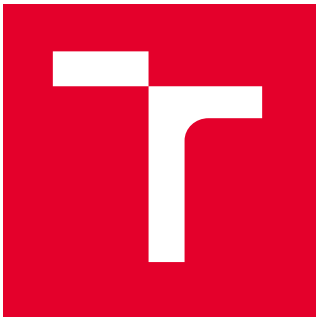


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

KYBERNETICKÁ BEZPEČNOST IOT ZAŘÍZENÍ VYUŽÍVAJÍCÍ PROTOKOL MQTT

CYBERSECURITY OF IOT DEVICES USING THE MQTT PROTOCOL

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Petr Hanák**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Radek Fujdiak, Ph.D.**
SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Petr Hanák ***ID:*** 240914

Ročník: 3 ***Akademický rok:*** 2023/24

NÁZEV TÉMATU:

Kybernetická bezpečnost IoT zařízení využívající protokol MQTT

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je navrhnout a implementovat bezpečnostní opatření pro komunikaci zařízení ESCON-C prostřednictvím protokolu MQTT. Výsledkem tak bude zabezpečená (hardened) verze ESCON-C s MQTT protokolem. V úvodní části student provede rešerši související s protokolem MQTT, zaměřenou na identifikaci hlavních bezpečnostních rizik a standardů v oblasti IoT komunikace. Využito bude odborné a vědecké literatury. Výstupem teoretické části bude bezpečnostní profil zařízení s identifikovanými vektory útoku, mírou rizika, a aktivy. Na základě rešerše student navrhne konkrétní bezpečnostní opatření, s důrazem na kvalitu a efektivitu zabezpečené komunikace. V praktické části student implementuje navržená opatření na zařízení ESCON-C a provede ověření bezpečnostním testováním. Na základě získaných výsledků student provede optimalizaci opatření a jejich finalizaci. Závěr práce bude obsahovat kompletní dokumentaci, včetně technických specifikací, metodiky a analýzy výsledků testování.

DOPORUČENÁ LITERATURA:

[1] CHOI, Seul-Ki; YANG, Chung-Huang; KWAK, Jin. System Hardening and Security Monitoring for IoT Devices to Mitigate IoT Security Vulnerabilities and Threats. KSII Transactions on Internet & Information Systems, 2018, 12.2.

[2] ECHEVERRÍA, Aarón, et al. Cybersecurity model based on hardening for secure internet of things implementation. Applied Sciences, 2021, 11.7: 3260.

Termín zadání: 5.2.2024 ***Termín odevzdání:*** 28.5.2024

Vedoucí práce: doc. Ing. Radek Fujdiak, Ph.D.

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

ABSTRAKT

Tato bakalářská práce se věnuje možnostem zabezpečení komunikace protokolem MQTT, který se hojně využívá v průmyslu a při komunikaci IoT zařízení. Práce pojednává o slabinách a zranitelnostech protokolu MQTT a následně opatření, které se dají aplikovat pro bezpečnou komunikaci v sítích obsahující takovéto zařízení. Zabezpečená komunikace je demonstrována na zabezpečeném experimentálním pracovišti obsahující zařízení ESCON-C, které pomocí protokolu MQTT komunikuje. Použitá strategie zabezpečení obsahuje primárně bezpečnou komunikaci napříč sítěmi skrz bezpečný komunikační kanál, kde se na jedné straně nachází MQTT klient a na druhé MQTT broker simulující nasazení zařízení ESCON-C v průmyslovém prostředí. Díky tomuto přístupu lze mitigovat většinu slabin, které protokol MQTT má.

KLÍČOVÁ SLOVA

Protokol, MQTT, komunikace, zranitelnost, zabezpečení, analýza

ABSTRACT

This bachelor's thesis focuses on the possibilities of securing communication using the MQTT protocol, which is widely used in industry and for IoT device communication. The thesis discusses the weaknesses and vulnerabilities of the MQTT protocol and subsequently the measures that can be applied for secure communication in networks containing such devices. Secured communication is demonstrated in a secure experimental workplace containing an ESCON-C device that communicates using the MQTT protocol. The security strategy used primarily involves secure communication across networks through a secure communication channel, where the MQTT client is on one side and the MQTT broker, simulating the deployment of the ESCON-C device in an industrial environment, is on the other. This approach mitigates most of the weaknesses inherent in the MQTT protocol.

KEYWORDS

Protocol, MQTT, communication, vulnerability, security, analysis

HANÁK, Petr. *Kybernetická bezpečnost IoT zařízení využívající protokol MQTT*. Bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2024. Vedoucí práce: Ing. Radek Fujdiak, PhD.

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Petr Hanák
VUT ID autora:	240914
Typ práce:	Bakalářská práce
Akademický rok:	2023/24
Téma závěrečné práce:	Kybernetická bezpečnost IoT zařízení využívající protokol MQTT

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/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu Ing. Radku Fujdiakovi, Ph.D. za jeho vedení, konzultace a podnětné rady a návrhy k práci. Dále bych rád poděkoval zaměstnancům firmy Easycon Solutions s. r. o. za jejich vstřícný přístup, rady a doporučení týkající se praktické části této práce.

Obsah

Seznam obrázků

Seznam výpisů

Úvod

MQTT protokol patří mezi hlavní standardizované protokoly v IoT (Internet of things), které zahrnují pravidla pro výměnu informací a dat mezi technickými zařízeními připojenými do stejné sítě. Jedná se o otevřený, obousměrný a flexibilní protokol s nízkou náročností na objem přenášených dat a s možností implementace na libovolném hardwaru nebo softwaru. Z jednoduchosti protokolu MQTT však vyplývají zranitelnosti a slabiny, které musí být při praktickém použití brány v potaz.

Teoretické část této bakalářské práce obsahuje popis struktury a architektury MQTT s ohledem na zabezpečení přenášených dat. Hlavní pozornost je věnována obecné analýze slabin a zranitelností protokolu MQTT, analýza zranitelností z databáze CVE a popis možností, kterými se dá dosáhnout bezpečné komunikace při použití MQTT. Součástí je také popis zabezpečované služby, STRIDE analýza jednotlivých interakcí v zabezpečovaném systému, strategie bezpečnostních opatření a návrh bezpečnostních opatření pro tyto dříve popsané interakce zařízení. Popsány byly také zařízení následně použité v praktické části.

Praktická část práce obsahuje schéma a popis experimentálního pracoviště, implementaci bezpečnostních opatření, která byla navržena v teoretické části na zařízení ESCON-C od firmy Easycon Solutions s. r. o. Implementovaná opatření se týkají pouze části komunikace, kde řídící jednotka komunikuje se serverem přes router, který zařízení ESCON-C obsahuje. Výsledkem jsou nakonfigurovaná bezpečnostní opatření, díky kterým služba komunikuje po zabezpečeném komunikačním kanálu a přístup k jednotlivým zařízením, která se v síti účastní komunikace, je silně omezen. Na závěr praktické části jsou tyto opatření testovány pomocí penetračního testování, které simuluje možné útoky na zabezpečovaný systém a následně je shrnuto fungování těchto bezpečnostních opatření pro tento konkrétní případ využití. Práce je zakončena aktualizací STRIDE a demonstrací MQTT komunikace na straně serveru a klienta.

