobnej linky a pridaných IoT zariadení. Útoky boli riadené jednak z vonkajšej siete internet, ako aj z vnútornej siete LAN. Boli realizované dva základne typy DDoS útokov.

- Prvý typ útokov bol nepriamy DRDoS. Útočník posielal pakety na neexistujúci port IoT zariadenia. IoT zariadenie tieto pakety reflektovalo na podvrhnutú IP adresu, ktorá patrila vybraným zariadeniam alebo PLC kontrolérom výrobnej linky.
- Druhý typ útokov bol priamy DDoS. Útočník posielal pakety na jednotlivé stroje alebo PLC kontroléry. V jednotlivých scenároch boli použité konkrétne typy útokov ICMP echo flood, TCP SYN flood, TCP ACK flood a UDP flood.

Posielanie paketov bolo nastavené na najvyššiu možnú rýchlosť. Dĺžka útokov nebola stanovená. Útoky prebiehali dovtedy, kým zariadenia, na ktoré sa útok realizoval, neprestali v sieti komunikovať. Cieľom útokov bolo skompromitovať výrobný proces zahltením jednotlivých komponentov výrobnej linky, a to či už priamym spôsobom na komponenty výrobnej linky alebo nepriamym spôsobom cez IoT zariadenia.

Tabuľka č.1. Stručný prehľad použitých typov útokov v jednotlivých scenároch.

Scenáre útokov	Typ útoku	Útok
Prvý scenár útoku	Reflektovaný(DRDoS)	ICMP flood
Druhý scenár útoku	Reflektovaný(DRDoS)	ICMP flood
Tretí scenár útoku	Reflektovaný(DRDoS)	UDP flood
Štvrtý scenár útoku	Priamy (DDoS)	TCP SYN flood
Piaty scenár útoku	Priamy (DDoS)	TCP ACK flood

3.2 Dopady DDoS a DRDoS útokov na výrobný proces

Útoky boli spustené počas plnej prevádzky výrobného procesu. Vykonané testovacie scenáre útokov mali významný dopad na výrobný proces. Každý scenár útoku sa prejavoval odlišne a vždy bol najskôr nesprávne identifikovaný a aj skúsený operátor ho vyhodnotil ako poruchu, ktorú bolo možné odôvodniť hardvérovým problémom, nastavením alebo zlyhaním nesprávne identifikovaných komponentov. Tieto závery nemožno pripísať nedostatku skúseností operátora, pretože dopad na výrobný proces počas testovaných útokov sa javil ako bežná prevádzková porucha. Monitorovací systém a integrácia výrobného procesu do systému MES neodhalili neobvyklé správanie výrobnej linky.

Nárast sieťovej komunikácie pre sieťové protokoly bol pozorovaný až s oneskorením a nestačil na identifikáciu zdroja problému. Pre príklad možno uviesť, že všetky vozíky zostali plné a kamera nedokázala prečítať QR kódy, čo viedlo k oneskoreniu výroby. Variabilita problémov a náhodnosť času, ako to dokazujú scenáre DDoS útokov, ukazujú, že je možné ovplyvniť výrobný proces bez jasnej identifikácie zdroja problémov. Zároveň je tu preukázaná skutočnosť, že útočník nemusí poznať infraštruktúru, ktorá je cieľom kybernetického útoku. Na druhej strane, ak útočník nepozná infraštruktúru, v niektorých prípadoch útok nemusí byť schopný degradovať výrobný proces, ako to ukázal scenár testu pre robot a jeho PLC.

Vo všeobecnosti je možné na základe testovacích scenárov konštatovať, že IoT zariadenia môžu predstavovať potenciálne nebezpečenstvo pre výrobný proces a ich základné bezpečnostné funkcie a nastavenia nemusia postačovať na ich zabezpečenie voči zneužitiu. Testami bol preukázaný dopad a platnosť tohto tvrdenia.

V tejto oblasti bola identifikovaná skutočnosť, že zabezpečenie IoT zariadení je prioritná súčasť riešení, ak je IoT zariadenie integrované do výrobnej linky. Integrácia IoT zariadení do výrobného procesu, predstavuje potenciálnu zraniteľnosť, ktorá môže spôsobiť vznik neočakávaných a neželaných stavov vo výrobnom procese, ktoré sa môžu líšiť podľa použitého hardvéru a zapojenia infraštruktúry.

4 Návrh bezpečnostných riešení pre výrobne infraštruktúry s integrovanými IoT zariadeniami.

Pomocou scenárov útokov a následných analýz útokov bolo zistené správanie výrobnej linky z hľadiska odolnosti komunikácie. Taktiež boli zistené možné hrozby a narušenia výrobného procesu, ktoré môžu nastať integrovaním IoT zariadení.

4.1 Základné odporúčania na zabezpečenie IoT zariadenia

Spoliehať sa iba na izolovanosť výrobnej infraštruktúry od vonkajšieho prostredia nie je dostatočným bezpečnostným opatrením. Priemyselné riadiace a kontrolné systémy SCADA ICS/DCS tvoria z pohľadu kybernetickej bezpečnosti rozsiahlu a donedávna nezávislú oblasť a predstava zabezpečenia spôsobom, kde systém je nedostupný a nemá prístup na internet, pri integrácii s IoT zariadeniami už je možná. Klasické riešenie izolácie infraštruktúry, nepredstavuje potrebné riešenie, nakoľko pre IoT zariadenia je nevyhnutná komunikácia s vonkajšou sieťou [11].

Kybernetické útoky zacielené na priemyselné zariadenia sú vážnou hrozbou. Napriek tomu vzdialený prístup k strojom prináša nemalé výhody pre výrobu. Až 63% údržbárskych prác na stroji je buď bežnou kontrolou, alebo sa zistí, že problém jednoducho neexistuje. Okrem toho 30% alebo viac z týchto opráv možno vykonať na diaľku úpravou parametrov cez internet alebo s malou pomocou zo strany osoby na mieste [12].

IoT zariadenia v priemysle alebo aj pre domáce použitie sú prevádzkované často na jednoduchom hardvéri, ktorý býva nasadený v rozdielnych prostrediach. Takéto široké nasadenie vedie k novým výzvam, jedinečným pre IoT zariadenia. Softvérové aktualizácie a správa zraniteľností sú veľmi dôležité a vyžadujú odlišné stratégie ako pri iných IT aplikáciách. Pri navrhovaní bezpečných IoT zariadení je potrebné zohľadniť oblasti: klasifikácia dát; fyzická bezpečnosť; bezpečné nasadenie zariadenia; bezpečné operačné systémy; aplikačná bezpečnosť; správa poverení; šifrovanie; sieťové pripojenia; aktualizácie softvéru; protokolovanie.

Pri navrhovaní IoT zariadení je potrebné vybudovať bezpečný internet vecí už od rannej fázy navrhovania procesu alebo prostredníctvom konzultácií a auditov v neskorších fázach. Zavedením včasných opatrení je možne predchádzať a zabrániť rôznym kybernetickým útokom, aby prenikli cez IoT zariadenia napríklad do sieťovej infraštruktúry a až k výrobnej linke, kde by mohli útoky spôsobiť veľké škody priamo vo výrobnom procese [13].

4.2 Navrhované riešenia na zmiernenie účinkov DDoS útokov

Na základe zistených skutočností uvedených v Kapitole 4, bolo potrebné navrhnúť vhodné riešenia, ktoré zabránia alebo zmiernia prienik DDoS útokov do sieťovej infraštruktúry. Na základe zistených zraniteľností výrobnej infraštruktúry prichádzajú do úvahy dva možné stratégie – statická a dynamická. Obidve stratégie berú do úvahy reálne nasadenie IoT zariadení vo výrobnom podniku z pohľadu už existujúceho chodu výrobného procesu a to tak, aby ich nasadenie neohrozilo funkčnosť výroby.

Pri návrhu bezpečnostných riešení je potrebné vychádzať z predpokladu, že firma nie je ochotná alebo nie je možné zmeniť existujúcu prevádzku, či už vzhľadom na rozpočet alebo na fakt, že návrh by ohrozil dodávky dohodnutých zákaziek.

Statické bezpečnostné riešenie definuje základné pravidlá firewallu a povolenia pre komunikáciu na základe povolených portov a protokolov, prípadne zabezpečenie integrácie zariadení pomocou virtuálnych privátnych sietí. Druhá možnosť je dynamický spôsob zabezpečenia, v ktorom je potrebné sa zamerať na sledovanie komunikačných údajov a ich priebežné a komplexné vyhodnocovanie. Obe riešenia sa uplatňujú obvykle spolu a výsledná realizácia býva kombináciou obidvoch stratégií.

