

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

DIPLOMOVÁ PRÁCE

Brno, 2022

Dáša Sedláková



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

ÚTOK A OBRANA V PROSTŘEDÍ ENERGETICKÝCH PRŮMYSLOVÝCH POČÍTAČOVÝCH SÍTÍ

CYBER SECURITY FOR POWER ENGINEERING

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. Dáša Sedláková

VEDOUCÍ PRÁCE

SUPERVISOR

doc. Ing. Petr Mlýnek, Ph.D.

BRNO 2022

Diplomová práce

magisterský navazující studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Dáša Sedláková

ID: 222419

Ročník: 2

Akademický rok: 2021/22

NÁZEV TÉMATU:

Útok a obrana v prostředí energetických průmyslových počítačových sítí

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je prakticky otestovat známé nebo odhalit nové možnosti kybernetických útoků v prostředí průmyslové počítačové sítě postavené na přenosových technologiích Ethernet a TCP/IP, kde jsou využívány protokoly dle norem IEC 60870-5 a IEC 61850 a také zhodnotit předpoklady pro využitelnost daných útoků. Praktické provedení útoků a jejich mitigace bude provedeno na reálných zařízeních s uvedenými normami (např. ochrany ABB REF 615). Výstupem práce je metodika proveditelnosti útoků a jejich mitigace s reálnými testy. Reálné testy na základě navržené metodiky proveditelnosti budou důkladně zdokumentovány pro jejich opakovatelnost.

DOPORUČENÁ LITERATURA:

- [1] COLBERT, Edward J. Cyber-security of SCADA and other industrial control systems. New York, NY: Springer Science+Business Media, 2016. ISBN 978-33-1932-123-3.
- [2] KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.

Termín zadání: 7.2.2022

Termín odevzdání: 24.5.2022

Vedoucí práce: doc. Ing. Petr Mlýnek, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

UPOZORNĚNÍ:

Autor diplomové práce nesmí při vytváření diplomové práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

Abstrakt

Priemyselné systémy sa z dôsledku konvergencie IT a OT sietí stávajú zraniteľné na rôzne formy bezpečnostných hrozieb vrátane neustále narastajúcich kybernetických útokov. Diplomová práca sa venuje analýze bezpečnostných odporúčaní stanovených súborom noriem IEC 62351, testovaniu zraniteľností priemyselných komunikačných protokolov (napríklad IEC 61850) a následnému návrhu mitigácií. Ako základ metodiky testovania zraniteľností je vybraný ATT&CK rámec pre ICS. Použitím vybraných taktík a techník z ATT&CK rámca sú prakticky testované skeny zraniteľností, útok napadnutia časovej synchronizácie SMV, GOOSE spoofing, MMS Man in the Middle a ICMP Flood. Testované útoky sú vyhodnotené prostredníctvom analýzy rizík. Následne sú navrhované mitigačné opatrenia na úrovni OT, IT, perimetrálnej a fyzickej úrovni.

Kľúčové slová

Smart Grid, IEC 61850, IEC 62351, OT, Mitre ATT&CK, Nessus, Nexpose, SMV, GOOSE Spoofing, MMS Man in the Middle, ICMP Flood, Mitigácia

Abstract

Due to the IT and OT networks convergence, industrial systems are becoming vulnerable to different forms of security threats including rapidly growing cyber-attacks. Thesis is focused on an analysis of security recommendations in IEC 62351, vulnerability testing of industrial communication protocols (e.g., IEC 61850) and mitigations proposal. An ATT&CK framework for ICS was chosen to become a methodology base for vulnerability testing. ATT&CK tactics and techniques were used to practically test vulnerability scans, SMV time synchronization, GOOSE spoofing, MMS Man in the Middle and ICMP Flood attacks. Attacks tested were evaluated with a risk analysis. Subsequently, mitigation measures were proposed on several levels (OT, IT, perimeter and physical level).

Keywords

Smart Grid, IEC 61850, IEC 62351, OT, Mitre ATT&CK, Nessus, Nexpose, SMV, GOOSE Spoofing, MMS Man in the Middle, ICMP Flood, Mitigation

Bibliografická citácia

SEDLÁKOVÁ, Dáša. *Útok a obrana v prostředí energetických průmyslových počítačových sítí* [online]. Brno, 2022 [cit. 2022-05-20]. Dostupné z: <https://www.vutbr.cz/studenti/zav-prace/detail/138121>. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce Petr Mlýnek.

Prohlášení autora o původnosti díla

Jméno a příjmení studenta:	Bc. Dáša Sedláková
VUT ID studenta:	222419
Typ práce:	Diplomová práce
Akademický rok:	2021/22
Téma závěrečné práce:	Útok a obrana v prostředí energetických průmyslových počítačových sítí

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

V Brně dne: 23. května 2022

podpis autora

Pod'akovanie

Najväčšia vďaka patrí vedúcemu tejto diplomovej práce doc. Ing. Petrovi Mlýnkovi, Ph.D. za nekončiacu trpezlivosť, ústretovosť, rady a nasmerovanie po metodologickej odbornej aj formálnej stránke. Veľmi si vážim, že to so mnou nevzdal ani po predĺžení a aj naďalej prácu viedol na vysoko odbornej úrovni s ľudským prístupom. Ďalej by som chcela poďakovať priateľovi Tomimu, mojej rodine a priateľom, ktorí mi poskytli dostatok priestoru a psychickej podpory na venovanie sa tomu, čo ma baví. V poslednom rade by som chcela poďakovať kolegom z práce, ktorý mi taktiež preukázali podporu, pochopenie a podali pomocnú technickú ruku, keď som ju potrebovala.

V Brně dne: 23. května 2022

podpis autora

Obsah

ZOZNAM OBRÁZKOV	9
ZOZNAM TABULIEK	10
ÚVOD	11
1. SMART GRID	12
1.1 IEC 61850.....	12
1.1.1 Časti súboru noriem IEC 61850	13
1.2 KOMUNIKÁCIA PODĽA IEC 61850.....	15
1.2.1 <i>Sampled Measured Values (SMV)</i>	15
1.2.2 <i>Generic Object Oriented Substation Event (GOOSE)</i>	15
1.2.3 <i>Manufacturing Messaging Specification (MMS)</i>	16
1.3 IEC 60870.....	16
1.4 KOMUNIKÁCIA PODĽA IEC 60870.....	16
1.4.1 IEC 60870-5-101	17
1.4.2 IEC 60870-5-104	18
1.5 IEC 62351.....	19
1.5.1 <i>Prehľad častí súboru noriem IEC 62351</i>	19
2. ANALÝZA A VYHODNOTENIE NORIEM A ŠTANDARDOV	21
2.1 ANALÝZA A VYHODNOTENIE IEC 61850.....	21
2.1.1 <i>GOOSE a Sampled Measured Values (SMV)</i>	21
2.1.2 <i>Manufacturing Message Specification (MMS)</i>	22
2.2 ANALÝZA A VYHODNOTENIE IEC 60870-5	24
2.3 SÚHRN VYHODNOTENIA IEC 62351	25
3. BEZPEČNOSTNÉ HROZBY	26
3.1 KYBERNETICKÉ ÚTOKY	27
3.1.1 <i>Zhrnutie</i>	28
3.2 ANALÝZA RIZÍK V SMART GRID	28
3.2.1 <i>Zhrnutie</i>	31
4. TESTOVACIE PROSTREDIE	32
4.1 IED REF615	33
4.1.1 <i>Ovládanie</i>	34
4.1.2 <i>Komunikácia</i>	34
4.1.3 <i>Natívna bezpečnosť</i>	35
4.1.4 <i>Zhrnutie</i>	36
5. METODIKA KYBERNETICKÝCH ÚTOKOV	37
5.1 METODICKÝ ZÁKLAD	37
5.2 MITRE ATT&CK PRE ICS	38
5.2.1 <i>Nerelevantné techniky</i>	40
5.2.2 <i>Predispozície</i>	40
5.2.3 <i>Presahujúce</i>	41
5.2.4 <i>Vhodné</i>	41
5.2.5 <i>Nebezpečné/Deštruktívne</i>	41
5.3 ÚTOKY NA TESTOVACIE PROSTREDIE	41

5.3.1	<i>Fáza 1: Prieskum</i>	41
5.3.2	<i>Nástroje na sieťový prieskum</i>	42
5.3.3	<i>Fáza 2: Analýza</i>	47
5.3.4	<i>Fáza 3: Realizácia kybernetického útoku</i>	49
5.3.5	<i>Zhodnotenie predpokladov využiteľnosti a rizika útokov</i>	63
6.	MITIGÁCIA ÚTOKOV	64
6.1	MITIGÁCIA NA ÚROVNI OPERAČNÝCH TECHNOLOGÍI (OT)	64
6.1.1	<i>Autentickosť správ</i>	65
6.1.2	<i>Distribúcia a riadenie kľúčov</i>	66
6.1.3	<i>Šifrovanie správ</i>	67
6.1.4	<i>Zoznam povolených IED</i>	67
6.1.5	<i>IEC (R)61850 Gateway</i>	67
6.1.6	<i>Vysoká dostupnosť</i>	67
6.1.7	<i>IEEE 802.1Q</i>	68
6.2	MITIGÁCIA NA ÚROVNI INFORMAČNÝCH TECHNOLOGÍI (IT).....	68
6.3	MITIGÁCIA NA ÚROVNI PERIMETRU	70
6.4	FYZICKÁ ÚROVEŇ.....	71
7.	VYHODNOTENIE	72
7.1	ZHRNUTIE METODIKY, VÝSLEDKOV A ODPORÚČANÍ.....	72
8.	ZÁVER	77
	LITERATÚRA	78
	ZOZNAM SYMBOLOV A SKRATIEK	82
	ZOZNAM PRÍLOH	84

ZOZNAM OBRÁZKOV

Obrázok 4.1	Zapojenie útočnického stroju k IED zariadeniam.	32
Obrázok 4.2	Schéma zapojenia testovacieho prostredia.	33
Obrázok 5.1	Vizualizácie fáz rámcu Attack Kill Chain.	38
Obrázok 5.2	Plánovanie testovacích techník v online nástroji MITRE ATT&CK® Navigator, od spoločnosti The MITRE Corporation, dostupnom na: https://mitre-attack.github.io/attack-navigator/	40
Obrázok 5.3	Výstup objavených služieb a zraniteľností z Nexpose.	43
Obrázok 5.4	Prikladná ukážka spustenia skenu so špeciálnym parametrom.	44
Obrázok 5.5	Zobrazenie počúvania na porte TCP8834 službou s ID 8092.	44
Obrázok 5.6	Definícia typu cieľových zariadení v rozhraní Nessus.	44
Obrázok 5.7	Grafické zhrnutie počtu detegovaných zraniteľností z rozhrania Nessus.	45
Obrázok 5.8	Grafické znázornenie konkrétnych odhalených zraniteľností v rozhraní Nessus.	45
Obrázok 5.9	Ukážka grafického rozhrania sieťového nástroja Wireshark.	47
Obrázok 5.10	Ukážka zachyteného MMS paketu.	49
Obrázok 5.11	Ukážka grafického rozhrania využitého nástroja Cat KARAT Packet Builder.	50
Obrázok 5.12	Originálny SMV rámec s hodnotou smpSynch: 1.	51
Obrázok 5.13	Modifikovaný SMV rámec na falošnú hodnotu smpSynch: 0.	52
Obrázok 5.14	Ukážka rámcu s pozmenenými prenášanými hodnotami.	52
Obrázok 5.15	Alarm poruchy vypínacieho okruhu získaný z nástroja PCM600.	53
Obrázok 5.16	Ukážka inkrementácie hodnoty stNum pri hlásení chyby.	53
Obrázok 5.17	Posledný zachytený legitímny rámec v stNum: 1 a nový falošný rámec.	54
Obrázok 5.18	Pôvodný GOOSE rámec.	55
Obrázok 5.19	Modifikovaný GOOSE rámec s farebnou legendou.	56
Obrázok 5.20	Výpis ARP tabuľky na windowsovej stanici.	57
Obrázok 5.21	Grafické rozhranie nástroja Ettercap počas prebiehajúceho MITM útoku.	58
Obrázok 5.22	Výpis ARP tabuľky na windowsovej stanici, zmena MAC adresy.	58
Obrázok 5.23	Ukážka zachyteného paketu smerujúceho na IED, ale s MAC adresou útočníka.	59
Obrázok 5.24	Zachytený paket s informáciou o primárnom SNTP servery.	60
Obrázok 5.25	Zachytený paket s informáciou o záložnom SNTP servery.	60
Obrázok 5.26	Spustenie záplavového útoku cez nástroj hping3 a legitímne testovanie dostupnosti z windowsovej stanice.	61
Obrázok 5.27	Výstup z analýzy komunikácie nástrojom WireShark počas útoku.	61
Obrázok 5.28	Ukážka možnosti zneužitia štandardných portov pre laterálny pohyb.	62
Obrázok 6.1	Výmena správ medzi klientom a serverom pre zostavenie TLS spojenia.	66

ZOZNAM TABULIEK

Tabuľka 2.1	Analýza a vyhodnotenie kryptografických algoritmov podľa IEC 62351	22
Tabuľka 2.2	Analýza a vyhodnotenie TLSv1.2 podľa IEC 62351	24
Tabuľka 4.1	Podporované TCP/UDP porty	34
Tabuľka 4.2	Prehľad možností užívateľov	36
Tabuľka 5.1	Prehľad a stručný popis taktík MITRE ATT&CK pre ICS	39
Tabuľka 5.2	Prehľad nástrojov na vykonanie prieskumných útokov	42
Tabuľka 5.3	Porovnanie testovaných skenerov zraniteľností	46
Tabuľka 5.4	Prehľad polí GOOSE PDU so stručnými informáciami	48
Tabuľka 5.5	Prehľad polí SMV PDU so stručnými informáciami	48
Tabuľka 5.6	Výpočet rizikovosti pre testované útoky	63
Tabuľka 6.1	Prehľad mitigačných opatrení na úrovni OT	65
Tabuľka 6.2	Prehľad mitigačných opatrení na úrovni IT	68
Tabuľka 7.1	Metodika testovania	72

ÚVOD

Konvergencia priemyselných OT sietí s tradičnými IT sieťami prináša celú radu prevádzkových benefitov vrátane jednotnej bezpečnostnej telemetrie. Priemyselné systémy už nie sú vyložene izolované a stávajú sa čoraz dostupnejšími pre účely vzdialenej správy, kontroly alebo opravy. Na jednej strane je konvergencia veľkým krokom vpred ku zdieľaniu dát, spolupráci, prehĺbenej viditeľnosti, a tým aj šetreniu zdrojov a výdavkov. Na druhej strane ale prináša nové bezpečnostné výzvy, ktoré sa stávajú jej neoddeliteľnou súčasťou a je potrebné na ich vznik patrične reagovať. Jedná sa napríklad o rozšírenie vektorov prieniku do infraštruktúry vrátane zneužitia ľudských zdrojov, možnosti laterálneho pohybu po infraštruktúre, ale aj zber a odcudzenie citlivých údajov. V kontexte prevádzkových technológií tak rastie pravdepodobnosť ich dosahu útočníkom a zneužitia často zastaralých a nedostatočne zabezpečených systémov.

Práca sa preto venuje komplexnému pohľadu na zaistenie bezpečnosti konvergovaných OT/IT sietí so zameraním na priemyselné energetické systémy, ktoré spadajú pod kritickú infraštruktúru a ich ochrana je preto mimoriadne dôležitá. V úvodnej časti práce je predstavený teoretický rámec energetických komunikačných protokolov s ich analytickým posúdením bezpečnosti. Následne sú prácou identifikované aktuálne bezpečnostné hrozby, medzi ktoré patria aj neustále narastajúce kybernetické úroky. Pre účel hodnotenia predpokladov a využiteľnosti kybernetických útokov je v práci predstavená metodológia analýzy rizík. Ich praktickému testovaniu je venovaná významná časť práce zakončená návrhom mitigačných opatrení.

1. SMART GRID

Označenie Smart Grid je využívané v energetickom priemysle pre modernú a rýchlo sa rozvíjajúcu podobu tradičnej elektrickej siete. Jedná sa o komplexný systém pre dodávku elektriny od jej výroby až k príjemcovi s dôrazom na integráciu komunikačných, operačných a informačných technológií pre vylepšenie celého procesu. Cieľom je zlepšenie spoľahlivosti, bezpečnosti a efektívnosti elektrického systému prostredníctvom obojsmernej sieťovej komunikácie a optimalizácie operácií, správy a plánovania [1]. Do systému sú tak integrované inteligentné elektrické zariadenia, vzdialené koncové jednotky, senzory, elektrické rozvodne, ochrany, SCADA a mnohé ďalšie systémy a zariadenia [2]. Hardware a software používaný na monitorovanie a riadenie fyzických komponentov priemyselnej siete je často označovaný ako prevádzková technológia (OT). Pre správnu interoperabilitu bola komunikácia v rámci Smart Grid štandardizovaná vo viacerých normách a protokoloch. Organizácia International Electrotechnical Commission (IEC) sa stará o prípravu a následne vydáva zmienené medzinárodné štandardy pre elektrotechnologické systémy. V tejto práci bude venovaná najväčšia pozornosť trom sadám noriem, ktoré definujú sieťovú komunikáciu a bezpečnosť v rámci Smart Grid. Tieto normy sú podľa IEC organizácie označované ako IEC 61850, IEC 60870-5 a IEC 62351.

1.1 IEC 61850

Súbor noriem IEC 61850 – Komunikačné siete a systémy v podriadených staniaciach je medzinárodný štandard špecifikujúci metódy komunikácie a komunikačné protokoly pre podriadené stanice v oblasti energetiky. Českým ekvivalentom súboru noriem IEC 61850 je ČSN EN 61850, publikovaný pod súbornými názvami „Komunikační sítě a systémy v podřízených stanicích“ a „Komunikační sítě a systémy pro automatizaci v energetických společnostech“. IEC 61850 predstavuje jednotnú metódu tvorby energetických komunikačných sietí, kde medzi sebou môžu komunikovať zariadenia rôznych výrobcov [3]. Tento súbor noriem popisuje pravidlá pre komunikáciu medzi zariadeniami v rozvodniach, určuje požiadavky, ktoré by z hľadiska komunikácie mali rozvodne a ich zariadenia spĺňať, obsahuje definície komunikačných protokolov a štandardy pre riadiace funkcie a inžiniering rozvodní [4].

Veľkú časť komunikácie v elektrických rozvodniach tvoria inteligentné elektrické zariadenia (IED), ktorých cieľom je najčastejšie zbierať prevádzkové dáta, nastavovať parametre regulácie a jednotlivé zariadenia na diaľku konfigurovať a ovládať. Vďaka protokolom IEC 61850 je okrem zmienených cieľov možné dosiahnuť aj prenášanie súborov a dát s informáciami o aktivitách z IED do systémov SCADA, kde neskôr môžu byť použité k analýze udalostí. Protokoly IEC 61850 využívajú štandardnú technológiu Ethernet s MMS a TCP/IP, vďaka čomu je možné využiť mnoho známych nástrojov využívaných zariadeniami bežnej komunikačnej infraštruktúry. IEC 61850 špecifikuje dátové modely založené na objektovo orientovanom programovaní, čo prináša spojenie

programov a dát do objektov na jednom mieste, a to následne zjednodušuje modifikáciu vytvorených systémov a prispôsobenie novým požiadavkám. Dátové modely sú špecifické pre doménu, obsahujú sémantiku a ich základnými prvkami sú logické uzly, ktoré predstavujú informačný obsah internej funkcie pre automatizačný systém rozvodne alebo informáciu z externého procesného zariadenia. Pre výmenu informácií o konfigurácii je využívaný SCL jazyk založený na XML, vďaka čomu je možné využiť konfiguračné informácie aj mimo konkrétnej rozvodne. Architektúra komunikačného systému podľa IEC 61850 prináša veľkú komunikačnú flexibilitu, nakoľko je jej hlavná časť založená na type komunikácie klient-server. Oproti klasickej architektúre klient-server sa ale líši tým, že prináša možnosť aj klientskym staniciam aby riadili prenos dát. To dovoľuje presunúť riadiace a komunikačné funkcie bližšie k prevádzkovým procesom a vytvára tak flexibilitu v systéme. Ďalej zároveň podporuje metódy, ktoré môžu byť využité na rýchlu výmenu informácií v reálnom čase medzi IED. Mapovanie na už existujúce komunikačné protokoly ako je MMC a TCP/IP cez Ethernet rieši pomocou abstraktnej podoby v ACSI rozhraní [5].

1.1.1 Časti súboru noriem IEC 61850

Súbor noriem IEC 61850 sa skladá z niekoľko častí a rozšírení. Prvé štyri časti popisujú a špecifikujú prostredie, terminológiu, požiadavky na zariadenia atď. Ďalej časti 5 až 10 sa zaoberajú vlastnou komunikáciou. Jedná sa o [4] [6, 8, 9] :

1. IEC/TR 61850-1, v českej terminológii zavedená ako ČSN 33 4850-1 *Komunikační sítě a systémy v podřízených stanicích – Část 1: Úvod a přehled*, ktorá poskytuje úvod a prehľad o celom súbore noriem IEC 61850.
2. IEC/TS 61850-2, ako ČSN IEC/TS 61850-2 *Komunikační sítě a systémy v podřízených stanicích – Část 2: Výklad zvláštních výrazů*, ktorá obsahuje slovník základnej terminológie a výklad výrazov v kontexte systémov energetických služieb.
3. IEC 61850-3, je v ČR zavedená ako ČSN EN 61850-3 *Komunikační sítě a systémy v podřízených stanicích – Část 3: Všeobecné požadavky*, ktorá špecifikuje všeobecné požiadavky na komunikačnú sieť.
4. IEC 61850-4, resp. ČSN EN 61850-4 *Komunikační sítě a systémy v podřízených stanicích – Část 4: Systémové a projektové řízení*, ktorá sa sústreďuje na požiadavky systémového a projektového riadenia a na špeciálne podporné nástroje pre inžinierske práce a systém skúšok rozvodní.
5. IEC 61850-5, resp. ČSN EN 61850-5 *Komunikační sítě a systémy v podřízených stanicích – Část 5: Požadavky na komunikaci pro funkce a modely zařízení*, je časť, ktorá špecifikuje komunikačné požiadavky vykonávaných funkcií v systémoch pre automatizáciu energetických služieb a na modely zariadení.
6. IEC 61850-6, resp. ČSN EN 61850-6 *Komunikační sítě a systémy v podřízených stanicích – Část 6: Konfigurační popisový jazyk pro komunikaci v elektrických stanicích*, ktorá sa zaoberá špecifikáciou formátu súborov pre popis konfigurácie jednotlivých IED a súborov parametrov spojených s komunikáciou a konfiguráciou komunikačného systému. Spolu s časťami 5 a 7 zaisťuje kompatibilitu inžinierskych nástrojov od rôznych dodávateľov.
7. IEC 61850-7 je ďalej rozdelená na niekoľko dielov:

- a. IEC 61850-7-1, resp. ČSN EN 61850-7-1 *Komunikační sítě a systémy v podřizovaných stanicích – Část 7-1: Základní komunikační struktura pro podřizované stanice a napájecí zařízení – Zásady a modely*, poskytuje přehled o architektúre komunikačných systémov a interakcií medzi zariadeniami rozvodní. Ďalej obsahuje popis vzťahov medzi ostatnými časťami IEC 61850-7-x a popis dosiahnutia interoperability zariadení.
 - b. IEC 61850-7-2, resp. ČSN EN 61850-7-2 *Komunikační sítě a systémy v podřizovaných stanicích – Část 7-2: Základní komunikační struktura pro podřizované stanice a napájecí zařízení – Abstraktní rozhraní pro komunikační služby (ACSI)*, popisuje dve rozhrania: prvé pre komunikáciu medzi klientom a vzdialeným serverom a druhé pre rýchle a spoľahlivé šírenie informácií o časovo kritických udalostiach v rámci celého systému rozvodne a na prenos súborov vzorkovaných hodnôt.
 - c. IEC 61850-7-3, resp. ČSN EN 61850-7-3 *Komunikační sítě a systémy v podřizovaných stanicích – Část 7-3: Základní komunikační struktura pro podřizované stanice a napájecí zařízení – Obecné třídy dat*, ktorá špecifikuje triedy dát pre informácie o stave zariadenia, vzorkovaných veličinách, informácie spojené s riadením stavu zariadení. Informácie o analógových žiadaných veličinách v regulačných slučkách a o konfigurácii zariadení.
 - d. IEC 61850-7-4, resp. ČSN EN 61850-7-4 *Komunikační sítě a systémy v podřizovaných stanicích – Část 7-4: Základní komunikační struktura pro podřizované stanice a napájecí zařízení – Třídy kompatibilních logických uzlů a třídy dat*, stanovuje názvy kompatibilných logických uzlov a názvy dát pre komunikáciu medzi programovateľnými elektronickými zariadeniami, vrátane vzťahu medzi logickými uzlami a dátami.
 - e. IEC 61850-7 má ďalej dva doplnkové diely, IEC 61850-7-410, resp. ČSN EN 61850-7-410 *Komunikační sítě a systémy pro automatizaci v energetických společnostech – Část 7-410: Vodní elektrárny – Komunikace pro sledování a řízení* a IEC 61850-7-420, resp. ČSN EN 61850-7-420 *Komunikační sítě a systémy pro automatizaci v energetických společnostech – Část 7-420: Základní komunikační struktura – Logické uzly pro decentralizované zdroje elektrické energie*.
8. IEC 61850-8-1, resp. ČSN EN 61850-8-1 *Komunikační sítě a systémy v podřizovaných stanicích – Část 8-1: Mapování specifických komunikačních služeb (SCSM) – Mapování na MMS (ISO 9506-1 a ISO 9506-2) a na ISO/IEC 8802-3*, špecifikuje metódy pre výmenu časovo kritických a nekritických dát po sieťach LAN pomocou mapovania ASCI na MMS a na rámce Ethernet z ISO/IEC 8802-3 (IEEE 802.3).
 9. IEC 61850-9-1, resp. ČSN EN 61850-9-1 *Komunikační sítě a systémy v podřizovaných stanicích – Část 9-1: Mapování specifických komunikačních služeb (SCSM) – Přenos vzorkovaných hodnot po sériovém jednosměrném (neorientovaném) vícebodovém spoji bod-bod*. Časť definuje mapovanie špecifických komunikačných služieb pre komunikáciu na úrovni poľa rozvodne. Platí pre elektronické transformátory s digitálnym vstupom cez zlučovaciu jednotku.
 10. IEC 61850-9-2, resp. ČSN EN 61850-9-2 *Komunikační sítě a systémy v podřizovaných stanicích – Část 9-2: Mapování specifických komunikačních služeb (SCSM) – Vzorkované hodnoty z ISO/IEC 8802-3*, je stanovené mapovanie SCSM pre prenos vzorkovaných hodnôt v súlade s abstraktné špecifikáciou podľa IEC 61850-7-2.

11. IEC 61850-10, resp. ČSN EN 61850-10 *Komunikační sítě a systémy v podřizovaných stanicích – Část 10: Zkoušky shody*, stanovuje metody a popisuje abstraktné prípady skúšok pre skúšanie zhody zariadení používaných v automatizovaných systémoch rozvodní.

1.2 Komunikácia podľa IEC 61850

Ako bolo spomínané v podkapitole 2.1, IEC 61850 popisuje komunikáciu a prenos dát s využitím moderných technológií počítačových sietí prostredníctvom modelov TCP/IP, ISO/OSI a techník zapuzdovania do Ethernetu. TCP/IP a ISO/OSI sú referenčné modely, ktoré rozdeľujú sieťovú komunikáciu do jednotlivých vrstiev a tým poskytujú koncepčný rámec, ktorý štandardizuje komunikáciu medzi heterogénnymi sieťami. IEC 61850 umožňuje využívať IP siete a komunikáciu uplatňujú tri hlavné služby, ktoré je možné rozdeliť na časovo kritické služby 1) Sampled Values (SV), 2) Generic Object Oriented Substation Event (GOOSE) a časovo nekritické 3) Manufacturing Messaging Specification (MMS) [10].

1.2.1 Sampled Measured Values (SMV)

SV predstavujú nespracované vzorkované dáta komunikované senzormi umiestnenými na primárnych zariadeniach energetických systémov. Dáta sú zvyčajne prenášané sériovými optickými vláknami do spojovacej jednotky (Merging Unit, MU), kde sú zapuzdrené do ethernetových rámcov a pomocou multicast alebo unicast prenosu odoslané do ďalších komponentov [11].

1.2.2 Generic Object Oriented Substation Event (GOOSE)

GOOSE sa používa pre vytváranie objektovo orientovaných udalostí rozvodne a je dôležitou funkciou pre ochranu, kontrolu a automatizáciu podriadených staníc. Takisto ako SV správy bývajú GOOSE zapuzdrené priamo do ethernetového rámcu, čo zlepšuje výkon v reálnom čase vďaka skracovaniu ethernetových rámcov (skratenie o réžiu protokolu vyššej vrstvy) a zníženiu času spracovania. Priame zapuzdrenie do ethernetu umožňuje využívanie hodnôt prioritných značiek na oddelenie kritického a vysoko prioritného prenosu od prenosu s nižšou prioritou. GOOSE pomocou multicasu poskytuje efektívny spôsob súčasného doručovania informácií o udalosti rozvodne pre viacero fyzických zariadení. Stavové dáta a hodnoty premenných sú pri prenose zoskupené do jedného dátového objektu a prenášané v danom časovom intervale. Na GOOSE komunikáciu sú vzhľadom na jej dôležitú funkciu kladené prísne požiadavky na rýchlosť a spoľahlivosť [12].

GSSE (Generic Substation Status Event) je oproti GOOSE generická stavová udalosť rozvodne. Prostredníctvom GSSE sa prenášajú iba stavové dáta. Využíva sa pritom stavový zoznam, teda reťazec bitov a nie dátový objekt. Správy GSSE sú typicky prenášané prostredníctvom MMS. V porovnaní s GOOSE trvá ich spracovanie a prenos dlhšie [13].