1 Protokol MQTT

Protokol MQTT (Message Queing Telemetry Transport) byl vyvinut jako protokol pro potřebu spojení senzorů na ropných potrubích se satelity v roce 1999 firmou IBM. Jedná se o asynchronní protokol fungující na síťové vrstvě ISO/OSI modelu. Navržen byl pro jednoduchá zařízení s omezeným výkonem, která se často vyskytují v prostředí, kde hrozí vysoká latence, malá šířka pásma a nespolehlivost sítě, ke které jsou připojené. Aktuální nejnovější verze MQTT je verze 5.0, která jako standard vyšla v roce 2019 [1].

1.1 MQTT architektura

Komunikace mezi zařízeními využívající MQTT funguje na principu Publisher / Subscriber. V síti se vyskytuje MQTT broker a klientská zařízení. MQTT broker slouží jako centrální jednotka, která přijímá všechny zprávy od klientských zařízení a poté je rozesílá všem zařízením, pro které jsou tyto zprávy určeny. Zařízení v síti mohou zprávy získávat tím, že se přihlásí jako tzv. Subscriber (odběratel) k danému Topic (tématu), do kterého je zpráva zařazena. Autor zprávy, zařízení v roli Publisher (vydavatel), odesílá zprávy s určeným tématem centrální jednotce, ta se dále stará o doručení těchto zpráv všem odběratelům tohoto tématu [2].

Témata se zapisují pomocí notace obsahující znak / a skládají se hierarchicky od nejvšeobecnějšího tématu po to nejvíce specifické, např.

Dům/První_patro/Byt2/kuchyně/senzor_teploty.

Zařízení, které bude chtít znát výsledky měření senzoru teploty se přihlásí k odběru tohoto tématu. Ovšem zařízení, které bude chtít znát výsledky měření všech měření senzorů v kuchyni, se přihlásí k odběru tématu

Dům/První_patro/Byt2/kuchyně/+,

kde + nahrazuje jakékoliv zařízení na této úrovni hierarchie. Zařízení sbírající údaje ze všech témat o prvním patře domu se přihlásí k tématu

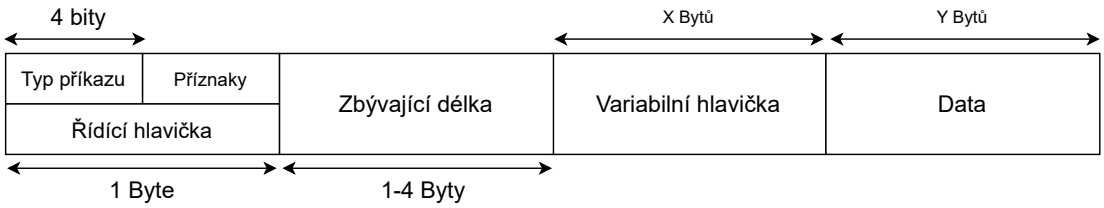
Dům/První_patro/#,

kde # nahrazuje několik úrovní hierarchie tématu. Tato architektura umožňuje jednoduché škálování sítě a počtu zařízení, protože nová zařízení připojená do sítě se jednoduše přihlásí k odběru témat, která jsou pro ně relevantní. Klientská zařízení

ani nepotřebují vědět, kolik zařízení a jaké v síti jsou, protože spolu nekomunikují přímo, ale komunikaci řídí MQTT broker a všechny zprávy v síti jdou přes něj [2].

1.2 Struktura MQTT packetu

Největší výhodou protokolu MQTT je jeho jednoduchost a nenáročnost. Typický packet obsahuje hlavičku o fixní velikosti 2 Byty a dále volitelnou hlavičku a data, která se ale ve zprávě vůbec nemusí vyskytovat.



Obr. 1.1: Struktura MQTT packetu. Zpracováno na základě [3].

První Byte je rozdělen na dvě 4bitové části, první část určuje typ příkazu, který packet přenáší. Toto je rozlišeno podle hodnoty, která nabývá čísel 0-15. Hodnoty 0 a 15 jsou při komunikaci zakázány, protože jsou rezervovány pro budoucí využití v novějších verzích protokolu. Druhá část specifikuje příznaky packetu, které využívají pouze některé typy packetů. Příznaky specifikují parametry QoS (Quality of Service), duplicitu packetu nebo tzv. Publish retain, čímž brokerovi říká, aby tuto zprávu pro dané téma uložil a každému novému zařízení odebírající toto téma ho poslal.[3] Zbývající délka určuje velikost packetu. Minimální velikost jsou 2 Byty, pokud packet neobsahuje žádné volitelné hlavičky a data. Maximální velikost packetu je $2^{28} = 256\,\text{MB}$. To umožňuje MQTT packetům být proměnlivé tak, aby se zbytečně nepřenášely pouze velké zprávy nebo naopak velké množství malých zpráv. Volitelná hlavička obsahuje identifikátor packetu, který obsahuje dodatečné informace k odesílané zprávě, ale povinný je jen pro tyto typy zpráv:

- CONNECT
- PUBLISH
- SUBSCRIBE
- SUBACK
- UNSUBSCRIBE
- UNSUBACK
- PUBACK, PUBREC, PUBREL, PUBCOMP.

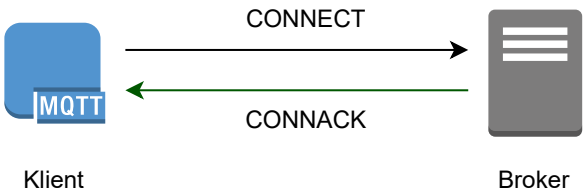
Např. zprávy typu PINGREQ a PINGRESP pro kontrolu spojení zařízení žádnou volitelnou hlavičku neobsahují. Poslední část packetu obsahuje samotná data, která jsou packetem přenášena [3].

Název	Hodnota	Směr komunikace	Popis
Rezervováno	0	Zakázáno	Rezervováno pro pozdější užití
CONNECT	1	Klient na Server	Požadavek klienta pro připojení k Serveru
CONNACK	2	Server na Klienta	Potvrzení přijetí CONNECT
PUBLISH	3	Oboustranná	Odeslání zprávy
PUBACK	4	Oboustranná	Potvrzení o přijetí zprávy
PUBREC	5	Oboustranná	Potvrzení o přijetí PUBLISH (QoS 2)
PUBREL	6	Oboustranná	Potvrzení o potvrzení přijetí PUBLISH (Qos 2)
PUBCOMP	7	Oboustranná	Potvrzení o konci komunikace (Qos 2)
SUBSCRIBE	8	Klient na Server	Požadavek klienta pro odběr zpráv
SUBACK	9	Server na Klienta	Potvrzení SUBSCRIBE
UNSUBSCRIBE	10	Klient na Server	Požadavek klienta o zrušení odběru zpráv
UNSUBACK	11	Server na Klienta	Potvrzení UNSUBSCRIBE
PINGREQ	12	Klient na Server	Klient informuje o svém připojení
PINGRESP	13	Server na Klienta	Potvrzení PINGREQ
DISCONNECT	14	Oboustranná	Klient se odpojuje od brokera
AUTH	15	Oboustranná	Autentizace zařízení při spojení

Tab. 1.1: Typy MQTT verze 5.0 zpráv. Zpracováno na základě [3].