4.3 Statická stratégia zabezpečenia pomocou transparentného firewall bridgu

Prvý návrh vychádza z predpokladu, že organizácia má bežiaci výrobný proces a linku, ktorá už je dávno zabehnutá a neprichádza do úvahy žiadna zmena na výrobnej infraštruktúre, ale zároveň je potrebné integrovať IoT zariadenia pre zvýšenie kvality alebo efektívnosti výrobných procesov. Uvedený spôsob znamená statickú stratégiu zabezpečenia. Transparentný firewall bridge predstavuje vylepšenie tohto prístupu, nakoľko tvorí nezávislú integráciu rôznych zariadení do výrobného procesu.

V prípade existujúcej výrobnej linky je riskantné meniť existujúcu infraštruktúru, ktorá je nasadená v podniku. Zásah do existujúcej a správne fungujúcej infraštruktúry môže spôsobiť nevyžiadané prerušenie výroby. Risk manažment pri takejto operácií zohľadňuje, či pridaná hodnota IoT zariadení má významný vplyv na riadenie alebo či integrácia samotného zariadenia nepredstavuje riziko výrobného procesu ako takého.

Pri hľadaní riešenia bol zohľadnený aj tento fakt a ako prvé riešenie bol zvolený transparentný bridge firewall. Jedná sa o zariadenie, ktoré umožní nasadenie ochrany pridaných IoT zariadení a fakticky ich odizoluje od existujúcej infraštruktúry. V prípade, že je známa komunikácia IoT zariadení, dajú sa definovať pravidlá, ktoré povolia len komunikáciu na základe stanovených požiadaviek a ostatná komunikácia bude blokovaná. Samotná ochrana a cena riešenia by nemala prekročiť cenu IoT zariadenia a z tohto dôvodu sa javí použitie minipočítača Raspberry Pi ako vhodné riešenie.

Pre jednoduchosť bolo vhodné nakonfigurovať zariadenie s mini počítačom Raspberry Pi, ktoré má dve sieťové karty. Karty boli nakonfigurované do zapojenia typu transparent bridge. Bridge funguje na úrovni MAC (Ethernet adresy) a medzi obomi kartami je preposielaná komunikácia. Dá sa povedať, že sa jedná o switch, ale len s dvoma portami. Pridaná hodnota je, že takto zapojený bridge môže slúžiť aj ako firewall. Nevyhnutná podmienka uvedenej implementácie je, že obidve sieťové karty musia podporovať promiskuitný režim (promiscuous mode).

Požiadavka vyplýva z povahy implementácie, nakoľko bridge musí byť schopný pracovať s inými adresami zo siete a samotná sieťová komunikácia nie je prepisovaná na adresy fyzických kariet, ktoré sú fyzicky prítomné na mini počítači. Takto realizovaný bridge sa označuje ako transparentný, práve kvôli vlastnosti, že v sieťovej prevádzke nemusí byť priamo viditeľný.

Zároveň uvedené riešenie predstavuje možnosť aktívneho sledovania sieťovej prevádzky a dá sa zapojiť aj ako monitorovacie zariadenie a pomocou protokolov NetFlow alebo sFlow a tak dokáže zabezpečiť dodatočné informácie o sieťovej prevádzke, čo vytvára aj základ pre implementáciu dynamickej stratégie zabezpečenia.

Pre testovanie konfigurácii implementácie transparentného firewall bridge zariadenia bol zvolený operačný systém Linux pre procesory ARM armbian. Operačný systém musí mať povolený bridge modul. Zaujímavosťou uvedeného riešenia je, že samotný bridge nemusí mať ani pridelenú IP adresu. Riešenie bez pridelenej IP adresy sa obvykle nepoužíva, nakoľko je dobré mať prístup k firewallu a pripadne urobiť potrebnú konfiguráciu alebo sledovať stav zariadenia.

Pre prípad monitorovania prevádzky je ešte vhodné navrhované riešenie rozšíriť na základe NetFlow protokolu o NetFlow kolektor. Stačí ak je sieťová infraštruktúra vybavená manažovateľným switchom, ktorý podporuje protokol NetFlow.

Protokol NetFlow prináša informácie z tretej a štvrtej vrstvy sieťového modelu ISO/OSI, ako sú informácie o IP adresách, protokoloch, portoch objemu prenesených dát, paketoch a ďalšie technické detaily. NetFlow možno prirovnať k výpisu telefónnych hovorov. A tým pádom je možné vedieť, kto s kým komunikoval, kedy, ako dlho, ako často. Nevýhodou NetFlow je, že nie je možné vedieť, aký bol obsah komunikácie. Pomocou zberu, ukladanie a analýzy takýchto informácií v agregovanej podobe môžu sieťový administrátori riešiť mnoho prevádzkových a bezpečnostných úloh [14].

Pre monitorovanie prevádzky z jedného PLC zariadenia bolo potrebné pridať do minipočítača Raspberry Pi ešte jednu sieťovú kartu. Pre realizáciu monitorovania prevádzky bol použitý minipočítač s tromi sieťovými kartami, ktorý bol nakonfigurovaný ako NetFlow kolektorom spolu s transparentným bridgom. Dve sieťové karty sú zapojené v režime transparent bridge a tretia sieťová karta slúži na NetFlow traffic, ktorý je odosielaný do minipočítača, ktorý slúži ako NetFlow kolektor. Takýmto spôsobom je možné pri použití protokolu NetFlow verzie 5 získať základné údaje o sieťovej prevádzke, v ktorej je možné vidieť ako zariadenia medzi sebou komunikujú.

Nakonfigurovaný minipočítač je vhodné použiť na meranie a zaznamenávanie paketov. Výhoda opísaného riešenia je jednoduchosť a presnosť merania a možnosť sledovať ako útok prebieha aj s tým, že je možné vidieť, kedy zariadenie prestáva odpovedať a sieťová komunikácia viditeľne klesá. Výhoda je aj, že v existujúcej infraštruktúre je možné monitorovať jednotlivé zariadenia bez rizika znefunkčnenia výrobnej linky. Nevýhoda riešenia je, že pre správne zabezpečenie by malo mať každé PLC svoj minipočítač. V prípade prítomnosti switchu, ktorý má podporu NetFlow, nutnosť násobného počtu minipočítačov odpadá a sieťovú komunikáciu je možné zmapovať priamo pomocou switchu. Druhou nevýhodou implementácie minipočítača do návrhu zabezpečenia výrobnej infraštruktúry je možnosť problému s nedostatkom systémových zdrojov počas útoku, čo môže viesť k skresleniu hodnôt pozorovanej sieťovej komunikácie. V prípade vykonaných experimentov so sieťovou komunikáciou, ktorú produkovali napadnuté IoT zariadenia k problému s nedostatkom systémových zdrojov nedošlo. Nevýhodou môže byť navyše aj zložitosť konfigurácie minipočítača, prípadne zabezpečenie viacerých sieťových kariet na minipočítači.

4.4 Stratégia dynamického zabezpečenia

Ďalším navrhnutým riešením je dynamická bezpečnostná stratégia. Na rozdiel od statického riešenia je založená na základe meniacich sa podmienok a prebiehajúcej sieťovej komunikácie a predstavuje širšie spektrum možností zabezpečenia. Obvykle ide o sledovanie sieťovej komunikácie a detekciu anomálií, ktorá je pozorovateľná v sieťovej prevádzke. Táto stratégia si vyžaduje základné prvky sieťovej infraštruktúry, ktoré sú schopné poskytovať informácie o dátovej komunikácií, ktorá prebieha medzi zariadeniami. Jedná sa obvykle zariadenia ako sú switche a routre, ktoré sú vybavené podporou L2 a L3 a nazývajú sa aj ako manažovateľné a majú podporu pre sledovanie sieťového toku alebo generovanie jeho vzoriek.

Získané generované dáta z výrobnej sieťovej komunikácie boli použite pre trénovanie a overovanie v neurónovej sieti. Najlepšie riešenie je switch s podporou protokolom NetFlow, pretože je schopný preposielať komunikáciu do samostatnej siete LAN bez toho, aby dochádzalo k zahlteniu výrobnej časti siete LAN. Pre sumár paketov bolo vykonávané základne testovanie, ktoré sa nezaznamenávalo v plnom rozsahu, ale len so sekundovým rozlíšením.