1.2.3 Manufacturing Messaging Specification (MMS)

MMS je medzinárodný štandard služieb používaný na spoľahlivú komunikáciu v reálnom čase zahŕňajúcu prenos procesných údajov a informácií o kontrole medzi zariadeniami v sieti a/alebo aplikáciami. Oproti SV a GOOSE je MMS protokol mapovaný priamo na aplikačnú vrstvu referenčného modelu ISO/OSI. MMS komunikácia je štruktúrovaná do dvoch odlišných rolí: MMS klient a MMS server. Klient je užívateľ, ktorý zadáva požiadavku a server je užívateľ, ktorý vykonáva požadovanú akciu alebo generuje požadovanú odpoveď. Väčšinou sa používa v automatizačných a riadiacich funkciách. MMS nemá žiadne výslovné požiadavky na načasovanie, ktoré výrazne uľahčujú zabezpečenie takejto komunikácie [14].

1.3 IEC 60870

IEC 60870 je komplexný súbor noriem pre vzdialenú správu v elektrotechnike a aplikáciách automatizácie energetických systémov. V českej terminológii je súbor zavedený ako ČSN EN 60870 s názvom „*Systémy a zařízení pro dálkové ovládání*“. Súbor pozostáva zo šiestich častí, kde piata časť sa zaoberá komunikáciou medzi SCADA systémami a ďalšími stanicami (jedná sa napríklad o primárne stanice – CC a sekundárne stanice - RTU). Využíva komunikáciu cez sériové linky (časť 101) aj cez siete (časť 104) [15] [16].

Prvé dve časti IEC 60870-1 a 60870-2 tvoria úvod do celého súboru noriem a zaoberajú sa všeobecnými zásadami, návodmi pre špecifikácie, výkladom výrazov, prevádzkovými podmienkami a podobne.

Tretia časť IEC 60870-3 popisuje elektrické charakteristiky rozhraní tak, aby bolo možné prepojenie rôznych prvkov do funkčného systému a následnej vzdialenej správy užívateľom.

Štvrtá časť 60870-4 sa zaoberá požiadavkami na vlastnosti, ktoré majú vplyv na prevádzku systémov vzdialenej správy a súvisia s vlastnosťami aplikácií a funkciami spracovania dát. Ďalej je tu zahrnutý súbor pravidiel pre hodnotenie a špecifikáciu požiadaviek na výkon podľa klasifikácie do výkonnostných tried [17].

1.4 Komunikácia podľa IEC 60870

Práve piata časť súboru noriem IEC 60870 je výrazne dôležitá pre komunikáciu systémov, pretože poskytuje komunikačný profil na zasielanie základných telekontrolných správ. Piata časť sa skladá zo šiestich hlavných častí a ďalších doplňujúcich [15][17]:

1. IEC 60870-5-1 Formáty prenosového rámca, kde sú popísané operácie fyzickej a linkovej vrstvy ako napríklad využitie protokolov half-duplex a full-duplex, štandardov pre kódovanie, formátovanie, synchronizácia rámcov alebo výber medzi 4 typmi rámcov linkovej vrstvy.

2. IEC 60870-5-2 Procedúry spojového prenosu, ktorá popisuje služby a procedúry pre sériový prenos dát. Definuje ďalej aj činiteľa inicializácie prenosu.
3. IEC 60870-5-3 Všeobecná štruktúra aplikačných dát, špecifikuje všeobecnú štruktúru dát na aplikačnej vrstve a pravidlá pre štruktúru jednotiek aplikačných dát v prenosových rámcoch.
4. IEC 60870-5-4 Definícia a kódovanie aplikačných informačných prvkov, popisuje pravidlá pre definovanie informačných prvkov a bežne používané informačné prvky a procesné parametre v aplikáciách.
5. IEC 60870-5-5 Základné aplikačné funkcie, definuje štandardy pre zaistenie interoperability zariadení v elektrizačnej sústave.
6. IEC 60870-5-6 Pokyny pre testovanie zhody pre sprievodné normy IEC 60870-5.

1.4.1 IEC 60870-5-101

Komunikačný protokol IEC 60870-5-101 patrí pod súbor noriem IEC 60870-5 a primárne určuje funkčný profil pre základné úlohy diaľkového ovládania (monitorovanie, kontrolu a súvisiacu komunikáciu pre telekontrolu, teleochranu a telekomunikácie pre energetické systémy). Definuje komunikácie medzi dvoma systémami (napríklad riadiacou stanicou a podriadenou stanicou) prepojenými permanentným dátovým obvodom (sériová linka). Je založený na architektúre EPA (Enhanced Performance Architecture), ktorá obsahuje iba tri vrstvy modelu ISO/OSI: fyzickú vrstvu, linkovú vrstvu a aplikačnú vrstvu.

Fyzická vrstva protokolu IEC 60870-5-101 definuje hardvérovo závislé špecifikácie komunikačného rozhrania IEC 60870-5-101. Táto vrstva ďalej poskytuje binárny symetrický a bez pamäťový prenos medzi DCE (zariadenie na ukončenie dátových obvodov) a DTE (dátové koncové zariadenie) primárnych (riadiacich) a sekundárnych (riadených) staníc.

Vrstva dátového spoja (linková vrstva) protokolu IEC 60870-5-101 definuje rámcové formáty a postupy prenosu komunikácie IEC. Linková vrstva pozostáva z niekoľkých postupov pre prenos linkami použitím výhradných Link Protocol Control Information (LPCI). Tieto procedúry sú schopné prenášať ASDU ako spojové užívateľské dáta. Linková vrstva prijíma, vykonáva a riadi funkcie prenosovej služby požadované vo vyšších vrstvách. Taktiež postupne po jednom riadi prenos rámcov a hlási úspech alebo neúspech prenosu do vyšších vrstiev spolu so stavom prenosového vedenia a stanice. Norma IEC 60870-5-101 definuje dva rôzne typy rámcov, rámec s pevnou dĺžkou (používaný pre riadiace správy) a rámec s premennou dĺžkou (používaný na prenos správ na úrovni aplikácie).

Aplikačná vrstva protokolu IEC 60870-5-101 definuje informačné prvky na štruktúrovanie dát aplikácií a funkcií komunikačných služieb. Aplikačná vrstva obsahuje množstvo „aplikačných funkcií“, ktoré zahŕňajú prenos ASDU medzi zdrojom a cieľom. Používa implicitné informácie o riadení protokolu. Táto vlastnosť je implicitná v obsahu

polí identifikátora dátových jednotiek ASDU a v type použitej linkovej služby. Link Protocol Data Unit (LPDU) obsahuje iba jedno ASDU, ktoré je zložené z identifikátora dátovej jednotky a jedného alebo viacerých informačných objektov. Správa odoslaná IEC 60870-5-101 môže nadobúdať dva smery komunikácie. Kontrolný smer, kde sa jedná o komunikáciu od riadiacej stanice smerom k vzdialenej stanici. Monitorovací smer, kde sa jedná o komunikáciu od vzdialenej stanice na riadiacu stanicu [15] [17].

1.4.2 IEC 60870-5-104

Protokol EC 60870-5-104 (IEC 104) je súčasťou normy IEC 60870-5 pre zariadenia a systémy, ktoré odosiľajú dozorné údaje a požiadavky na zber dát v elektrickom inžinierstve a automatizačných aplikáciách energetických systémov. Protokol poskytuje komunikačný profil na zasielanie základných telekontrolných správ medzi dvoma systémami v elektrotechnike a automatizácii energetických systémov. Protokol IEC 60870-5-104 je obdobou protokolu IEC 60870-5-101 a zatiaľ čo časť -101 špecifikuje mechanizmy prenosu dát, časť -104 stanovuje/odporúča ich použitie v bežných komunikačných sieťach, TCP/IP. Uvádza základné typy ASDU pre prevádzkové informácie v smere ovládania aj sledovania. Stanovuje požiadavky nevyhnutné pre funkčnú spoluprácu zariadení od rôznych výrobcov [15] [17].

1.5 IEC 62351

IEC 62351 je súbor noriem, ktorý sa predovšetkým zameriava na zdokonalenie bezpečnosti v systémoch a protokoloch, ktoré sa používajú v automatizačných systémoch distribúcie energie. Súbor noriem obsahuje ustanovenia informačnej bezpečnosti pre operácie riadenia energetických systémov a celkovým cieľom je zabezpečiť vlastnosti dôvernosti, integrity, dostupnosti, autentizácie a neodmietnutia v energetickom systéme, najmä zavedením autentifikačných mechanizmov [18].

1.5.1 Prehľad častí súboru noriem IEC 62351

Súbor noriem IEC 62351 je rozdelený do hlavných 10 častí, pričom každá sa zameriava na určitú oblasť systémov, protokolov alebo procedúr [18, 19]:

1. IEC 62351-1 obsahuje prehľad štandardu, ciele, úvod k ďalším častiam, bezpečnosť a hrozby a možné protiopatrenia.
2. IEC 62351-2 obsahuje definície termínov.
3. IEC 62351-3 stanovuje bezpečnosť na základe TCP/IP pre automatizované systémy v energetike. Zaoberá sa využitím TLS x X.509 certifikátmi, zaistením autenticity a integrity na sieťovej vrstve, dôvernosťou pomocou šifrovacích mechanizmov TLS. 3. časť normy ďalej stanovuje využitie obojstrannej autentizácie certifikátmi (klient aj server) a predpisuje algoritmy, stanovuje minimálne dĺžky používaných kľúčov a určuje postup spracovania tzv. revocation certifikátov.
4. IEC 62351-4 sa zameriava na bezpečnosť profilov ako napríklad MMS, ISO 2014 (IEC 61850-8-1 a IEC 60870-6). Obsahuje odporúčania pre používanie A-profilu, kde hovorí o využití X.509 certifikátov pre autentizovanie aplikácií a T-profilu, kde opisuje ako použiť TLS ako vrstvu medzi TCP a ISO Transport Service a stanovuje TLS šifry, ktoré musia byť podporované.
5. IEC 62351-5 stanovuje bezpečnosť pre protokoly IEC 60870-5, DNP3, message-based protokoly, kde opisuje autentizáciu per-message. V stanovách berie do úvahy limitovanú procesnú silu a ďalej sa zaoberá napríklad popisom vzdialenej aktualizácie kľúčov používaných pre šifrovanie.
6. IEC 62351-6 stanovuje bezpečnosť pre protokol MMS IEC 61850 a priamu aplikáciu časti IEC 62351-4. Popisuje bezpečnostné rozšírenie 61850 GOOSE a SV pridaním security poľa do PDU a rozširuje Substation Configuration Language o povolenie definície certifikátov.
7. IEC 62351-7 popisuje využitie SNMP na správu operácií systémov a využívanie modelov dátových objektov.
8. IEC 62351-8 Stanovuje kontrolu prístupu. Rozdeľuje priamy a vzdialený prístup a prístup človeka a automatizovaného stroju. Stanovuje 3 formáty prístupových tokenov – X.509 ID certifikáty s rozšíreniami, X.509 atribútové certifikáty a softvérové tokeny.
9. IEC 62351-9 popisuje štandardizáciu používaných certifikátov a management kľúčov. Definuje ako ich generovať, distribuovať a narábať s nimi.

10. IEC 62351-10 stanovuje smernicu pre architektúru energetických systémov, náhľad bezpečnostných kontrol a podobne.
11. IEC 62351-11 definuje zabezpečenie súborov XML. Poskytuje mechanizmus na autentifikáciu zdroja súboru a mechanizmus na detekciu neoprávnenej manipulácie.

2. ANALÝZA A VYHODNOTENIE NORIEM A ŠTANDARDOV

Súbory noriem a štandardov teoreticky popísané v predošlých kapitolách sa stali významným prvkom v zaistení interoperability zariadení, sieťovej komunikácie ale aj bezpečnosti v energetickom priemysle. Nakoľko sa ale jedná o komplexné a kritické systémy, je dôležité prikladať dôraz nielen na aplikovanie noriem a štandardov ako takých, ale hlavne na vhodnosť ich aplikácie a časovú relevantnosť stanov z noriem vyplývajúcich. Táto kapitola je z tohto dôvodu zameraná na analýzu a vyhodnotenie stanov, ktoré zo súborov noriem vyplývajú s dôrazom na aktuálnosť odporúčaných bezpečnostných štandardov a relevantnosti ich aplikácie.

Aktuálnosť bezpečnostných štandardov bude v kapitole analyzovaná na základe odporúčaní vydanými významnými organizáciami, ktoré cieľia na oblasť kybernetickej bezpečnosti. Medzi tieto organizácia patrí Národný úrad pro kybernetickú a informačnú bezpečnosť (NÚKIB), National Institute for Standard and Technology (NIST) a European Union Agency for Cybersecurity (ENISA) [20, 21, 22].

2.1 Analýza a vyhodnotenie IEC 61850

Súbor noriem IEC 61850 je v rámci energetických systémov jedným z najdôležitejších a najpoužívanejších štandardov pre automatizáciu rozvodní, najmä vďaka jeho objektovo orientovanému a interoperabilnému dizajnu. Súbor noriem IEC 61850 definuje rôzne protokoly pre výmenu informácií, nedefinuje však ako tento prenos zabezpečiť. Zabezpečenie týchto protokolov je preto odkázané na aplikovaní ďalších bezpečnostných postupov, ktoré napríklad definuje práve IEC 62351.

2.1.1 GOOSE a Sampled Measured Values (SMV)

Z rôznych komunikačných protokolov IEC 61850 je bezpečnosť GOOSE správ o niečo kritickejšia, nakoľko prenáša časovo dôležité informácie týkajúce sa prevádzky energetického systému. Ak dôjde k narušeniu GOOSE správy, môže to mať katastrofické dopady na prevádzku časti alebo celku energetického systému. IEC 62351-1 identifikuje autentickosť a integritu správ GOOSE/SV za najdôležitejšie bezpečnostné požiadavky a ich naplneniu sa venuje v časti IEC 62351-6 aplikovaním kryptografických algoritmov. Práve u kryptografických algoritmov je možné identifikovať hneď niekoľko výziev. V prvom rade hrá významnú rolu prísna časová požiadavka na doručenie GOOSE správ do 3 ms. Ďalšie problémy môžu nastať v hardwarovej predispozícii komunikujúcich zariadení, ktoré sú často limitované pamäťou a výpočtovým výkonom.

Stanovy podľa IEC 62351-6-2007 popisujú použitie digitálnych podpisov generovaných hashovacím algoritmom SHA256 a následným podpisom hodnôt hashu algoritmom RSASA-PSS a RSA algoritmom pre vytvorenie kľúčov. Tento digitálny podpis by mal byť generovaný pre každú GOOSE/SV správu a následne k správe pripojený ako nové pole rozšírenia Extensions. Celková pridaná režia síce záleží od dĺžky

použitých kľúčov a výkonu procesoru, ale v reálnom nasadení aj pri minimálnych štandardoch je veľmi náročné dosiahnuť stanovenú rýchlosť doručenia správ. Z tohto dôvodu novela pôvodného štandardu, IEC 62351-6-2020 navrhuje alternatívu digitálnemu podpisu, použitím symetrického algoritmu Message Authentication Code (MAC), kedy v reálnom nasadení aj pri minimálnych kryptografických štandardoch už je možné dosiahnuť časovú požiadavku správ. Hodnota MAC je znovu pridávaná ako nové pole rozšírenia Extensions. Na druhej strane je možné za nevýhodu MAC algoritmu považovať nutnosť pred-zdieľaných kľúčov pre obe strany, kde je potrebné dbať na ich správnu distribúciu, časovú platnosť, uchovávanie, zmenu a súčinné operácie [19]. Stanovy v IEC 62351 popisujú minimálne kryptografické algoritmy odporúčané pre využitie v sieťovej komunikácii. Ich relevantnosť a vyhodnotenie je popísané v tabuľke 2.1, zobrazenej nižšie.

Tabuľka 2.1 Analýza a vyhodnotenie kryptografických algoritmov podľa IEC 62351

Odporúčanie podľa IEC 62351	Stanovisko NÚKIB, NIST a ENISA	Vyhodnotenie
SHA-256	Aktuálne bezpečné	U starších systémov je využitie SHA-256 v poriadku, pre novo implementované systémy, prípadne s ohľadom do budúcnosti je odporúčané využitie minimálne SHA-384.
RSA-1024 (spätná kompatibilita)	Aktuálne neodporúčané	RSA-1024 bolo považované za bezpečné do roku 2020, z tohto dôvodu je odporúčané využiť RSA s dĺžkou kľúčov minimálne 2048b.
RSA-2048	Aktuálne bezpečné	U starších systémov je použitie RSA-2048, s ohľadom do budúcnosti (2030) je odporúčané využiť RSA-3072.
RSASSA-PSS	Aktuálne bezpečné s dosluhujúcou dĺžkou kľúčov 2048b	Bezpečné do budúcnosti (2030) s využitím dĺžky kľúčov minimálne 3072b.
ECDSA-256	Aktuálne bezpečné	U starších aj nových systémov je využitie ECDSA-256 v poriadku, s ohľadom do budúcnosti je odporúčané zvážiť použitie silnejšieho ECDSA-512.
ECDSA-512	Aktuálne bezpečné	Bezpečné aj do budúcnosti (2030).
HMAC-SHA256-224	Dosluhujúce	Výstup veľkosti 224b je dostačujúci, ale do budúcnosti je odporúčaný minimálne 256b, ideálne 384b a viac.
HMAC-SHA256-256	Aktuálne bezpečné	Bezpečné aj do budúcnosti (2030), odporúčané je využitie veľkosti výstupu minimálne 384b.

2.1.2 Manufacturing Message Specification (MMS)

Ďalšou kritickou službou je protokol MMS definovaný v IEC 61850. Norma IEC 62351 vzhľadom k MMS stanovuje za dôležité bezpečnostné požiadavky dôvernosť, integritu a autenticitu. Bezpečnosť v MMS je podľa IEC 62351-4:2007 delená cez OSI vrstvy na transportný profil (fyzická vrstva, linková vrstva, sieťová vrstva a transportná vrstva) a aplikačný profil (relačná vrstva, prezentačná vrstva a aplikačná vrstva).

Na úrovni transportného profilu je podľa normy IEC 62351-4 odporúčané využívať TLS 1.2 definované podľa RFC 5246 s využitím špeciálneho TCP portu 3782 miesto štandardného TCP 102. Minimálnou požiadavkou na použitý súbor šifier sa podľa normy stáva `TLS_DH_DSS_WITH_AES_256_CBC_SHA` pre natívny režim. Vo výnimočných prípadoch pre kompatibilný režim je možné využiť minimálne TLS 1.0. Nakoľko je protokol TLS 1.0 považovaný za bezpečnostne nedostačujúci a náchylný na rôzne formy útokov, je použitie vysoko neodporúčané a preferované by malo byť použitie TLS 1.2 alebo TLS 1.3. Pre zaistenie autenticity komunikujúcich strán je štandardom odporúčané využitie certifikátov formátu X.509 s maximálnou veľkosťou 8192B.

Na úrovni aplikačného profilu dochádza k deleniu na peer-to-peer bezpečnostnú špecifikáciu (P2P profil) a end-to-end aplikačnú bezpečnosť (E2E profil). P2P profil stanovuje zaistenie autentifikácie prostredníctvom pridania autentifikačnej informácie do asociačných správ. Tieto informácie sa skladajú zo zakódovaného X.509 certifikátu, digitálneho podpisu a časovej hodnoty. Na rozdiel od E2E bezpečnostného profilu je pri P2P profile nutná implementácia transportného profilu pre zaistenie bezpečnej komunikácie [26].

Pridanie TLS zabezpečenia ale zároveň zavádza výpočtové latencie pri spracovaní MMS správ, ktorých veľkosť závisí od použitých šifrovacích algoritmov. MMS správy ale nie sú časovo kritické ako GOOSE správy, preto je pridanie zabezpečenia vysoko odporúčané [22]. IEC 62351 stanovuje minimálne kryptografické algoritmy, ktoré sú odporúčané pre využitie v TLS. Nakoľko TLS 1.0 už nie je vo všeobecnosti považovaná za bezpečnú, sú prezentované výsledky vyhodnotenia a relevantnosti algoritmov pre TLS 1.2, zobrazené v tabuľke 2.2 nižšie. Ďalej je dôležité poznamenať, že implementácie MMS by mali zaistiť podporu TLS verzií 1.0 a 1.1 z dôvodu spätnej kompatibility aj napriek ich aktuálnemu nevyužívaniu.

Tabuľka 2.2 Analýza a vyhodnotenie TLSv1.2 podľa IEC 62351

Odporúčanie podľa IEC 62351 pre TLS 1.2	Stanovisko NÚKIB, NIST a ENISA	Vyhodnotenie
TLS_RSA_WITH_AES_128_CBC_SHA256	Dosluhujúce	Aktuálne bezpečné, ale cipher suite by mal byť rozšírený o minimálne DHE algoritmus a CBC by malo byť nahradené GCM.
TLS_DH_RSA_WITH_AES_128_CBC_SHA256	Nedostatočné	DH nepodporuje funkciu PFS, čím sa komunikácia stáva náchylná na útoky a cipher suite preto nie je odporúčané používať. Navyše CBC by malo byť nahradené GCM.
TLS_DH_RSA_WITH_AES_128_GCM_SHA256	Nedostatočné	DH nepodporuje funkciu PFS, čím sa komunikácia stáva náchylná na útoky a cipher suite preto nie je odporúčané používať.
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Bezpečné	Odporúčané je zvýšiť dĺžku výstupu hashovacej funkcie na 384b.
TLS_DH_RSA_WITH_AES_256_GCM_SHA384	Nedostatočné	DH nepodporuje funkciu PFS, čím sa komunikácia stáva náchylná na útoky a cipher suite preto nie je odporúčané používať.
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	Bezpečné	Bezpečné a odporúčané aj do budúcnosti. (2030)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	Bezpečné	Bezpečné a odporúčané aj do budúcnosti. (2030)
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	Bezpečné	Bezpečné a odporúčané aj do budúcnosti. (2030)

2.2 Analýza a vyhodnotenie IEC 60870-5

Súbor noriem IEC 60870-5 definuje dôležité komunikačné protokoly a štandardy najmä pre telekontrolu (SCADA systémy) a aplikácie automatizácie energetických systémov. Podobne ako súbor noriem IEC 61850, tak ani IEC 60870-5 sám o sebe nedefinuje zabezpečenie komunikácie a je preto takisto nutné aplikovanie ďalších bezpečnostných postupov, akým je práve IEC 62351, ktoré vo svojom znení bezpečnosť IEC 60870-5 priamo adresuje. Najdôležitejšou časťou sa stáva IEC 62351-5, ktorá poskytuje rôzne riešenia pre sériovú komunikáciu (predovšetkým IEC 60870-5-101) a sieťovú komunikáciu (predovšetkým IEC 60870-5-104).

Jadrom tejto časti sa stáva odporúčanie autentifikačného mechanizmu používajúceho HMAC s pred zdieľanými kľúčmi pre zaistenie požiadavky na integritu, spolu so

stanovami na vzdialenú aktualizáciu kľúčov (symetrických aj asymetrických). Komplikácie ale môžu nastať hneď v niekoľkých prípadoch. Prvým nedostatkom štandardu je stanovenie zneplatnenia kľúčov relácie pokiaľ stanica obdrží viacero správ, ktoré obsahujú neplatné autentifikačné údaje. Stanica sa následne nepokúša o opätovné zadanie kľúča sama od seba ale iba v dôsledku ďalšej udalosti (ako napríklad reštart zariadenia alebo vypršanie doby platnosti kľúča). Riešením by preto mala byť buď implementácia mechanizmu, ktorý by opätovné zadanie kľúča povolil alebo prehodnotenie vynucovania zneplatnenia kľúča po prijatí viacerých správ s neplatnými autentifikačnými údajmi.

Štandard IEC 62351-5 ďalej stanovuje, že zatiaľ čo stanica čaká na odpoveď na autentifikačnú výzvu, mala by zahodiť všetky nesúvisiace správy prijaté v medzičase. Tento mechanizmus je ale rizikový, nakoľko otvára príležitosť útočníkovi udržiavať stanicu v stave zahadzovania všetkých správ [18].

Najväčším rizikom, ktoré IEC 62351 adresuje je, že na aplikačnej vrstve dáta tečú nešifrovane, čo umožňuje hneď niekoľko útokov. Toto riziko sa týka oboch protokolov IEC 60870-5-101 aj -104, nakoľko sú obidva protokoly mapované okrem iného aj na aplikačnú vrstvu. IEC 62351 toto riziko adresuje odporúčaním pre použitie TLS protokolu, ktorý je popísaný v časti IEC 62351-3 a rieši bezpečnostné požiadavky na integritu aj dôvernosť správ. Analýza konkrétnych odporúčaných kryptografických algoritmov je popísaná v Tabuľke 2.1 a 2.2 tohto dokumentu.

2.3 Súhrn vyhodnotenia IEC 62351

Súbor noriem IEC 62351 definuje riziká technológii energetického priemyslu, ktoré následne adresuje priamymi a najmä konkrétnymi mechanizmami pre ich minimalizáciu. Veľkým prínosom súboru noriem je, že odporúčané mechanizmy sú priebežne vyhodnocované v spolupráci s bezpečnostnými organizáciami ako napríklad NIST alebo NSA. Nevýhodou naopak, že aktualizácie častí noriem nie sú tak dynamické ako technologický posun. Čo môžeme pozorovať napríklad z vyhodnotenia odporúčaných algoritmov v tabuľke 2.1 a tabuľke 2.2 tohto dokumentu. Nakoľko je v rámci energetického priemyslu nevyhnutné zachovať možnosti spätnej kompatibility, normy a následne aj implementácie v praxi budú vždy obsahovať slabšie bezpečnostné varianty. Tieto varianty bezpečnostných mechanizmov tak môžu byť útočníkmi využité ako jeden z primárnych vektorov útokov. Čím prichádza v dôležitosť časť normy IEC 62351-7, ktorá navrhuje mechanizmus sledovania stavu sietí a systémov a najmä zisťovanie možných narušení bezpečnosti. Každá podozrivá komunikácia (napríklad využitie slabších bezpečnostných algoritmov) by mala byť operátorovi oznámená alarmom, prípadne priamo blokována pomocou bezpečnostných riešení ako napríklad IPS alebo firewall.

3. BEZPEČNOSTNÉ HROZBY

V kontexte Smart Grid prevádzka energetického systému silno závisí od presných a aktuálnych informácií. Informačná a prevádzková infraštruktúra musí byť udržiavaná a riadená tak, aby jej spoľahlivosť bola na dostatočne vysokej úrovni, podobne ako je spoľahlivosť celkovej infraštruktúry energetického systému. Energetický systém predstavuje kritickú infraštruktúru a je vystavovaný rôznym kybernetickým útokom a škodlivým činnosťami. Vo všeobecnosti komunikačné protokoly využívané v energetickom systéme sami o sebe neimplementujú bezpečnostné opatrenia. Tieto opatrenia navyše musia presahovať bežnú autentifikáciu používateľa a šifrovanie protokolov napríklad plánovaním zabezpečenia, správou kľúčov a mechanizmami kontroly prístupu [24]. Bezpečnostné požiadavky sa tradične členia do troch hlavných kategórií, označované ako CIA triáda [25]:

1. Dôvernosť (zabránenie neoprávnenému prístupu k informáciám)
2. Integrita (zabránenie zmenám informácií počas ich prenosu)
3. Dostupnosť (zabránenie odmietnutia služby a poskytnutia oprávneného prístupu k informáciám)

Do CIA triády sú ďalej mapované ďalšie princípy bezpečnostných požiadaviek:

1. Autentickosť - Integrita
2. Nepopierateľnosť - Integrita
3. Správnosť v špecifikácii – Integrita a Dostupnosť
4. Zodpovednosť - Integrita
5. Integrita ľudí - Integrita
6. Dôvera – Dôvernosť a Integrita
7. Etickosť - Integrita
8. Správa identít – Dôvernosť, Integrita a Dostupnosť

Model CIA triády je všeobecne rešpektovaný a tvorí základ pre architektúru bezpečnostných systémov a politik vo svete informačných aj operačných technológií. CIA model je často používaný pri vyhľadávaní zraniteľností systémov ako aj pri identifikácii vhodných metód na ich riešenie a odstránenie. Vytvorenie a naplnenie všetkých troch požiadaviek vyplývajúcich z CIA triády je výzva, s ktorou sa stýka celý bezpečnostný priemysel. Model je zároveň škálovateľný v závislosti od typu príslušného systému, na ktorý cieľ. Zreteľné rozdiely sú napríklad pri celení na informačné a prevádzkové technológie využívané v priemyselnom odvetví. Aj napriek silnej konvergencii týchto technológií si OT zachovávajú svoju jedinečnosť vo výraznej dominancii požiadavky dostupnosti voči dôvernosti a integrite. Systémy, ktoré riadia priemyselné procesy netolerujú neočakávané výpadky a dokonca aj zdanlivo neškodné oneskorenie systému dokáže spôsobiť výrazné škody. Z tohto dôvodu je nevyhnutné pristupovať k bezpečnosti OT systémov pomocou osobitných stratégií.

Norma IEC 62351-1 rozdeľuje hrozby pre Smart Grid do dvoch kategórií:

1. Neúmyselné hrozby
 - a. Poruchy bezpečnosti

- b. Poruchy nástrojov
 - c. Neopatrnosť
 - d. Prírodné katastrofy
2. Zámerné hrozby
- a. Všeobecné
 - b. Nespokojný zamestnanec
 - c. Priemyselná špionáž
 - d. Vandalizmus
 - e. Kybernetický hackeri
 - f. Vírusy a červy
 - g. Krádež
 - h. Terorizmus

Táto práca je špecificky zameraná na hrozbu kybernetických útokov.