1.3 Komunikace mezi zařízeními

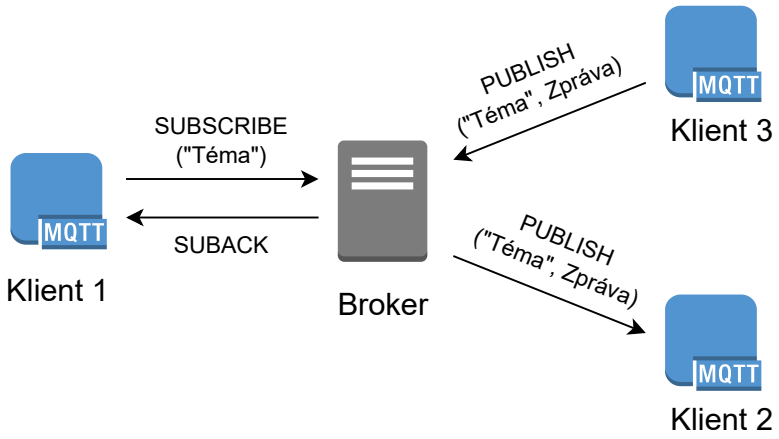
Při počáteční komunikaci mezi zařízením a MQTT brokerem posílá zařízení MQTT brokerovi zprávu typu CONNECT. Ve zprávě zařízení specifikuje, jestli data obsahují přihlašovací jméno a heslo, informace, zda se jedná o nové spojení nebo pokračování spojení, které už bylo v minulosti navázáno a také informace o tom, jestli a jakou zprávu má broker odeslat na předem definovaná témata, pokud zařízení nečekaně ztratí spojení s MQTT brokerem tzv. Will. Broker odesílá jako odpověď zprávu CONNACK. Pokud se zařízení připojilo úspěšně, ve volitelné hlavičce packetu bude nastavena hodnota 0. Při neúspěšném připojení se v hlavičce nachází číselná hodnota, podle které se dá zjistit, z jakého důvodu nebylo připojení úspěšné [4].



Obr. 1.2: Připojení zařízení k MQTT brokerovi [3].

Nejnovější verze MQTT, MQTT verze 5.0, může mezi tyto dvě zprávy klient i broker přidat zprávu AUTH, ve kterých specifikují pokročilé metody autentizace obou stran a nemusí tak využívat pouze uživatelské jméno a heslo, které se dá standardně posílat v CONNECT. Využity mohou být např. metody SCRAM nebo Kerberos. Obě strany mohou také protistranu ověřit znovu, aniž by museli spojení přerušovat [5].

Po úspěšném navázaní spojení jsou zařízení připravena posílat data a přijímat data od jiných zařízení. Klientské zařízení odešle požadavek SUBSCRIBE brokerovi, ve kterém uvede téma, od kterého chce dostávat zprávy. Poté zařízení čeká na zprávy, které jsou určeny pro jeho zvolené téma, nebo samo odesílá zprávy pomocí PUBLISH. Ve zprávě PUBLISH definuje, pro jaké téma je tato zpráva určena a odesílá ho brokerovi, který bude zprávu dále posílat jiným zařízením [4].



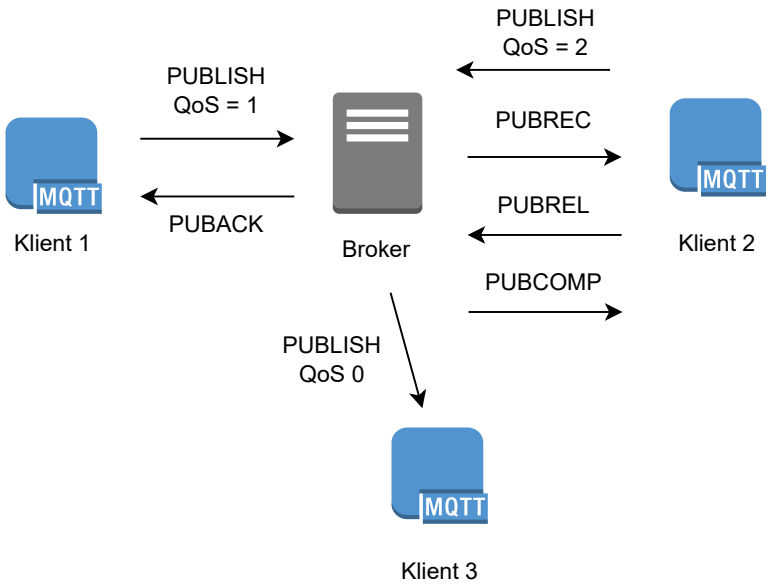
Obr. 1.3: Komunikace zařízení připojených k MQTT brokerovi [3].

MQTT protokol je schopný garantovat doručení zpráv. K tomuto se využívá paramter QoS, který se nachází v příznaku packetů ve fixní hlavičce. Jsou na něj vyhrazeny 2 bity a nabývá hodnot 0-2.

QoS 0 *„delivery at most once“* – V tomto módu klientská stanice nečeká na potvrzení příjmu dat a předpokládá, že data byla doručena. Zprávu si neukládá pro případná znovu odeslání.

QoS 1 *„delivery at least once“* – Klient odešle zprávu a nechá si ji uloženou a od příjemce zprávy čeká na potvrzení doručení PUBACK. Pokud po určité době nepřijde, zprávu odesílá znova.

QoS 2 *„exactly once“* – Pro doručení zprávy se využívá čtyřcestný handshake. Klient odesílá zprávu a čeká na potvrzení PUBACK od příjemce. Když dostane potvrzení příjemce, pošle příjemci zprávu PUBREL, že může původní zprávu smazat a obratem dostane zprávu PUBCOMP, že výměna zpráv byla provedena úspěšně [6].



Obr. 1.4: Komunikace zařízení s různou úrovní QoS [3].

Zařízení, které je k brokerovi připojeno, ale aktuálně nekomunikuje, odesílá zprávy PINGREQ, kterými brokerovi dává vědět, že je stále připojené a nemá být odpojeno. Každé zařízení má nastavenou svou hodnotu KeepAlive, po které se tento packet odesílá. Broker na tyto zprávy odpovídá PINGRESP, kterými potvrzuje připojení. V případě, že brokerovi žádné PINGREQ zprávy nepřijdou, po určité době se zařízením přeruší spojení.