Zaznamenávanie a analýza plného dátového toku by predstavovali pri rozsiahlej výrobnej linke kapacitný problém a náklady na realizáciu by ľahko mohli prekročiť hodnotu očakávaného prínosu IoT zariadenia. Preto bolo potrebné analyzovať ďalšie možnosti získavania údajov v sieťovej komunikácie. Bol vybratý variant Flow protokolu sFlow. sFlow je aj uznávaný ako priemyselný štandard, ktorý je podporovaný a implementovaný v širokej škále sieťových switchov a routrov vo vrstve L2. Výstupom protokolu sFlow sú informácie vo forme vzorky – tzv. sample, ktoré nie sú úplné a nemusia obsahovať presné informácie. Hoci tento fakt môže ovplyvniť presnosť, na druhej strane poskytuje prehľad o sieťovej komunikácií, ktorý je dostatočne dobrý na vytvorenie obrazu o vyťaženosti siete. sFlow pozostáva z dvoch samostatných častí: Agent a Kolektor. Časť Agent posiela údaje časti Kolektor. Údaje je možné zbierať pomocou sFlow protokolu verzie 5. Vo výrobnej sieťovej infraštruktúre s integrovanými IoT zariadeniami boli počas reálnej prevádzky identifikované aj komunikačné protokoly, ktoré sú uvedené v tabuľke č. 2:

Tabuľka č. 2. Použité komunikačné protokoly

Ethernet	Popis
0x0800	Internet Protocol version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x86dd	Internet Protocol version 6 (IPv6)
0x8892	PROFINET Protocol
0x88cc	Link Layer Discovery Protocol (LLDP)

Komunikáciu v IPv4 predstavovali prevažne IoT zariadenia alebo komunikačný MES systém, ktorý zabezpečoval riadenie a monitorovanie výroby. Ďalším skúmaným protokolom bol IPv6, kde bolo analyzované, že pripojené IoT zariadenie sa snažilo o komunikáciu na protokole IPv6, hoci tento protokol nebol vo výrobnej infraštruktúre používaný. Zvyšok komunikácie tvorili

protokoly ARP a LLDP. Aj keď ARP a LLDP sú zastúpené, slúžia ako doplnková komunikácia a nie sú relevantné pre analýzu sieťového prenosu.

Najpodstatnejšia časť sieťovej komunikácie prebiehala na protokole PROFINET, ktorý bol požitý na takmer celú integráciu výrobnej linky a predstavoval 95% celkovej komunikácie v sieti. Pre zbieranie údajov bol použitý sFlow kolektor, ktorý zabezpečuje zber údajov pomocou agentov, v tomto prípade dva switche podporujúce sFlow. sFlow kolektor je spustený ako server proces a odchytáva údaje posielané agentmi na UDP porte číslo 6343.

Prijímané sFlow datagramy boli konvertované do štruktúrovaných dát, kde jednotlivé dáta sú oddeľované čiarkou. Dáta sú podobné formátu CSV. Takto pripravené dáta boli posielané na spracovanie do neurónovej siete. Výstupom je stream údajov so zálohovaním do formátu CSV pre dodatočnú analýzu a overenie správnosti.

Apache Spark je jednotný analytický nástroj pre rozsiahle spracovanie údajov. Spark poskytuje niekoľko možností implementácie strojového učenia a to konkrétne v knižnici Spark's machine learning (MLLib), ktorá je vhodná aj pre testované riešenie, pretože spĺňa predpoklad škálovateľnosti [15]. Na výber bol natívny jazyk SCALA, ktorý sa vyznačuje výkonom a širokou podporou alebo jazyk Python, ktorý podľa dostupných dát je o niečo menej výkonný, na druhej strane umožňuje ľahkú integráciu použitých komponentov. Knižnica MLLib podporuje obidve možnosti. Vstupné dáta prešli procesom normalizácie.

Výber neurónovej siete bol realizovaný vzhľadom na potrebu odlíšiť legitímnu sieťovú premávku, ktorá predstavuje štandardnú a želanú komunikáciu a potenciálne nechcenú komunikáciu, ktorá môže predstavovať nebezpečenstvo pre výrobný proces. Neurónová sieť slúži na vyhodnocovanie vzoriek sieťového prenosu. Vzhľadom na povahu riešenej problematiky bolo potrebné zaviesť klasifikáciu a vyhodnotiť, ktoré pakety sú chápané ako žiaduca komunikácia a ktoré ako nežiaduca.

Rovnako je potrebné uvažovať, či aj hodnota množstva generovaných paketov má byť zahrnutá do vyhodnotenia, alebo či má zmysel viac uvažovať o ostatných parametroch sieťovej prevádzky, ktoré predstavujú napr. adresy, typy komunikácie, ich porty, priorita paketov a podobne. Množstvo generovaných paketov nemusí, ale aj môže byť smerodajný údaj o vzniku bezpečnostného incidentu. DDoS útoky predstavujú odstavenie služby na základe zahltenia zariadenia, na druhej strane prípadná zvýšená aj žiadaná komunikácia môže viesť k chybnej identifikácií. Tento typ a aj podobné problémy bolo potrebné vyriešiť a identifikovať vhodné parametre, ktoré určia prioritu a vplyv vstupov na výsledok.

Riešenie klasifikácie sa javí ako vhodné a bola vybratá logistická regresia, ktorá je určená na predpoveď binárnych výsledkov a využíva binomickú logistickú regresiu [16]. Predstavuje ju jednovrstvová neurónová sieť [17].

Binárna klasifikácia bola použitá logistická regresia, ktorá je vhodná na spracovanie dát, kde sa očakáva binárny výstup, ktorý v tomto prípad bude klasifikovať sieťovú prevádzku ako korektnú alebo nebezpečnú, čím je splnený predpoklad binárneho výstupu. Bola vykonaná konverzia všetkých vstupných údajov na číselné hodnoty. Boli detegované nulové a prázdne hodnoty a tie boli odstránené. Nepredstavujú stratu informácie, nakoľko ich vplyv vzhľadom na

neexistenciu alebo nulovú hodnotu dát predstavujú len šum v sieťovom toku. Zároveň je táto metóda nenáročná na výkon aplikácie, nakoľko pracuje len s číselnými hodnotami.

Realizácia logistickej regresie bola implementovaná v programe Apache Spark pomocou pySpark a jej rozširujúcej knižnice pre strojové učenie (SparkML). Knižnica poskytuje binomickú logistickú regresiu alebo multinomickú logistickú regresiu. Typ je možné nastaviť explicitne alebo je možné ponechať tento parameter prázdny a samotná knižnica SparkML identifikuje na základe dát, ktorý spôsob je lepší a tak zvoliť metódu, ktorá bude viac vyhovovať množine výcvikových údajov. Transformácia údajov, bola vykonaná v pySpark. Bola vygenerovaná množina údajov, ktorá sa používa na vytvorenie tréningovej sady. Táto predstavovala 70% zachytených dát. Zvyšných 30% bolo použitých na testovanie a overenie nacvičeného modelu.

Výsledný vektor je vypočítaný zo vstupných parametrov. Každý vstupný parameter predstavuje hodnotu, ktorá môže alebo nemusí mať vplyv na určenie výsledného vektora. Bola realizovaná a vyhodnotená hodnota korelácie vstupných údajov. Hodnota korelácie môže byť v rozmedzí od 1 po -1. Ak je hodnota blízko 1, znamená to, že existuje silná pozitívna korelácia; ak sa nachádza v blízkosti -1 je to silná negatívna korelácia. Treba brať do úvahy, že silná pozitívna aj negatívna korelácia predstavuje významný vplyv parametra na určenie výsledku. Silná negatívna korelácia však neznamená, že hodnota nie je vhodná alebo dokonca nežiaduca, práve naopak, hodnota -1 predstavuje marginálny vplyv na výsledok klasifikácie. Nezaujímavé alebo nie veľmi dôležité sú tie parametre, ktoré sa pohybujú v okolí nulových hodnôt.