3.1 Kybernetické útoky

Kybernetické útoky voči priemyselným systémom boli preslávené malwarom STUXNET v roku 2010. Od tej doby dochádza ku kontinuálnemu nárastu počtu kybernetických útokov vedených na priemyselné organizácie. Medzi najznámejšie patria: Industoyer, BlackEnergy, Havex alebo Triton. Útočníci si dobre uvedomujú aké riziká konvergencia IT a OT sietí pre priemyselné odvetvia prináša a naopak aj vektory, ktoré vďaka konvergencii vznikajú a sú zneužiteľné k preniknutiu do infraštruktúry a následnému páchaniu škôd. Príkladom takýchto vstupných vektorov je zneužitie techník sociálneho inžinierstva, ktoré sa aktuálne stávajú jednými z najčastejšie využívaných s najvyšším podielom úspešnosti. Prostredníctvom sociálneho inžinierstva je možné do IT/OT prostredia prepašovať škodlivý kód, vytvoriť si zadné vrátka alebo napríklad zneužiť získané užívateľské prístupové údaje na priamy vstup. Vďaka konvergencii sietí by sa mohol útočník ďalej laterálne pohybovať a vyhľadať vhodné ciele a použiteľné metódy. Medzi najčastejšie typy kybernetických útokov na priemyselné prostredia patrí:

1. Muž uprostred (Man in the Middle)
2. Odcudzenie hesla (Password stealth)
3. Podvrhávanie (Spoofing)
4. Nepovolený prístup (Unauthorized access)
5. Analýza sieťovej komunikácie (Traffic analysis)
6. Odpočúvanie (Eavesdropping)
7. Manipulácia (Tampering)
8. Prehrávanie (Replay)
9. Vkladanie dát (Data Injection)
10. Synchronizácia času (Time Synchronization)
11. Úprava dát (Data Modification)
12. Záplavové útoky (Flooding)

13. Odoprenie služby (DoS/DDoS)
14. Rušenie (Jamming)
15. Pretečenie vyrovnávacej pamäte (Buffer Overflow)
16. Škodlivý software (Malware)

3.1.1 Zhrnutie

OT systémy majú štandardnú životnosť kľudne aj 10 rokov, kvôli čomu sa v nich nachádza množstvo známych starších aj nových zraniteľností. Ich odstránenie nie je jednoduché, nakoľko aplikovanie záplat a aktualizácií na prevádzkových systémoch môže vyvolať oneskorenie až dočasnú úplnú nedostupnosť systémov, čo v operačnom prostredí nie je tolerované. Na druhej strane OT zariadenia disponujú veľkým množstvom bezpečnostných a kontrolných vlastností a operátori sú často zdatní pri vnímaní neštandardných stavov, vďaka čomu nie je vykonanie úspešného a nedetekovateľného útoku na priemyselné systémy úplne jednoduché. ICS zariadenia sú veľmi krehké a útočníci tak musia byť opatrní a hlavne mať silný znalostný základ pre úspešnú exploitáciu a vyhnutie sa odhaleniu. Pokiaľ ale k úspešnému útoku dôjde, dôsledky sú príliš vysoké na to aby sa brala bezpečnosť na ľahkú váhu a preto je riziko kybernetických útokov pre priemyselné prostredia veľmi vysoké.

3.2 Analýza rizík v Smart Grid

Riziká v kontexte Smart Grid je možné identifikovať viacerými metódami. Medzi tieto metódy patria napríklad súlad a audit štandardov, SME metóda využívajúca expertov na danú problematiku alebo prístup založený na výkone a efektívite. Nakoľko je v práci predpokladané využívanie bezpečnostných štandardov a hlavný dôraz je kladený na zavedenie mitigačných opatrení, bola pre účely vyhodnotenia bezpečnostných rizík v tejto práci využitá metóda založená na výkone a efektívite. Výhodou metódy je jej opakovateľnosť a reprezentácia v číselných hodnotách. Podľa tejto metódy je možné bezpečnostné riziko v Smart Grid definovať ako pravdepodobnosť, že útočník zneužije zraniteľnosť a spôsobí škodu na počítači, sieti, systéme alebo obslužnom prostriedku, čo bude mať za následok prevádzkové a obchodné dopady. Kvantitatívna reprezentácia rizika je podľa pôvodnej metódy autormi vyjadrená ako súčin pravdepodobnosti úspešného útoku s dôsledkom [23]:

$$R = P_A \times (1 - P_E) \times C \quad (3.1)$$

Pravdepodobnosť úspešného útoku je hodnotená na základe súčinu pravdepodobnosti útoku, pravdepodobnosti prerušenia útoku (s ohľadom na zistenie a zhodnotenie útoku, oneskorenie a odpoveď) s pravdepodobnosťou neutralizácie:

$$P_E = P_I \times P_N \quad (3.2)$$

Dôsledok je následne stanovený na základe súčiny geografických vplyvov, času na opätovné zotavenie systému a rozsahu finančných dopadov:

$$C = I - (I - C_A) \times (I - C_T) \times (I - C_C) \quad (3.3)$$

Prvky metódy boli v práci využité a doplnené o nové prvky určené na prispôsobenie aktuálnym bezpečnostným požiadavkám v Smart Grid podľa CIA triády. V definícii pravdepodobnosti úspešného útoku bola pôvodná premenná pravdepodobnosti prerušenia útoku (P_I) modifikovaná na pravdepodobnosť zásahu (P_Z), ktorá je určovaná schopnosťou odhalenia útoku a iniciáciou zásahu. Ďalej bola vykonaná zásadná zmena v definícii premennej dôsledku (C), ktorá je v originálnom znení vyjadrovaná na základe geografických, časových a finančných vplyvov. V tejto práci boli na pôvodnú premennú aplikované 3 najdôležitejšie bezpečnostné požiadavky pre Smart Grid, ktorými sú dôvernosť, integrita a dostupnosť. A práve na základe miery narušenia týchto bezpečnostných požiadaviek je vyjadrená nová premenná dôsledku (D), ktorá plne nahradzuje pôvodnú. Základná definícia rizika je využitá z pôvodnej metódy vyjadrená ako:

$$\text{Riziko} = \text{Pravdepodobnosť úspešného útoku} \times \text{Dôsledok}$$

Rovnica sa snaží o koreláciu rôznych elementov rizika a môže byť ďalej vyjadrená ako:

$$R = P_U \times (1 - P_E) \times D \quad (3.4)$$

Kde:

R reprezentuje predpokladanú úroveň rizika, alebo zvyškovú mieru rizika po nasadení bezpečnostných mechanizmov. Nadobúda hodnotu medzi 0 a 1, ktorá predstavuje kombináciu pravdepodobnosti útoku na systém, účinnosť obrany systému a dôsledok úspešného útoku.

P_U reprezentuje pravdepodobnosť útoku s nadobúdacou hodnotou znovu medzi 0 a 1, kedy hodnota 1 reprezentuje 100% pravdepodobnosť.

P_E reprezentuje pravdepodobnosť účinnosti bezpečnostného mechanizmu a $(1 - P_E)$ meria nedostatočnosť bezpečnostných opatrení.

D reprezentuje dôsledok úspešného útoku so závažnosťou vyjadrenou znovu hodnotami medzi 0 a 1.

P_E môže byť ďalej rozšírené:

$$P_E = P_Z \times P_N \quad (3.5)$$

Kde:

P_Z reprezentuje pravdepodobnosť zásahu, určenou pravdepodobnosťou odhalenia útoku a iniciovaným zásahom.

P_N reprezentuje pravdepodobnosť neutralizácie hrozby, teda ako efektívny bol vykonaný zásah voči zastaveniu útoku.

D môže byť ďalej rozšírené:

$$D = 1 - (1 - D_b) \times (1 - D_i) \times (1 - D_o) \quad (3.6)$$

Kde:

D_b reprezentuje dopad na požiadavku dôvernosti.

D_i reprezentuje dopad na požiadavku integrity.

D_o reprezentuje dopad na požiadavku dostupnosti.

Konkrétne reprezentácie hodnôt sú uvedené v *Prílohe A - Tabuľky hodnôt pre atribút D* tohto dokumentu.

Pre zreteľnejšie pochopenie použitej metodológie je znázornené príkladné hodnotenie rizika, ktoré predstavuje Spoofing útok pre GOOSE správy komunikujúce na druhej vrstve ISO/OSI, definované v súbore noriem IEC 61850. V prvom kroku sú stanovené podmienky pri ktorých je možné útok vykonať a rozsiahlosť už implementovaných bezpečnostných mechanizmov.

Vychádzajúc z povahy GOOSE správ je prvou podmienkou dosah útočníka na cieľový systém vďaka úspešnému prieniku do siete (či už fyzicky, prostredníctvom kompromitovaných interných zariadení alebo z externého prostredia). V tomto príklade predpokladáme úspešný prienik do siete a dosah útočníka na cieľový systém. Nasleduje už samotný výpočet:

$$R = P_v \times (1 - (P_z \times P_N)) \times (1 - (1 - D_b) \times (1 - D_i) \times (1 - D_o)) \quad (3.7)$$

V atribúte P_v je hodnotené s akou pravdepodobnosťou útočník po úspešnom prieniku vykoná práve daný útok, na základe jeho zložitosti a efektivity. V tomto prípade sa jedná o zvýšenú náročnosť útoku, nakoľko je nutná znalosť princípu GOOSE správ a možnosť modifikácie rámca. Predpokladáme, že útočník cielili priamo na IEC 61850, z čoho vyplýva znalosť daného protokolu, ale na druhej strane nemusí v momente prieniku do siete disponovať potrebnými nástrojmi na modifikáciu rámca (pokiaľ napríklad k cieľovému systému prenikol fyzicky). Spoofing útokom je možné získať prístup k prenášaným dátam ako aj vykonať odopretie dostupnosti služby, na základe čoho hodnotíme 70% (0.7) pravdepodobnosť, že by daný útočník vykonal práve Spoofing útok.

Nakoľko jedným z hlavných cieľov tejto práce je určiť efektívne mitigačné opatrenia voči kritickým útokom, sú v atribúte P_e predpokladané minimálne až žiadne bezpečnostné mechanizmy. Atribút P_z uvažuje pravdepodobnosť odhalenia útoku ako takého, s tým, že už počiatkový prienik sa predpokladá ako neodhalený a tým nastavuje počiatkovú hodnotu atribútu $P_z = -0.5$. Atribút P_N uvažuje pravdepodobnosť neutralizácie útoku s ohľadom na odhalenie a následne zastavenie prieniku, čo znovu stanovuje počiatkovú hodnotu atribútu $P_N = -0.5$. Nakoľko môže pri pokuse o útok dochádzať k častému vypínaniu/zmenám vo funkčnosti systému je porucha ľahko detekovateľná (80%, $P_z = 0.8$), ale na druhej strane skrz modifikáciu rámcov je náročnejšia detekcie útoku bez

dôsledkov ako sú viditeľné zmeny vo funkčnosti (-30%, $P_z = 0.8-0.3$) x časovo náročnejší troubleshooting a rozpoznanie problematických rámcov (-60%, $P_N = 0.4$) = -0.5 x (0.5 x 0.4) = 0

V poslednom kroku ostáva vyhodnotiť potencionálne dôsledky úspešne vykonaného útoku, ktorých konkrétne hodnoty sú uvedené v *Prílohe A - Tabuľky hodnôt pre atribút D*. Vďaka priamemu prístupu k nezabezpečenej GOOSE komunikácii sa útočník dostane k prevažnej časti informácií v cieľovom systéme, $D_o = 0.7$. Všetky dáta, ku ktorým sa útočník dostane môžu byť počas ich prenosu modifikované, z čoho vyplýva, že dôjde k narušeniu integrity triedy II; $D_i = 1$. Doba nedostupnosti cieľového systému je podmienená samotným zistením nedostupnosti/výpadku/oneskorenia a následnou reakciou na incident. Keďže sa môže jednať o nedostupnosť v rámci milisekúnd ale aj výpadok v rámci desiatok minút (doba kým sa k zariadeniu fyzicky dostaví zodpovedná osoba) je premenná vsadená na maximálnu hodnotu, $D_o = 1$. Po dosadení hodnôt do rovnice dosiahneme výsledok rizikovosti útoku na konkrétny systém pre definované požiadavky a prostredie.

$$0.7 = 0.7 \times (1 - (0)) \times (1 - (1 - 1)) \times (1 - 0.7) \times (1 - 1) \quad (3.8)$$

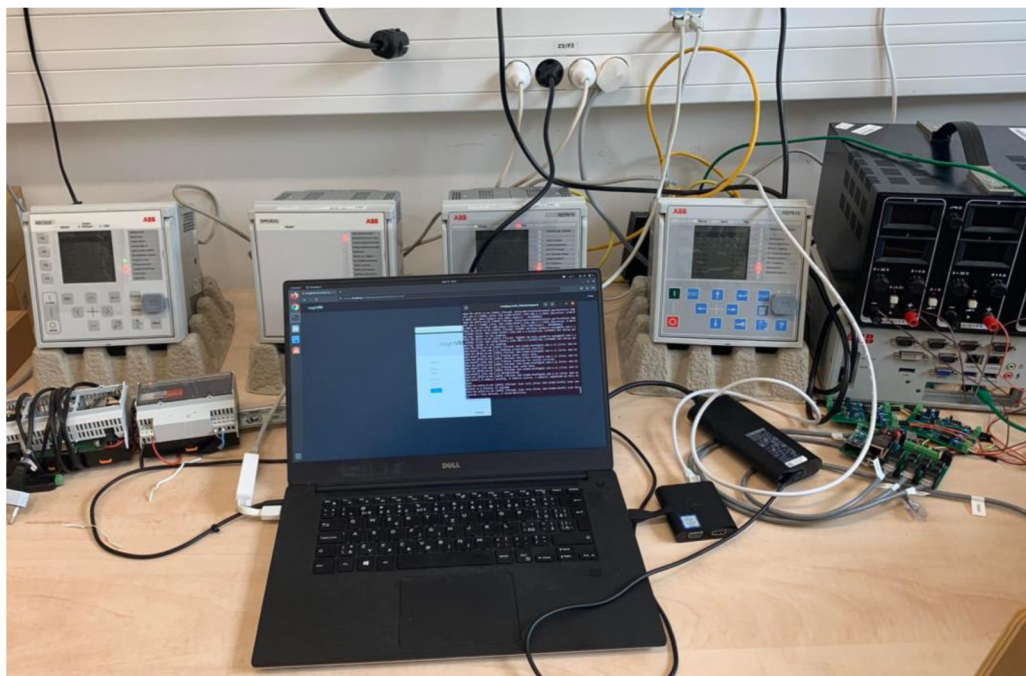
3.2.1 Zhrnutie

Rizikovosť jednotlivých kybernetických útokov závisí od viacerých faktorov, najmä aktuálneho stavu bezpečnostných mechanizmov nasadených v prostredí a potencionálne dopady na základné bezpečnostné požiadavky CIA triády v prípade úspešnosti útoku. Použitím vybranej metódy analýzy rizík budú v práci hodnotené testované zraniteľnosti, ktoré vyplývajú z implementácie súborov noriem IEC 61850 a IEC 60870. Vďaka jednotnej forme hodnotenia rizikovosti bude možné využiť teoretický základ analýzy rizík pre vlastnú adaptáciu a praktické prevedenie analýzy pre podklad navrhovania mitigačných opatrení.

4. TESTOVACIE PROSTREDIE

V rámci semestrálnej práce bolo pripravené prostredie, ktoré bude následne využité pre praktické testovanie vybraných kybernetických útokov a návrhu mitigačných opatrení. Prostredie sa skladá z desktopového počítača s operačným systémom Windows 10 Pro, ktorý je sieťovo pripojený ku dvom IED REF615 zariadeniam a jednému RER615, ktoré podporujú súbor noriem IEC 61850. Vo vytvorenom testovacom prostredí je využívaný software Teamviewer, ktorý umožňuje vzdialený prístup ku GUI desktopového počítača a ktorý je využívaný na vzdialenú správu prostredia. Teamviewer pre komunikáciu využíva cloudové servery v doméne *.teamviewer.com a špecifický TCP/UDP port 5938 alebo štandardne používané TCP 443 a TCP 80.

Ochranné zariadenia REF615 budú slúžiť ako cieľ testovaných kybernetických útokov. Pre účely vykonávania reálnych útokov je do testovacieho prostredia pripojený laptop DELL s operačným systémom Ubuntu, inštaláciou software Nexpose a virtuálnou distribúciou Kali Linux. Sieťové prepojenie všetkých prvkov testovacieho prostredia je realizované prostredníctvom nemenežovateľného switchu a priradeniu adresácie 192.168.2.0/24. Jedná sa o oddelenú privátnu podsieť bez akéhokoľvek ďalšieho sieťového prestupu. Východiskovou bránou je windowsový stroj, ktorý disponuje dvomi sieťovými rozhraniami, prestupom do WAN a inštaláciou aplikácie PCM600 čím zároveň pre prostredie slúži ako inžinierska stanica.



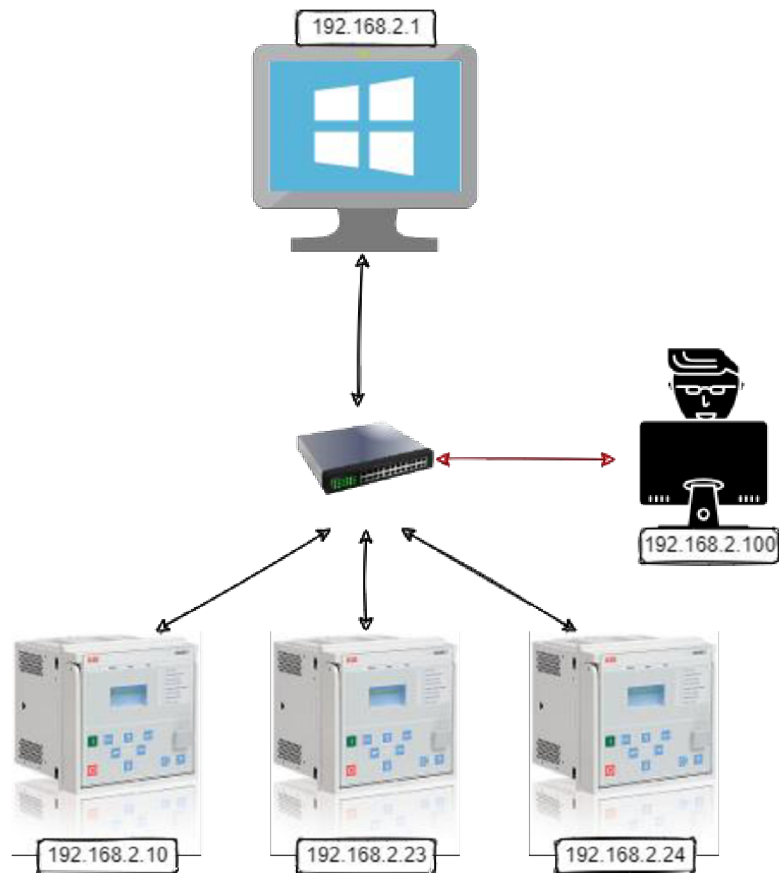
Obrázok 4.1 Zapojenie útočnického stroju k IED zariadeniam.

4.1 IED REF615

IED REF615 je špecifické zariadenie vývodu určené pre chránenie, ovládanie, meranie a monitorovanie systémov v rozvodniach energetických spoločností aj v energetických systémoch priemyselných podnikov, vrátane radiálnych, okružných a zauzlených distribučných sietí s distribuovanou výrobou aj bez výroby elektrickej energie. Použité REF615 sú výrobkom produktovej skupiny Relion® firmy ABB. Zariadenia podporujú celú radu protokolov vrátane protokolu IEC 60870-5 a IEC 61850 vrátane časovo kritického protokolu GOOSE.

Na konfiguráciu signálov bude využitá grafická aplikačná funkcia nástroja PCM600 (Protection and Control IED Manager), ktorá zároveň podporuje tvorbu viacvrstvových logických funkcií, ktoré v kombinácii sa ochrannými funkciami umožňujú IED prispôbiť aj náročnejším aplikačným požiadavkám. Komunikácia medzi PCM600 a IED zariadeniami prebieha na sieťovej vrstve ISO/OSI [30]. Schéma zapojenia s pridruženými IP adresami použitými pre komunikáciu je zobrazená na obrázku 4.2, zobrazenom nižšie.

Medzi základné vlastnosti REF615 patrí napríklad monitorovanie signálu, riadenie komunikácie, aplikačné konfigurácie alebo zobrazenie zmenových stavov udalostí a disponuje množstvom ochranných a kontrolných funkcií.



Obrázok 4.2 Schéma zapojenia testovacieho prostredia.

4.1.1 Ovládanie

REF615 disponuje možnosťou ovládania lokálne cez čelný panel (LHMI) s LCD displejom alebo diaľkovým riadením (WHMI, COM600, PCM600). Okrem bloku pre ovládanie vypínača je IED vybavené aj dvoma blokmi riadenia, ktoré sú určené pre ovládanie odpojovača alebo podvozku vypínača s motorovým pohonom a pre indikáciu polôh týchto prvkov. IED ďalej ponúka jeden blok riadenia, ktorý je určený pre ovládanie jedného uzemňovača s motorovým pohonom a pre indikáciu jeho polohy. [29]

4.1.2 Komunikácia

REF615 disponuje natívnou podporou štandardu IEC 61850 vrátane horizontálneho prenosu binárnych a analógových správ GOOSE. Podporuje aj procesnú zbernicu so vzorkovanými hodnotami analógových fázových napätí. Disponuje rýchlou komunikačnou schopnosťou, trvalou kontrolou integrity systému ochrán aj komunikačného systému a značnou flexibilitou. IEC 61850 podporuje všetky monitorovacie a kontrolné funkcie. Použitím protokolu IEC 61850-8-1 sa okrem toho sprístupnia záznamy porúch a poruchové zápisy. Súbor záznamov porúch sú k dispozícii v štandardnom formáte COMTRADE pre akúkoľvek aplikáciu, ktorá pracuje na báze Ethernetovej komunikácie. Implementácia komunikačného profilu IEC 61850-8-1 GOOSE umožní vysielat' dáta binárnych signálov z IED a tieto dáta tiež prijímať z iných IED (3ms). Podporuje aj vysielanie a príjem analógových dát a vypínanie prostredníctvom správ GOOSE a komunikáciu až s 5 rôznymi klientami na zbernici. Súhrn všetkých podporovaných komunikačných protokolov predstavuje tabuľka 4.1.

Tabuľka 4.1 Podporované TCP/UDP porty

Číslo portu	Typ	Default stav	Popis
20, 21	TCP	Otvorený	FTP,FTPS
102	TCP	Otvorený	IEC 61850
80	TCP	Uzatvorený	Web Server HTTP
443	TCP	Uzatvorený	Web Server HTTPS
123	UDP	Neaktívny	NTP
502	TCP	Uzatvorený	Modbus TCP
2000	TCP	Uzatvorený	DNP TCP
2000	UDP	Uzatvorený	DNP UDP

REF615 podporuje vertikálnu komunikáciu mapovaním podľa IEC 61850-8-1. Ochrany REF615 môžu súčasne sprístupniť dáta až piatim klientom (pokiaľ sa nejedná o ovládanie primárnych prvkov). V rámci služby MMS je poskytovaný zber dát a monitoring.

Podporované komunikačné protokoly:

- IEC 61850 – GOOSE, SMV a MMS
- Protokoly časovej synchronizácie – IEEE 1588 (PTP), HSR/PRP (IEC 62439-3), SNMP a IRIG-B
- Ďalšie protokoly - DNP3, Modbus, RSTP a Profibus DPV1

4.1.3 Natívna bezpečnosť

REF615 podporuje autentizáciu, preverovacie záznamy (audit trail), zabezpečenie prístupu ku konfigurácii a prenos súborov. Ochrany uchovávajú až 2048 udalostí v audit trail a 1024 procesných udalostí v event list. Tieto zoznamy fungujú na princípe FIFO (First in First out). Logované sú tu napríklad udalosti spojené s prihlásením ako Login/Logout a Violation remote/local - z IEC 61850-8-1 (MMS), WHM, FTP alebo LHMI, zmenou času, kde sa ale neloguje legitímna synchronizácia s dedikovaným protokolom (SNTP, IRIG-B, IEEE 1588 v3) a napríklad užívateľské auditné udalosti podľa IEEE 1686, ktoré sú dostupné cez IEC 61850-8-1, PCM600, LHMI a WHMI..

Ochrany REF615 disponujú 3 úrovňami zabezpečenia súborov. Pri nízkej úrovni zabezpečenia nie je vykonávaná žiadna kontrola podpisu nahrávaného súboru. Pri strednej úrovni je vykonávané overovanie digitálneho podpisu každého binárneho súboru pred jeho nahratím a pri vysokej úrovni zabezpečenia je vykonávané vylepšené overenie podpisu binárnych súborov, čím REF615 adresuje požiadavku integrity. Žiadne heslá v REF615 nie sú ukladané v čistom texte, ale šifrované pomocou hashovacej funkcie SHA256 a sú na nich kladené bezpečnostné požiadavky pri ich vytváraní. Požiadavky na heslo pre LHMI sú: 4-8 znakov, a pre WHMI: 9-20 znakov, pričom za znak sú považované čísla 0-9, písmená a-z, A-Z, medzera a špeciálne znaky "#%&'()*+,-./:;<=>?@[\\]^_`{|}~). [35]

Ochrana prístupu je riešená pomocou protokolu DAA (HTTP Digest Access Authentication) podľa RFC2617 vo forme „užívateľské meno“ + „heslo“. Tabuľka Tab. 6-3 predstavuje prehľad možností užívateľov.

REF615 ďalej disponuje bezpečnostným parametrom „Secure Communication“, ktorý automaticky vynúti využitie TLS pre WHMI a FTPS pre prenos súborov, kde TLS spojenie je šifrované pomocou AES256 alebo AES128 algoritmu a kľúč pre šifrovací algoritmus je zdieľaný pomocou RSA kľúčového páru.

Tabuľka 4.2 Prehľad možností užívateľov

Typ užívateľa	Práva užívateľa	LHMI default heslo	WHMI default heslo
Viewer	Read only	"0001"	"remote0001"
Operator	Kontrola, zmena setting groups,...	"0002"	"remote0002"
Engineer	Zmena nastavení, premazanie listov,...	"0003"	"remote0003"
Administrator	Všetko + zmena hesiel, factory reset, logy...	"0004"	"remote0004"

4.1.4 Zhrnutie

REF615 od spoločnosti ABB podporujú plné spektrum funkcií ochrany, kontroly alebo monitoringu rozložených do variabilných konfiguračných profilov. Pre zaistenie operácie a konfigurácie funkcií zariadení, disponujú podporou pre viaceré komunikačné protokoly vrátane štandardizovaných protokolov (napr. IEC 61850).

Z pohľadu bezpečnosti ale disponujú minimálnymi mechanizmami pre zaistenie základných bezpečnostných požiadaviek na dôvernosť, integritu a dostupnosť.

Vďaka podpore analyzovaných komunikačných protokolov a minimálnym bezpečnostným mechanizmom sú REF615 považované za vhodný prostriedok pre testovanie potenciálnych kybernetických hrozieb a návrh relevantných opatrení v rámci tejto práce.

5. METODIKA KYBERNETICKÝCH ÚTOKOV

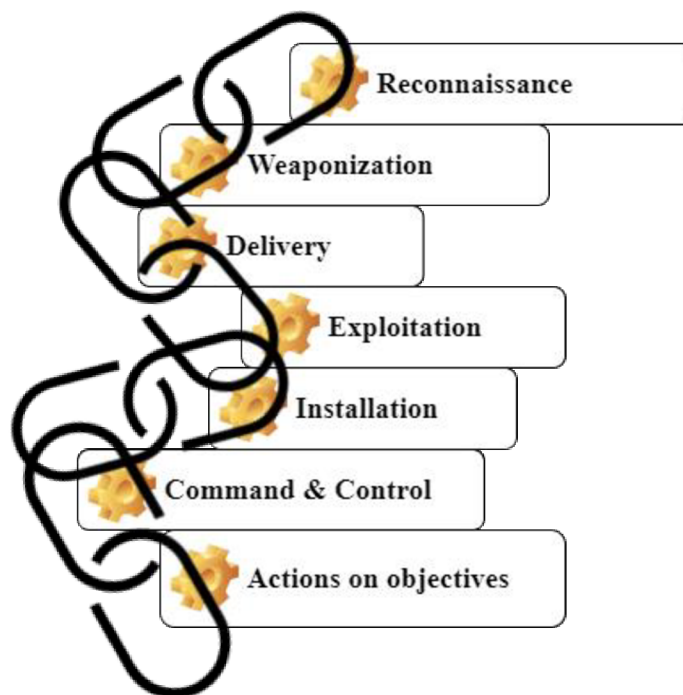
Úspešné vykonanie kybernetického útoku je vo všeobecnosti komplexný proces pozostávajúci hneď z niekoľkých fáz a často aj rôznych predispozícií a premenných. V rámci kapitoly je preto najprv venovaná pozornosť teoretickej rovine zostavenia kybernetického útoku. Predstavený je metodický základ kybernetických útokov využiteľný špecificky pre priemyselné kontrolné systémy. Metodický základ je v ďalšej časti kapitoly aplikovaný v praktickej rovine na zostavenie jednotlivých testov.

5.1 Metodický základ

Pre získanie prehľadnosti a porozumenia v rámci celého životného cyklu kybernetického útoku boli vyvinuté štruktúry, ktoré identifikujú a mapujú jednotlivé kroky útočníka pri podnikaní kybernetického útoku. Vyvinuté štruktúry poskytujú bezpečnostným pracovníkom a akademikom východiskový bod pre testovanie bezpečnosti ale aj nasadzovanie bezpečnostných opatrení. Medzi najznámejšie štruktúry kybernetických útokov patrí Cyber Kill Chain® a MITRE ATT&CK.

Cyber Kill Chain, vytvorená bezpečnostným kontraktorom Martinom Lockheed, aplikuje tradičnú vojenskú koncepciu útoku na kybernetický útok. Štruktúra rozkladá útok do presne definovanej sekvencie siedmich fáz od prieskumu po akcie na dosiahnutie cieľov. Zámer takéhoto reťazca je zlepšiť obranu pomocou analýzy útočnickeho správania a zabránenie aktívnemu útoku pomocou narušenia reťazca v ktoromkoľvek bode. Jednotlivé kroky sú zobrazené na obrázku 5.1.

MITRE ATT&CK, vydaná neziskovou organizáciou The MITRE Corporation v roku 2015, je neustále sa rozvíjajúci rámec spoločných taktík, techník a postupov (TTP) využívaných hackerskými skupinami a jednotlivcami, ktoré spoločnosť sprístupňuje súkromnému sektoru, vládam, profesionálom v oblasti kybernetickej bezpečnosti aj širokej verejnosti. Na rozdiel od Cyber Kill Chain, ATT&CK mapuje a indexuje útoky do matice a to z pohľadu oboch strán, útočníka aj obrancu. V roku 2020 bola spoločnosťou vydaná matica taktík, techník a postupov špecializujúca sa na priemyselné riadiace systémy (ICS), ktorej znázornenie predstavuje obrázok 5.2.