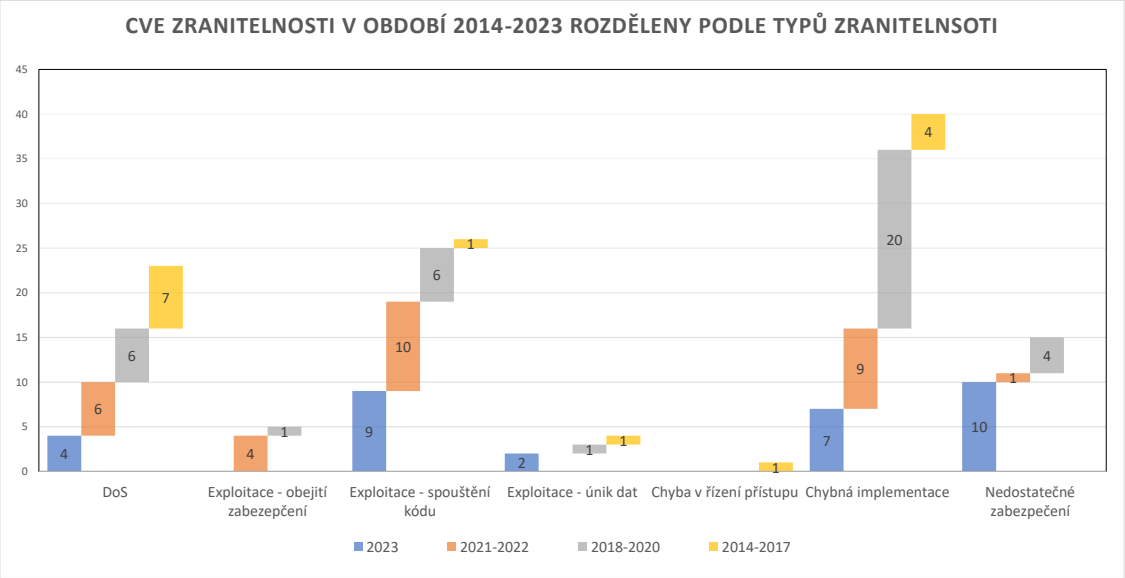
Komunikace zařízení probíhá do té doby, dokud jsou zařízení připojená k MQTT brokerovi. Zařízení se může odpojit pomocí zprávy DISCONNECT, kterou pošle brokerovi a oznamuje mu tím, že ukončuje spojení. Ve zprávě specifikuje pomocí číselného kódu, z jakého důvodu došlo k odpojení. Zařízení také mohlo být odpojeno nečekaně, např. kvůli poruše, ztrátě spojení nebo jiného důvodu. V tomto případě broker, pokud má od připojeného zařízení uloženou Will zprávu, odesílá tuto zprávu na téma, kterou při připojení zařízení definovalo [4].

2 Rizika a zranitelnosti MQTT protokolu

IoT zařízení využívající protokol MQTT mají často omezený výkon. Tento fakt společně s častým zanedbáním jakéhokoliv zabezpečení vystavuje tyto zařízení mnoha hrozbám.

Organizace OWASP (Open Worldwide Application Security Project) periodicky vydává doporučení týkající se zranitelností a chyb tzv. OWASP Top 10. Při vydaní poslední aktualizace svého žebříčku OWASP IoT Top 10 uvedla, že mezi nejčastější zranitelnosti a hrozby pro IoT zařízení jsou použití slabých nebo defaultních hesel pro přístup k zařízením, nedostatečné nebo chybějící šifrování dat při přenosu, ale také při ukládaní a také nedostatečný hardening zařízení. Mezi ten můžeme zařadit neaktuální verze software běžícího na použitých zařízeních, nedostatečné omezení nepotřebných služeb a celkové nastavení zařízení [7].

Dalším relevantním zdrojem informací je databáze zranitelností CVE. V databázi CVE se nachází 114 zranitelností protokolu MQTT nasbíraných od roku 2014. Konkrétní vyhledané zranitelnosti aktuální k datu 11. 12. 2023 jsou uvedeny v příloze A tohoto dokumentu. Ty se dají kategorizovat do těchto obecných skupin:



Obr. 2.1: Typy MQTT zranitelností v databázi CVE.

Nejčastěji se vyskytují problémy související se špatnou implementací aplikace nebo zařízení, díky které se dají jednoduše kompromitovat. Dále útočníci často využívají zranitelnosti, které jim umožní spouštět škodlivý kód a nebo zařízení odstavit z provozu. Jak data od organizace OWASP potvrzují, špatné zabezpečení je často se vyskytující problém. Většinou se jedná o konkrétní verze aplikací nebo firmwaru zařízení, která v nových verzí bude opravena [8].

2.1 Vektory útoku IoT zařízení

Vektor útoku je způsob, jakým útočník může využít zranitelnost a kompromitovat tak zařízení nebo systém. Vektory útoku na IoT zařízení můžeme rozdělit podle jejich cíle.

2.1.1 Útoky na zařízení

Sem se nejčastěji řadí útoky na samotné fyzické zařízení, kdy k němu útočník má přímý přístup. Útočník se může zařízení pokusit kompromitovat přes otevřené porty nebo záměnou jeho komponent, nahrát na něj škodlivý software a získat tak zařízení pod svou kontrolu. Další možností je odpojení zařízení od komunikační infrastruktury nebo rušení komunikace (v případě bezdrátových sítí použití rušičky signálu nebo narušení spojení přes kabely) anebo zničení celého zařízení.

Pokud útočník nemá přímý přístup k zařízení, stále může zařízení vyřadit z provozu pomocí Dos (Denial of Service) nebo DDos (Distributed denial of service) útoků, pomocí kterých zahltí zařízení požadavky, které nebude stíhat procesor zařízení vyřizovat a pro legitimního uživatele se zařízení stane nedostupné [9].

2.1.2 Útoky na komunikační infrastrukturu

Útokem na komunikační strukturu útočník snaží zamezit legitimnímu uživateli použití zařízení nebo služby, která s daným zařízením pracuje. V případě MQTT, které může být nasazeno na síti s omezenou šířku pásma nebo vysokou latenci, bude zahlcení sítě jinými požadavky nebo provozem ještě více destabilizující a může na čas vyřadit celou infrastrukturu z provozu [9].

2.1.3 Útok na rozhraní pro komunikaci se zařízením

V případě útoku na rozhraní pro komunikaci se zařízením se útočník většinou snaží převzít kontrolu nad zařízením nebo celou sítí, ve které jsou zařízení připojena. Kompromitací může útočník taky získat přístup k datům, která se ukládají v cloudu a může dojít k jejich úniku, což může poškodit reputaci vlastníkovi a působit další problémy. Útočník může data taky smazat nebo poškodit, což může ohrozit fungování dalších systémů nebo zařízení, která jsou na těchto datech závislá [9].

2.2 Zranitelnosti MQTT protokolu

2.2.1 Filtrace packetů

Packety MQTT mají své číslo portu. Pro standardní MQTT se používá port 1883 a pro MQTT využívající TLS 8883. Ačkoliv může být administrátorem brokera nastaveno jiné, unikátní číslo portu pro náročnější filtraci podle čísla portu, zpráva CONNECT obsahuje název protokolu, takže může být jednoduše vyfiltrována tímto způsobem. Ačkoliv samotné číslo portu nijak významně neovlivňuje zabezpečení samotné komunikace, i tak je vhodné používat nestandardní číslo portu, které může útočníka zmást nebo zpomalit [10].