Na základe meraných a zozbieraných údajov a ich analýzy bol vyhodnotený vplyv údajov, ktoré sú silné pozitívne korelácie ako napríklad vstupné parametre INPUTPORT, OUTPUTPORT a DST_MAC. Naopak koeficient blízko k -1, ktorý predstavuje silnú negatívnu koreláciu a tu bol identifikovaný vstupný parameter ETHERNET_TYPE a v menšej miere aj SRC_MAC. Zvyšné hodnoty okolo nuly nemajú lineárnu koreláciu a nie sú potrebné, ale ich spracovaním nie je možné dosiahnuť presnejšiu klasifikáciu. Detailný prehľad vstupných parametrov je uvedený v tabuľke č. 3

Tabuľka č.3. Korelácia vstupných parametrov vzhľadom na výsledok

Stĺpec	**Korelácia**
AGENT_ADRESS	Nulová hodnota
INPUTPORT	0.6188414212601262
OUTPUTPORT	0.5909340090255149
SRC_MAC	-0.3779526827561006
DST_MAC	0.5892544767914198
ETHERNET_TYPE	-0.5886118381226132
IN_VLAN	Nulová hodnota
OUT_VLAN	Nulova hodnota
SRC_IP	0.08049091599517895
DST_IP	0.07355890187601573
IP_PROTOCOL	-0.07407919159621763
IP_TOS	Nulová hodnota
IP_TTL	-0.05768954593765455
SRC_PORT_OR_ICMP_TYPE	-0.0676195969509869
DST_PORT_ICMP_CODE	-0.042113943046892865

TCP_FLAGS	-0.06061824921449012
PACKET_SIZE	-0.0733419036600926
IP_SIZE	-0.06770010213058673
SAMPLING_RATE	Nulová hodnota

Tabuľka č.4. Zhrnutie modelu

Zhrnutie	**Stav**	**Predpoveď**
Count of training data	4970	4970
mean	1.0643863179074446	1.0643863179074446
stddev	0.24568714463363647	0.24568714463363647
Min	1	1
Max	2	2

Algoritmus logistickej regresie vyhodnocuje vstupné dáta a klasifikuje ich tak, že identifikuje jeden z dvoch stavov: buď vzorový dataset vyhovuje dátovému toku a je označený ako povolená sieťová komunikácia, alebo nevyhovuje a je označený ako neželaná a potenciálne nebezpečná sieťová komunikácia a mala by byť blokovaná. Naučený model a súhrn výsledkov sú uvedené v tabuľke č. 4. Cieľom bolo vyhodnotiť vzorku sFlow a predpovedať, či je obsiahnutý sieťový prenos bezpečný alebo nie.

Zhrnutie natrénovaného modelu z tabuľky č.4 bolo vygenerované na základe tréningových dát z programu Spark. Počet jedinečných vzoriek použitých na natrénovanie modelu bol 4970. Tendencia údajov v priemere bola vyhodnotená v časti mean a predstavuje hodnotou pre rozdelenie pravdepodobnosti. Šírenie údajov - odchýlka, štandardná odchýlka (standard deviation) bola vyčíslena v riadku stddev. Model bol trénovaný na dve hraničné hodnoty klasifikácie, kde hodnota Min rovná 1, predstavuje korektný dátový tok v sieti a Max hodnota 2 je vyhodnotenie vzorky, ktorá predstavuje dátový tok, ktorý by mal byť blokovaný.

Testovanie bolo realizovane pomocou knižnice strojového učenia, konkrétne nástroja na hodnotenie binárnej klasifikácie (Binary Classification Evaluator). Testovaný dataset bol overený a výsledný koeficient bol 1.0, čo predstavuje 100% úspešnosť. Kvalita klasifikácie modelu bola overovaná ďalšou validáciou na výrobnej linke, pri spustení výrobného procesu. Model, ktorý bol naučený bol ďalej testovaný v praxi.

Výsledky, ktoré neurónová sieť dosiahla, je možné naďalej rozvíjať a prispôsobovať. Pre kontinuálnu stratégiu zabezpečenia je nutné sledovať bezpečnostné problémy a pre zachovanie kvality je nutné vytvárať ďalšie scenáre a testovacie dátové sety a tak udržať kvalitu identifikácie útokov. Tento proces je nutné opakovať a navrhované riešenie je potrebné udržiavať v stave, ktorý odzrkadlí trendy na novovzniknuté situácie a útoky. Klasifikácia na úrovni 100% predstavuje ohraničené vstupy a odzrkadľuje komunikáciu, ktorá bola generovaná. Výsledky z reálneho testu sú opísane v ďalšej kapitole.

5 Overenie a zhodnotenie navrhovaných riešení

Celkové dopady závisia od kvality integrácie a od použitých komponentov výrobnej linky a jej infraštruktúry. Na druhej strane treba dodať, že pri niektorých zariadeniach náhodný útok bez znalosti infraštruktúry by mohol negatívne ovplyvniť niektoré operácie, ale pravdepodobne by nemal dostatočnú účinnosť na celkové zlyhanie výroby, skôr by sa jednalo o degradáciu časti výrobného procesu. Toto bolo overené a analyzované syntetickým testom scenárov útokov, ktoré boli realizovane na robota a jeho riadiaci PLC modul.

5.1 Overenie a zhodnotenie statického zabezpečenia

Pri aplikácii statického zabezpečenia bolo možné pozorovať výkonnostné limity minipočítača. Pri testovaní aplikovaného statického zabezpečenia pred DDoS a reflektovanými DDoS útokmi, nastal prípad, kedy prišlo k samotnému zrúteniu minipočítača, ktorý bol aplikovaný ako transparent bridge firewall. Riešenie zabezpečenia vychádzalo z predpokladu, že pri blokovaní DDoS útokov z iptables, je veľmi dôležité aby pravidlá iptables boli dostatočne rýchlo spracované a aby ich výkon stačil na zabráneniu takémuto typu útoku. DDoS útoky založené na protokole TCP obvykle zahlcujú infraštruktúru veľkým množstvom paketov, a hrozí, že zariadenie, ktoré pakety filtruje nezvládne taký vysoký tok paketov a prestane pracovať. Systém, ktorý má plniť monitorovaciu funkciu musí byť dostatočne dimenzovaný a vynára sa otázka, či je minipočítač vhodný na to, aby zvládol monitorovaciu funkciu. Väčšina zdrojov uvádza ošetrenie DDoS útokov práve na INPUT strane iptables [18].

Problém je, že INPUT pravidlá sa spracovávajú až za pravidlami PREROUTING a FORWARD a pravidlá pre INPUT chain sa aplikujú až po prechode predchádzajúcimi dvoma skupinami pravidiel, kde každá skupina odčerpáva systémové prostriedky a alokovanú pamäť zariadenia. Toto môže mať za následok vyťaženie systému. Prvý chain, ktorý spracováva pakety v iptables je PREROUTING chain; avšak tu nie je možné použiť pre konfiguráciu štandardnú filter tabuľku. Na druhej strane existuje možnosť použiť tzv. mangle tabuľku, ktorá je obvykle používaná pre fragmentáciu paketov a ktorá vyžaduje len jeden krát alokovanú pamäť pre spracovanie prichádzajúcich paketov. Pre mangle tabuľku je možné aplikovať takmer všetky pravidlá ako pre INPUT tabuľku. Toto statické riešenie pri transparentom firewalle bridge používalo pravidlá pre FORWARD. Uvedený spôsob je možné ešte vylepšiť práve zmenou na PREROUTING pravidlá s použitím mangle tabuľky a ušetriť tak procesorový čas a aj pamäť a minipočítač tak môže zvládnuť väčšiu sieťovú premávku. Teoreticky sa jedná až o 50% ušetrenia výkonu na zabezpečenie, nakoľko nie je potrebné vykonávať alokáciu pamäte pre INPUT a FORWARD fronty a presúvanie príslušných paketov medzi nimi. Obe pravidlá pre IoT zariadenie fungovali, a vzhľadom na výkon IoT zariadenia a jeho zraniteľnosť a kapacitu, ktorou dokáže odrážať pakety, je riešenie dostatočné. V prípade intenzívneho útoku z masívneho botnetu, došlo k zlyhaniu už na predchádzajúcom zariadení napríklad routery, ktorý zabezpečuje konektivitu z inej siete alebo internetu.