Obrázok 5.1 Vizualizácie fáz rámcu Attack Kill Chain.

Cyber Kill Chain je skvelým východiskom pri počítačových návrhoch bezpečnostných analýz a architektúr. Pri dnešnej dynamickosti a sofistikovanosti kybernetických útokov sa ale môže stať, že tento teoretický model sa v praxi zjaví ako nedostatočný napríklad z dôvodu nedostatočnej škálovateľnosti a rozvoja. Množstvo bezpečnostných profesionálov a vendorov sa preto pri implementácii bezpečnostných postupov a riešení riadi ATT&CK maticou a vedomostnou základňou, ktorú spoločnosť MITRE Corporation ponúka. Pre účel zjednotenia teoretickej základne celého procesu testovania, hodnotenia a mitigovania kybernetických útokov a širokého spektra možností využitia je pre metodiku použitá štruktúra MITRE ATT&CK.

5.2 MITRE ATT&CK pre ICS

MITRE ATT&CK pre ICS sa po architektonickej stránke zameriava na systémy a funkcie spojené s funkčnými úrovňami 0 - 2 architektúry Purdue, ktoré sú zároveň primárnym cieľom útočníkov. Jedná sa o základné kontrolné systémy ako sensory, pumpy, ventily a podobne na nulte úrovni, distribuované kontrolné systémy a PLC na prvej úrovni a inžinierske stanice a HMI na úrovni druhej. Systémy spájané s vyššími funkčnými úrovňami sú pokryté v pôvodných podnikových maticiach, kde je primárne zameranie na IT technológie najmä v spojitosti s windowsovými a linuxovými platformami. Matica pre ICS reaguje na konvergenciu IT a OT technológií a preto využíva podnikové matice ako základ pre systémy nachádzajúce sa na prelome ako napríklad PLC, HMI alebo RTU. Samotná štruktúra matice sa skladá z taktík, na ktoré sú nadviazané konkrétne techniky, postupy a mitigácie. [35]

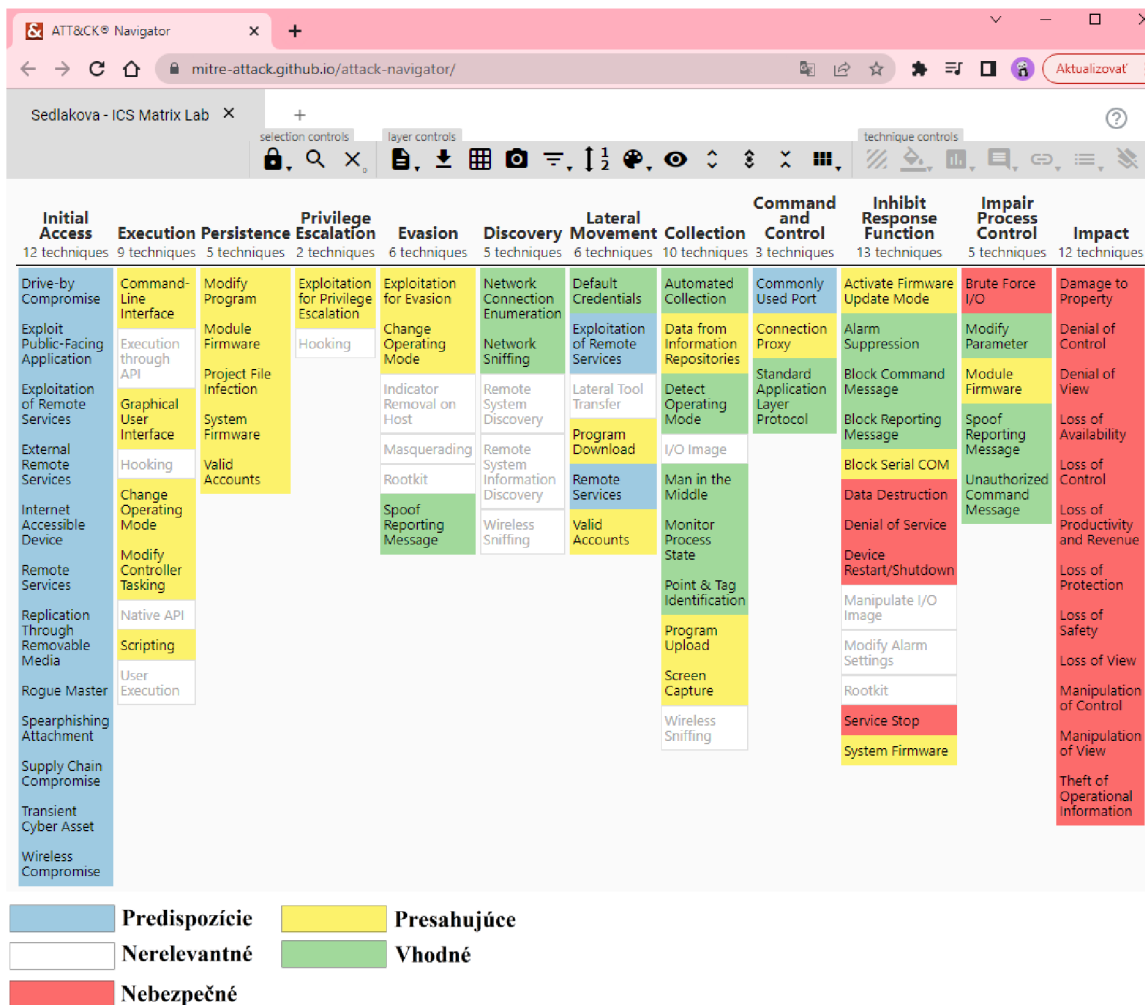
Tabuľka 5.1 Prehľad a stručný popis taktík MITRE ATT&CK pre ICS

Taktika	Popis
Initial Access	Útočník sa snaží preniknúť do prostredia ICS.
Execution	Útočník sa pokúša spustiť kód alebo manipulovať systémovými funkciami, parametrami a údajmi.
Persistence	Útočník sa snaží zachovať svoju pozíciu v cieľovom ICS prostredí.
Privilege Escalation	Útočník sa snaží získať povolenia vyššej úrovne na systéme alebo v sieti.
Evasion	Útočník sa snaží vyhnúť povšimnutiu bezpečnostnej obrany.
Discovery	Útočník vyhľadáva dostupné informácie k vyhodnoteniu a identifikácii cieľov.
Lateral Movement	Útočník sa snaží pohybovať v rámci prostredia ICS.
Collection	Útočník sa snaží zhromaždiť zaujímavé a relevantné dáta o cieľovom prostredí pre vyhodnotenie cieľov a techník.
Command and Control	Útočník sa snaží komunikovať a zároveň kontrolovať napadnuté systémy vďaka prístupu do cieľového prostredia.
Inhibit Response Function	Útočník sa snaží zabrániť tomu, aby rôzne bezpečnostné mechanizmy reagovali na vytvorenú poruchu, nebezpečenstvo alebo neštandardný stav.
Impair Process Control	Útočník sa snaží zmanipulovať, deaktivovať alebo poškodiť procesy fyzického zariadenia.
Impact	Útočník sa pokúša zmanipulovať, prerušiť alebo zničiť cieľové ICS systémy, dáta a ich okolité prostredie.

Matica disponuje mapovaním bezpečnosti naprieč celým priemyselným odvetvím a nie je preto aplikovateľná priamo v surovej forme na akékoľvek prostredie. Je dôležité maticu revidovať a prispôbiť konkrétnemu prostrediu, na ktoré sa bude implementovať. Priamo MITRE Corporation ponúka viaceré nástroje použiteľné pre revíziu a prispôbenie štruktúry:

- ATT&CK Navigator - webový nástroj na anotovanie, skúmanie a vizualizáciu matic.
- ATT&CK Workbench - aplikácia umožňuje používateľom skúmať, vytvárať, komentovať a zdieľať rozšírenia vedomostnej základne ATT&CK.
- ATT&CK Python Utilities - množstvo Python skriptov využiteľných na priamu prácu s ATT&CK alebo ako príklady pre programátorskú prácu s ATT&CK.

Pre vizualizáciu relevantných techník bol použitý nástroj ATT&CK navigator a výsledný stav znázorňuje obrázok 5.2.



Obrázok 5.2 Plánovanie testovacích techník v online nástroji MITRE ATT&CK® Navigator, od spoločnosti The MITRE Corporation, dostupnom na: <https://mitre-attack.github.io/attack-navigator/>.

5.2.1 Nerelevantné techniky

V prvej fáze boli oddelené techniky, ktoré nie sú pre vytvorené testovacie prostredie relevantné. Jedná sa o techniky zneužívajúce API, užívateľskú interakciu, potlačenie a modifikáciu alarmov, bezdrôtové technológie, vzdialené technológie, rootkity a I/O.

5.2.2 Predispozície

Prvou podmienkou pre vykonanie akéhokoľvek útoku v energetickej sieti je dosah útočníka na daný cieľový systém. Tento prienik je možné dosiahnuť hneď niekoľkými vektormi, medzi ktoré patrí napríklad fyzický prístup k cieľovému zariadeniu, infikovanie užívateľského, testovacieho alebo inžinierskeho počítaču, ktorý je pripojený k cieľovému zariadeniu alebo staničnej zbernici, kompromitácia úložiska nastavení a testovacích dokumentov, kompromitácia riadiaceho centra, zraniteľnosti v známych protokoloch, databázové útoky, prípadne kompromitácia sieťových prvkov. Takýto prienik je pre

testovanie kybernetického útoku nevyhnutný a pre účel práce sú preto techniky spájané s prvotným prienikom do siete považované za predispozičné.

5.2.3 Presahujúce

Ďalšou oddelenou skupinou sú techniky, ktorých podstata je zacielená na PLC zariadenia, inžinierske a operačné stanice a napríklad grafické užívateľské rozhrania. Tieto systémy nie sú primárnym predmetom záujmu práce a preto nebudú testované dopodrobna. Nakoľko je ich význam pre bezpečnosť rozvodne a celkovo ICS veľmi dôležitý, je predstavený teoretický rámec ich využiteľnosti. Využitiu techník opäť predchádza požiadavka dosahu útočníka na cieľový systém, ako je popísané v kapitole 5.2.2.

5.2.4 Vhodné

Pre účel práce najdôležitejšou kategóriou sú techniky označené ako vhodné a ktorých praktickému aplikovaniu a popisu sa venuje podkapitola 5.3.

5.2.5 Nebezpečné/Deštruktívne

Poslednou kategóriou sú techniky, ktoré môžu na systéme spôsobiť mierne odchýlky, oneskorenia, dočasnú nedostupnosť služieb a celého systému až trvalé následky. Využitie týchto techník pre testovanie bezpečnosti v ICS je odporúčané iba v izolovanom testovacom prostredí.

5.3 Útoky na testovacie prostredie

Vybrané kybernetické útoky sú na prostredí testované v troch fázach. Prvú fázu tvorí prieskum prostredia, kde sú využité najmä taktiky Discovery a Collection z ATT&CK rámca. Druhá fáza sa zameriava na vyhodnotenie získaných informácií z prvej fázy a vytvára tak podklady, stanovuje ciele a navrhuje techniky pre ďalšie pokračovanie testovania. Tretiu fázu tvorí samotná realizácia kybernetického útoku, ktorá využíva zvyšné taktiky ako napríklad Impair Process Control alebo Evasion.

5.3.1 Fáza 1: Prieskum

Prieskum prostredia a zber relevantných informácií sú najčastejšie využívané počiatočné body kybernetických útokov alebo etického penetračného testovania v bežných IT prostrediach, a je možné ich aplikovať aj na OT prostredia. V tejto fáze sa útočníci snažia zmapovať prostredie spolu so všetkými jeho aktívnymi a pasívnymi prvkami a získať čo najviac informácií o aktívach, užívateľoch a napríklad typoch dát a rôznych interakcií. Pre tieto úkony sú obvykle používané nástroje na zachytávanie sieťovej prevádzky a prípadne sociálne inžinierstvo. Sociálne inžinierstvo je technika zneužívajúca nepozornosť a nevedomosť ľudského faktora. Nakoľko v laboratórnom prostredí bol jediným ľudským faktorom útočník, pre túto fázu sú využité iba sieťové nástroje.

Predispozíciou pre zachytávanie sieťovej prevádzky je priamy dosah útočníka na danú sieť a to kompromitovaním aktívneho alebo pasívneho prvku. Vo vytvorenom laboratórnom prostredí bola táto predispozícia dosiahnutá fyzickým zapojením útočnickej stanice do nemenežovateľného switchu, ktorý pracuje na druhej vrstve referenčného modelu ISO/OSI. Následne bola stroju staticky priradená adresa z rovnakého subnetu, v akom sa nachádzajú ciele. Po úspešnom splnení predispozícií je možné pristúpiť k ďalšiemu kroku, ktorým je výber vhodného nástroja.

5.3.2 Nástroje na sieťový prieskum

Sieťových nástrojov vyvinutých na prieskum prostredia je v dnešnej dobe mnoho, ale len niektoré z nich sú prispôsobené špecifikám ICS technológií. Postupne dokonca vznikajú aj bezpečnostné nástroje špecificky zamerané na ICS prostredia. Takýmto nástrojom je napríklad mladá, ale aktívne vyvíjaná linuxová distribúcia ControlThings I/O, ktorej predchodcami boli distribúcie SamuraiWTF a SamuraiSTFU. Distribúcia ponúka zopár vstavaných nástrojov špecializovaných na bezpečnostné hodnotenie a interakciu s binárnymi sériovými zariadeniami, so zariadeniami využívajúcimi Modbus (TCP/UDP aj sériovými (RTU/ASCII)), s EEPROM, Flash čipmi a ďalšími vstavanými čipmi pomocou SPI alebo I2C a na interakciu s PLC Velocio. Okrem spomínaných funkcií disponuje distribúcia platformou pre vytváranie vlastných nástrojov. Ďalej existujú verejne dostupné špecializované skripty, pluginy a nadstavby na už existujúce nástroje ako napríklad na knižnicu libiec61850 alebo sieťový nástroj scapy. Napriek tomu, že majú tieto nástroje značný potenciál, ich vývoj bol vo väčšine prípadov pozastavený, dokumentácia limitovaná alebo ich účel jednosmerný. Ich využitie je preto často sprevádzané s nutnosťou časovej investície na riešenie problémov a závislostí. Z tohto dôvodu sa realizácia fáze 1 vykoná pomocou známych a overených nástrojov. Tabuľka 5.2 predstavuje často používané prieskumné nástroje zaradené podľa typu. Hlavným zámerom je využitie skeneru zraniteľností z dôvodu jeho komplexity, nakoľko takýto nástroj často priamo využíva skenery portov aj webových služieb.

Tabuľka 5.2 Prehľad nástrojov na vykonanie prieskumných útokov

Skenovanie portov	Webové služby	Skeny zraniteľností
NMap	Nikto	Nexpose
Netcat	Burp Suite	Nessus
Advanced Port Scanner	ZAP	OpenVAS

Všeobecne najvyužívanejším skenerom zraniteľností medzi penetračnými testerami je Nessus od spoločnosti Tenable. Nessus primárne slúži pre komerčné využitie a ponúka možnosť 7-dňovej trial licencie pre testovacie účely. Okrem skeneru zraniteľností Tenable ponúka napríklad riešenie `tenable.ot` slúžiace na inventarizáciu aktív, správu zraniteľností, forenznú podporu a konfiguráciu ovládacích prvkov v rámci OT prostredia.

Konkurenčným riešením je skener zraniteľností Nexpose od výrobcu Rapid7. Jedná sa taktiež o komerčný produkt, ale bez možnosti trial licencie. Významnou výhodou oproti Nessusu je priame napojenie na Metasploit, svetovo najpoužívanejší nástroj na penetračné testovanie, ktorý je taktiež pod záštitou Rapid7. V rámci zamerania na OT disponuje Nexpose možnosťou spojenia s treťostranovým doplnkom SCADAfence, vďaka čomu je možné dosiahnuť hlbší prehľad nad OT infraštruktúrou a jej rizikami.

OpenVAS je open-source skenovací nástroj od spoločnosti Greenbone Networks, ktorý plne vystačí na bežné hodnotenie zraniteľností v IT svete. V porovnaní s komerčnými skenermi ale nie je na OT infraštruktúru dostatočne pripravený a pri jeho spustení by mohlo dôjsť k výraznému ovplyvneniu produkcie.

Útočníkova stanica disponuje softwarom Nexpose, ktorý bol pre účel vykonania prieskumnej fázy zapožičaný od spoločnosti COMGUARD a.s.. Spoločnosť COMGUARD sa špecializuje na oblasť bezpečnosti informačných technológií, produktov a služieb v pozícii distribútora s pridanou hodnotou. Na stanici je taktiež nasadená virtualizovaná linuxová distribúcia Kali cez platformu VirtualBox. Distribúcia Kali bude využitá v neskoršej fáze na vykonanie Man-in-the-Middle útoku.

Skener Nexpose disponuje intuitívnym webovým grafickým rozhraním, cez ktoré sa manažuje celý proces prieskumu od konfigurácie konkrétnej inštancie skenu až po reporting. Už v základe prichádza s viacerými preddefinovanými šablónami, vrátane šablóny určenej ku prieskumu SCADA a priemyselných systémov s názvom SCADA audit. Táto šablóna bola duplikovaná a upravená tak aby bola k cieľovým systémom čo najšetrnejšia. Výsledkom bolo odhalenie živých aktív 192.168.2.1, 192.168.2.10, 192.168.2.23 a 192.168.2.24, využívaných služieb a potencionálnych zraniteľností.

SERVICES

Service Name	Port	Protocol	Vulnerabilities	Users	Groups
FTP	21	TCP	0	0	0
iso-tsap (tsap ISO-TSAP Class 0)	102	TCP	0	0	0

VULNERABILITIES

Vulnerability	Severity	Instances
TLS/SSL Birthday attacks on 64-bit block ciphers (SWEET32)	Severe	1
TLS Server Supports TLS version 1.0	Severe	1
TLS/SSL Server is enabling the BEAST attack	Severe	1
TLS Server Supports TLS version 1.1	Moderate	1
TLS/SSL Server Supports The Use of Static Key Ciphers	Moderate	1
TLS/SSL Server Supports 3DES Cipher Suite	Moderate	1

Obrázok 5.3 Výstup objavených služieb a zraniteľností z Nexpose.

Za živé aktívum sa považuje stroj, ktorý odpovedá na sieťové výzvy. Typicky sa jedná o využitie protokolov ICMP, ARP alebo TCP. Na odhalenie aktív využíva Nexpose priamo nástroj nmap so špeciálnymi parametrami tak, aby zariadenia nezahltli a nespôsobili im tak stav DoS. Pokiaľ by bol využitý nástroj nmap samostatne, jeho spustenie by obsahovalo špeciálny parameter `-sT`, ktorý zabezpečí aby bola každá otvorená relácia aj správne ukončená. Týmto úkonom sa predchádza vytvoreniu veľkého počtu polo-otvorených relácií, ktoré by mohli mať negatívne až kritické dopady na prevádzku. Príklad takéhoto skenu je uvedený na obrázku 5.4, ktorý popisuje bezpečný prieskum zariadení z IP rozsahu 192.168.2.1-192.168.2.99 so zameraním na konkrétne porty.

```
(root@ DESKTOP-FLCH5SN) - [~/kali]
# nmap -sT --scan-delay 1s -p 21,80,102,443,2404 192.168.2.1-192.168.2.99
```

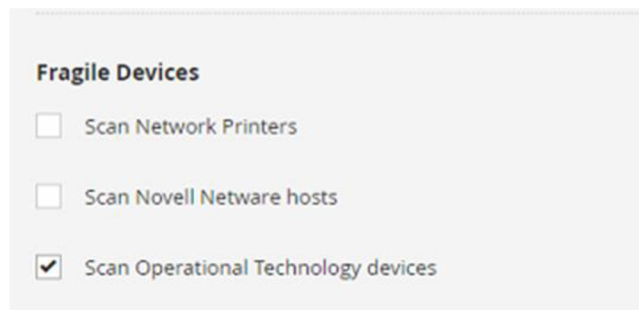
Obrázok 5.4 Príkladná ukážka spustenia skenu so špeciálnym parametrom.

Rovnaký prieskum bol vykonaný aj za pomoci software Nessus, ktorý bol inštalovaný priamo na windowsovú stanicu 192.168.2.1. Jedná sa o ľahký software, ktorý na lokálnom porte TCP 8834 otvorí prístup na webové rozhranie, cez ktorý sa jednotlivé inštancie skenov riadia. Webové rozhranie je dostupné na adrese <https://localhost:8834>.

```
C:\Users\labSG>netstat -aof | findstr :8834
TCP    0.0.0.0:8834          DESKTOP-FLCH5SN:0    LISTENING           8092
TCP    [::]:8834           DESKTOP-FLCH5SN:0    LISTENING           8092
```

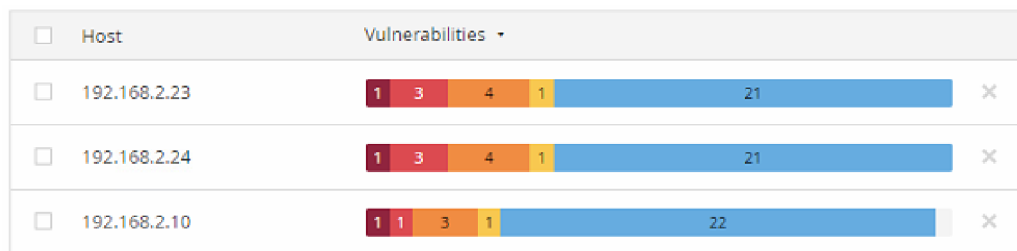
Obrázok 5.5 Zobrazenie počúvania na porte TCP8834 službou s ID 8092.

Vo webovom rozhraní sa definujú ciele skenu, metódy, plugíny, následne je sken uložený a pripravený na spustenie. Pozornosť bola vzťahnutá na špeciálne nastavenie šetrnosti skenu, kde Nessus priamo disponuje možnosťou označiť ciele za zariadenia OT. Toto nastavenie zapríčini, že sa sken prepne do takzvaného pasívneho stavu a nespôsobí zariadeniam záťaž ani škodu.

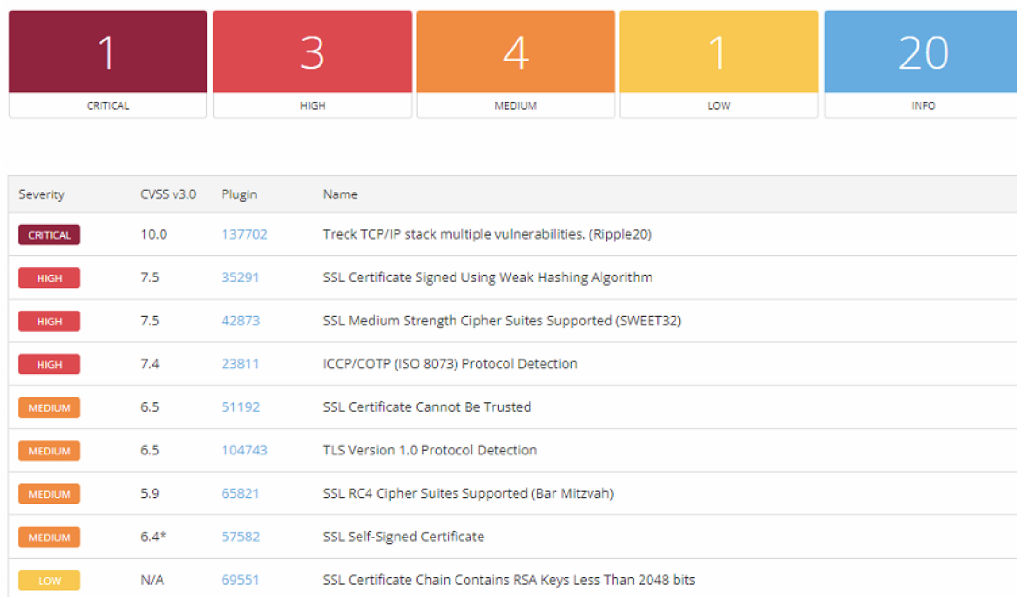


Obrázok 5.6 Definícia typu cieľových zariadení v rozhraní Nessus.

Výsledkom skenu bolo, podobne ako u Nexpose, odhalenie využívaných služieb a nájdenie potencionálnych zraniteľností, ktoré sú zobrazené na obrázkoch 5.7 a 5.8. Oproti Nexpose skenu došlo k odhaleniu potencionálnej kriticky závažnej zraniteľnosti nazývanej Ripple20. Jedná sa o sadu 19 zraniteľností objavených v implementácii TCP/IP spoločnosti Treck. Ďalšie odhalené zraniteľnosti boli veľmi podobné u obidvoch skenovacích nástrojov, ako napríklad zraniteľnosť sweet32 v slabej implementácii protokolu SSL alebo využívanie služby ICCP/COTP. Výsledky z automatických skenov nemusia byť vždy presné a preto je všeobecne odporúčané výskyt odhalených potencionálnych zraniteľností aj prakticky overiť v ďalších fázach penetračného testu.



Obrázok 5.7 Grafické zhrnutie počtu detegovaných zraniteľností z rozhrania Nessus.



Obrázok 5.8 Grafické znázornenie konkrétnych odhalených zraniteľností v rozhraní Nessus.

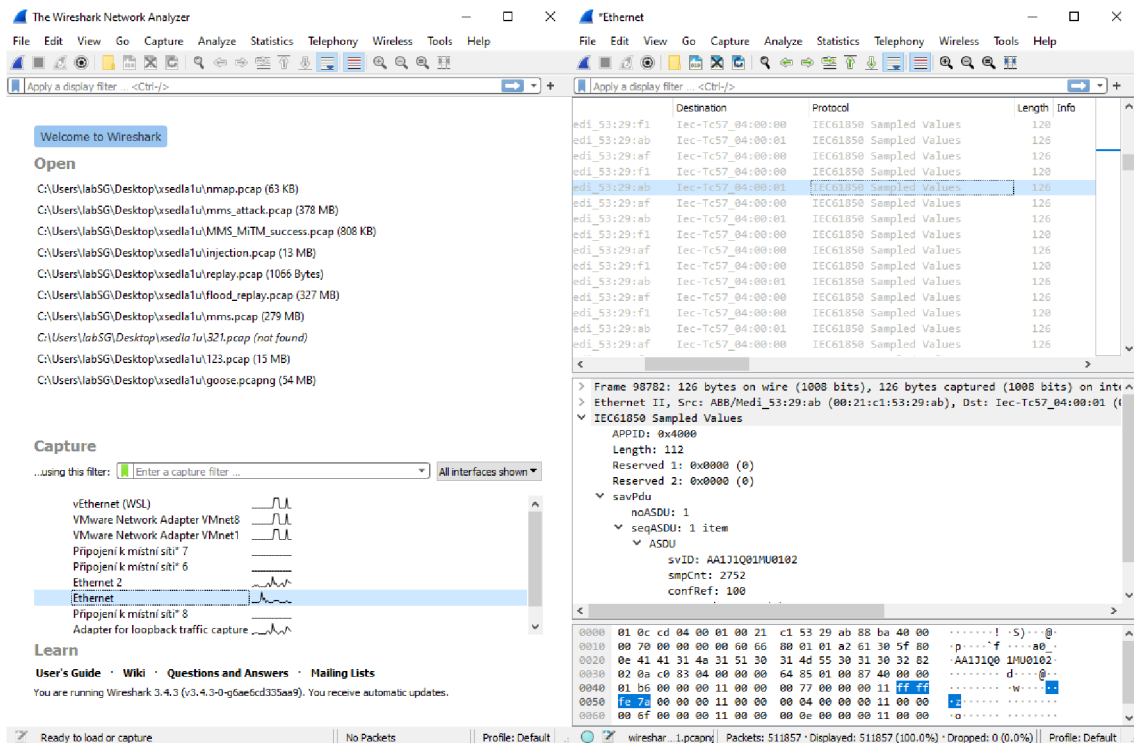
V priebehu celého trvania skenu nedošlo k narušeniu cieľových zariadení ani ich komunikácií vrátane služieb GOOSE a SMV. Tabuľka 5.3 poskytuje stručné porovnanie výsledkov oboch technológií, z ktorej je možné usúdiť, že Nessus je v základe lepšie pripravený na hodnotenie zraniteľností priemyselných technológií. Limitáciou porovnania je, že nedošlo k otestovaniu Nexpose rozšírenia od spoločnosti SCADAfence, ktoré sa špecializuje na OT kyberbezpečnosť.

Tabuľka 5.3 Porovnanie testovaných skenerov zraniteľností

Funkcia	Nexpose (Rapid7)	Nessus (Tenable)
Odhalenie aktív	Áno	Áno
Stav portov	Čiastočne	Áno
Zraniteľnosti	6	20
Trvanie skenu	40 minút	19 minút

Na základe informácií zo skenovacích nástrojov si je možné vytvoriť základný prehľad o prostredí, teda koľko živých aktív sa v ňom nachádza, aké služby sú využívané a na aké zraniteľné miesta je možné ďalšie fáze zamerať. Získaný prehľad do prostredia sa v ďalšom kroku prehĺbi vďaka odchyteniu a následnej analýze sieťovej prevádzky. Nakoľko je útočník pripojený do rovnakej siete s IED zariadeniami, môže vykonať odchyt rámcov/paketov priamo na svojom sieťovom rozhraní. K tomuto účelu je použitá tzv. Network Sniffing technika z ATT&CK rámcu.

Medzi najpoužívanejšie verejne dostupné nástroje patrí napríklad nástroj WireShark a Tcpdump. Tcpdump je nástroj sieťovej analýzy určený pre rýchlu prácu v príkazovom riadku. WireShark disponuje grafickým rozhraním a okrem zachytávania umožňuje sieťový tok uložiť, analyzovať alebo aj dešifrovať. Navyše je podporovaný na viacerých platformách a preto bol nainštalovaný ako na útočnický stroj tak aj na windowsovú inžiniersko-operačnú stanicu. Jeho funkcionality sú založené na knižniciach libpcap pre unixové distribúcie a Npcap alebo staršia WinPcap pre windowsové platformy. Knižnice je možné využiť na nekomerčné účely aj pre vývoj vlastných nástrojov určených na interakciu so sieťovou prevádzkou. Po spustení WireShark si používateľ zvolí na ktorom sieťovom rozhraní chce na prevádzku naslúchať. Obrázok 5.9 ukazuje nastavenie zachytávania na Windowsovej stanici, kde bolo zvolené fyzické rozhranie Ethernet, ktoré je pripojené do siete s IED zariadeniami, a príklad prehľadu zachytených rámcov.