2.2.2 Šifrování dat

Protokol MQTT ze základu nepoužívá žádné šifrování dat, aby zůstal jednoduchý a posílal jen co nejmenší zprávy. Toto je ovšem veliký problém, protože útočník při komunikaci přes nezabezpečený kanál může komunikaci zachytit a velice jednoduše získat přenášené informace a téma, pro které byly určeny. Přenášená komunikace musí být šifrována a nebo útočník nesmí být schopný komunikaci zachytit. Při použití MQTT je tedy vhodné nasazení VPN, např. technologie TLS nebo IPsec [10].

VPN

Pro bezpečnou komunikaci zařízení s MQTT brokerem může být použit VPN tunel, který bezpečně odděluje komunikaci od nezabezpečeného prostředí internetu, po kterém se komunikace přenáší. Pomocí VPN se dá zaručit, že komunikace nebude po cestě možná odposlouchávat a data nebudou moct být při přenosu zaměněna, ani přečtena. Technologie VPN sama o sobě nezajišťuje žádné šifrování dat, pouze to, že data jsou přenášena bezpečně. Díky využití VPN je také možné se k síti připojit odkudkoliv a fakticky tak být se zařízeními na stejné síti i na dálku [11].

TLS

TLS umožňuje před začátkem komunikace dvou zařízení ustanovit bezpečný komunikační kanál. Útočník už poté není schopný komunikaci odposlouchávat. Použitím TLS můžeme garantovat autentizaci obou stran komunikace, integritu dat a že data budou při přenosu šifrována.

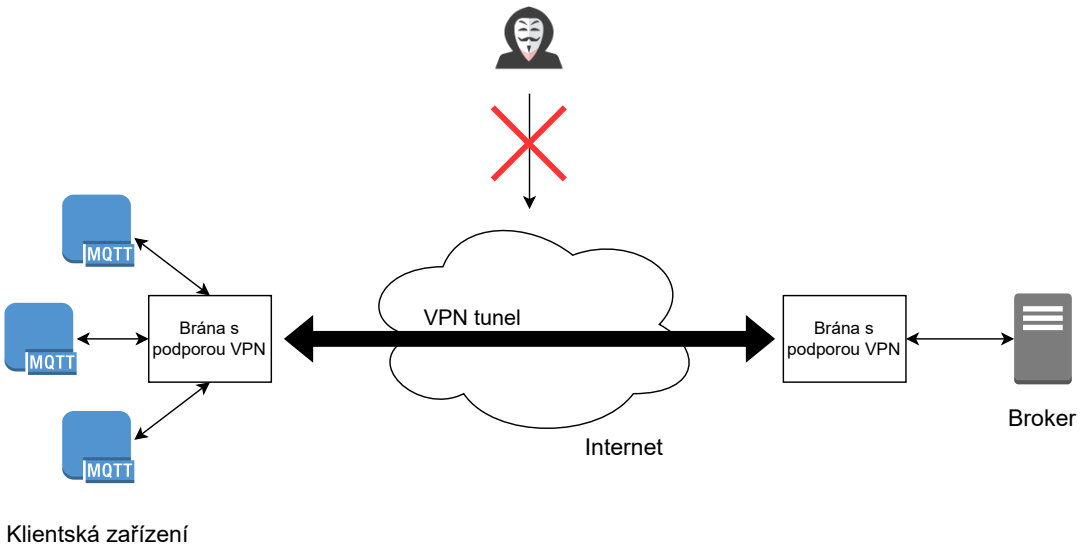
Na začátku probíhá tzv. TLS handshake, pomocí kterého se zařízení s MQTT brokerem domluví na verzi TLS (ta bývá zvolena podle toho, jakou nejnovější verzi zařízení komunikující s brokerem podporuje), způsobu šifrování dat, vymění si informace o svých certifikátech (MQTT broker odešle informace o svém certifikátu

a může si vyžádat od zařízení jeho certifikát, tím obě strany ví, s kým komunikují) a proběhne výpočet symetrického klíče, složeného z asymetrických klíčů obou zařízení, který je následně používán pro šifrování a dešifrování komunikace mezi těmito zařízeními.

Nasazení TLS může být v některých případech problematické, protože pro zařízení s nízkým výkonem bude handshake a šifrování komunikace spotřebovávat velké množství systémových zdrojů, a to zvedne vytížení procesoru a také spotřebu elektřiny. Další problém může nastat u sítí s nízkou šířkou pásma. Zprávy s šifrovaným obsahem budou obsahovat více dat a narůstá riziko, že zprávy nemusejí být doručeny celé nebo že nebudou doručeny vůbec [12].

IPsec

IPsec při použití nabízí dva hlavní módy, transportní a tunelový. Pro potřebu IoT zařízení se více hodí tunelový mód, kdy chytrá zařízení jsou jsou na jedné straně IPsec tunelu a broker, ke kterému jsou připojeny, je na druhé straně. S použitím IPsec v tunelovém módu pro zabezpečení komunikace se dá garantovat integrita a potencionální útočník nebude schopný odposlouchávat komunikaci. Pro použití IPsec je nutné speciálních zařízení, které IPsec podporují, sloužící jako brány na koncích VPN tunelu[13].



Obr. 2.2: Příklad komunikace pomocí tunelového režimu VPN [13].

2.2.3 Autentizace klientů

MQTT broker může využívat systém ověření klientů. Broker má svoje přihlašovací jméno a heslo které zabraňuje útočníkům, aby se bez ověření stali klientem v síti s rolí Publisher nebo Subscriber. Útočník, který je ve stejné síti jako klientská zařízení však stále může odposlouchávat komunikaci, která není šifrovaná a při pokusu připojení nového zařízení může ze zprávy CONNECT vyčíst přihlašovací jméno a heslo. Zpráva CONNECT také obsahuje parametr KeepAlive, který určuje dobu, po kterou je zařízení k brokerovi připojeno a poté se znovu připojuje. Pokud nedojde k obnovení této doby pomocí PINGREQ, může této situace útočník využít pro získaní přihlašovacích údajů [10].

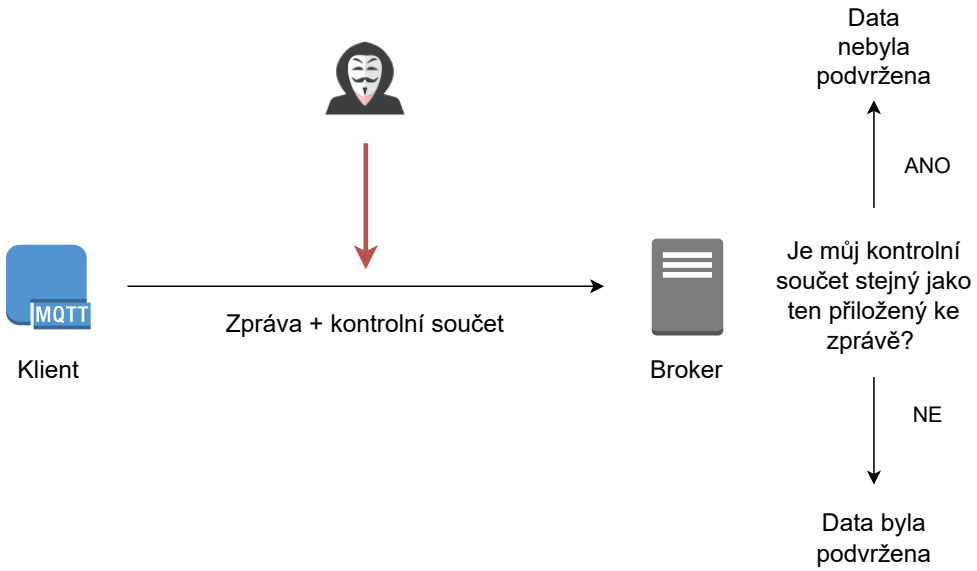
Zařízení je nutné autentizovat. Použito může být přihlašování, které podporuje MQTT protokol, ale data musí být při přenosu šifrována, aby nešla jednoduše odposlechnout. Dalším řešením je použití certifikátů, díky kterým můžou klient i broker před začátkem komunikace ověřit, že komunikují se správným, důvěryhodným zařízením [10].