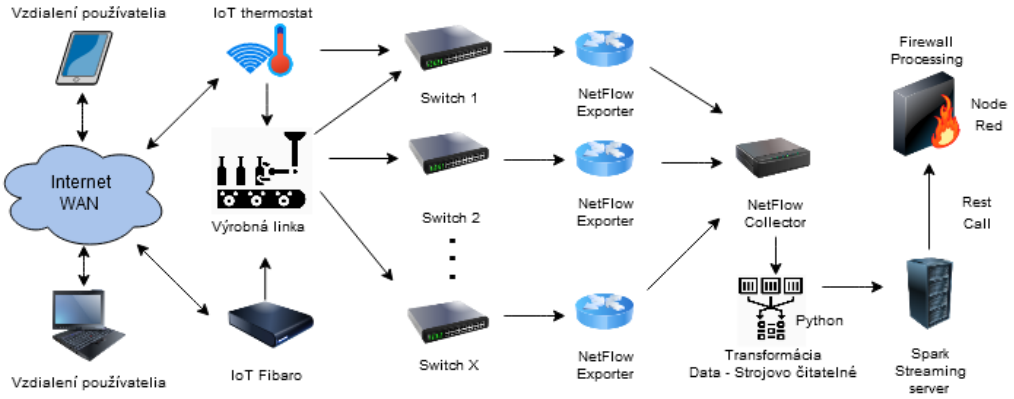
Pri DRDoS útokoch, hoci bol aplikovaný základný monitoring siete a bol po hľadaní zdroja identifikovaný nadmerný tok dát z IoT zariadenia, stále nebolo možné identifikovať zdroj, ktorý

tento nadmerný tok generoval. Uvedené problémy boli vyriešené nakoniec výmenou switcha a zapnutím NetFlow bol rozšírený sieťový monitoring výrobnej linky. Ako ukázali realizované testy, hlavnou prioritou je zabezpečiť IoT zariadenie, ktoré má poskytovať dodatočné dáta pre riadenie výrobného procesu a je nutné povoliť komunikáciu do internetu alebo do inej siete, ktorá nie je izolovaná v rámci výrobnej linky.

Riešenie môže byť úplne jednoduché v prípade, že je možné konfigurovať sieťovú infraštruktúru. Ak je ale nemožné sieťovú infraštruktúru konfigurovať, respektíve je obava meniť nastavenie výrobnej linky z dôvodu možnosti zlyhania plynulého procesu výroby, ako bolo možné vidieť v tomto prípade, je možné komunikáciu IoT zariadení rozšíriť o modul, ktorý zabezpečí sieťovú komunikáciu a prípadne aj poskytne dáta pomocou Flow protokolu pre monitorovanie sieťových aktivít IoT zariadenia, kde je možné plne identifikovať všetky prichádzajúce a odchádzajúce pakety a merať a zaznamenávať sieťovú aktivitu zariadenia a komunikácie. Tento prístup môže priniesť chýbajúcu transparentnosť a možnosť generovania dodatočných dát o priebehu komunikácie známeho alebo neznámeho zariadenia, ktoré je integrované do výrobného procesu a sprístupniť tak informácie, ktoré nie sú zariadením poskytované automaticky. Uvedený princíp bol použitý aj pri návrhu modelu pre dynamické zabezpečenie.

5.2 Overenie a zhodnotenie dynamického zabezpečenia

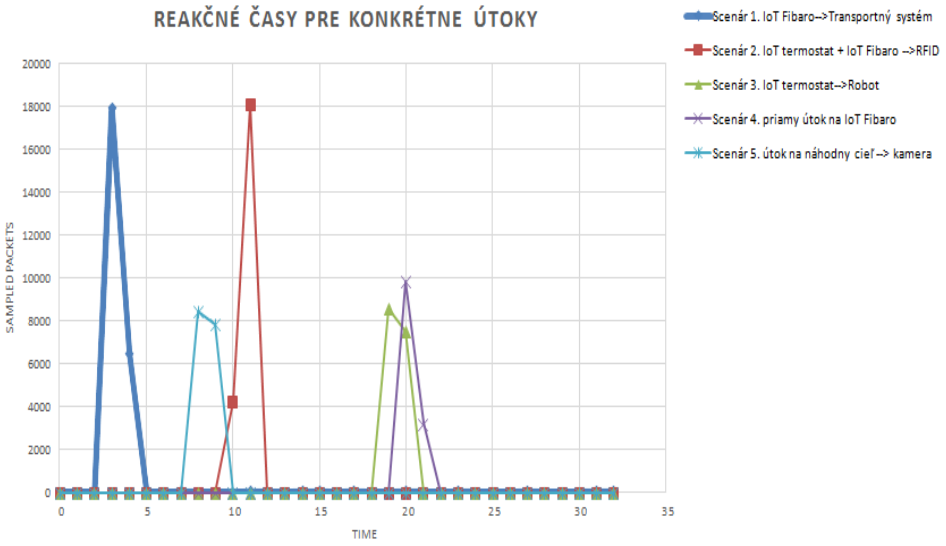
Navrhované dynamické riešenie zabezpečenia zamerané na sledovanie komunikácie je možné použiť aj pri väčších sieťových infraštruktúrach. Testovanie návrhu prebehlo s dvomi switchmi, ktoré boli zapojené v režime monitorovania a nadstavené pre potreby komunikácie výrobnej linky. Špecifikum bolo povolenie multicast sieťovej komunikácie a zároveň boli obidva switche schopné zachytávať a generovať vzorky (sample) sieťovej komunikácie výrobnej linky. Sledovaný tok vzoriek bol zo switchov odosielaný na samostatnej fyzickej aj adresnej sieti do sFlow kolektor, ktorý bol spustený na serveri s operačným systémom Linux. sFlow kolektor spracovával streamované dáta a slúžil ako vstupná brána, ktorá posielala spracované dáta v štruktúrovanom formáte CSV na spracovanie do Apache Spark. Apache Spark vstupné dáta normalizoval, pričom bola aplikovaná analýza pomocou MLlib. Výsledky sieťového toku dát boli vyhodnotené na základe klasifikácie a v prípade identifikácie nebezpečnej komunikácie bolo vygenerované REST volanie pre Node Red, ktorý aplikoval zabezpečovacie pravidlá na sieťové prvky. Zapojenie overovanej výrobnej linky je znázornené na obrázku č. 3.



Obr. 3. Návrh sieťovej infraštruktúry s dynamickým zabezpečením

Proces vyhodnotenia sieťovej komunikácie a jej predikcia musia zabezpečiť konečné blokovanie nebezpečného sieťového dátového toku v takom čase, aby ostatné zariadenia zostali byť schopné prevádzky. Kritický čas od začiatku útoku je podľa uskutočnených experimentálnych scenárov útokov v čase 12 sekúnd, ako je vidieť aj na grafoch v štvrtej kapitole.

Jednotlivé časti dynamického riešenia zabezpečenia, menovite vzorkovanie toku dát, zber dát, ich transformácia, analýza pomocou neurónovej siete a samotné zabezpečenie, sa preto musia stihnúť vykonať do času, kým útok neovplyvní zariadenia na výrobnej linke. To znamená, že celý proces zabezpečenia sa musí uskutočniť skôr ako sa niektoré zariadenie dostanú do stavu, keď ich komunikačné schopnosti zlyhajú a nie sú schopné naďalej riadne fungovať a treba ich reštartovať. Samotný sFlow protokol potrebuje určitý čas na vytvorenie a doručenie informácií, takže vzniká oneskorenie. Veľkosť vzorky alebo frekvencia vzorkovania je voliteľná a môže sa jednať o milisekundy alebo aj stovky sekúnd. DDoS a DRDoS útoky generujú veľký dátový tok, takže v tomto prípade sa javí sFlow ako vhodnejší zdroj dát než NetFlow, ktorý sleduje zmenu pri každom pakete. Transformácia sFlow na čitateľné dáta je urobená v časti sFlow kolektora a spracovanie je rýchle. Doručovanie sFlow informácií je zabezpečené UDP protokolom a veľkosť informácií o vzorkách je oproti reálnemu sieťovému vyťaženiu minimálna. Veľkosť datagramu je v rozmedzí 200 až 1468 bytes a vzorky, ktoré popisujú sieťovú premávku, boli orientované na sumár dát pre jednotlivé protokoly, porty a zdrojové a cieľové adresy, kde frekvencia vzorkovania bola nastavená na jednu sekundu.