Obrázok 5.9 Ukážka grafického rozhrania sieťového nástroja Wireshark.

5.3.3 Fáza 2: Analýza

Po zachytení toku dát prichádza na rad analytická fáza, v ktorej dochádza k ich preskúmaniu. V testovacom prostredí aktívne komunikujú tri IED zariadenia odosielaním IEC 61850 SMV rámcov, z ktorých dve posielajú aj IEC 61850 GOOSE rámce, čo potvrdzuje zachytená komunikácia aj výsledky zraniteľnostných skenov. Štruktúra zachytených rámcov je rozdelená na jednotlivé polia [33]:

- Preambula (8 bajtov),
- Hlavička MAC (16 bajtov) - obsahujúca cieľovú multicast MAC adresu definovanú ako 01:0c:cd:xx:xx:xx (6 bajtov) a zdrojovú MAC adresu IED zariadenia (6 bajtov),
- Voliteľné označenie priority a VLAN príslušnosti (4 bajty),
- Typ Ethernet (2 bajty) - fixná hodnota 0x88B8 pre GOOSE a 0x88ba pre SMV,
- APPID (2 bajty) - aplikačný identifikátor,
- Dĺžka (2 bajty) - počet oktetov PDU začínajúc od APPID,
- 2 x Rezervované (2 bajty),
- GOOSE/SMV PDU – Jednotlivé polia sú zobrazené v tabuľke 5.4 a tabuľke 5.5,
- FCS (4 bajty) - sekvencia kontroly rámca.

Tabuľka 5.4 Prehľad polí GOOSE PDU so stručnými informáciami

Pole	Dátový typ	Veľkosť	Popis
gocbRef	String	Max. 65 bajtov	Referencia inštancie GOOSE kontrolného bloku v rámci LLNO.
timeAllowedtoLive	Integer	Max. 2 bajty	Čas inkrementácie atribútu stNum a informácia o čase opakovania správy.
datSet	Integer	Max. 65 bajtov	Referencia súborov dát, ktorých hodnoty budú zasielané.
goID	String	Max. 65 bajtov	Špecifický identifikátor pridelený užívateľom.
t	Timestamp	Max. 8 bajtov	Čas inkrementácie atribútu stNum.
stNum	Integer	Max. 8 bajtov	Počítadlo inkrementované pri každom odoslaní správy GOOSE a detekovanej zmene hodnoty DataSet.
sqNum	Integer	Max. 8 bajtov	Aktuálne poradové číslo správy, inkrementované pri každom odoslaní GOOSE správy a počiatočnou hodnotou 0
Simulation/test	Boolean	Max. 1 bajt	Nastavené pokiaľ sa jedná o testovací rámec.
confRev	Integer	Max. 8 bajtov	Revízia konfigurácie a označenie zmeny.
ndsCom	Boolean	Max. 8 bajtov	Oznámenie o prípadnej potrebe zásahu v prípade pravdivej hodnoty.
numDataSetEntries	String	Max. 1 bajt	Počet záznamov súborov dát.
allData	List	Max. 65 bajtov	Zoznam užívateľom definovaných informácií.

Tabuľka 5.5 Prehľad polí SMV PDU so stručnými informáciami

Pole	Dátový typ	Veľkosť	Popis
noASDU	Integer	Max. 8 bajtov	Počet ASDU v rámci jedného APDU.
svID	String	Max. 65 bajtov	Špecifický identifikátor pridelený užívateľom.
smpCnt	Integer	Max. 8 bajtov	Počítadlo inkrementované pri každom odobratí novej vzorkovanej hodnoty.
confRev	Integer	Max. 8 bajtov	Revízia konfigurácie a označenie zmeny.
smpSynch	Enumeration	Max. 8 bajtov	Informácia o synchronizácii SMV.
PhsMeas1	List	Max. 65 bajtov	Aktuálne dáta

Okrem pravidelne odosielaných GOOSE a SMV rámcov boli v testovacom prostredí zachytené komunikácie protokolu MMS a FTPS. GOOSE/SMV rámce je možné cez WireShark odchytiť na ktoromkoľvek aktívne nachádzajúcom sa na lokálnej sieti, teda aj na útočnickej stanici, nakoľko sa jedná o multicastovú prevádzku typu publisher-subscriber. Komunikačné protokoly MMS a FTPS prebiehajú na aplikačnej vrstve ISO/OSI modelu a na komunikáciu vyžadujú dve zariadenia vzťahu klient-server. Odchytiť ich je preto možné priamo na jednom z komunikujúcich aktív, na aktívnom/pasívnom sieťovom prvku typu smerovač alebo prepínač alebo za pomoci techniky muža uprostred (Man in the Middle) uvedenej v ATT&CK rámci pod taktikou

Collection. Táto technika bude testovaná v nasledujúcej fáze útoku. Pre účely analýzy bola prevádzka zachytená na windowsovej stanici.

Príkladný paket z MMS komunikácie je uvedený na obrázku 5.10, z ktorého je možné spozorovať hneď niekoľko relevantných informácií:

1. Informácie o komunikujúcich zariadeniach - zdrojová IP 192.168.2.1 (klient) a cieľová IP 192.168.2.23 (server),
2. Mapovania na jednotlivé vrstvy ISO/OSI referenčného modelu,
3. Jedná sa o nešifrovanú prevádzku,
4. Jedná sa o MMS prevádzku typu potvrdenej služby,
5. Komunikácia je vo fáze dopytovania na VMD objekt pomocou služby GetNameList.

```

> Frame 1408458: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
> Ethernet II, Src: SpeedDra_9c:80:47 (00:13:3b:9c:80:47), Dst: ABB/Medi_53:29:ab (00:21:c1:53:29:ab)
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.23
> Transmission Control Protocol, Src Port: 50734, Dst Port: 102, Seq: 217, Ack: 185, Len: 36
> TPKT, Version: 3, Length: 36
> ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
> ISO 8327-1 OSI Session Protocol
> ISO 8327-1 OSI Session Protocol
> ISO 8823 OSI Presentation Protocol
▼ MMS
  ▼ confirmed-RequestPDU
    invokeID: 63
    ▼ confirmedServiceRequest: getNameList (1)
      ▼ getNameList
        ▼ extendedObjectClass: objectClass (0)
          objectClass: domain (9)
        ▼ objectScope: vmdSpecific (0)
          vmdSpecific

```

```

0000  00 21 c1 53 29 ab 00 13 3b 9c 80 47 08 00 45 00  -!-S) ... ;--G--E-
0010  00 4c 64 14 40 00 80 06 00 00 c0 a8 02 01 c0 a8  -Ld:@ ... .....
0020  02 17 c6 2e 00 66 79 43 89 4f 6d 29 2a 34 50 18  -...fyC -Om)*4P-
0030  04 03 85 a7 00 00 03 00 00 24 02 f0 80 01 00 01  -.....-$.....
0040  00 61 17 30 15 02 01 03 a0 10 a0 0e 02 01 3f a1  -a-0.....?-.
0050  09 a0 03 80 01 09 a1 02 80 00  -.....

```

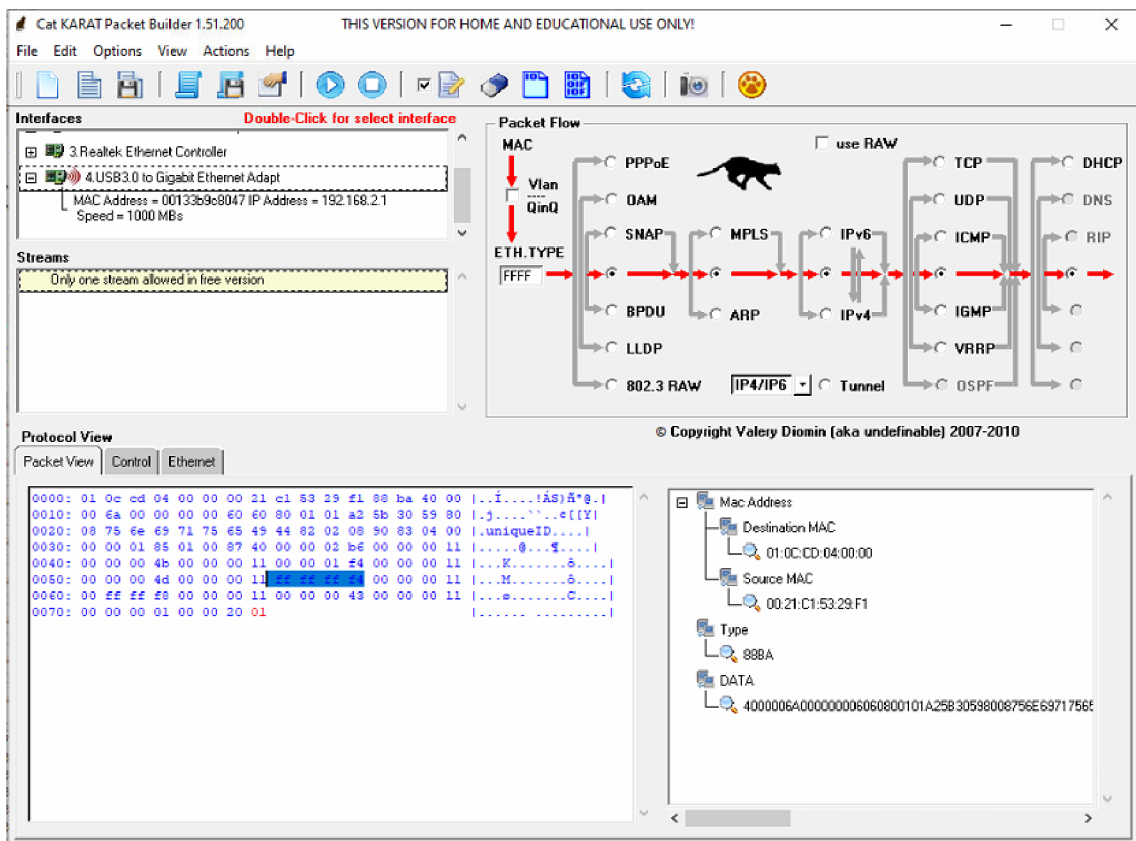
Obrázok 5.10 Ukážka zachyteného MMS paketu.

Vďaka početným získaným informáciám z predchádzajúcich fáz je možné pokračovať realizáciou cieleného kybernetického útoku. Využitie budú techniky z ATT&CK rámca predstaveného v kapitole 5.2, vyhodnotené za vhodné.

5.3.4 Fáza 3: Realizácia kybernetického útoku

Všetky zachytené dátové toky sú v rámci testovacieho prostredia zasielané bez použitia akéhokoľvek šifrovacieho alebo autentizačného mechanizmu. Zasluchou toho je možné do prevádzky nahliadať a analyzovať prenášané dáta. Okrem zmienenej viditeľnosti to ponúka príležitosť do prevádzky vkladať vlastné dáta alebo modifikovať stávajúce, na čo budú zamerané vykonané útoky. Komunikačné protokoly GOOSE a SMV definované v IEC 61850 sú spravidla odosielané multicastovo vydavateľom na L2 vrstve referenčného modelu ISO/OSI. Odberateľ túto prevádzku sleduje a vyčítava z nej relevantné dáta. Útočník by tak mohol takúto legitímnu prevádzku imitovať a vsadiť do

nej vlastné alebo modifikované dáta. Protokoly MMS alebo IEC 60870-5-104 využívajú až L7 vrstvu referenčného modelu ISO/OSI, čím sa komunikácia stáva komplexnejšou. Pre modifikovanie dát v rámci komunikácie sa preto využíva technika muža uprostred, v ktorej je legitímna komunikácia preposielaná obom stranám skrz prostredníka, ktorý následne môže jednotlivé správy aj napríklad upravovať alebo blokovať. Z dôvodu náročnej požiadavky na časové oneskorenie u správ GOOSE a SMV a všeobecnej limitácie zdrojov IED zariadení a podobných je reálne nasadenie odporúčaní IEC 62351 veľmi náročné. Komunikácia tak v praxi môže často ostať nešifrovaná a práve preto sú spomenuté techniky útočníkmi využívané najčastejšie. Pre účel úprav a následného odoslania rámcov do siete bol využitý nástroj Cat Karat Packet Builder [36]. Tento nástroj je využiteľný na windowsových platformách a disponuje grafickým rozhraním, cez ktoré je úprava rámcov/paketov pomerne jednoduchá.



Obrázok 5.11 Ukážka grafického rozhrania využitého nástroja Cat KARAT Packet Builder.

Prvým testovaným kybernetickým útokom je zachytenie GOOSE/SMV komunikácie, jej modifikácia a následné odoslanie do siete tak, aby došlo k podvedeniu odberateľských zariadení. Aby odberateľské zariadenie rámce prijalo musia byť splnené určité podmienky. Prvou podmienku je, že rámce musia byť odoslané s reálnou MAC adresou IED vydavateľského zariadenia v rámci zdroja. Ďalej musia byť zachované základné polia rámcov a pri modifikácii parametrov je potrebné myslieť na úpravu všetkých pridružených polí.

Prvým cieľom je napadnutie časovej synchronizácie SMV rámcov [37]. IEC 61850-9-2 definuje pole v SMV rámci nazvané smpSynch, ktoré prenáša informáciu o zdroji časovej synchronizácie, ktorý využíva zdrojové IED. Pole môže nadobúdať nasledovné hodnoty:

- SmpSynch = Remote (2); SMV sú synchronizované voči globálnym hodinám,
- SmpSynch = Local (1); SMV sú synchronizované voči lokálnym hodinám a
- SmpSynch = None (0); SMV môžu mať synchronizačný problém.

Z analytickej fáze útočník zistí v akom stave sa hodnota nachádza a tú následne vynuluje. V testovacom prostredí pole prenáša hodnotu SmpSynch: local (1), na základe čoho boli príslušné bity vynulované na SmpSynch: none (0). Ukážka originálneho rámcu s hodnotou local (1) a správnymi vzorkovanými hodnotami sa nachádza na obrázku 5.12 a rámec so zmenenou hodnotou smpSynch je ukázaný na obrázku 5.13. Ďalej bola inkrementová hodnota cmpCnt naznačujúca nový odber SMV hodnôt a do PhsMeas1 boli vsadené nové schválne nevalidné hodnoty, ukázané na obrázku 5.14.

```

ASDU
  svID: uniqueID
  smpCnt: 2191
  confRef: 1
  smpSynch: local (1)
  PhsMeas1
    value: 702
    > quality: 0x00000000, validity: good, source: process
      value: 70
    > quality: 0x00000000, validity: good, source: process
      value: 499
    > quality: 0x00000000, validity: good, source: process
      value: 82
    > quality: 0x00000000, validity: good, source: process
      value: 35
    > quality: 0x00000000, validity: good, source: process
      value: -32
    > quality: 0x00000000, validity: good, source: process
      value: -30
    > quality: 0x00000000, validity: good, source: process
      value: -9
    > quality: 0x00002000, validity: good, source: process, derived

```

```

00 08 75 6e 69 71 75 65 49 44 82 02 08 8f 83 04 00  .uniqueID.....
00 00 00 01 85 01 01 87 40 00 00 02 be 00 00 00 00  .....@.....
00 00 00 00 46 00 00 00 00 00 00 01 f3 00 00 00 00  ...F.....
00 00 00 00 52 00 00 00 00 00 00 00 23 00 00 00 00  ...R.....#....
ff ff ff e0 00 00 00 00 00 ff ff ff e2 00 00 00 00  .....
ff ff ff f7 00 00 20 00 .....

```

Obrázok 5.12 Originálny SMV rámec s hodnotou smpSynch: 1.

```

  IEC61850 Sampled Values
  APPID: 0x4000
  Length: 106
  Reserved 1: 0x0000 (0)
  Reserved 2: 0x0000 (0)
  savPdu
  noASDU: 1
  seqASDU: 1 item
  ASDU
  svID: uniqueID
  smpCnt: 2192
  confRef: 1
  smpSynch: none (0)
  PhsMeas1

```

```

0000 01 0c cd 04 00 00 00 21 c1 53 29 f1 88 ba 40 00 .....!·S)···@·
0010 00 6a 00 00 00 00 60 60 80 01 01 a2 5b 30 59 80 ·j··········[0Y·
0020 08 75 6e 69 71 75 65 49 44 82 02 08 90 83 04 00 ·uniqueI D·····
0030 00 00 01 85 01 00 87 40 00 00 02 b5 00 00 00 00 ····J·@·····
0040 00 00 00 4a 00 00 00 00 00 00 01 f3 00 00 00 00 ···J·········
0050 00 00 00 4c 00 00 00 00 ff ff ff f3 00 00 00 00 ···L·········
0060 ff ff ff f7 00 00 00 00 00 00 00 42 00 00 00 00 ··········B···
0070 00 00 00 0e 00 00 20 00 .....

```

Obrázok 5.13 Modifikovaný SMV rámec na falošnú hodnotu smpSynch: 0.

```

  ASDU
  svID: uniqueID
  smpCnt: 2192
  confRef: 1
  smpSynch: none (0)
  PhsMeas1
  value: 694
  > quality: 0x00000011, validity: invalid, bad reference, source: process
  value: 75
  > quality: 0x00000011, validity: invalid, bad reference, source: process
  value: 500
  > quality: 0x00000011, validity: invalid, bad reference, source: process
  value: 77
  > quality: 0x00000011, validity: invalid, bad reference, source: process
  value: -12
  > quality: 0x00000011, validity: invalid, bad reference, source: process
  value: 16777208
  > quality: 0x00000011, validity: invalid, bad reference, source: process
  value: 67
  > quality: 0x00000011, validity: invalid, bad reference, source: process
  value: 1
  > quality: 0x00002001, validity: invalid, source: process, derived

```

```

31 0c cd 04 00 00 00 21 c1 53 29 f1 88 ba 40 00 .....!·S)···@·
30 6a 00 00 00 00 60 60 80 01 01 a2 5b 30 59 80 ·j··········[0Y·
38 75 6e 69 71 75 65 49 44 82 02 08 90 83 04 00 ·uniqueI D·····
30 00 01 85 01 00 87 40 00 00 02 b6 00 00 00 11 ····@·····
30 00 00 4b 00 00 00 11 00 00 01 f4 00 00 00 11 ···K·········
30 00 00 4d 00 00 00 11 ff ff ff f4 00 00 00 11 ···M·········
30 ff ff f8 00 00 00 11 00 00 00 43 00 00 00 11 ··········C···
30 00 00 01 00 00 20 01 .....

```

Obrázok 5.14 Ukážka rámcu s pozmenenými prenášanými hodnotami.

Po prijatí takto upraveného rámcu odberateľ reaguje rôznymi spôsobmi. Funkcie, ktoré sú citlivé na rozdiel fázového uhla medzi meraniami sú automaticky zablokované, čo následne môže viesť k celkovej poruche v rámci neštandardného stavu. Pri správnej implementácii protokolu SMV odberateľskej stanice dôjde k chybe “LDS_SmpSynchMismatch = 5”, ktorá označí časovú synchronizáciu odoberaných SMV za rozdielnu voči vlastnému nastaveniu a rámec neprijme.

Ďalším cieľom je takzvaný spoofingový útok na GOOSE rámce, v ktorom sa jedná o vkladanie falošných rámcov do prevádzky tak, aby sa prijímacie zariadenia domnievali, že prijímajú správne dáta odoslané od legitímneho vydavateľského IED. Ako počiatočný bod útoku je použité útočnicke prostredie z fáz 1 a 2, ktoré dovoľuje legitímne rámce

fyzicky prijímať, dekódovať a analyzovať. Po rozbalení rámču sú modifikované určité polia, rámec opäť zabalený a následne odoslaný do siete po L2 vrstve ISO/OSI referenčného modelu pomocou maskovania za legitímne vydavateľské IED. Rámec musí byť z tohto dôvodu odoslaný so zdrojovou MAC adresou legitímneho IED, ktoré je v testovacom prípade 00:21:c1:53:29:af.

V testovacom scenári ochrana REF615 pomocou funkcie kontroly vypínacieho obvodu odhalí reálnu chybu označenú ako TCS, ktorá je zobrazená na obrázku 5.15. Toto hlásenie indikuje poruchu vypínacieho okruhu a automaticky o chybe odosiela GOOSE správu určenú pre svojich odberateľov aby mohli sami spustiť ochranné funkcie a prípadne dať povel k prerušeniu obvodu. Pri detegovanej zmene hodnoty v rámci posielených dát (DataSet) je v rámci inkrementované počítadlo stNum na vyššiu hodnotu a s ním je zároveň vynulované počítadlo sqNum. Nové hodnoty odosieleného rámču sú zobrazené na obrázku 5.16.

Type	Date & Time	Signal name	Status
P	18.04.2022 1:49:45.272	SCHLCCH2 CH2LIV	True
P	18.04.2022 1:49:22.567	TCS(1) ALARM	True
P	18.04.2022 1:49:22.567	TCS(2) ALARM	True

Obrázok 5.15 Alarm poruchy vypínacieho okruhu získaný z nástroja PCM600.

```
> Ethernet II, Src: ABB/Medi_53:29:af (00:21:c1:53:29:af), Dst: Iec-Tc57_01:00:03 (01:0c:cd:01:00:03)
  GOOSE
    APPID: 0x0004 (4)
    Length: 194
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  goosePdu
    gobcRef: AA1J1Q01A1LD0/LLN0$G0$gcbCWXU1
    timeAllowedtoLive: 11000
    dataSet: AA1J1Q01A1LD0/LLN0$CWXU1
    goID: AA1J1Q01A1LD0/LLN0.gcbCWXU1
    t: Apr 18, 2022 01:49:34.267029464 UTC
    stNum: 2
    sqNum: 0
    simulation: False
    confRev: 100
    ndsCom: False
    numDataSetEntries: 9
  > allData: 9 items

0000 01 0c cd 01 00 03 00 21 c1 53 29 af 88 b8 00 04 .....! $).....
0010 00 c2 00 00 00 00 61 81 b7 80 1f 41 41 31 4a 31 .....a...AA1J1
0020 51 30 31 41 31 4c 44 30 2f 4c 4c 4e 30 24 47 4f Q01A1LD0 /LLN0$G0
0030 24 67 63 62 43 4d 4d 58 55 31 81 02 2a f8 82 19 $gcbCWXU1-...
0040 41 41 31 4a 31 51 30 31 41 31 4c 44 30 2f 4c 4c AA1J1Q01 A1LD0/LL
0050 4e 30 24 43 4d 4d 58 55 31 83 1c 41 41 31 4a 31 N0$CWXU1-...AA1J1
0060 51 30 31 41 31 4c 44 30 2f 4c 4c 4e 30 2e 67 63 Q01A1LD0 /LLN0.gc
0070 62 43 4d 4d 58 55 31 84 08 62 5c c3 ae 44 5c 0b bCWXU1- b\-\D\
0080 f2 85 01 02 06 03 00 00 00 87 01 00 88 01 64 89 ...-d-
0090 01 00 8a 01 09 ab 39 87 05 08 00 00 00 00 87 05 .....9-
00a0 08 00 00 00 00 87 05 08 00 00 00 00 87 05 08 00 .....
00b0 00 00 00 87 05 08 00 00 00 00 87 05 08 00 00 00 .....
00c0 00 84 03 03 00 00 84 03 03 00 00 84 03 03 00 00 .....
```

Obrázok 5.16 Ukážka inkrementácie hodnoty stNum pri hlásení chyby.

Útočník snažiaci sa napáchať čo najviac škôd do komunikácie vstúpi vlastnými rámčami, a pokúsi sa zmiast' odberateľské IED aby práve jeho rámce považovalo za legitímne a nové rámce s hodnotou stNum 2 za podvrhnuté a tie odmietlo. Vďaka zachytávaniu prevádzky sa z komunikácie vytiahne posledný rámec odoslaný pred vzniknutou chybou, dekóduje sa, inkrementuje sa hodnota sqNum a zakódovaný sa opäť odošle na lokálnu sieť. Pôvodný legitímny rámec aj novo vytvorený falošný rámec je

ukázaný na obrázku 5.17. U takéhoto typu útoku je veľmi dôležité správne načasovanie. Zo zachyteného pôvodného rámca je vytiahnutá hodnota `timeAllowedtoLive: 11000`, ktorá predstavuje frekvenciu odosielania GOOSE rámcov v milisekundách. Modifikovaný rámec je odoslaný o niečo skôr ako 11 sekúnd od pôvodného, nakoľko je potrebné aby dorazil pred ďalším legitímnym.

```

> Ethernet II, Src: ABB/Medi_53:29:af (00:21:c1:53:29:af),> Ethernet II, Src: ABB/Medi_53:29:af (00:21:c1:53:29:af)
  < GOOSE                               < GOOSE
    APPID: 0x0004 (4)                    APPID: 0x0004 (4)
    Length: 194                          Length: 194
    Reserved 1: 0x0000 (0)                Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)                Reserved 2: 0x0000 (0)
    < goosePdu                            < goosePdu
      gocbRef: AA1J1Q01A1LD0/LLN0$G0$gcbCMMXU1  gocbRef: AA1J1Q01A1LD0/LLN0$G0$gcbCMMXU1
      timeAllowedtoLive: 11000                timeAllowedtoLive: 11000
      datSet: AA1J1Q01A1LD0/LLN0$CMMXU1        datSet: AA1J1Q01A1LD0/LLN0$CMMXU1
      goID: AA1J1Q01A1LD0/LLN0.gcbCMMXU1      goID: AA1J1Q01A1LD0/LLN0.gcbCMMXU1
      t: Apr 12, 2022 10:25:50.267028868 UTC    t: Apr 12, 2022 10:25:50.267028868 UTC
      stNum: 1                                stNum: 1
      sqNum: 156236                            sqNum: 156237
      simulation: False                        simulation: False
      confRev: 100                             confRev: 100
      ndsCom: False                            ndsCom: False
      numDatSetEntries: 9                     numDatSetEntries: 9
    > allData: 9 items                      > allData: 9 items
  
```

Obrázok 5.17 Posledný zachytený legitímny rámec v `stNum: 1` a nový falošný rámec.

Vďaka pravidelnému odosielaniu ďalších nadväzných rámcov modifikovaných o inkrementáciu `sqNum` je po určitý čas možné docieľiť stavu, kedy odberateľské IED považuje útočnicke rámce za legitímne a ostatné zahadzuje. Vďaka tomu môže dôjsť k šíreniu reálnej chyby s potencionálnymi závažnými následkami.