2.2.4 Integrita dat

Integrita dat zaručuje, že data při přenosu nebyla zaměněna. Útočník, který vysledoval MQTT packety, může změnit obsah jejich dat. Toho může být dosaženo např. použitím programu Ettercap, který je přes filtry schopný změnit obsah dat přenášených zpráv [10]. Obzvlášť problematické to může být v případě, když jsou posílány například odkazy, odkud si stáhnout systémový nebo jiný update. Změnou tohoto odkazu může útočník zařízení donutit stáhnout nežádoucí software, díky kterému zařízení přidá do botnetu nebo ho kompletně vyřadí z provozu. Je několik metod, pomocí nichž se dá integrita dat zaručit:

Kontrolní součet – velmi rychlá varianta kontroly i pro větší zprávy, ale i tak mohou být data zaměněna, pokud zná útočník algoritmus součtu. Zařízení posílá data a k nim přidá výsledek kontrolního součtu. Druhé zařízení, které zprávu přijme, stejným algoritmem provede kontrolní součet a pokud se součty shodují, data nebyla po cestě zaměněna [14].

MAC algoritmus (Message authentication code algoritmus) – Algoritmus data šifruje symetrickým klíčem. Pro bezpečné použití se předpokládá, že komunikující strany si klíč před komunikací ustanovili bezpečně. Podobnou variantou je také HMAC (Hash-based MAC), kde se k symetrickému klíči přidá ještě hashovací funkce a výsledný MAC vypočítá použitím hashovací funkce, ke které se přidá symetrický klíč. Zařízení příjmající zprávu pomocí stejného klíče a stejné hashovací funkce vypočítá MAC a porovná ho s přijatým MAC [14].



Obr. 2.3: Použití kontrolního součtu pro ověření integrity dat.

Digitální podpis – Tato metoda je založena na asymetrické kryptografii. Každé zařízení je vybaveno dvojicí klíčů – soukromým a veřejným. Klient odesílající data je „podepíše“ svým soukromým klíčem a zprávu odešle. Zařízení, pro které jsou data určena, ověřuje podpis veřejným klíčem odesilatele, protože ten není tajný a je mu znám. Útočník nedokáže falšovat zprávy a není schopen se vydávat za cizí zařízení, protože nezná soukromý klíč, který je tajný [14].

3 Analýza rizik

Analýzou rizik se rozumí proces, při kterém se hledají způsoby, kterými by mohl být chráněný systém ohrožen. Hledají se zranitelnosti, které by mohly vést k přímému narušení systému útočníkem, ale také zranitelnosti, které vyplývají ze špatné konfigurace systému. Hlavním cílem analýzy rizik je včasné zjištění zranitelností, které systém obsahuje, a jejich mitigace, aby nemohly být zneužity při případném reálném útoku [15].

3.1 STRIDE analýza

STRIDE analýza je metoda analýzy rizik, při které se u chráněného systému hledají způsoby, jakými by na něj mohly být vedeny útoky. Zaměřuje se na šest hlavních typů hrozeb.

1. *Spoofing* – Útočník se při útoku bude snažit vydávat za jiného uživatele nebo jiné zařízení.
2. *Tampering* – Při útoku dojde k modifikaci dat nebo kódu, což může ohrozit funkčnost systému.
3. *Repudation* – Útočníkovi se podaří provézt neoprávněnou operaci a systém není schopný detekovat a správně logovat, kdo danou operaci provedl.
4. *Information disclosure* – Útočník neoprávněně získá přístup k souborům s daty cizích uživatelů nebo je odposlechne při jejich přenosu.
5. *Denial of service* – Snaha útočníka co nejvíce zamezit běžnému fungovaní zařízení a snaha znepřístupnit službu nebo zařízení běžnému uživateli.
6. *Elevation of privilege* – Útočník se při neoprávněném vniknutí do systému snaží získat práva uživatele s vyššími právy.

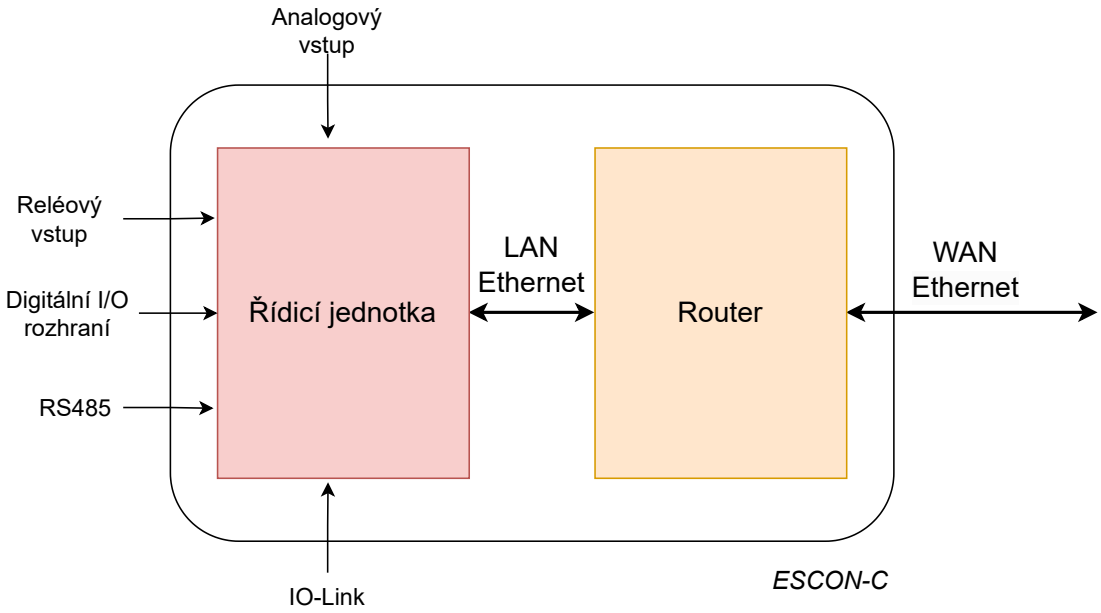
Později byl přidán také sedmý typ zranitelnosti, Lateral movement, který udává, jak daleko v síti nebo chráněném systému se útočník může dostat po neoprávněném přístupu dostat. Tento typ zranitelnosti byl přidán hlavně kvůli lepšímu využití STRIDE pro kybernetická ryzika na síťové hrozby[16]. Vhodné je si testovaný systém rozdělit na jednotlivé entity pomocí Data flow diagramu, který mapuje tok v systému. STRIDE analýza se poté dá provádět dvěma způsoby, STRIDE per Element a STRIDE per Interaction. STRIDE per Element se aplikuje na každou entitu samostatně a STRIDE per Interaction se aplikuje na interakci dvou entit.