Graf č. 1. Reakčné časy blokovania konkrétnych útokov

Ako uvádza graf č.1 všetky scenáre útokov preukázali takmer rovnaký čas reakcie na nebezpečnú sieťovú komunikáciu a blokácia prebehla do 2 sekúnd od zaznamenania útoku. Testovanie bolo realizované so zámerom demonštrovať vplyv dĺžky časového okna a jeho vplyv na rýchlosť reakcie. Výber vhodnej vzorkovacej rýchlosti paketov je dôležitou súčasťou konfigurácie sFlow na prepínači. Rýchlosť zasielania (pooling interval) vyhodnotených vzoriek je možné konfigurovať v rozsahu 0 až 429496729. Tento parameter je definovaný sFLow štandardom tak, že 0 predstavuje vypnutý systém sFlow a minimálna hodnota zasielania je jedna sekunda, ktorá bola použitá pri testovaní. Najrýchlejšia možná reakcia systému je teda jedna

sekunda plus čas, ktorý je potrebný na doručenie informácie o vzorkách, čas potrebný na vyhodnotenie a čas potrebný na aplikovanie nového pravidla.

5.3 Celkové zhrnutie a porovnanie navrhovaných riešení

Scenáre útokov preukázali zraniteľnosti a dopady na výrobný proces a zariadenia. Vzhľadom na fakt, že prevádzka výrobnej linky je orientovaná na produkciu a zásahy do sieťovej infraštruktúry predstavujú riziko nefunkčnosti výrobného procesu, boli tieto fakty zapracované do návrhov riešenia. Na základe overenia zraniteľností a dopadov na výrobný proces bola vykonaná analýzy a boli navrhnuté riešenia opatrení.

Prvý návrh statického zabezpečenia predstavuje riešenie transparentného firewall bridgu riešenie, ktoré povyšuje základné štandardné zabezpečenie a je možné ho realizovať aj na sieťovej infraštruktúre tak, aby bolo možné bez väčšieho rizika integrovať do výrobného procesu IoT zariadenia, ktoré predstavujú potenciálne riziko z hľadiska bezpečnosti a aplikácie útokov. V časti návrhu je vylepšená časť filtrovania a zabezpečenia sieťového toku, kde minipočítač dokáže reagovať a zabezpečiť základné požadované bezpečnostné pravidlá tak, aby boli ochránené IoT zariadenia a ich funkčnosť. Výzvu predstavoval výkon minipočítača a jeho systémové prostriedky, ktoré boli vyriešené spôsobom, aby boli minimalizované operácie alokácie pamäte a presun sieťovej premávky do ďalších vrstiev fierewallu Tok dát ostal na prvej vrstve, ktorá rozhoduje o pre-routingu a boli vytvorené pravidlá, ktoré využívajú používateľom definované tabuľky na filtrovanie komunikácie. Tým pádom štandardné pravidlá pre firewall, ktoré sú označované ako INPUT alebo OUTPUT, nie je nutné využívať.

Takto odľahčený systém dokáže vykonávať požadované akcie firewallu s menšími systémovými nárokmi a je aj skrátený čas spracovania pravidiel, ktoré sú uplatňované na sieťovú komunikáciu. Uvedené riešenie má výhodu ľahkej integrácie do siete a použiteľnosť je univerzálna aj pre potreby zabezpečenia iných zariadení. Nie je nutná konfigurácia a ani pridelenie IP adresy. Transparentný firewall bridge je možné zapojiť do siete IPv4 alebo IPv6 a zadefinované pravidlá budú uplatňované ihneď po štarte systému. Nevýhodou takéhoto riešenie je statická konfigurácia pravidiel, kde je nutné neustále sledovať zmeny a na nové typy útokov, je nutné definovať vždy nové pravidlá a systém je nutné neustále aktualizovať.

Kvôli väčšej flexibilnosti boli vykonané aj ďalšie analýzy zabezpečenia a bol vytvorený aj návrh dynamického zabezpečenia, kde je využitá vlastnosť počítačového učenia neurónovej siete a to konkrétne klasifikácia, ktorá bola použitá na identifikáciu a rozhodovanie o bezpečnej alebo nebezpečnej sieťovej komunikácie. Tento prototyp riešenia bol vyvíjaný so zámerom zabezpečenia výrobnej linky s integrovanými IoT zariadeniami a jej celkovej infraštruktúry. Samotný princíp fungovania je opäť možné uplatniť a aplikovať aj všeobecne. V tomto prípade bol otestovaný aj zásah do konfigurácie infraštruktúry výrobnej linky, ale nie je to nevyhnutnou podmienkou. Je možné urobiť aj kombináciu transparentného firewall bridgu a dynamického riešenia, kde provisioning nových firewall pravidiel bude aplikovaný na transparentný firewall bridge.

Z hľadiska komplexnosti a flexibility riešenia tu bola zámerne otestovaná aj širokospektrálna ochrana celej sieťovej infraštruktúry, kde boli generované pravidlá, ktoré aktívne zabezpečujú

komunikáciu sieťovej infraštruktúry. Na tento typ riešenia boli zvolené neštandardne vzorky sieťovej komunikácie, ktoré sú obvykle používané len na monitorovanie sieťovej premávky. Na základe týchto údajov bolo však preukázané, že je ich možné využiť aj na špecifické potreby ochrany výrobného procesu, kde dáta, ktoré sú vzorkované ako sample a neobsahujú plnú komunikáciu, sú dostatočné na detegovanie nežiaducej sieťovej komunikácie. Klasifikácia pomocou neurónovej siete, ktorá bola natrénovaná na základe reálne sieťovej prevádzky, bola schopná vykonať klasifikáciu známych útokov až so 100% úspešnosťou, čo je možné pripisovať práve faktu, že sa jedná o doteraz známe útoky a uzavretý systém štandardizovanej komunikácie výrobnej linky spolu s integrovanými IoT zariadeniami.

Výhodou navrhnutého riešenia je možnosť ochrany celej infraštruktúry a integrovať klasifikáciu aj do systémov monitorovania tak, že o útokoch je dostupná a viditeľná informácia takmer okamžite. Riešenie je navyše pripravené aj na dodatočné zmeny. Je možná opätovná príprava trénovacích setov, ktoré udržia klasifikáciu sieťovej prevádzky na vysokej úrovni. Riešenie predstavuje aj istú nevýhodu, nakoľko tak, ako v prvom riešení, ho nie je možné pokladať za ukončené vzhľadom na neustále sa vyvíjajúce bezpečnostné problémy a jedná sa pravdepodobne o nekončiaci proces aktualizácie. Opäť je ale možné uplatniť navrhnutý koncept na viaceré varianty a typy infraštruktúr, ktoré používajú štandardné sieťové protokoly a umožňujú vytvoriť návrh komplexnej ochrany, kde je možné uplatniť navrhované riešenie vo všeobecnosti aj mimo priemyselné prostredie.

Obe navrhnuté riešenia vychádzajú zo zadaných téz a reprezentujú aktuálnu situáciu a trendy z pohľadu riešenia bezpečnosti. Základné prvky zabezpečenia boli preskúmané a identifikované ako slabé stránky. Cieľ práce sa podarilo naplniť a predstavuje dva všeobecne uplatniteľné spôsoby riešení na zvýšenie bezpečnosti akejkoľvek prevádzky. Útoky, ktoré predstavujú riziko DoS a DDoS, predstavujú väčší problém, ktorý je z pohľadu bezpečnosti ťažko riešiteľný ako samostatne riešená úloha alebo úloha riešená len na jednom uzle sieťovej architektúry.

V práci bolo preukázané, že tieto typy útokov sú často šírené pomocou IoT zariadení. Preto bolo potrebné tento stav eliminovať predloženými návrhmi riešenia, ktoré nie len pokrývajú samotnú problematiku zabezpečenia zariadení, ale potenciálne ponúkajú aj ďalšie možnosti prípravy a poskytovania doplnkových informácií pre ďalšie úrovne monitoringu a riadenia.

6 Prínosy dizertačnej práce

Hlavným cieľom dizertačnej práce bolo analyzovať, navrhnúť, implementovať, otestovať a zhodnotiť možné bezpečnostné opatrenia a riešenia proti zvoleným kybernetickým DDoS a reflektovaným DRDoS typom útokov s prihliadnutím na kompromis medzi pripojením a bezpečnosťou, ktorý je dôležitou výzvou pri integrácií priemyselných IoT zariadení do výroby. Hlavný cieľ bol naplnený splnením stanovených čiastkových cieľov, ktoré zahŕňali štúdium, analýzu a spracovanie teoretických východísk a poznatkov zo skúmanej problematiky z domácej a zahraničnej literatúry a vedeckých štúdii, analýzou a testovaním možných spôsobov DDoS a reflektovaných DRDoS útokov na výrobnú infraštruktúru s integrovanými priemyselnými IoT zariadeniami, čo napomohlo k návrhu nových bezpečnostných riešení, ktoré majú široké uplatnenie nielen v koncepte Industry 4.0, ale aj v sieťových infraštruktúrach v iných odvetviach. Ďalej sú uvedené najdôležitejšie prínosy dizertačnej práce pre oblasti: teória, prax a veda.