Opačným scenárom je pokus útočníka o vytvorenie falošnej informácie o chybe. Podobne ako u predošlých útokov je východiskom zachytávanie sieťovej komunikácie a analýza rámcov. Následne opäť dochádza k modifikácii polí, zabalenia dát do Ethernetového rámcu a odoslanie do lokálnej siete v čase `packetT + timeAllowedtoLive`, kde `packetT` značí časovú známku odoslania pôvodného rámcu. Obrázok 5.18 znázorňuje pôvodný zachytený rámec odoslaný IED zariadením s MAC adresou `00:21:c1:53:29:ab` a obrázok 5.19 následný modifikovaný rámec. Cieľom je informovať odberateľské zariadenia a prípadne aj administrátorov o neštandardnom stave a potrebnom zásahu. Nakoľko sa jedná o falšovanie zmeny dát, je v prvom rade potrebná aktualizácia časovej známky zmeny, teda poľa `t` na novú hodnotu. Následne je inkrementované pole `stNum` a vynulované pole `sqNum`. Tieto úpravy odberateľskému IED naznačia, že vydavateľské zariadenie zaznamenalo problémovú udalosť, o ktorej informuje ďalej. Úprava poľa `ndsCom` na pravdivú hodnotu zaisťuje vyžiadanie fyzickej pozornosti administrátorov. Pole `ndsCom` je totiž častou indikáciou konfiguračnej nezhody v zariadení. Posledným krokom modifikácie je úprava konkrétnych prenášaných hodnôt, ktoré sú priamym vyjadrením vzniknutého neštandardného stavu na monitorovanom úseku. Po vykonanej modifikácii polí je za pomoci nástroja Cat KARAT Packet Builder rámec opätovne poskladaný, maskovaný za adresou `00:21:c1:53:29:ab` a multicastovo odoslaný na LAN. Odberateľské zariadenie rámec prijíma, vykonáva patričnú nakonfigurovanú činnosť a administrátorov informuje o nutnosti preverenia zaisielateľského zariadenia. Útočníci týmto spôsobom

docielia vytvorenie falošného incidentu, ktorý zároveň odlákal pozornosť administrátorov od skutočného problému alebo chystanej série útokov.

```

▼ GOOSE
  APPID: 0x0001 (1)
  Length: 195
  Reserved 1: 0x0000 (0)
  Reserved 2: 0x0000 (0)
  ▼ goosePdu
    gocbRef: AA1J1Q01A2LD0/LLN0$GO$gcbCMXXU1
    timeAllowedtoLive: 11000
    dataSet: AA1J1Q01A2LD0/LLN0$CMXXU1
    goID: AA1J1Q01A2LD0/LLN0.gcbCMXXU1
    t: Mar 14, 2022 20:27:43.354215562 UTC
    stNum: 208
    sqNum: 404165
    simulation: False
    confRev: 100
    ndsCom: False
    numDataSetEntries: 9
  ▼ allData: 9 items
    ▼ Data: floating-point (7)
      floating-point: 0800000000
    ▼ Data: floating-point (7)
      floating-point: 0800000000
    ▼ Data: floating-point (7)
      floating-point: 0800000000
  0000 01 0c cd 01 00 00 00 21 c1 53 29 ab 88 b8 00 01 .....! .S).....
  0010 00 c3 00 00 00 00 61 81 b8 80 1f 41 41 31 4a 31 .....a. ...AA1J1
  0020 51 30 31 41 32 4c 44 30 2f 4c 4c 4e 30 24 47 4f Q01A2LD0 /LLN0$GO
  0030 24 67 63 62 43 4d 4d 58 55 31 81 02 2a f8 82 19 $gcbCMXX U1..*...
  0040 41 41 31 4a 31 51 30 31 41 32 4c 44 30 2f 4c 4c AA1J1Q01 A2LD0/LL
  0050 4e 30 24 43 4d 4d 58 55 31 83 1c 41 41 31 4a 31 N0$CMXXU 1..AA1J1
  0060 51 30 31 41 32 4c 44 30 2f 4c 4c 4e 30 2e 67 63 Q01A2LD0 /LLN0.gc
  0070 62 43 4d 4d 58 55 31 84 08 62 2f a5 3f 5a ad df bCMXXU1..b/.?Z..
  0080 18 85 02 00 d0 86 03 06 2a c5 87 01 00 88 01 64 .....*.-----d
  0090 89 01 00 8a 01 09 ab 39 87 05 08 00 00 00 00 87 .....9 .....
  00a0 05 08 00 00 00 00 87 05 08 00 00 00 00 87 05 08 .....
  00b0 00 00 00 00 87 05 08 00 00 00 00 87 05 08 00 00 .....
  00c0 00 00 84 03 03 00 00 84 03 03 00 00 84 03 03 00 .....
  00d0 00
  
```

Obrázok 5.18 Pôvodný GOOSE rámec.

```

GOOSE
  APPID: 0x0001 (1)
  Length: 195
  Reserved 1: 0x0000 (0)
  Reserved 2: 0x0000 (0)
  goosePdu
    gocbRef: AA1J1Q01A2LD0/LLN0$G0$gcbCMWXU1
    timeAllowedtoLive: 11000
    datSet: AA1J1Q01A2LD0/LLN0$CMWXU1
    goID: AA1J1Q01A2LD0/LLN0.gcbCMWXU1
    t: Mar 14, 2022 20:27:44.362029492 UTC
    stNum: 209
    sqNum: 0
    simulation: False
    confRev: 100
    ndsCom: True
    numDatSetEntries: 9
    allData: 9 items
      Data: floating-point (7)
        floating-point: 000000000
      Data: floating-point (7)
        floating-point: ffffffff
      Data: floating-point (7)
        floating-point: ffffffff
  0000 01 0c cd 01 00 00 00 21 c1 53 29 ab 88 b8 00 01 .....! S)....
  0010 00 c3 00 00 00 00 61 81 b8 00 1f 41 41 31 4a 31 .....a...AA1J1
  0020 51 30 31 41 32 4c 44 30 2f 4c 4c 4e 30 24 47 4f Q01A2LD0 /LLN0$G0
  0030 24 67 63 62 43 4d 4d 58 55 31 81 02 2a f8 82 19 $gcbCMWX U1...*...
  0040 41 41 31 4a 31 51 30 31 41 32 4c 44 30 2f 4c 4c AA1J1Q01 A2LD0/LL
  0050 4e 30 24 43 4d 4d 58 55 31 83 1c 41 41 31 4a 31 N0$CMWXU 1-AA1J1
  0060 51 30 31 41 32 4c 44 30 2f 4c 4c 4e 30 2e 67 63 Q01A2LD0 /LLN0.gc
  0070 62 43 4d 4d 58 55 31 84 08 62 2f a5 40 5c ad f7 bCMWXU1- /b/ @\...
  0080 5f 05 02 00 d1 06 03 00 00 00 87 01 00 00 01 64 ?.....d
  0090 89 01 01 8a 01 09 ab 39 87 05 00 00 00 00 87 .....9.....
  00a0 05 ff ff ff ff ff 87 05 08 00 00 00 00 87 05 08 .....
  00b0 00 00 00 00 87 05 08 00 00 00 00 87 05 08 00 .....
  00c0 00 00 84 03 03 00 00 84 03 03 00 00 84 03 03 .....
  00d0 00

```

- Aktualizácia časovej známky
- Úprava stNum a sqNum
- Úprava ndsCom
- Zmena v prenášaných dátach

Obrázok 5.19 Modifikovaný GOOSE rámec s farebnou legendou.

V rámci série útokov na modifikáciu polí v rámcoch je možné zacieliť napríklad aj na VLAN pole. Niektoré prostredia aktívne pracujú s VLAN informáciami prenášanými v paketoch. Výnimkou tak nemusia byť ani IED, ktoré môžu byť nakonfigurované aby u SMV alebo GOOSE rámcov vyžadovali správne priradenú VLAN značku (tag). Pokiaľ by odberateľ obdržal neoznačkový rámec, teda bez informácie o VLAN, mohol by rámec zahodiť a správu neprijat'. Útočník sa v tomto prípade môže zacieliť na konkrétnu 4 bajtovú časť v rámci IEEE 802.1Q hlavičky a upraviť v nej hodnotu VID, ktorá prenáša VLAN identifikátor. Pokiaľ vo VID už hodnota nastavená bola, IED s ňou počíta a útočník ju môže buď vynulovať alebo prestaviť na inú. V rámci testovacieho prostredia neboli VLAN využité, preto je tento útok predstavený ako potenciálne rozšírenie testovania.

Ďalším testovaným kybernetickým útokom je muž uprostred (Man in The Middle). Jedná sa o jednu z najčastejšie používaných techník cielených najmä na nešifrované komunikačné toky, kde sa útočník stavia medzi dve komunikujúce strany. Prostredníctvom spoofingových techník falšuje svoju identitu vždy za jednu z komunikujúcich strán. Pôvodné komunikujúce strany tak ostávajú v domnienke, že sa na druhej strane nachádza legitímny komunikátor, ale v realite sa ním stáva útočník.

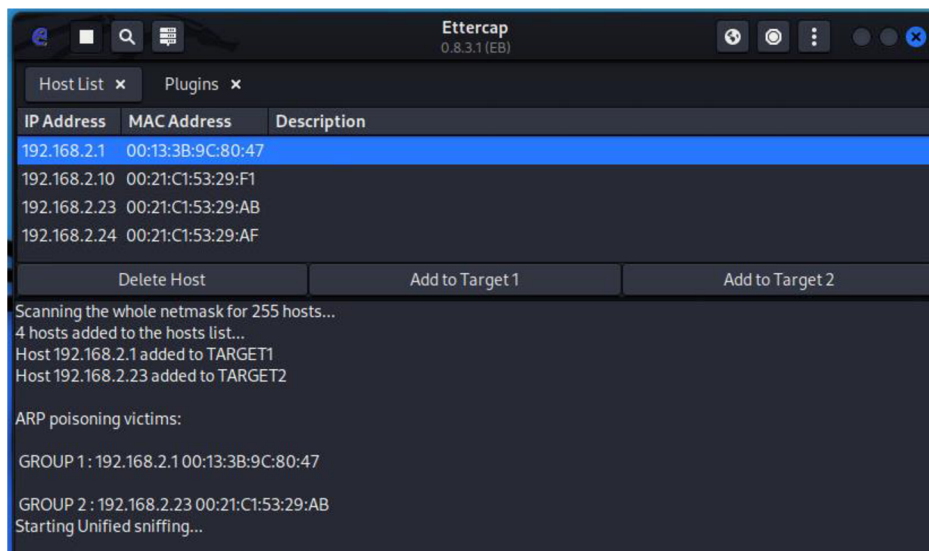
V prvom kroku je vykonaný útok otrávenia ARP protokolu. ARP protokol je využívaný na objavenie MAC adries zariadení nachádzajúcich sa na lokálnej sieti a ich mapovanie na IP adresy do ARP tabuliek nachádzajúcich sa na každom komunikujúcom zariadení. Tento proces je napadnuteľný napríklad prostredníctvom nástroja Ettercap, ktorý na windowsovú stanicu a IED zariadenie odošle vlastnú ARP správu tváriaci sa ako protistrana, čím sú vo výsledku prepísané hodnoty v ARP tabuľke. Pre overenie pôvodných hodnôt je vypísaná ARP tabuľka na windowsovej stanici pomocou príkazu `arp -a`, zobrazená na obrázku 5.20. Cieľom pre útok sa stáva IED zariadenie s MAC adresou 00-21-c1-53-29-ab a IP adresou 192.168.2.23.

```
Interface: 192.168.2.1 --- 0xf
Internet Address      Physical Address      Type
192.168.2.10         00-21-c1-53-29-5f    dynamic
192.168.2.23         00-21-c1-53-29-ab    dynamic
192.168.2.24         00-21-c1-53-29-af    dynamic
192.168.2.100        08-00-27-0e-34-8d    dynamic
192.168.2.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250     01-00-5e-7f-ff-fa    static
```

Obrázok 5.20 Výpis ARP tabuľky na windowsovej stanici.

Na útočnickej stanici s distribúciou Kali Linux je v prvom kroku upravená sieťová konfigurácia pre povolenie zachytávania a preposielania IP komunikácie prostredníctvom príkazu `echo 1 > /proc/sys/net/ipv4/ip_forward`. Obdobné nastavenie je aj priamo v konfiguračnom súbore nástroja Ettercap, ktorý sa obvykle v adresárovej štruktúre nachádza v `/etc/ettercap/etter.conf`. Konkrétne sa jedná o príkazy `redir_command_on` a `redir_command_off`, ktoré je potrebné odkomentovať. Výsledný stav prezentuje obrázok. Následne je spustené grafické rozhranie nástroja pomocou príkazu `ettercap -G`.

V grafickom rozhraní sa špecifikuje zachytávanie prevádzky na Unified sniffing a vyberie sa konkrétne sieťové rozhranie, na ktoré sa bude zachytávanie vzťahovať. V ďalšom kroku sa vyberú ciele útoku na základe rýchleho automatického skenu siete. Najprv je z menu vybraná možnosť Host > Scan for hosts, ktorá sken inicializuje a jeho úspešné dokončenie značí výpis, že boli hosty pridané na host list. Z menu sa opäť vyberie možnosť Host a ďalej tento krát Hosts list. Výstupom je prehľadný zoznam zariadení vo formáte IP adresa, MAC adresa a prípadný popis. Zo zoznamu sa pomocou kliknutia priamo na adresu a následne na tlačidlo Add to Target zariadenie označí za cieľ. Z menu Mitm je následne vybraný útok arp poisoning a spustený cez možnosť Start > Start sniffing. Priebeh útoku je zobrazený na obrázku 5.21.



Obrázok 5.21 Grafické rozhranie nástroja Ettercap počas prebiehajúceho MITM útoku.

Úspešné prepísanie je overené opätovným vypísaním ARP tabuľky na windowsovej stanici. Výsledok je zobrazený na obrázku 5.22, na ktorom je už nová asociácia IP adresy 192.168.2.23 s MAC adresou útočnického stroja 08-00-27-0e-34-8d.

```
Interface: 192.168.2.1 --- 0xf
Internet Address      Physical Address      Type
192.168.2.10         00-21-c1-53-29-5f    dynamic
192.168.2.23         08-00-27-0e-34-8d    dynamic
192.168.2.24         00-21-c1-53-29-af    dynamic
192.168.2.100        08-00-27-0e-34-8d    dynamic
192.168.2.255        ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250     01-00-5e-7f-ff-fa    static
```

Obrázok 5.22 Výpis ARP tabuľky na windowsovej stanici, zmena MAC adresy.

Akákolvek komunikácia medzi cieľovými zariadeniami prechádza cez prostredníka - útočnicku stanicu. Sieťová prevádzka oboch cieľových staníc s inými systémami je z dôvodu minimalizácie detekcie nepozmenená. Predmetom záujmu útočníka je práve komunikácia protokolu MMS, ktorá prebieha priamo na úrovni cieľových staníc. Obrázok 5.23 predstavuje zachytený MMS paket originálne smerovaný na IED zariadenie, kde je vďaka útoku pozmenená MAC adresa cieľového zariadenia za útočnickovu a reálne je tak paket presmerovaný.

```

> Frame 1772100: 139 bytes on wire (1112 bits), 139 bytes captured (1112 bits) on interface \Device\NPF_
  Ethernet II, Src: SpeedDra_9c:80:47 (00:13:3b:9c:80:47), Dst: PcsCompu_0e:34:8d (08:00:27:0e:34:8d)
    Destination: PcsCompu_0e:34:8d (08:00:27:0e:34:8d)
    Source: SpeedDra_9c:80:47 (00:13:3b:9c:80:47)
    Type: IPv4 (0x0800)
  Internet Protocol Version 4, Src: 192.168.2.1, Dst: 192.168.2.23
  Transmission Control Protocol, Src Port: 52224, Dst Port: 102, Seq: 262990, Ack: 104076, Len: 85
  TPKT, Version: 3, Length: 85
  ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
  ISO 8327-1 OSI Session Protocol
  ISO 8327-1 OSI Session Protocol
  ISO 8823 OSI Presentation Protocol
  MMS
    confirmed-RequestPDU
      invokeID: 3223
      confirmedServiceRequest: write (5)
        write
          variableAccessSpecificatn: listOfVariable (0)
            listOfVariable: 1 item
            listOfData: 1 item
              Data: integer (5)
                integer: 200

```

```

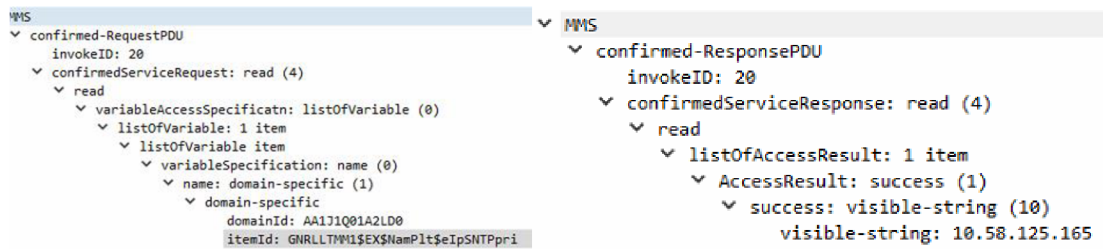
0000 08 00 27 0e 34 8d 00 13 3b 9c 80 47 08 00 45 00  . . . . 4 . . . ; . G . E .
0010 00 7d 8e 28 40 00 80 06 00 00 c0 a8 02 01 c0 a8  } . ( @ . . . . .
0020 02 17 cc 00 00 66 b8 4e 24 84 81 4e 38 ff 50 18  . . . . f N $ . N8 P .
0030 03 ff 85 d8 00 00 03 00 00 55 02 f0 80 01 00 01  . . . . . U . . . . .
0040 00 61 48 30 46 02 01 03 a0 41 a0 3f 02 02 0c 97  ah0F . . . . A ? . . . .
0050 a5 39 a0 31 30 2f a0 2d a1 2b 1a 0d 41 41 31 4a  -9 10 / . . . + . AA1J
0060 31 51 30 31 41 32 4c 44 30 1a 1a 46 52 50 54 4f  1001A2LD 0 . FRPT0
0070 46 32 24 53 45 24 4f 70 44 6c 54 6d 6d 73 24 73  F2$E$0p DLTmms$S
0080 65 74 56 61 6c a0 04 85 02 00 c8                etVal . . . . .

```

Obrázok 5.23 Ukážka zachyteného paketu smerujúceho na IED, ale s MAC adresou útočníka.

Z tohto bodu ma útočník viacero možností a smerov, ktorými by v útoku mohol pokračovať. Najbezpečnejším variantom je komunikáciu preposielať bez zásahu, vďaka čomu má možnosť do prenášaných informácií priamo nahliadať s nízkym predpokladom odhalenia. Tento smer je založený na taktikách Persistence, Discovery a Collection z ATT&CK rámca, ktoré môžu byť využité ako medzi fáza pri komplexných kybernetických útokoch. Sledovaním komunikácie je možné získať podrobnejšie informácie o komunikujúcich zariadeniach, ale zároveň aj informácie o ďalších potenciálnych cieľoch a zraniteľnostiach. Aktívnejšími smermi je priama interakcia s preposielanými paketmi vo forme modifikácie stávajúcich dotazov a informácií, vkladanie vlastných dát až celých paketov alebo zastavenie preposielania, čím dôjde k úplnej blokácii MMS komunikácie.

Obrázky 5.24 a 5.25 predstavuje príklad zachytenej MMS komunikácie pomocou MitM útoku, v ktorej boli objavené dotazy na premenné GNRLLTMM1\$EX\$NamPlt\$IpsSNTppri a GNRLLTMM1\$EX\$NamPlt\$IpsSNTPsec, ktoré v odpovedi vracajú informácie o IP adrese primárneho SNTp serveru 10.58.125.165 a záložného SNTp serveru 192.168.2.165. Pri pokračovaní útoku by útočník mohol zneužiť zraniteľnosť na objavených SNTp serveroch alebo prostredníctvom manipulácie s MMS komunikáciou na IED zariadenie poslať príkaz na zmenu IP adresy SNTp, čo by mohlo spôsobiť reboot zariadenia a tým pádom jeho nedostupnosť v rámci sekúnd až minút.



Obrázok 5.24 Zachytený paket s informáciou o primárnom SNTP servery.



Obrázok 5.25 Zachytený paket s informáciou o záložnom SNTP servery.

Ďalším prakticky testovaným útokom voči IED zariadeniam je záplavový útok, ktorý je známy aj ako Denial of Service (DoS). Pri záplavových útokoch útočníci posielajú na cieľový systém veľmi vysoký a frekventovaný objem prevádzky so zámerom zahltiť komunikačný kanál cieľového zariadenia natoľko, aby nedokázalo prijímať legitímnu komunikáciu. Takýto útok je pomerne jednoduchý na vykonanie, ale na druhej strane prináša útočníkovi obrovskú pozornosť. Na vykonanie záplavového útoku sú štandardne zneužívané sieťové protokoly TCP, UDP, HTTP, ICMP a podobné v závislosti od podpory cieľového systému. Pre testovanie odolnosti REF615 voči záplavovým útokom bol zvolený protokol ICMP a verejne prístupný nástroj hping3. Jedná sa o sieťový testovací nástroj dostupný pre linuxové platformy ovládateľný cez terminál. Nástroj umožňuje kontrolovať veľkosť, množstvo a fragmentáciu odoslaných paketov s cieľom zahltiť cieľový systém. Obrázok 5.26 v prvej časti predstavuje spustenie inštancie záplavy s parametrami:

- flood, definujúci využitie čo najväčšieho možného objemu odoslaných paketov a neočakávanie odpovedí,
- icmp, definujúci využitie protokolu ICMP echo request,
- V, definujúci verbositu,
- 192.168.2.23, definujúci cieľový systém.

V druhej časti obrázku 5.26 je na windowsovej stanici paralelne spustený príkaz ping, ktorý kontroluje odozvu cieľového systému. Hneď je pozorovaná stratovosť.

```

root@DESKTOP-FLCH5SN: /home/kali
└─(root@ DESKTOP-FLCH5SN)-[~/home/kali]
└─# hping3 --flood --icmp -V 192.168.2.23
using eth0, addr: 172.20.199.168, MTU: 1500
HPING 192.168.2.23 (eth0 192.168.2.23): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown

Príkazový riádek - ping 192.168.2.23 -t
C:\Users\labSG>ping 192.168.2.23 -t

Pinging 192.168.2.23 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.2.23: bytes=32 time=3ms TTL=255
Reply from 192.168.2.23: bytes=32 time<1ms TTL=255
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.

```

Obrázok 5.26 Spustenie záplavového útoku cez nástroj hping3 a legitímne testovanie dostupnosti z windowsovej stanice.

Útok prebiehal po dobu 3 minút, počas ktorých bolo odoslaných 14 143 347 paketov. Útočiaca stanica po celú dobu od zariadenia neobdržala žiadnu odozvu, čo zobrazuje obrázok. Windowsová stanica obdržala minimálny počet paketov s celkovou stratovosťou 93% a maximálnou latenciou 3ms.

Výsledok útoku je prezentovaný na obrázku 5.27 zo sledovania komunikácie nástrojom Wireshark. Počas doby trvania útoku úspešne došlo k zahlteniu komunikačného kanálu, ktorý nedokázal spracovávať všetky prijímané správy a vo výsledku na ne nereagoval. Po dobu zahltenia zariadenie nereagovalo ani na legitímne správy, kvôli čomu by v prípade reálnej chyby nespracovalo GOOSE správu od odosielateľa. Vďaka ušetreným zdrojom nereagovaním na prichádzajúce správy zariadenie dokázalo poslať svoje vlastné GOOSE a SMV správy aj počas zahltenia kanálu.

No.	Time	Source	Destination	Protocol	Length	Info
925051	2022/128	23:35:48,700284	192.168.2.1	192.168.2.23	42	ICMP Echo (ping) request id=0x0404, seq=10777/6442, ttl=63 (no response)
925052	2022/128	23:35:48,700289	192.168.2.1	192.168.2.23	42	ICMP Echo (ping) request id=0x0404, seq=11033/6443, ttl=63 (no response)
925053	2022/128	23:35:48,700294	192.168.2.1	192.168.2.23	42	ICMP Echo (ping) request id=0x0404, seq=11289/6444, ttl=63 (no response)
925054	2022/128	23:35:48,700297	192.168.2.1	192.168.2.23	42	ICMP Echo (ping) request id=0x0404, seq=11545/6445, ttl=63 (no response)
925055	2022/128	23:35:48,700299	192.168.2.1	192.168.2.23	42	ICMP Echo (ping) request id=0x0404, seq=11801/6446, ttl=63 (no response)
925056	2022/128	23:35:48,700301	192.168.2.1	192.168.2.23	42	ICMP Echo (ping) request id=0x0404, seq=12057/6447, ttl=63 (no response)
925057	2022/128	23:35:48,700303	192.168.2.1	192.168.2.23	42	ICMP Echo (ping) request id=0x0404, seq=12313/6448, ttl=63 (no response)
925058	2022/128	23:35:48,700352	ABB/medi_53:29:ab	Iec-Tc57_01:00:00	208	GOOSE
925059	2022/128	23:35:48,700352	ABB/medi_53:29:ab	Iec-Tc57_04:00:01	126	IEC6185...

Obrázok 5.27 Výstup z analýzy komunikácie nástrojom WireShark počas útoku.

Pre útočníka zaujímavým cieľom je v rámci testovacieho prostredia aj windowsová stanica a to z dôvodu, že jej kompromitácia by mohla otvoriť dvere do celého OT prostredia. V praxi sú taktiež stanice nachádzajúce sa na prelome IT/OT často označované za rizikové, nakoľko je vďaka ich príslušnosti do IT možná kompromitácia prostredníctvom väčšieho spektra taktík a vektorov a vďaka presahu do OT ponúkajú priestor pre laterálny pohyb útočníka. Presah windowsovej stanice medzi IT/OT je zobrazený na obrázku 5.28, ktorý vyjadruje sieťový dosah na IED zariadenie s IP adresou

192.168.2.23 overený programom ping a zároveň dosah na internetové služby overené programom telnet smerovaným na štandardne používaný TCP port 443. V reálnych prostrediach často býva povolená odchádzajúca komunikácia z týchto staníc cez štandardné porty ako TCP 80 alebo TCP 443, ktoré môžu byť zneužívané pre maskovanie škodlivej komunikácie alebo pre komunikáciu škodlivého softvéru s riadiacim centrom. Technikám komunikácie s riadiacim centrom v rámci priemyselných prostredí sa venuje taktika Command and Control z ATT&CK rámcu.

```
(root@DESKTOP-FLCH5SN)-[~/kali]
# ping 192.168.2.23
PING 192.168.2.23 (192.168.2.23) 56(84) bytes of data.
64 bytes from 192.168.2.23: icmp_seq=1 ttl=254 time=2.24 ms
64 bytes from 192.168.2.23: icmp_seq=2 ttl=254 time=1.17 ms
64 bytes from 192.168.2.23: icmp_seq=3 ttl=254 time=1.19 ms
64 bytes from 192.168.2.23: icmp_seq=4 ttl=254 time=1.80 ms
64 bytes from 192.168.2.23: icmp_seq=5 ttl=254 time=2.44 ms
^C
--- 192.168.2.23 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 1.173/1.768/2.444/0.523 ms

(root@DESKTOP-FLCH5SN)-[~/kali]
# telnet mordor.cgict.cz 443
Trying 194.182.86.15...
Connected to mordor.cgict.cz.
Escape character is '^]'.
```

Obrázok 5.28 Ukážka možnosti zneužitia štandardných portov pre laterálny pohyb.

V rámci zacielenia a zneužitia windowsovej stanice v testovacom prostredí je z ATT&CK rámcu možné použiť hneď niekoľko techník. Príkladom je technika zvýšenia oprávnení, kde po prvotnom preniknutí do systému môže útočník operovať iba s určitou úrovňou oprávnení a často sa jedná o nižšie úrovne procesov, ktoré mu bránia v prístupe k určitým zdrojom. Na systéme ale môžu existovať zraniteľnosti, ktorých zneužitím získa vyššie úrovne a napríklad prejde z neprivilegovaných alebo užívateľských oprávnení priamo na SYSTEM alebo root v závislosti od zraniteľného komponentu. Ďalším spôsobom ako dosiahnuť zvýšenia privilégii môže byť aj využitie techniky Brute-Force či sociálneho inžinierstva pre získanie prístupových údajov k už existujúcemu vysoko privilegovanému účtu. Vo vytvorenom testovacom prostredí je k dispozícii najvyššie možné oprávnenie na úrovni systému. Z dôvodu udržania konzistentnosti boli testované útoky zamerané na IED zariadenia a OT časť.

5.3.5 Zhodnotenie predpokladov využiteľnosti a rizika útokov

Na základe stanovenej metódy analýzy rizík v priemyselných prostrediach z kapitoly 5.2 je zostavená tabuľka 5.6 predstavujúca predpoklad využiteľnosti testovaných útokov a riziko na základe ich dopadu a aktuálne nasadených mitigačných opatrení. Jednotlivé výpočty s odôvodnením hodnôt sa nachádzajú v prílohe B tejto práce.

Tabuľka 5.6 Výpočet rizikovosti pre testované útoky

Útok	P _U	P _E	D	R
Analýza sieťovej komunikácie/Odpočúvanie	1	0	0.3	0.3
Časová synchronizácia SMV	0.4	0.19	1	0.33
GOOSE Spoofing	0.4	0.32	1	0.27
MMS MitM pasívny	0.85	0.04	0.3	0.24
MMS MitM aktívny	0.85	0.49	1	0.43
DoS ICMP Flood	1	0.54	1	0.54

Výsledky analýzy rizík testovaných útokov ukazujú, že najrizikovejším útokom pre testovacie prostredie je DoS a v tesnom závесе aktívna verzia útoku MitM. Aj napriek tomu, že sú útoky ľahko detekovateľné, čo značia vyššie hodnoty P_E, je ich rizikovosť najvyššia vďaka pôsobeniu vysokého oneskorenia na cieľových systémoch. Dostupnosť a nízke oneskorenie sú najdôležitejšou ale zároveň najťažšie ochrániteľnou bezpečnostnou požiadavkou priemyselných energetických systémov. Útoky, ktorým sa podarí túto požiadavku narušiť sú považované za závažné a je dôležité predchádzať ich úspechu nasadením správnych mitigačných mechanizmov.

6. MITIGÁCIA ÚTOKOV

V tak dynamickom odvetví akým je kybernetická bezpečnosť je dôležité dbať na zabezpečenie z komplexného hľadiska. Denne je objavené množstvo nových systémových zraniteľností, bezpečnostných dier ale aj prevádzkových vlastností, ktoré je možné zneužiť na kompromitáciu cieľového systému alebo jeho časti. Bezpečnostní pracovníci síce pohotovo reagujú na objavené nedostatky implementáciou záplat a bezpečnostných mechanizmov, ale útočníci paralelne nachádzajú spôsoby ako tieto mechanizmy obchádzať. V priemyselnom odvetví sa navyše často jedná o zastaranejšie a výpočtovo limitované systémy. Nasadenie bezpečnostných aktualizácií a mechanizmov na takéto systémy vyžaduje časovo náročné testovanie a ladenie, čo v produkčnom prostredí môže znamenať oneskorenie reálneho nasadenia. Z tohto dôvodu je často jednovrstvová bezpečnosť nedostatočná a preto by implementácia mitigačných mechanizmov mala prebiehať vo viacerých vrstvách. Hlavnou výhodou je dosiahnutie komplexného bezpečnostného riešenia pre detekciu, ohlásenie, kontrolu a blokovanie a tým zaistenie základných bezpečnostných požiadaviek dôvernosti, integrity a dostupnosti. Navrhovanými vrstvami sú:

1. Úroveň operačných technológií (OT)
2. Úroveň informačných technológií (IT)
3. Úroveň perimetru
4. Fyzická úroveň

6.1 Mitigácia na úrovni operačných technológií (OT)

Primárnym dokumentom, ktorý sa zaoberá zabezpečením priemyselných protokolov a z ktorého je odporúčané vychádzať pri nasadzovaní mitigačných opatrení je súbor noriem IEC 62351. Ako ale bolo naznačené v kapitole 2, latencia je hlavnou prekážkou pri priamej implementácii stanovených bezpečnostných opatrení. Napríklad protokol GOOSE preto so svojou požiadavkou 3 ms maximálnej odozvy nie je predisponovaný prijať šifrovacie opatrenia alebo akékoľvek iné opatrenia, ktoré by zvýšili komunikačné oneskorenie alebo latenciu. Nasledujúca tabuľka 6.1 sumarizuje dostupné mitigačné mechanizmy aplikovateľné priamo na IED zariadenia a príslušné využívané komunikačné protokoly.