4 Experimentální pracoviště

4.1 Experimentální pracoviště

Pro realizaci a testování opatření, která jsou součástí této práce bude použito zařízení ESCON-C od firmy EASYCON Solutions s. r. o. K zařízení, které slouží jako řídicí jednotka, jsou připojeny konkrétní průmyslová zařízení přes různá rozhraní, kterými ESCON-C disponuje. Data jsou dále periodicky odesílána do řídicí jednotky, která je poté pomocí protokolu MQTT odesílá na server. Pro komunikaci zařízení ESCON-C obsahuje router RUTX11, který zajišťuje připojení k internetu a slouží taky jako brána VPN tunelu, aby byla nemohla být komunikace odposlouchávána.

4.2 Zařízení ESCON-C



Obr. 4.1: Schéma zařízení ESCON-C, zpracováno na základě [17].

4.2.1 Řídicí jednotka

Řídicí jednotka zařízení ESCON-C obsluhuje softwarovou službu, která řídí sběr dat připojených průmyslových zařízení a jejich následné odesílání na server. Je možné k ní připojit zařízení přes tyto typy rozhraní:

- Digitální I/O
- Analogové vstupní rozhraní
- Reléový vstup
- Sériová sběrnice RS485
- IO-Link
- Ethernet
  S využitím TCP/IP je také možné použít protokoly pro vyčítání dat, například Modbus TCP a Profinet. [17]

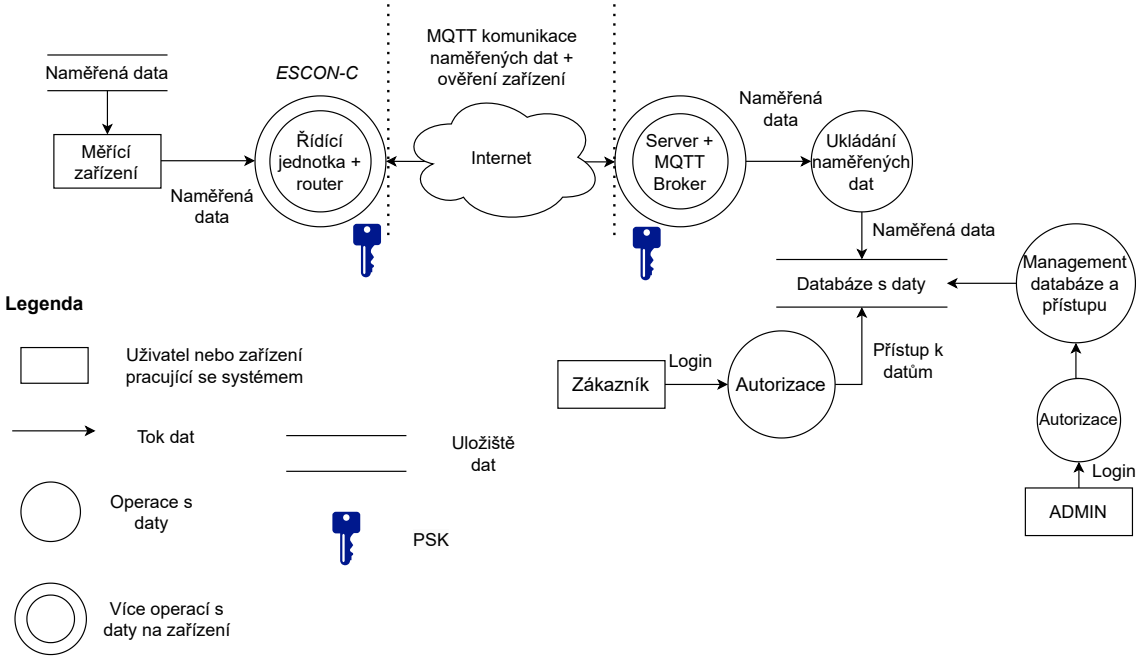
4.2.2 Router RUTX11

Router RUTX11 zajišťuje konektivitu zařízení ESCON-C se servery, na kterých se ukládají a zpracovávají data. Jedná se o router, který je určen pro nepřetržité použití ve stížených podmínkách. K routeru je možné se připojit pomocí tří LAN rozhraní a k internetu je připojený pomocí jednoho rozhraní WAN. V prostředí, kde není možné router připojit fyzicky k internetu kabelem, umožňuje router také připojení pomocí mobilní sítě, případně slouží mobilní síť jako redundantní zdroj internetového připojení. Router se dá na dálku spravovat pomocí RMS (Remote Management Systému), který výrobce nabízí a díky němuž může být jednoduše konfigurace routeru měněna na dálku. Dále podporuje také technologie Bluetooth a GPS a různé možnosti technologie VPN, jako jsou IPsec, OpenVPN, ZeroTier, Stunnel, WireGuard a další. [17]

5 Vstupní STRIDE analýza

Jednotlivé entity diagramu

- Naměřená data – Úložiště zařízení, do kterého se ukládají sbíraná data
- Naměřená data <-> Měřící zařízení – Naměřená data jsou připravena pro přenos na řídicí jednotku
- Měřící zařízení – Zařízení, které odesílá naměřená data do řídicí jednotky zařízení ESCON-C
- Měřící zařízení <-> Řídicí jednotka + router – Měřící zařízení odesílá naměřená data do řídicí jednotky
- Řídicí jednotka + router – Zařízení ESCON-C, které zpracovává nasbíraná data od zařízení sbírající data
- Řídicí jednotka + router <-> Server + MQTT broker – Přenos naměřených dat přes MQTT na server s MQTT brokerem
- Server + MQTT klient – Server obsahující MQTT brokera, který přijímá data od nasazených ESCON-C
- Ukládání naměřených dat – Proces ukládání dat
- Server + MQTT klient <-> Databáze s daty – Uložení dat do databáze na serveru
- Databáze s daty – Centrální úložiště naměřených dat
- Autorizace – Proces autorizace



Obr. 5.1: Vstupní Data flow diagram služby.

- Management databáze a přístupu – Správa databáze a přístupových práv pro uživatele
- Zákazník – Zákazník, který si chce prohlížet naměřená data
- Zákazník <-> Databáze s daty – Přístup zákazníka k naměřeným datům v databázi
- ADMIN – Administrátor databáze
- ADMIN <-> Databáze s daty – Přístup administrátora k databázi naměřených dat

Dvojice entit označené pomocí <-> bude předmětem STRIDE analýzy. Použita bude metoda STRIDE-LM per interaction, tedy analýza rizik při interakci dvou entit v diagramu, v tomto případě interakce dvou zařízení nebo zařízení a datového úložiště.