Prínosy dizertačnej práce pre teóriu:

- Analýza a spracovanie teoretických východísk a poznatkov súčasného stavu zo skúmanej problematiky z domácej a zahraničnej literatúry a vedeckých štúdii pre oblasti zabezpečenia sieťových priemyselných infraštruktúr a IoT zariadení.
- Podrobný opis možných kybernetických hrozieb ako sú DDoS a reflektované DRDoS útoky na IoT zariadenia.
- Zmapovanie zraniteľnosti konkrétnych integrovaných IoT zariadení a ďalších výrobných zariadení.

Prínosy dizertačnej práce pre prax:

- Zhrnutie teoretických poznatkov a súčasného stavu o hrozbách a zabezpečení IoT zariadení integrovaných do výrobného procesu.
- Identifikácia problémov zabezpečenia výrobných infraštruktúr s integrovanými IoT zariadeniami.
- Definovanie dopadov vo výrobnom procese s integrovanými IoT zariadeniami spôsobené kybernetickými DDoS a reflektovanými DRDoS útokmi.
- Navrhnuté nové bezpečnostné riešenia výrobnej infraštruktúry s integrovanými IoT zariadeniami z pohľadu už existujúceho chodu výrobného procesu a to tak, aby ich nasadenie neohrozilo funkčnosť výroby.

Prínosy dizertačnej práce pre vedu:

- Riešením dizertačnej práce so zameraním na zabezpečenie IoT zariadení sa reálnymi experimentami útokov potvrdili bezpečnostné hrozby výrobných infraštruktúr s integrovanými IoT zariadeniami. Tieto hrozby boli v literatúre iba predpokladané, ale nikdy neboli reálne potvrdené.

- Výsledky dizertačnej práce preukázali opodstatnenosť ďalšieho skúmania bezpečnosti IoT zariadení vo výrobnom procese.
- Výsledky dizertačnej práce boli publikované v karentovaných časopisoch Q1 a Q2 a prezentované na svetovom kongrese.
- Získané výsledky je možne využiť pre tvorbu vedeckých štúdii a príspevkov so zameraním na výskum problematiky dizertačnej práci.

Záver

Dizertačná práca bola svojím obsahom zameraná na riešenie problematiky zabezpečenia výrobných infraštruktúr spolu s integrovanými IoT zariadeniami. V práci bolo experimentálnymi scenármi DDoS a reflektovanými DRDoS útokmi zistené, že IoT zariadenia predstavujú z hľadiska bezpečnosti potencionálnu hrozbu pre výrobný proces, čo potvrdili aj prezentované dopady DDoS útokov na reálny výrobný proces. Na základe zistených skutočnosti boli v práci navrhnuté dve možné varianty bezpečnostných riešení. Prvé z nich bolo statické bezpečnostné riešenie založené na konfigurácii transparent bridge firewallu. Druhé bolo dynamické riešenie, v ktorom bola naučená neurónová sieť na rozpoznávanie štandardnej a neštandardnej komunikácie. V práci bola použitá vedecká a odborná literatúra, z ktorej boli vybrané časti zapracované do analytických častí.

Hlavným cieľom dizertačnej práce bolo analyzovať, navrhnúť, implementovať, otestovať a zhodnotiť možné bezpečnostné opatrenia a riešenia proti zvoleným kybernetickým DDoS a reflektovaným DRDoS typom útokov s prihliadnutím na kompromis medzi pripojením a bezpečnosťou, ktorý je dôležitou výzvou pri integrácií priemyselných IoT zariadení do výroby.

Splnenie hlavného cieľa dizertačnej práce bolo podmienené naplnením stanovených čiastkových cieľov, ktoré sú sformulované nasledovným spôsobom:

- Analýza a spracovanie teoretických východísk a poznatkov zo skúmanej problematiky z domácej a zahraničnej literatúry a vedeckých štúdii.
- Stanovenie cieľov a výskumných okruhov.
- Analýza a testovanie možných spôsobov útokov na priemyselné IoT zariadenia.
- Návrh a implementácia bezpečnostných riešení.
- Overenie a zhodnotenie navrhnutých riešení.
- Posúdenie prínosov dizertačnej práce pre špecifikovanú oblasť.

Na základe realizovaných všetkých čiastkových úloh a cieľov je možne skonštatovať, že hlavný stanovený cieľ dizertačnej práce bol naplnený.

Zoznam publikačnej činnosti

ADC Vedecké práce v zahraničných karentovaných časopisoch

ADC01 **HORÁK, Tibor** - STŘELEC, Peter - HURAJ, Ladislav - TANUŠKA, Pavol - VÁCLAVOVÁ, Andrea - KEBÍSEK, Michal. The Vulnerability of the Production Line Using Industrial IoT Systems under DDoS Attack. In *Electronics*. Vol. 10, iss. 4 (2021), s. 1-32. ISSN 2079-9292 (2019: **2.412 - IF , Q2 - JCR Best Q** , 0,303 - SJR , Q2 - SJR Best Q). V databáze: DOI: https://doi.org/10.3390/electronics10040381; SCOPUS: 2-s2.0-85100446535 ; WOS: 000623355200001 ; CC: 000623355200001.
[Vnútrofakultná kategória: A].

ADC02 HURAJ, Ladislav - ŠIMON, Marek - **HORÁK, Tibor**. Resistance of IoT Sensors against DDoS Attack in Smart Home Environment. In *Sensors*. Vol. 20, iss. 18 (2020), s. 1-23. ISSN 1424-8220 (2019: **3.275 - IF , Q1 - JCR Best Q** , 0,653 - SJR , Q1 - SJR Best Q). V databáze: DOI: https://doi.org/10.3390/s20185298; SCOPUS: 2-s2.0-85090907330 ; WOS: 000581974200001 ; CC: 000581974200001. [Vnútrofakultná kategória: A].

ADC03 HURAJ, Ladislav - **HORÁK, Tibor** - STŘELEC, Peter - TANUŠKA, Pavol. Mitigation against DDoS Attacks on an IoT-Based Production Line Using Machine Learning. In *Applied Sciences*. Vol. 11, iss. 4 (2021), s. 1-18. ISSN 2076-3417 (2019: **2.474 - IF , Q2 - JCR Best Q** , 0,418 - SJR , Q1 - SJR Best Q). V databáze: DOI: https://doi.org/10.3390/app11041847; SCOPUS: 2-s2.0-85101984331 ; WOS: 000632078900001 ; CC: 000632078900001. [Vnútrofakultná kategória: A].

AFC Publikované príspevky na zahraničných vedeckých konferenciách

AFC01 **HORÁK, Tibor** - ČERVEŇANSKÁ, Zuzana - HURAJ, Ladislav - VAŽAN, Pavel - JÁNOŠÍK, Ján - TANUŠKA, Pavol. The vulnerability of securing IoT production lines and their network components in the Industry 4.0 concept. *In IFAC-PapersOnLine. Vol. 53, iss. 2: IFAC World Congress, Berlín, Germany*, 12-17 July 2020 (2020), s. 11237-11242. ISSN 2405-8963 (**2019: 0,332 - SJR , Q2 - SJR Best Q**). V databáze: DOI: https://doi.org/10.1016/j.ifacol.2020.12.354 ; SCOPUS: 2-s2.0-85105104163.
[Vnútrofakultná kategória: A].

AFC02 **HORÁK, Tibor** - HURAJ, Ladislav. Smart Thermostat as a Part of IoT Attack. In Cybernetics and Automation Control Theory Methods in Intelligent Algorithms : *Proceedings of 8th Computer Science On-line Conference 2019* , 24. - 27. Apríl 2019, Zlín, Czech Republic, Vol. 3. Part of the Advances in Intelligent Systems and Computing book series, volume 986. 1. vyd. Cham : Springer Nature Switzerland AG, 2019, S. 156-163. ISSN 2194-5357. ISBN 978-3-030-19812-1. V databáze: DOI: https://doi.org/10.1007/978-3-030-19813-8_17; SCOPUS: 2-s2.0-85065927412 ; WOS: 000485163400017.
[Vnútrofakultná kategória: B].