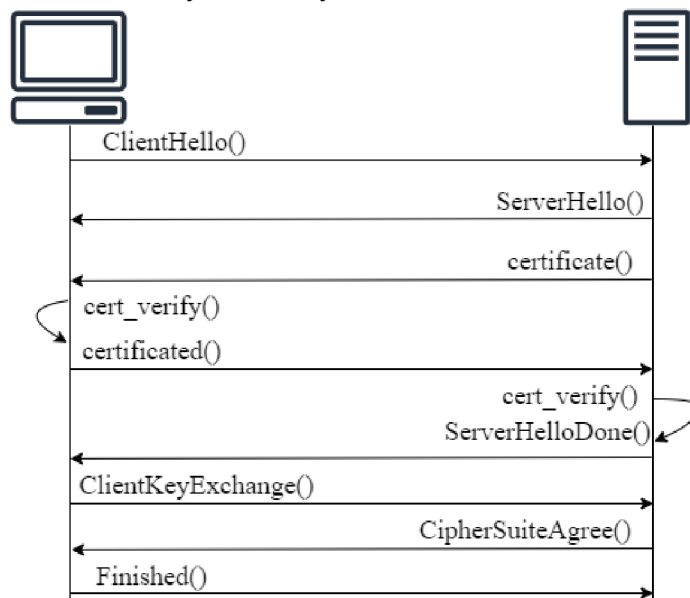
Tabuľka 6.1 Prehľad mitigačných opatrení na úrovni OT

Mitigácia	Popis	Bezpečnostná požiadavka	GOOSE	SMV	MMS/-104
Autentickosť správ	Pridanie HMAC hodnoty do poľa Extension pre GOOSE/SMV a autentizačné mechanizmy na úrovni MMS.	Integrita	Áno	Áno	Áno
Riadenie kľúčov	Nasadenie mechanizmu distribúcie a správy kľúčov.	Integrita, Dôvernosť	Áno	Áno	Áno
Šifrovanie správ	Využitie symetrických kryptografických šifrier, TLS.	Dôvernosť	Nie	Nie	Áno
Zoznam povolených IED	Prijímanie rámcov na odberateľskej stanici iba od povolených zariadení	Dôvernosť	Áno	Áno	Nie
IEC (R)61850 Gateway	Využitie brány na prechod L2 protokolov na smerovateľné a šifrované toky.	Integrita, Dôvernosť	Áno	Áno	Nie
Vysoká Dostupnosť	Nasadenie viacerých IED zariadení na rovnaký segment.	Dostupnosť	Áno	Áno	Áno
IEEE 802.1Q	Priradenie rámcov/paketom VLAN príslušnosť.	Dôvernosť	Áno	Áno	Áno

6.1.1 Autentickosť správ

Na úrovni GOOSE/SMV rámcov je možné doceliť dôvernosti správ a zároveň aj požadovanej časovej odozve prostredníctvom kryptografického autentizačného mechanizmu HMAC, ktorý je zároveň bezpečnostným odporúčaním podľa IEC 62351. Pôvodným odporúčaním IEC 62351 na zaistenie dôvernosti a integrity odosielaných SMV/GOOSE rámcov je využitie digitálnych podpisov generovaných pomocou SHA256 hashovacej funkcie a kybernetického algoritmu RSA. Výsledná hodnota by bola pripojená do poľa Extensions. Nakoľko bolo viacerými výskumníkmi pozorované prekročenie vyžadovanej 3ms odozvy kvôli výpočtovým zaťaženiám, je odporúčané využitie ľahšieho mechanizmu – HMAC. Rezervované polia v odosielaných rámcoch podľa IEC 62850-8-1 môžu byť využité aj na prenášanie hodnoty HMAC a potrebných informácií na jej interpretáciu. Konfigurácia IED na využívanie bezpečnostných rozšírení v rámcoch sa vykoná pomocou SCL. Následne je pre generovanie a overovanie hodnoty HMAC na úrovni IED potrebná distribúcia pred zdieľaných kľúčov a tým pádom aj zavedený kľúčový management definovaný podľa IEC 62351-9. Konkrétne odporúčané kryptografické algoritmy sú vyhodnotené v tabuľke 2-1 tejto práce.

Dosiahnutie autentickosti správ protokolu MMS môže byť zaistené nasadením autentizačného mechanizmu založeného na certifikátoch, ktorý je priamym bezpečnostným odporúčaním podľa IEC 62351-4. IEC 62351-4 ďalej stanovuje minimálne a odporúčané šifrovacie sady pre zostavenie bezpečného TLS spojenia, ktoré sú vyhodnotené v tabuľke 2-2 tejto práce. Zostavenie bezpečného spojenia využíva port 3782 sieťovej vrstvy a začína zriadením a vyjednaním TLS relácie, kedy sú vymenené a voči certifikačnej autorite overené X.509 certifikáty klienta a následne serveru. Po úspešnej autentizácii pokračuje zostavovanie bezpečného spojenia výmenou tajného kľúču využitím kryptografického algoritmu výmeny verejných kľúčov ako napríklad Diffie-Hellman (DH) alebo RSA. Použitím tajného kľúču dôjde k dohodnutiu celej šifrovacej sady. Po vyjednaní a založení bezpečného spojenia dochádza k prenosu samotných dát. Priebeh vyjednania TLS spojenia je zobrazený na obrázku 6.1, kde na ľavej strane je predstavený klient komunikujúci na server na pravej strane. Na obrázku sú ďalej znázornené jednotlivé kroky s funkčnými názvami.



Obrázok 6.1 Výmena správ medzi klientom a serverom pre zostavenie TLS spojenia.

6.1.2 Distribúcia a riadenie kľúčov

IEC 62351-9 zahŕňa aspekty riadenia kľúčov požadovaného všetkými protokolmi a systémami definovanými v skupine noriem IEC 62351 a preto sa stáva primárnym dokumentom pri implementácii kľúčového riadenia. V závislosti od využívaných komunikačných protokolov a na nich nasadených bezpečnostných mechanizmov je potrebné v rámci kľúčového riadenia implementácia rôznych mechanizmov. Pre zaistenie správnej HMAC funkčnosti je potrebné distribuovať na komunikujúce IED stanice pred zdieľané kľúče. Pre funkčnosť TLS u protokolu MMS je potrebné zaistenie vydávania, overovania a distribúcie bezpečnostných certifikátov X.509 (prostredníctvom vlastnej certifikačnej autority alebo využitím dôveryhodných verejných autorít).

Dôležitú úlohu zohráva prijatie skupinovej domény interpretácie (GDOI) definovanej v RFC 6407. Táto interpretácia zaisťuje, že vydavateľské a odberateľské stanice

využívajúce GOOSE môžu generovať a používať platné kľúče relácie efektívnym a bezpečným spôsobom.

6.1.3 Šifrovanie správ

Z dôvodu kombinácie časovej kritickosti a všeobecne nízkeho výpočtového výkonu IED zariadení, nie je použitie šifrovacích algoritmov pre GOOSE a SMV správy v praxi odporúčané. Nutnosťou by bolo zvýšenie výkonu samotných IED zariadení, čo je vzhľadom na požadovanú interoperabilitu príliš nákladové. Šifrovanie komunikácie je preto odporúčané až pre aplikácie využívajúce 3. a vyššiu vrstvu referenčného modelu ISO/OSI ako napríklad MMS alebo IEC 60870-5-104. Odporúčaním je taktiež využívať šifrované protokoly HTTPS (namiesto HTTP), SFTP (namiesto FTP) a SSH.

6.1.4 Zoznam povolených IED

Operátor môže definovať a vytvoriť zoznam povolených vydavateľských IED s informáciou o príslušných dátach v PDU na základe kontroly svID a goID . Použitie nedefinovaného ID by sa dalo ľahko zistiť. Sledovať by bolo možné aj neštandardné opakovania rámcov alebo GOOSE/SMV počítadlá obsahujúce číslo mimo očakávaného poradia (stNum, sqNum a smpCnt). Limitom takejto mitigácie je nízka účinnosť voči útočníkom maskujúcim sa za legitímnych IED vydavateľov.

6.1.5 IEC (R)61850 Gateway

Jednou z najjednoduchších implementácií prechodu L2 GOOSE/SMV na smerovateľné GOOSE/SMV je použitie brány, ktorá je na jednej strane odberateľom „tradičných“ správ L2 GOOSE/SMV vydávaných IED pripojenými k lokálnej sieti, ale na druhej strane zverejňuje prijaté správy ako UDP/IP multicast premávku. Využitie prechodových brán v internej infraštruktúre môže poskytnúť IED zariadeniam externé prostriedky využiteľné pre zostavenie šifrovaného komunikačného média. Komunikácia medzi vydavateľským a odberateľským IED by tak bola šifrovaná aspoň na úrovni medzi dvoma bránami, čím by došlo k čiastočnému plneniu požiadaviek dôvernosti a integrity a zachovaniu nízkej časovej odozvy. V praxi je využitie brány cielené na komunikáciu mimo lokálnych sietí alebo cez WAN.

6.1.6 Vysoká dostupnosť

IEC 62351 nedisponuje bezpečnostnými odporúčaniami, ktoré by dokázali naplniť požiadavku dostupnosti. V priemyselných systémoch je požiadavka dostupnosti najdôležitejšia, ale zároveň najnáročnejšia na zaistenie. Príkladom mitigačného mechanizmu pre zaistenie dostupnosti je nasadenie IED zariadení v režime vysokej dostupnosti. Prakticky by boli na kritické segmenty a obvody nasadené duplicitné vydavateľské IED zariadenia, ktoré by slúžili pre potvrdenie a overenie prípadnej nedostupnosti. V testovacom prostredí by sa jednalo o ďalšie REF615 zariadenia vykonávajúce rovnakú kontrolnú, ochrannú činnosť a publikujúce rovnaké datasety ako originálne IED. V prípade úspešného cieleného útoku na primárne zariadenie by tak

dopad na chránený segment mohol byť vďaka duplicitnému zariadeniu úspešne mitigovaný.

6.1.7 IEEE 802.1Q

IEC 61850 rámce disponujú priestorom pre pridanie VLAN značky do IEEE 802.1Q hlavičky. Pridanie VLAN označenia do komunikácie zhoršuje útočníkovi bez hlbšej znalosti infraštruktúry podmienky na vykonanie útokov niektorých útokov (napríklad modifikácie a vkladanie vlastných správ). V prípade nesprávneho nasadenia protokolu 802.1Q ale môže dôjsť k vytvoreniu úplne nových vektorov útoku, ak napríklad cieľové IED zariadenie nebude schopné zahodiť prijatý rámec bez očakávanej VLAN ID hodnoty alebo obsahujúci inú ako známu hodnotu.

V testovacom prostredí bolo praktické testovanie mitigačných mechanizmov limitované na reálne využívané IED zariadenia a dostupné prvky. Z pohľadu vysokej dostupnosti boli v prostredí nasadené identické REF615 zariadenia publikujúce GOOSE a SMV správy. Ďalej bolo na oboch zariadeniach vynútené využitie SFTP protokolu namiesto zraniteľného FTP pomocou konfiguračného nástroja PCM600.

Na druhej strane, využitie IED REF615 nepodporovali TLS pre MMS, v aktuálnom prostredí sa nenachádzal prepínač umožňujúci VLAN značkovanie ani implementácia kľúčového riadenia, kvôli čomu nebolo možné nasadiť ďalšie odporúčania podľa IEC 62351-6.

Ďalšími obrannými technikami, už na prelomovej úrovni OT/IT, by mohlo byť pridanie prepínačov a smerovačov špecifických pre štandard IEC 61850 s hĺbkovou kontrolou správ GOOSE/SMV, hoci toto riešenie má nevýhodu v predĺžení času odoslania správy.

6.2 Mitigácia na úrovni informačných technológií (IT)

Po prekročení hranice medzi OT a IT technológiami sú mitigačné odporúčania cieleňé na dve dôležité oblasti: 1) bezpečnosť koncových staníc (napríklad inžinierske a operačné zariadenia) a 2) sieťová bezpečnosť.

Koncovou stanicou je myslené zariadenie pripojené a komunikujúce po počítačovej sieti. Môže sa jednať o inžinierske stanice, užívateľské stanice alebo napríklad servery, ktoré sú kvôli svojej komunikačnej povahe častým terčom kybernetických útokov. Konkrétne sa môže jednať o infikovanie zariadenia malwarom, sledovanie aktivity užívateľa na zariadení, znepřístupnenie zariadenia kvôli výkupnému, využívanie zariadenia ako súčasť botnetu, na ťažbu kryptomien alebo ako východiskový bod na laterálny pohyb po sieti. Z dôvodu vysokej početnosti možných útokov je odporúčané nasadenie hneď niekoľkých mitigačných opatrení, ktoré sú predstavené v tabuľke:

Tabuľka 6.2 Prehľad mitigačných opatrení na úrovni IT

Mitigácia	Stručný popis	Odporúčanie k nasadeniu
-----------	---------------	-------------------------

Pravidelné aktualizácie	Väčšina vendorov operačných systémov a aplikácií aktívne reaguje na objavené zraniteľnosti v produktoch pravidelným vydávaním opravných záplat a aktualizácií.	Vyhľadávanie a následné aplikovanie bezpečnostných aktualizácií na pravidelnej báze a vždy po odhalení významnej alebo kritickej zraniteľnosti. Príkladovým odporúčaním je sledovanie Patch Tuesday a následné nasadenie aktualizácií v druhej polovici každého mesiaca.
Kontrola prístupu	Nasadenie Identity and Access Management (IAM) rámcu pre efektívnu identifikáciu, autentizáciu a kontrolu prístupu užívateľov.	Priradenie konkrétnych a iba nevyhnutných povolení prístupu užívateľom ku kritickým informáciám a neznámym aplikáciám. Prakticky by mali byť nasadené viacfaktorové autentizačné mechanizmy pre ochranu minimálne kritických informácií a privilegované účty pre správu koncových zariadení.
Anti-Malware	Nasadenie dedikovaného anti-malware riešenia na všetky koncové stanice.	Nasadenie aktuálnych ochranných systémov presahujúcich tradičné antivirus riešenia založené na signatúrach. Novodobé anti-malware produkty dokážu efektívne využívať princípy strojového učenia, reputačné kontroly, anti-ransomware techniky, webovú alebo aplikačnú kontrolu priamo v rámci jedného riešenia. Odporúčaním je zamerať sa pri výbere na dostupné produkty a porovnať škálu funkcionalít. Následne software rozdistribuovať na koncové stanice.
Host IPS/Firewall	Host'ovský firewall reguluje premávku na základe definovaných pravidiel. Host'ovský Intrusion Prevention System (HIPS) reguluje významné dianie na zariadení na základe definovaných škodlivých udalostí, procesov a podobností.	HIPS funkcionality sú často obsiahnuté v novodobých anti-malware riešeniach. Pokiaľ ale funkciou disponuje, stojí za zváženie nasadenie dedikovaného HIPS riešenia, ktoré ochraňuje cieľový systém na základe širších kontextov diania ako napríklad proces snažiaci sa spustiť iný proces, snaha o zmenu kľúčov registra alebo sťahovanie inštalácia súborov a ovládačov.
DLP	Data Loss Prevention systém dokáže efektívne detekovať a predísť únikom citlivých údajov z organizácie.	Informácie sú čoraz silnejšou zbraňou a preto je odporúčané aktívne zabraňovať ich nedovolenému šíreniu. Spôsobom ako úniku predísť je nasadenie DLP systému najčastejšie na úrovni koncového zariadenia alebo emailovej brány. Na úrovni koncového zariadenia dokáže DLP systém monitorovať plné spektrum interných informácií a zabrániť rôznym pokusom o ich exfiltráciu. Na druhej strane ale často za cenu zvýšeného využitia výpočtových zdrojov systému, na ktorom je nasadený. Emailová komunikácia patrí stále medzi dominantu vo väčšine organizácií a preto nasadenie DLP na tejto úrovni môže byť taktiež veľmi účinné. V porovnaní s nasadením na koncový bod nebude zachytené rovnaké množstvo pokusov, bude ale ušetrený výkon staníc.

XDR	Extended Detection and Response (XDR) je technológia rozšírenej jednotnej telemetrie pri hodnotení rizík koncových staníc, ktorá poskytuje viditeľnosť o dianí na stanici spolu s možnosťou priamej reakcie.	Prvým krokom je nasadenie agentov na koncové stanice, ktoré získavajú telemetriu a prehľad o cieľovom systéme, napríklad o bežiacich procesoch, prístupujúcich užívateľoch alebo sieťovej prevádzke. Tieto informácie sú následne korelované s typickými škodlivými udalosťami, vďaka čomu môžu byť zachytené škodlivé udalosti na ich počiatku. XDR je navyše možné využiť aj pre aktívne vyhľadávanie hrozieb práve vďaka poskytnutej viditeľnosti.
-----	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Na úrovni sieťovej bezpečnosti je základnou a najdôležitejšou mitigačnou požiadavkou segmentácia siete. V priemyselných infraštruktúrach je táto požiadavka ešte dôležitejšia ako v tradičných IT sieťach, nakoľko je veľmi dôležité oddeliť technologické/priemyselné segmenty od zvyšku infraštruktúry. Segmentáciu je možné vynútiť na úrovni aktívnych sieťových prvkoch, akým sú smerovačov a prepínače. Po prvotnom prieniku do infraštruktúry sú aktívne sieťové prvky častým nasledovným terčom útokov, nakoľko predstavujú rýchly prístup ku mnohým relevantným sieťovým informáciám a tým pádom aj informáciám o komunikujúcich systémoch. Okrem všeobecnej segmentácie je preto odporúčané na úrovni aktívnych sieťových prvkov taktiež nasadiť príslušné mitigačné mechanizmy, medzi ktoré patrí napríklad bezpečnosť portov, zakázanie nepoužívaných portov alebo vynútenie bezpečnej autentizácie do správy zariadení.

Ďalším významným mitigačným mechanizmom na sieťovej úrovni sú interné firewally, ktoré zaisťujú reguláciu prevádzky prechádzajúcej medzi jednotlivými segmentmi a interné IPS systémy, zabezpečujúce zachytenie útoku preniknutého do infraštruktúry. IPS systémy štandardne detegujú a zachytávajú útoky na základe preddefinovaných signatúr alebo aplikovaním princípov strojového učenia a umelej inteligencie pre vyhľadávanie prevádzkových anomálií. Čoraz častejšie sú vyvíjané a testované signatúry pre zachytávanie škodlivých dátových tokov protokolov definovaných v súboroch noriem IEC 61850 a IEC 60870-5. Jedným z vendorov bezpečnostných riešení, ktorý dokáže na úrovni IPS implementovať ochranu energetických protokolov je napríklad Fortinet. Okrem verejne známych vendorov sa vývoju energetických signatúr venuje aj množstvo akademických prací, vďaka čomu je možné očakávať vyššiu dostupnosť relevantných riešení pre priemyselné prostredia.

6.3 Mitigácia na úrovni perimetru

Jedným zo všeobecne najdôležitejších mitigačných opatrení je silné zabezpečenie perimetru infraštruktúry. Jedná sa o časť infraštruktúry, ktorá je vystavená širokej verejnosti a je preto najdostupnejším počiatočným vektorom prieniku. Hlavným stavebným prvkom perimetru by mal byť firewall s dôkladne špecifickou politikou, ktorá povoľuje iba nevyhnutné dátové toky. Odporúčaním je nad nasadenou politikou vykonávať pravidelné audity a revízie. V praxi sa občas stáva, že administrátori na

firewalle ponechajú testovacie povolenia, ktoré bývajú útočníkmi pohoťovo zneužitú. Vhodným riešením je postaviť pred firewall IPS systém, ktorý by slúžil na filtrovanie prichádzajúcich škodlivých a útočných komunikácií, ktoré by zahodil už v počiatku komunikácie a ušetril by tak firewallu výkon využitelný pre legítimnú komunikáciu.

Okrem fyzického perimetru je dôležité uprieť pozornosť aj na dostatočné zabezpečenie vzdialených užívateľov a dodávateľov. Vhodným riešením je sprístupniť vzdialeným používateľom a dodávateľom iba nevyhnutné aplikácie a bezpečným spôsobom. Príkladom je využitie virtuálnej privátnej siete (VPN) postavenej voči perimetrovému firewallu alebo dedikovanému VPN koncentrátoru nachádzajúcemu sa vo vnútornej sieti. U vzdialených používateľov je navyše taktiež odporúčané aplikovať mitigačné opatrenia z kapitoly 6.2, podobne ako u interných používateľov.

6.4 Fyzická úroveň

Nakoľko niektoré z testovaných komunikačných protokolov pracujú na druhej vrstve ISO/OSI referenčného modelu, ich napadnutie je limitované fyzickým dosahom útočníka. Z tohto dôvodu je na príslušné systémy nutné aplikovať aj základné princípy fyzickej bezpečnosti ako kontrola fyzického prístupu, dohľad a pravidelné testovanie. Medzi odporúčané mitigačné opatrenia na úrovni fyzickej bezpečnosti patrí nasadenie CCTV kamerových systémov, ochranné zámky a bariéry, detekcie narušenia, odstrašujúce alarmy a iné systémy určené na ochranu osôb a majetku.

Mimo technické ciele sa útočníci radi zameriavajú aj na ľudskú nepozornosť a nevedomosť. V súčasnosti patrí medzi najčastejšie útočnicke techniky sociálne inžinierstvo vykonávané prostredníctvom rôznych foriem phishingu. Jedná sa o podvodné techniky snažiace sa zmanipulovať užívateľa a donútiť ho za nevedomosti vykonať útočníkom chcenú škodlivú akciu. Typicky sa napríklad jedná o poskytnutie citlivých a prístupových údajov alebo stiahnutie škodlivého kódu. Mitigačným odporúčaním voči sociálnemu inžinierstvu je pravidelné školenie zamestnancov a užívateľov o aktuálnych útočnických technikách, obranných mechanizmoch a všeobecných základoch a princípoch kybernetickej bezpečnosti. Vhodnou mitigáciou môžu byť aj zakúpené testovacie simulácie sociálneho inžinierstva, kedy je objednaná phishingová kampaň od etických hackerov. Vďaka čomu je získaný aktuálny prehľad o informovanosti zamestnancov nasledovaný poučením na reálnej chybe.

Finálnou navrhnutou mitigáciou je nasadenie a aktívne využívanie Security Information and Event Management (SIEM) riešenia, pretože čo nie je možné ochrániť, je možné aspoň sledovať. Jedná sa o robustný systém využívaný pre získavanie a centralizáciu logov z udalostí rôznych integrovaných systémov. Následná normalizácia, korelácia a analýza získaných informácií umožňuje SIEMu vykonanie detekcie škodlivých činností a ich ohlásenie prostredníctvom rôznych foriem notifikácií. Okrem detekčnej činnosti disponujú SIEM riešenia základom pre aktívne vyhľadávanie hrozieb, forenzej činnosti a vybudovanie bezpečnostného operačného centra (SOC).

7. VYHODNOTENIE

Vďaka nedostatočnosti bezpečnostných mechanizmov využívaných v testovacom prostredí a vhodne zvolenej metodike prebehli testované kybernetické útoky úspešne. Bezpečnostné mechanizmy neboli v testovacom prostredí nasadené za účelom demonštrácie zraniteľností a zároveň z dôvodu nedostatočnej podpory zo strany využitých reálnych IED zariadení. Základ metodiky tvoril rámec taktík a techník MITRE ATT&CK špecificky zameraný na priemyselné systémy. Konkrétne techniky a postupy boli zvolené na základe zámeru otestovať širšie spektrum útočných vektorov a taktiež cieľových protokolov. Okrem testovaných útokov existuje množstvo ďalších možných útokov a zneužitelných zraniteľností, ako boli predstavené v tretej kapitole tejto práce. Väčšina možných útokov zneužíva nešifrovanú a ľahko čitateľnú a narušiteľnú formu nasadených komunikačných protokolov a fakt, že u niektorých protokolov nemusí nikdy dôjsť k ich šifrovaniu (napr. GOOSE a SMV). Protokol MMS je navyše mapovaný priamo na TCP/IP štruktúru, vďaka čomu je možné naň smerovať aj tradičné taktiky a techniky využívané v IT prostrediach.

7.1 Zhrnutie metodiky, výsledkov a odporúčaní

Z dôvodu lepšej uchopiteľnosti výstupov práce je vypracovaná súhrnná tabuľka metodiky obsahujúca mapovanie MITRE ATT&CK taktík a techník na konkrétne testované kybernetické útoky, stručný postup testovania, výstupy a odporúčania autorky.

Tabuľka 7.1 Metodika testovania

MITRE ATT&CK		Útok - Popis, postup, vyhodnotenie, odporúčanie
Taktika	Technika	
Automatizovaný sken portov a zraniteľností		
Collection	Automated Collection	<p>Popis: Zber informácií o prostredí pomocou automatizovaných nástrojov alebo skriptov.</p> <p>Postup:</p> <ol style="list-style-type: none">1. Nasadenie skeneru alebo skriptu v sieťovom dosahu cieľových zariadení. Vytvorenie sieťových prestupov a pridanie skeneru na potrebné výnimky.2. Konfigurácia inštancie skenu s ohľadom na krehkosť cieľových zariadení.3. Spustenie inštancie skenu na cieľový rozsah a monitorovanie dostupnosti zariadení. V prípade výskytu nedostupnosti produkčného zariadenia je nutné sken manuálne zastaviť.4. Sumarizácia výsledkov a ich vyhodnotenie.

		<p>Vyhodnotenie:</p> <p>Skenery zraniteľností Nessus a Nexpose objavili na cieľových zariadeniach reálne bežiacie služby a relevantné závažné zraniteľnosti k manuálnemu prevereniu.</p> <p>Odporúčanie:</p> <p>Vykonávať skeny zraniteľností na pravidelnej báze a dbať na dôkladne nastavenie bezpečných parametrov získavania informácií o službách (stav TCP/UDP portov). A na druhej strane nasadenie prísnych politík na úrovni perimetru, ktoré filtrujú pokusy o externé nelegitímne skeny.</p>
Zachytávanie sieťovej prevádzky		
Discovery	Network Connection Enumeration Network Sniffing	<p>Popis:</p> <p>Monitorovanie a zachytávanie informácií o komunikačných vzoroch a o ciele prostredníctvom sieťového rozhrania.</p> <p>Postup:</p> <ol style="list-style-type: none"> 1. Implementácia knižnice libpcap (Unixové systémy) alebo npcap (Windowsové systémy). 2. Inštalácia nástroju pre zachytávanie a analýzu sieťovej prevádzky (napríklad Wireshark a TCPdump) alebo vytvorenie vlastného nástroju využitím dostupných knižníc. 3. Spustenie zachytávania dátových tokov na fyzickom sieťovom rozhraní zariadenia. 4. Analýza obsahu zachytených rámcov/paketov a ich export. <p>Vyhodnotenie:</p> <p>Vďaka analýze zachytenej sieťovej prevádzky boli rozpoznané vydavateľské IED zariadenia a datasety, ktoré prostredníctvom IEC 61850 zasielajú. Zachytená bola ďalej komunikácia cez protokol MMS a FTPS.</p> <p>Odporúčanie:</p> <p>Zabrániť dosahu útočníka na komunikáciu operačných technológií (najmä na 2. vrstve ISO/OSI) nasadením sieťovej segmentácie a bezpečnostných politík na aktívnych sieťových prvkoch. Nasadenie šifrovania komunikácií prebiehajúcich na 3. a vyššej vrstve ISO/OSI, napríklad využitím protokolu TLS.</p>
Collection	Detect Operating Mode Monitor Process State Point & Tag Identification	
Napadnutie časovej synchronizácie SMV		
Evasion	Spoof Reporting Message	<p>Popis:</p> <p>Modifikácia poľa časovej synchronizácie v zachytených SMV rámcoch a ich následné odoslanie na cieľové IED zariadenie pre spôsobenie neštandardného stavu.</p> <p>Postup:</p> <ol style="list-style-type: none"> 1. Odchyt legitímnych SMV rámcov pomocou útoku zachytávania sieťovej prevádzky. 2. Rozbalenie rámcu a analýza polí. 3. Modifikácia poľa smpSynch na hodnotu None (0). 4. Inkrementácia hodnoty cmpCnt.
Impair Process Control	Modify Parameter	

		<p>5. Modifikácia obsahu PhsMeas1.</p> <p>6. Zabalenie polí naspäť do Ethernet rámcu.</p> <p>7. Zmena MAC adresy zariadenia na MAC adresu vydavateľského IED a odoslanie rámcu multicastovo naspäť do siete.</p> <p>Vyhodnotenie: Pri správnej implementácii SMV dôjde pri prijímaní rámcu k označeniu chyby SmpSynchMismatch a neprijatiu rámcu. Pri nesprávnej konfigurácii odberateľského IED dôjde k prijatiu falošného rámcu, zablokovaniu časovo kritických funkcií a neštandardnému stavu zariadenia.</p> <p>Odporúčanie: Vynútenie kontroly poľa smpSynch u prijímaných rámcov na úrovni odberateľského IED voči vlastnému nastaveniu časovej synchronizácie. A nasadenie kryptografickej autentizačnej techniky HMAC podľa IEC 62351-6 do rozšíreného poľa Extension za použitia pred zdieľaného kľúča pre zaistenie integrity.</p>
GOOSE Spoofing		
Evasion	Spoof Reporting Message	<p>Popis: Modifikácia parametrov v zachytených GOOSE rámcoch a ich následné odoslanie na cieľové IED zariadenie pre zakrytie reálne vzniknutej chyby. A v opačnom prípade simulácia chybného stavu pre manipuláciu funkcií cieľového zariadenia.</p> <p>Postup:</p> <ol style="list-style-type: none"> 1. Odchyt legitímnych GOOSE rámcov pomocou útoku zachytávania sieťovej prevádzky. 2. Rozbalenie rámcu a analýza polí. 3. Modifikácia polí v závislosti od zámeru: <ol style="list-style-type: none"> a. Inkrementácia sqNum pre potlačenie/neprijatie legitímnych rámcov o novo vzniknutej chybe. b. Inkrementácia stNum, vynulovanie sqNum a úprava časovej známky t pre vytvorenie falošných informácií o chybe. c. Úprava poľa ndsCom na pravdivú hodnotu pre upútanie pozornosti administrátorov. d. Úprava konkrétnych prenášaných dát v allData. 4. Zabalenie polí do Ethernet rámcu, zmena MAC adresy zariadenia na MAC adresu vydavateľského IED a odoslanie na základe hodnoty timeAllowedtoLive tak, aby rámec na cieľové zariadenie dorazil pred legitímnym. <p>Vyhodnotenie: Pri správnom načasovaní odoslaných rámcov dochádza k prijatiu falošných rámcov odberateľským zariadením a zahodeniu legitímnych rámcov. V prípade zahadzovania legitímnych rámcov môže dôjsť k nechcenému šíreniu vzniknutej chyby a v najhoršom</p>
Impair Process Control	Modify Parameter	
	Unauthorized Command Message	
Inhibit Response Function	Alarm Supression	

		<p>případe aj k stavu odoprenia služby. Pri prijatí falošných rámcov môže dôjsť k vynúteniu spustenia ochranných funkcií.</p> <p>Odporúčanie: Útok je možné mitigovať nasadením mechanizmov ochrany integrity, akým je technika HMAC podľa IEC 62351-6.</p>
Man-in-the-Middle		
Collection	Man-in-the-Middle	<p>Popis: Podvrhnutie útočnickej MAC adresy na prepísanie ARP tabuliek a následné preposielanie a blokovanie komunikácií z pozície prostredníka.</p> <p>Postup:</p> <ol style="list-style-type: none"> 1. Zapojenie útočnickej stanice v sieťovom dosahu cieľových zariadení na úrovni 2. vrstvy ISO/OSI. 2. Úprava sieťovej konfigurácie na útočnickej stanici (povolenie zachytávania a preposielania IP komunikácie). 3. Vyhľadanie cieľových zariadení (napr. pomocou nástroja Ettercap). 4. Zaslание falošných odpovedí na ARP dotazy prostredníctvom špecializovaného nástroja alebo vlastného skriptu/programu. 5. Preposielanie komunikácie medzi cieľovými zariadeniami pre udržanie zdanlivo štandardného stavu. 6. Pasívne pokračovanie útoku: <ol style="list-style-type: none"> a. Analýza informácií v komunikácii pre následné zneužitie. (napr. vynútenie zmeny pozorovaných SNTP serverov) 7. Aktívne pokračovanie útoku: <ol style="list-style-type: none"> a. DoS - Zastavenie preposielania prijatých správ pre aktívne blokovanie komunikácie. b. Pri modifikačnom útoku a útoku vkladania vlastných správ do komunikácie je nutné pred odoslaním prepočítanie checksum v TCP hlavičke a poľa length. Ďalej je nevyhnutné udržiavať v odoslaných paketoch sequences (pre predídanie ukončeniu/resetu) a dropnutie/odmietnutie odpovedí zariadenia. <p>Vyhodnotenie: Útokom došlo k úspešnému prepísaniu ARP tabuliek, zachyteniu, analýze a preposielaniu správ vymieňaných medzi komunikujúcimi uzlami.</p> <p>Odporúčanie: Zabrániť dosahu útočníka na komunikáciu 2. vrstvy ISO/OSI nasadením sieťovej segmentácie a bezpečnostných politík na aktívnych sieťových prvkoch. Nasadenie a vynútenie TLSv1.2 alebo TLSv1.3 kryptografického protokolu u komunikácií protokolu MMS.</p>
Inhibit Response Function	Block Command Message	
	Block Reporting Message	
	Device Restart/Shutdown	
	Denial of Service	

ICMP Flood		
Impact	Loss of Control	<p>Popis: Zasielanie vysoko frekventovaných správ s cieľom zahltenia komunikačného kanálu a spôsobenie stavu odoprenia služby.</p> <p>Postup:</p> <ol style="list-style-type: none"> 1. Zaistenie sieťového dosahu útočníka na cieľovú stanicu na úrovni 2.-7. vrstvy ISO/OSI v závislosti od zneužívaného protokolu. U ICMP sa jedná o dostupnosť 3. vrstvy. 2. Spustenie odosielania ICMP echo request paketov vo vysokej frekvencii na cieľové zariadenie prostredníctvom špecifického nástroja alebo vlastného skriptu. <p>Vyhodnotenie: Cieľové IED zariadenie po dobu útoku nebolo schopné prijímať legitímnu komunikáciu, ktorú zahadzovalo. Vďaka ušetreniu zdrojov bolo schopné pokračovať v generovaní a odosielaní GOOSE/SMV správ.</p> <p>Odporúčanie: Neustále sledovanie dostupnosti OT zariadení prostredníctvom monitorovacích nástrojov a využívanie mechanizmu upozornení pri nedostupnosti (napríklad prostredníctvom emailu alebo SMS). Nasadenie sieťovej segmentácie a IPS bezpečnostných sond.</p>
	Loss of View	
	Denial of View	
	Denial of Control	

8. ZÁVER

V rámci záverečnej práce boli identifikované, otestované a zdokumentované bezpečnostné hrozby, ktoré vyplývajú priamo zo špecifickosti priemyselných systémov alebo z konvergencie OT/IT sietí. Na základe vykonaných testov boli stanovené mitigačné opatrenia a výstup práce tvorí metodický súhrn podstúpených testov s výsledkami a odporúčaniami.

V úvodných kapitolách boli predstavené priemyselné komunikačné protokoly podľa súborov noriem IEC 61850, IEC 60870-5 a ich bezpečnostné nadstavby podľa IEC 62351. Z analýzy bezpečnostných odporúčaní možno pozorovať nedostatočnú dynamiku prezentovaných kryptografických algoritmov, ktorá je spôsobená nutnosťou udržiavania spätnej kompatibility starších systémov. U vybraných časovo kritických protokolov, menovite GOOSE a SMV, je podľa IEC 62351 vyslovene neodporúčané šifrovanie komunikácie z dôvodu nedostatočných výkonov a tým potenciálne spôsobenie nárastu odozvy. Protokoly GOOSE a SMV tým pádom zostávajú náchylné na útoky zneužívajúce dôvernosť a je dôležité pojať ich bezpečnosť a najmä mitigáciu rizík zo širšieho kontextu.

Pre kategorizáciu bezpečnostných hrozieb bol v práci použitý koncept CIA triády, ktorá hrozby hodnotí na základe narušenia dôvernosti, integrity a dostupnosti, čo sú zároveň tri všeobecne najdôležitejšie bezpečnostné požiadavky. Koncept CIA triády bol následne aplikovaný na existujúcu metodológiu analýzy rizík, z čoho vznikla nová odroda metodológie pre zhodnotenie predpokladov využiteľnosti testovaných útokov a stanovenie ich rizika.

Následne bol prácou predstavený metodický základ testovania postavený na matici ATT&CK pre ICS a selekcii vhodných techník pre vytvorené testovacie prostredie. V testovacom prostredí sa nachádzali 3 IED zariadenia plniace funkciu zraniteľných cieľov, windowsová stanica simulujúca prevádzkovú/inžiniersku stanicu a DELL laptop využitý ako útočná stanica. Na základe selekcie vhodných techník boli prakticky otestované kybernetické útoky v troch fázach. V prieskumnej fáze boli porovnávané dva nástroje automatizovaného testovania zraniteľností (Nexpose a Nessus) a v analytickej fáze došlo k podrobnému rozboru zachytených rámcov. V poslednej útočnej fáze boli prostredníctvom dostupných nástrojov vykonané útoky na časovú synchronizáciu SMV protokolu, útok podvrhovania GOOSE rámcov v dvoch scenároch, útok muža uprostred na protokol MMS a nakoniec záplavový útok zneužitím protokolu ICMP. Testované útoky bolo pomocou zvolenej metódy analýzy rizík hodnotené na predpoklad zneužiteľnosti s výsledným najrizikovejším záplavovým útokom nakoľko dokáže spôsobiť stav odoprenia služby, prístupu alebo kontroly.

Posledné časti práce sú venované vytvoreniu komplexného rámca mitigačných opatrení postaveného na 4 úrovniach: OT, IT, perimeter a fyzická bezpečnosť zahrňujúca ľudský faktor. Navrhnuté mitigácie vychádzajú z normy IEC 62351 a z praktických skúseností autorky, ktoré nadobudla štúdiom a prácou ako bezpečnostný konzultant.

LITERATÚRA

- [1] SHABANZADEH, MORTEZA, MOGHADDAM a MOHSEN. *What is the Smart Grid? Definitions, Perspectives, and Ultimate Goals*. [online]. 2013, Power System Conference(13-E-SMG-2046), 1-5 [cit. 2020-10-25]. Dostupné z: doi:10.13140/2.1.2826.7525
- [2] KHURANA, HIMANSHU, HADLEY, MARK, LU, NING, FRINCKE a DEBORAH. *Smart-Grid Security Issues*. Security & Privacy: IEEE [online]. 2010, (8), 81 - 85 [cit. 2020-12-08]. Dostupné z: doi:10.1109/MSP.2010.49
- [3] P. VLADYKA. *IEC 61850: soubor norem pro komunikaci v energetice s velkým potenciálem výhod*. AUTOMA – časopis pre automatizační techniku [online]. 2010, 16(3–2010), 8 [cit. 2020-10-20]. Dostupné z: https://automa.cz/Aton/FileRepository/pdf_articles/40771.pdf
- [4] R. E. MACKIEWICZ. *Overview of IEC 61850 and benefits*. 2006 IEEE Power Engineering Society General Meeting: IEEE [online]. 2006, 8 [cit. 2020-10-24]. Dostupné z: doi:10.1109/PES.2006.1709546
- [5] C. BRUNNER. *IEC 61850 for power system communication*. IEEE/PES Transmission and Distribution Conference and Exposition [online]. 2008, 1-6 [cit. 2020-10-24]. Dostupné z: doi: 10.1109/TDC.2008.4517287.
- [6] ABB. *615 series, Cyber Security Deployment Guideline*. [online]. [cit. 2021-03-17]. Dostupné z: https://library.e.abb.com/public/312f8a33d7944236b68561932441f737/RE_615_c_sdepl_758280_ENc.pdf
- [7] ČSN EN 61850-5 ed. 2. *Komunikační sítě a systémy v podřízených stanicích – Část 5: Požadavky na komunikaci pro funkce a modely zařízení*. Praha. 2013
- [8] ČSN EN 61850-7-1 ed. 2+A1. *Komunikační sítě a systémy pro automatizaci v energetických společnostech – Část 7-1: Základní komunikační struktura – Zásady a modely*. Praha. 2021
- [9] BAIGENT a DREW. *IEC 61850 communication networks and systems in substations: An overview for users*. SISCO Systems [online]. 2004, 1-15 [cit. 2020-11-15]. Dostupné z: <https://store.gegridsolutions.com/faq/Documents/General/iec61850.pdf>
- [10] HORALEK, J., J. MATYSKA a V. SOBESLAV. *Communication protocols in substation automation and IEC 61850 based proposal*. 2013 IEEE 14th International Symposium on Computational Intelligence and Informatics (CINTI) [online]. 2013, 321-326 [cit. 2020-11-20]. Dostupné z: doi: 10.1109/CINTI.2013.6705214
- [11] GEORG, H., N. DORSCH, M. PUTZKE a C. WIETFELD. *Performance evaluation of time-critical communication networks for smart grids based on IEC 61850*. 2013 Proceedings IEEE INFOCOM, Turin [online]. 2013, , 3417-3422 [cit. 2020-11-22]. Dostupné z: doi: 10.1109/INFOCOM.2013.6567174
- [12] PHAM a T. GIANG. *Integration of IEC 61850 MMS and LTE to support smart metering communications*. MS thesis. University of Twente [online]. 2013 [cit. 2020-11-22]. Dostupné z:

- <http://essay.utwente.nl/64424/1/MSc.%20Report%20Giang%20v4%20-%20Final.pdf>
- [13] LOPES, Y., D. C. MUCHALUAT-SAADE, N. C. FERNANDES a M. Z. FORTES. *Geese: A traffic generator for performance and security evaluation of IEC 61850 networks*. 2015 IEEE 24th International Symposium on Industrial Electronics (ISIE), Buzios [online]. 2015, 687-692 [cit. 2020-11-22]. Dostupné z: doi:10.1109/ISIE.2015.7281552
- [14] YOUSSEF a A. TAREK. *IEC 61850: Technology standards and cyber-threats*. 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC). [online]. 2016 [cit. 2020-11-23]. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/7555647>
- [15] MATOUŠEK, Petr. *Description and analysis of IEC 104 Protocol*. Faculty of Information Technology, Brno University of Technology, Tech. Rep, [online] 2017. [cit. 2020-11-22]. Dostupné z: <https://www.fit.vut.cz/research/publication-file/11570/TR-IEC104.pdf>
- [16] MEDINA, Veronica, *IEC-60870-5 application layer over TCP/IP for an open and flexible remote unit*. 2009 IEEE International Symposium on Industrial Electronics. IEEE, [online] 2009, 420-425. [cit. 2020-11-22]. Dostupné z: <https://ieeexplore.ieee.org/abstract/document/5217929>
- [17] RUDZINSKI, Y., VLADYKA, P. *Komunikační protokoly pro dálkové ovládání IEC/ISO 60870-5*. Automa [online]. 2010. [cit. 2020-11-22]. Dostupné z: http://automa.cz/cz/casopis-clanky/komunikacni-protokoly-pro-dalkove-ovladani-iec/iso-60870-5-2010_02_40552_5799/
- [18] SCHLEGEL, Roman, OBERMEIER, Sebastian, SCHNEIDER, Johannes. *A security evaluation of IEC 62351*. Journal of Information Security and Applications, [online]. 2017, 197-204. [cit. 2020-11-22]. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S2214212616300771>
- [19] HUSSAIN, SUHAIL, USTUN, TAHA SELIM, KALAM a AKHTAR. *A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges*. IEEE Transactions on Industrial Informatics [online]. 2020, (16), 5643-5654 [cit. 2020-11-25]. Dostupné z: doi:10.1109/TII.2019.2956734
- [20] NÚKIB. *Minimální požadavky na kryptografické algoritmy: doporučení v oblasti kryptografických prostředků* [online]. 2018, 1-8 [cit. 2020-12-07]. Dostupné z: www.nukib.cz/download/uredni_deska/Kryptograficke_prostredky_doporuceni_v_1.0.pdf
- [21] ENISA. *Algorithms, Key Sizes and Parameters Report* [online]. 2013, 1-94 [cit. 2020-12-07]. Dostupné z: <https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report>
- [22] MARRON, J. A., A. M. GOPSTEIN, N. BARTOL a L. FELDMAN. *Cybersecurity Framework Smart Grid Profile*. Technical Note (NIST TN) – 2051. [online]. 2019, 1-137 [cit. 2020-12-07]. Dostupné z: <https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2051.pdf>
- [23] CLEMENTS, S. L., H. KIRKHAM, M. ELIZONDA a S. LU. *Protecting the smart grid: a risk-based approach*. IEEE Power and Energy Society General

- Meeting [online]. 2011, (16), 1-7 [cit. 2020-11-20]. Dostupné z:
<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6039120>
- [24] LAMBERT, E. *State of the Art -TSO-DSO Interoperability*. TDX-ASSIST. Project ID – 774500. Ref. Ares(2018)6183847 - 03/12/2018. [online]. 2017, 1-146 [cit. 2020-12-02]. Dostupné z:
<https://ec.europa.eu/research/participants/documents/downloadPublic?documentId=s=080166e5bfb18002&appId=PPGMS>
- [25] SAMONAS, Spyridon a David COSS. *The CIA strikes back: redefining confidentiality, integrity and availability in security*. Journal of Information System Security [online]. 2014, 21-45 [cit. 2020-12-02]. ISSN 1551-0123. Dostupné z: <http://www.proso.com/dl/Samonas.pdf>
- [26] TAHA SELIM USTUN a S. M. SUHAIL HUSSAIN. *IEC 62351-4 Security Implementations for IEC 61850 MMS Messages*. Fukushima Renewable Energy Institute, National Institute of Advanced Industrial Science and Technology [online]. 2020, 123979-123985 [cit. 2020-12-05]. Dostupné z: doi:1109/ACCESS.2020.3001926
- [27] ABB. *IED pro chránění a ovládání vývodu REF615*. Popis a technická data výrobku: 1MRS756379 [online]. 2014, 1-83 [cit. 2020-12-06]. Dostupné z: https://library.e.abb.com/public/fbceacb37aa648f886f789fcb497144/REF615_pg_756625_CZd.pdf
- [28] ABB. *IED rady 615, Návod pro instalaci*. [cit. 2021-03-17]. Dostupné z: <https://new.abb.com/medium-voltage/cs/ochranne-terminaly/numericka-rele/ochrana-a-kontrola-podavace/relion-pro-vysoke-napeti/ochrana-a-ovladani-podavace-ref615>
- [29] ABB. *IED rady 615, Návod pro obsluhu*. [cit. 2021-03-17]. Dostupné z: <https://new.abb.com/medium-voltage/cs/ochranne-terminaly/numericka-rele/ochrana-a-kontrola-podavace/relion-pro-vysoke-napeti/ochrana-a-ovladani-podavace-ref615>
- [30] ABB. *REF615 5.0 IEC, Popis a technická data výrobku*. [cit. 2021-03-17]. Dostupné z: <https://new.abb.com/medium-voltage/cs/ochranne-terminaly/numericka-rele/ochrana-a-kontrola-podavace/relion-pro-vysoke-napeti/ochrana-a-ovladani-podavace-ref615>
- [31] ABB. *Feeder Protection and Control REF615, IEC 60870-5-103 Point List Manual*. [cit. 2021-03-17]. Dostupné z: https://library.e.abb.com/public/99fdd6b510bab1d9c1257b2f0041c9fd/REF615_ie_c103point_756712_ENe.pdf
- [32] MATOUŠEK, Petr. *Description of IEC 61850 Communication*. Faculty of Information Technology, Brno University of Technology, Tech. Rep. [online] 2018. [cit. 2022-04-19]. Dostupné z: <https://www.fit.vut.cz/research/publication-file/11832/TR-61850.pdf>
- [33] ČSN EN 61850-8-1 ed. 2+A1. *Komunikační sítě a systémy pro automatizaci v energetických společnostech – Část 8-1: Mapování specifických komunikačních služeb (SCSM) – Mapování na MMS (ISO 9506-1 a ISO 9506-2) a na ISO/IEC 8802-3*. Praha. 2020

- [34] ALEXANDER, BELISE, STEELE a MITRE. *MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy*. Mitre att&ck. [online] 2020. [cit. 2022-05-05]. Dostupné z: https://collaborate.mitre.org/attackics/img_auth.php/3/37/ATT&CK_for_ICS_-_Philosophy_Paper.pdf.
- [35] VALERY a YAKOV. *Cat Karat Packet Builder*. [online] 2010. [cit. 2022-05-05]. Dostupné z <https://sites.google.com/site/catkaratpacketbuilder/>.
- [36] OZANSOY, ZAYEGH a KALAM. *Time synchronisation in a IEC 61850 based substation automation system*. Power Engineering Conference, 2008. AUPEC '08. Australasian Universities. 1 - 7. [online] 2009. [cit. 2022-04-19]. Dostupné z: https://www.researchgate.net/publication/224400747_Time_synchronisation_in_a_IEC_61850_based_substation_automation_system
- [37] MOCANU, Stéphane a Jean-Marc THIRIET. *Experimental study of performance and vulnerabilities of IEC 61850 process bus communications on HSR networks*. EuroS&PW 2020 - IEEE European Symposium on Security and Privacy Workshops [online]. 2020, (10.1109/EuroSPW51379.2020.00085), 584-593 [cit. 2022-05-05]. Dostupné z: <https://hal.archives-ouvertes.fr/hal-02921495/document>
- [38] SCHLEGEL, Roman; OBERMEIER, Sebastian; SCHNEIDER, Johannes. *A security evaluation of IEC 62351*. Journal of Information Security and Applications, 2017, 34: 197-204. [cit. 2022-05-05]. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S2214212616300771?via%3Dihub#fn0015>
- [39] ZAHRADNÍK, Jiří. *Testování zranitelností v průmyslových sítích*. Brno, 2020, 81 s. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Petr Blažek. [cit. 2022-05-05]. Dostupné z: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=209361

ZOZNAM SYMBOLOV A SKRATIEK

Skratky:

ACSI	Abstraktné rozhranie komunikačných služieb
AES	Pokročilý štandard šifrovania
APDU	Application Protocol Data Unit
APPID	Aplikačný identifikátor
ARP	Protokol rozlišovania adries
ASDU	Dátová jednotka aplikačnej služby
CBC	Režim činnosti blokovej šifry
CC	Riadiaca stanica
CIA	Dôvernosť, integrita, dostupnosť
CLI	Rozhranie príkazového riadku
ČSN	Česká technická norma
DCE	Zariadenie na ukončenie dátových obvodov
DH	Diffie-Hellman
DoS/DDoS	Odmietnutie služby/Distribuované odmietnutie služby
DTE	Dátové koncové zariadenie
ENISA	Agentúra Európskej únie pre kybernetickú bezpečnosť
EPA	Vylepšená výkonná architektúra
GCM	Galois/Opačný mód
GOOSE	Generická objektovo orientovaná udalosť rozvodne
GSSE	Generická udalosť stavu rozvodne
GUI	Grafické užívateľské rozhranie
HMAC	Hashovaný autentifikačný kód správy
ICMP	Internet Control Message Protocol
ICS	Priemyselné riadiace systémy
IDPS	Systémy detekcie a prevencie narušenia
IEC	Medzinárodná elektrotechnická komisia
IED	Inteligentné elektronické zariadenie
IEEE	Inštitút elektrických a elektrotechnických inžinierov
IP	Internetový protokol
ISO	Medzinárodná organizácia pre štandardizáciu
LPCI	Informácie o riadení protokolu spojenia
LPDU	Dátová jednotka linkového protokolu
MAC	Overovací kód správy
MMS	Špecifikácia výrobnnej správy
MU	Spojovacia jednotka
NIST	Národný inštitút pre štandard a technológiu
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OSI	Prepojenie otvorených systémov

OT	Prevádzková technológia
PCM	Správca ochrany a kontroly
PDU	Protokolová dátová jednotka
PDU	Protokolová dátová jednotka
PFS	Perfektné budúce tajomstvo
PLC	Programovateľný logický ovládač
PoC	Proof-of-Concept
POU	Organizačná jednotka programu
PSS	Pravdepodobnostná podpisová schéma
RDP	Protokol vzdialenej pracovnej plochy
RFC	Žiadosť o pripomienky
RSA	Rivest, Shamir, Adleman – kryptografický algoritmus
RTU	Vzdialená koncová jednotka
SCADA	Systémy pre dohľad, riadenie a zber dát
SCL	Jazyk konfigurácie rozvodne
SCSM	Mapovanie špecifických komunikačných služieb
SHA	Zabezpečený hašovací algoritmus
SNMP	Jednoduchý riadiaci protokol siete
SSH	Secure Shell
SV	Vzorkované hodnoty
TCP	Protokol na kontrolu prenosu
TCS	Trip Circuit Supervision
TLS	Zabezpečenie transportnej vrstvy
VMD	Virtuálne výrobné zariadenie
VPN	Virtuálna privátna sieť
XML	Rozšíriteľný značkovací jazyk

Symboly:

<i>C/D</i>	dôsledok
<i>C_A</i>	dôsledok geografického vplyvu
<i>C_C</i>	finančný dôsledok
<i>C_T</i>	časový dôsledok
<i>D_D</i>	dopad na požiadavku dôvernosti
<i>D_I</i>	dopad na požiadavku integrity
<i>D_O</i>	dopad na požiadavku dostupnosti
<i>P_A/P_U</i>	pravdepodobnosť útoku
<i>P_E</i>	pravdepodobnosť účinnosti bezpečnostného mechanizmu
<i>P_I</i>	pravdepodobnosti prerušenia útoku
<i>P_N</i>	pravdepodobnosť neutralizácie hrozby
<i>P_Z</i>	pravdepodobnosť zásahu
<i>R</i>	riziko

ZOZNAM PRÍLOH

PŘÍLOHA A - TABULKY HODNŮT PRE ATRIBÚT D	85
PŘÍLOHA B - VÝPOČET ANALÝZY RIZÍK TESTOVANÝCH ÚTOKOV	86

Příloha A - Tabuľky hodnôt pre atribút D

A.1 Tabuľka hodnôt D_d reprezentujúcich dopad na požiadavku dôvernosti*

Rozsah narušenia dôvernosti	D_d
Všetky informácie v systéme	1.0
Prevažná časť informácií v systéme	0.7
Polovica informácií v systéme	0.5
Niektoré informácie (s presahom konkrétnej komunikácie)	0.3
Informácie v rámci 1 komunikácie	0.1

* Dôvernosť je hodnotená na základe rozsahu neautorizovaného prístupu.

A.2 Tabuľka hodnôt D_i reprezentujúcich dopad na požiadavku integrity*

Rozsah narušenia integrity (trieda dátovej integrity)	D_i
Narušenie I1 (10^{-6})	1.0
Narušenie I2 (10^{-10})	0.5
Narušenie I3 (10^{-14})	0.1

*Integrita je hodnotená ako pravdepodobnosť dátovej chyby na základe tried dátovej integrity v IEC 61850-5 Kapitola 11.3.2, pomerovo upravená.

A.3 Tabuľka hodnôt D_o reprezentujúcich dopad na požiadavku dostupnosti.*

Trvanie nedostupnosti systému podľa typu komunikácie			D_o
Client-server (MMS/-104)	IED-IED (MMS)	Kritické komunikácie (GOOSE/SMV)	
800 ms	12 ms	>3 ms	1.0
400 ms	8 ms	Jednotky vynechaných vzoriek	0.5
100 ms	4 ms	3 ms	0.1

*Dostupnosť je hodnotená ako celkový čas oneskorenia potrebný pri zotavení komunikácie, na základe stanov v IEC 61850-5 Kapitola 11.4.4, pomerovo upravené.

Příloha B - Výpočet analýzy rizík testovaných útokov

Analýza sieťovej komunikácie/Odpočúvanie

- P_U = Pokiaľ útočník prenikol do siete, je pomerne jednoduché komunikáciu odchytať/odpočúvať nakoľko nie je šifrovaná. Z tohto dôvodu je stanovená pravdepodobnosť využitia útoku na 100%. **$P_U = 1$**
- $P_E = P_Z \times P_N$ = Jedná sa o pasívny útok, ktorý sám o sebe nie je možné detegovať nakoľko prebiehal z útočnickej stanice (0) x Pokiaľ útok nie je detegovaný, je minimálna pravdepodobnosť jeho neutralizácie (10%). **$P_E = 0 \times 0.1 = 0$**
- $D = 1 - (1 - D_D) \times (1 - D_I) \times (1 - D_O) =$ Dopad na dôvernosť sa týka iba prenášaných informácií po sieti (0.3), integrita a dostupnosť nie je narušená. **$D = 0.3$**
- Výsledok: Predpoklad využiteľnosti útoku je 100%, ale jeho riziko iba 30%.

Časová synchronizácia SMV

- P_U = Náročnosť útoku na základe nutnej znalosti polí SMV rámcu a dosah na vkladanie vlastných hodnôt -60% **$P_U = 0.4$**
- $P_E = P_Z \times P_N$ = Nakoľko dochádza k oneskoreniu služby a následnému neštandardnému stavu je porucha pomerne ľahko detekovateľná (75%) x Pre neutralizáciu útoku po odhalení je nutný zásah administrátora a navrátenie hodnôt. (-75 %). **$P_E = 0.75 \times 0.2 = 0.1875$**
- $D = 1 - (1 - D_D) \times (1 - D_I) \times (1 - D_O) = 1 - (1 - 0.3) \times (1 - 0.5) \times (1 - 1) = 1$
- Výsledok: Predpoklad využiteľnosti útoku je 40%, ale jeho riziko 33%.

GOOSE spoofing

- P_U = Zvýšená náročnosť útoku, nakoľko je nutná znalosť princípu GOOSE a možnosť modifikácie rámcu -60%. **$P_U = 0.4$**
- $P_E = P_Z \times P_N$ = Nakoľko môže dochádzať k častému vypínaniu/zmeny vo funkčnosti systému je porucha ľahko detekovateľná (80%) x časovo náročnejší troubleshooting a rozpoznanie problematických rámcov (-60%) **$P_E = 0.4 \times 0.4 = 0.32$**
- $D = 1 - (1 - D_D) \times (1 - D_I) \times (1 - D_O) = 1 - (1 - 0.3) \times (1 - 0.5) \times (1 - 1) = 1$
- Predpoklad využiteľnosti útoku je 40%, ale jeho riziko 27%.

MMS Man in the Middle - pasívny

- P_U = Vysoký predpoklad odchytenia ARP správy a zneužitie ARP na MitM nakoľko nie je komunikácia šifrovaná= 85% **$P_U = 0.85$**
- $P_E = P_Z \times P_N$ = Nakoľko sa jedná o pasívny útok, je nízky predpoklad odhalenia (20%), a odhalenie je očakávané jedine v prípade ak by operátor sledoval ARP tabuľku x Pokiaľ útok nie je detegovaný, je zároveň náročne ho neutralizovať (20%) **$P_E = 0.2 \times 0.2 = 0.04$**
- $D = 1 - (1 - D_D) \times (1 - D_I) \times (1 - D_O) = 1 - (1 - 0.3) \times (1 - 0) \times (1 - 0) = 0.3$

- Výsledok: Predpoklad využiteľnosti útoku je 85%, ale jeho riziko iba 30%, nakoľko nenaruša požiadavku dostupnosti.

MMS Man in the Middle – aktívny

- $P_U =$ Vysoký predpoklad odchytenia ARP správy a zneužitie ARP na MitM nakoľko nie je komunikácia šifrovaná = 85%. **$P_U = 0.85$**
- $P_E = P_Z \times P_N =$ Nakoľko sa už jedná o aktívny útok, je očakávaný výpadok/neštandardný stav a tým pádom rýchlejšie odhalenie (70%) x neutralizáciou je navrátenie ARP tabuliek a lokalizácia útočníka, čo je náročné na zdroje (ľudské aj časové) (70%) **$P_E = 0.7 \times 0.7 = 0.49$**
- $D = 1 - (1 - D_D) \times (1 - D_I) \times (1 - D_O) = 1 - (1 - 0.3) \times (1 - 0.5) \times (1 - 1) = 1$
- Výsledok: Predpoklad využiteľnosti útoku je 85% a jeho riziko 43%, nakoľko naruša bezpečnostnú požiadavku dostupnosti, ale je zároveň jednoducho detekovateľný.

DoS ICMP Flood

- $P_U =$ Veľmi jednoducho vykonateľný útok pomocou dostupných nástrojov **$P_U = 1$**
- $P_E = P_Z \times P_N =$ Nakoľko dochádza k častej nedostupnosti/zmene vo funkčnosti systému je porucha ľahko detekovateľná (90%), najmä keď sa jedná o ICMP protokol x Nutnosť zásahu administrátora a v prípade nedostupnosti cieľového systému aj fyzický zásah (60 %). **$P_E = 0.9 \times 0.6 = 0.54$**
- $D = 1 - (1 - D_D) \times (1 - D_I) \times (1 - D_O) = 1 - (1 - 0) \times (1 - 0) \times (1 - 1) = 1$
- Výsledok: Predpoklad využiteľnosti útoku je 100% a jeho riziko je taktiež vyššie 54%. Využiteľnosť je vysoká z dôvodu jednoduchosti vykonania a riziko je vyššie z dôvodu výpadku dostupnosti a spôsobenie vysokého oneskorenia.