AFC03 **HORÁK, Tibor** - ŠIMON, Marek - HURAJ, Ladislav - BUDJAČ, Roman. Vulnerability of smart IoT-based automation and control devices to cyber attacks. In Applied Informatics and Cybernetics in Intelligent Systems. CSOC 2020 : *9th Computer Science On-line Conference 2020* , April 23,2020 - April 26,2020. 1. vyd. Cham : Springer, 2020, S. 287-294. ISSN 2194-5357 ISBN 978-3-030-51973-5 V databáze: DOI: https://doi.org/10.1007/978-3-030-51974-2_27; SCOPUS: 2-s2.0-85089620744.
[Vnútrofakultná kategória: B].

AFC04 HURAJ, Ladislav - ŠIMON, Marek - **HORÁK, Tibor**. IoT measuring of UDP-based distributed reflective DoS attack. In SISY 2018 : *IEEE 16th International Symposium on Intelligent Systems and Informatics*, 13. - 15. 9. 2018, Subotica, Serbia. 1. vyd : IEEE, 2018, S. 209-214. ISBN 978-1-5386-6841-2. V databáze: DOI: 10.1109/SISY.2018.8524703 SCOPUS: 2-s2.0-85057977981 ; WOS: 000465218500036. [Vnútrofakultná kategória: B].

AFC05 ŠIMON, Marek - HURAJ, L. - **HORÁK, Tibor.** DDoS reflection attack based on loT: A case study. *In Cybernetics and Algorithms in Intelligent Systems* : Vol. 3. s.44-52. ISSN 2194-5357. V databáze: SCOPUS: 2-s2.0-85048047285 ; DOI: https://doi.org/10.1007/978-3-319-91192-2_5
[Vnútrofakultná kategória: B].

AFD Publikované príspevky na domácich vedeckých konferenciách.

AFD01 **HORÁK, Tibor** - JÁNOŠÍK, Ján - HURAJ, Ladislav. Employment of industrial IoT devices with data in Industry 4.0. In Applied Natural Sciences 2019. ANS 2019 : *7th International Scientific Conference,* 25. - 27. 9. 2019, Tále, SR. 1. vyd. Trnava : University of ss. Cyril and Methodius in Trnava, 2019, S. 76-81. ISBN 978-80-572-0011-6. DOI: https://ans2019.ucm.sk/files/inline-files/ANS2019_Proceedings.pdf [Vnútrofakultná kategória: C].

AFH Abstrakty príspevkov z domácich vedeckých konferencií

AFH01 **HORÁK, Tibor** - JÁNOŠÍK, Ján - HURAJ, Ladislav. The position of IoT devices in Industry 4.0 concept and their data work. In Applied Natural Sciences 2019. ANS 2019 : *7th International Scientific Conference,* 25. - 27. 9. 2019, Tále, SR. 1. vyd. Trnava : University of ss. Cyril and Methodius in Trnava, 2019, S. 93. ISBN 978-80-572-0011-6. DOI: https://ans2019.ucm.sk/files/inline-files/ANS2019_Book-of-Abstracts.pdf [Vnútrofakultná kategória: C].

Úspešne ukončené projekty:

Názov: Zraniteľnosť bezpečnostných IoT systémov kybernetickými útokmi v koncepte Industry 4.0. Mladý výskumník 2019, Zodpovedný riešiteľ: T. Horák

Názov: Aplikácia konceptu Industry 4.0 v rámci modernizácie predmetu Technické prostriedky automatizovaného riadenia. KEGA 040STU-4/2016, Garant: B. Juhásová, Spoluriešiteľ: T. Horák

Štatistika: kategória publikačnej činnosti k 31.5.2021 :

ADC Vedecké práce v zahraničných karentovaných časopisoch.....3

AFC Publikované príspevky na zahraničných vedeckých konferenciách.....5

AFD Publikované príspevky na domácich vedeckých konferenciách.....1

AFH Abstrakty príspevkov z domácich vedeckých konferencií.....1

Súčet.....10

Štatistika: kategórie ohlasov k 31.5.2021 :

1 - Citácie v zahraničných publikáciách, registrované v citačných indexoch Web of Science a databáze SCOPUS.....17

Zoznam bibliografických odkazov

1. Derhab, A.; Guerroumi, M.; Gumaei, A.; Maglaras, L.; Ferrag, M.A.; Mukherjee, M.; Khan, F.A. Blockchain and Random Subspace Learning-Based IDS for SDN-Enabled Industrial IoT Security. *Sensors* **2019**, *19*, 3119. doi: 10.3390/s19143119
2. Bucci, G.; Ciancetta, F.; Fiorucci, E.; Fioravanti, A.; Prudenzi, A.; Mari, S. An IoT condition monitoring system for resilience based on spectral analysis of vibration. *2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT.* Roma, Italy, July 2020, pp. 38-43. doi:10.1109/metroind4.0iot48571.2020.9138177
3. Sari, A.; Lekidis, A.; Butun, I. Industrial Networks and IIoT: Now and Future Trends. In Industrial IoT. Springer, Cham, 2020. 3-55. doi: 10.1007/978-3-030-42500-5_1
4. Prinsloo, J.; Sinha, S.; von Solms, B. A Review of Industry 4.0 Manufacturing Process Security Risks. Appl. Sci. 2019, 9, 5105. doi: 10.3390/app9235105
5. Frey, M.; Gündoğan, C.; Kietzmann, P.; Lenders, M.; Petersen, H.; Schmidt, T. C.; Wählisch, M. Security for the Industrial IoT: The case for information-centric networking. In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), IEEE, Limerick, Ireland, April 2019, pp. 424-429. doi: 10.1109/WF-IoT.2019.8767183
6. Apiecionek, L.; Großmann, M.; Krieger, U. R. Harmonizing IoT-Architectures with Advanced Security Features-A Survey and Case Study. J. UCS, 2019, 25(6), 571-590. doi: 10.3217/jucs-025-06-0571
7. A. Sajid, H. Abbas and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges," in IEEE Access, vol. 4, pp. 1375-1384, 2016, doi: 10.1109/ACCESS.2016.2549047.
8. Tempest: Production line description. User manual. Tempest. 2014.
9. Siemens: SIMATIC S7-1200 Easy Book Manual. 2015 [online]. [cit.2020-11-28]. Dostupné na internete: <https://euroec.by/assets/files/siemens/s71200_easy_book_en-US_en-US.pdf />
10. Horák T.; Šimon M.; Huraj L.; Budjač R. Vulnerability of Smart IoT-Based Automation and Control Devices to Cyber Attacks. In Silhavy R. (eds) Applied Informatics and Cybernetics in Intelligent Systems. CSOC 2020. Advances in Intelligent Systems and Computing, vol 1226. Springer, Cham, April 2020; pp: 287-294. doi: 10.1007/978-3-030-51974-2_27
11. A. Sajid, H. Abbas and K. Saleem, "Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges," in IEEE Access, vol. 4, pp. 1375-1384, 2016, doi: 10.1109/ACCESS.2016.2549047.
12. Boyes, H., Hallaq, B., Cunningham, J., & Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. Computers in Industry, 101, 1–12. doi:10.1016/j.compind.2018.04.015
13. Younan, M., Houssein, E. H., Elhoseny, M., & Ali, A. A. (2019). Challenges and Recommended Technologies for the Industrial Internet of Things: A Comprehensive Review. Measurement, 107198. doi:10.1016/j.measurement.2019.107198
14. Ivanović, I,. Slavko G. "Recommendations for network traffic analysis using the NetFlow protocol." (2016).
15. Meng, X., Bradley, J., Yavuz, B., Sparks, E., Venkataraman, S., Liu, D., Freeman, J., Tsai, D.B., Amde, M., Owen, S. and Xin, D., . Mllib: Machine learning in apache spark. The Journal of Machine Learning Research, 17(1),2016. pp.1235-1241.
16. He, H.; Li, S.; Hu, L.; Duarte, N.; Manta, O.; Yue, X.-G. Risk Factor Identification of Sustainable Guarantee Network Based on Logistic Regression Algorithm. Sustainability 2019, 11, 3525.
17. Miguel, M.L.F.; Jamhour, E.; Pellenz, M.E.; Penna, M.C. SDN Architecture for 6LoWPAN Wireless Sensor Networks. Sensors 2018, 18, 3738.
18. Apiecionek, Łukasz, Jacek M. Czerniak, and Wojciech T. Dobrosielski. "Quality of services method as a DDoS protection tool." *Intelligent Systems' 2014*. Springer, Cham, 2015. 225-234.