5.1 STRIDE analýza interakcí

5.1.1 Naměřená data <-> Měřící zařízení

1) Tampering
   - Útočník by se mohl k zařízení, které má odhalené porty, fyzicky připojit a ukrást uložená naměřená data nebo měnit konfiguraci.
   - Útočník může zaměnit zařízení za jiné nebo ho poškodit.
2) Information disclosure
   - Uložená naměřená data by mohl útočník přečíst, pokud by se k nim dostal, což není žádoucí.

5.1.2 Měřící zařízení <-> Řídicí jednotka + router

1) Spoofing
   - Řídicí jednotka musí mít jistotu, že komunikuje se správným zařízením.
2) Tampering
   - Komunikační infrastruktura a zařízení mohou být fyzicky poškozeny.
3) Repudation
   - Jakékoliv zařízení může odesílat data na řídicí jednotku a nedá se dohledat, kdo všechno data posílá.
4) Denial of service
   - Útočník se může připojit k síti se zařízeními a zaplavit síť jiným provozem. To může síť destabilizovat.

5.1.3 Řídicí jednotka + router <-> Server + MQTT broker

1) Spoofing
   - Řídicí jednotka musí mít jistotu, že komunikuje se správným zařízením a také server musí mít jistotu, že komunikuje s důvěryhodným zařízením.
2) Tampering
   - Útočník může data při přenosu odposlouchávat a získat tím citlivé informace.
   - Útočník může data při přenosu odposlouchávat a zaměnit.
   - Řídicí jednotka může být fyzicky upravena nebo poškozena.
3) Repudation
   - Mohou být odesílány škodlivá data a tento moment se zpětně nedá identifikovat.
   - Útočník se připojí k řídicí jednotce a tento moment se zpětně nedá dohledat.
4) Information disclosure
   - Data přenášena v čitelné formě útočník dokáže při odposlechnutí jednoduše přečíst.
   - Útočník ví, kdy probíhá komunikace.
   - Útočník dokáže jednoduše filtrovat komunikaci podle defaultních port čísel protokolu MQTT.
5) Denial of service
   - Útočník se může pokusit zaplavit zařízení na obou stranách různými požadavky a znepřístupnit je pro jejich normální využití.
6) Elevation of Privilege
   - Útočník, který se připojí na řídicí jednotku pomocí ukradených přístupových údajů má plná práva.
   - Útočník se může pokusit zneužít jinou službu běžící na serveru nebo řídicí jednotce pro neoprávněný přístup.
7) Lateral Movement
   - Útočník se díky kompromitaci řídicí jednotky je schopný připojit k serveru.

5.1.4 Server + MQTT broker <-> Databáze dat

1) Spoofing
   - Databáze ukládá data i od jiného zdroje, než je server.
2) Tampering
   - Neoprávněný uživatel může změnit data v databázi ručně.
   - Neoprávněný uživatel má fyzický přístup k serveru a úložišti, kde se nachází databáze s daty.
3) Repudation
   - Není známo, kdy byly ukládány nová data.

4) Information disclosure
   - Neoprávněný uživatel si může přečíst data, která jsou uložena v čitelné formě.
5) Denial of service
   - Server nestíhá ukládat velké množství dat a to vyústí v Denial of service a ztrátě dat
6) Lateral Movement
   - Útočník dokáže po přihlášení k databázi získat přihlašovací údaje ostatních uživatelů.

5.1.5 Zákazník <-> Databáze s daty

1) Spoofing
   - Útočník se může pokusit získat neoprávněný přístup do databáze.
2) Tampering
   - Uživatel získá přístup k datům, ale při tom začne měnit i konfigurační nastavení databáze.
3) Repudation
   - Uživatelské operace nejsou logovány.
   - Přístup jednotlivých uživatelů není logován.
4) Information disclosure
   - Útočník se může pokusit zachytit přihlašovací jméno a heslo uživatele a poté se přihlásit jeho údaji.
5) Denial of service
   - Útočník se bude snažit přihlašovat pomocí bruteforce útoku.
6) Lateral Movement
   - Uživatel si může zobrazit data jiných uživatelů, která mu nepatří.
   - Uživatel se snaží získat přístup mimo databázi.

5.1.6 ADMIN <-> Databáze s daty

Hrozby pro uživatele Admin pro přístup k databázi jsou obdobné, jako hrozby pro běžné uživatele. Účet Admin ale oproti od běžnému uživatelského účtu má práva pro změnu nastavení databáze, přístup k datům a spravuje uživatele a přístup útočníka k databázi by měl dopad pro všechna uložená data a všechny uživatele, kteří k databázi přistupují.

6 Návrh strategie a bezpečnostní opatření

6.1 Strategie zabezpečení

Komunikaci z průmyslového podniku je potřeba zabezpečit tak, aby se data naměřená přístroji bezpečně dostala až na server, kde se uloží do databáze a bude k nim možný přístup přes webové rozhraní. Zařízení měřící data by mělo být na bezpečném místě, ke kterému by měli mít přístup pouze oprávněné osoby aby nedošlo k poškození nebo úpravě zařízení. Data ze zařízení by na řídicí jednotku měla být odesílána v nečitelné podobě, pokud je toto možné, a řídicí jednotka by měla po přijetí dat zkontrolovat jejich integritu. Řídicí jednotka by měla být umístěna na bezpečném místě, aby k ní mohli fyzicky přistupovat pouze oprávnění uživatelé. Většina konfigurace probíhá na dálku. Před začátkem komunikace řídicí jednotky a serveru obě strany ověří, že opravdu komunikují se správným protějškem pomocí předem nakonfigurovaným PSK. Řídicí jednotka bude na server MQTT komunikaci posílat zabezpečeným kanálem vytvořeným pomocí VPN tunelu (TLS nebo IPsec). Tunel útočníkům zamezí, aby při přenosu dat z podniku data odposlouchávali a případně je byli schopni zaměnit.

Poté, co data přijdou na server, je ověřena jejich integrita a jsou bezpečně uloženy do databáze, je nutné řídit přístup uživatelů, kterým naměřená data patří. Uživatelé při přístupu k webovému rozhraní, pomocí kterého získají přístup k datům, musí používat zabezpečený kanál, pro přenos dat z databáze, aby ani v tomto momentu nemohla být komunikace odposlouchávána nebo zaměněna za přenosu.

6.2 Bezpečnostní opatření

6.2.1 Naměřená data <-> Měřící zařízení

1) Tampering
   - Zařízení by mělo být umístěno na bezpečném místě, kde k němu nemá přístup neoprávněná osoba.
   - Zařízení by mělo být umístěno v zamčeném racku nebo skříni, aby se k němu nemohla neoprávněná osoba připojit přes odhalené porty nebo ho fyzicky poškodit.

2) Information disclosure
   - Data uložena na zařízení by neměly být uloženy v čitelné formě (Pokud toto zařízení umožňuje a má dostatečný výkon).

6.2.2 Měřící zařízení <-> Řídicí jednotka + router

1) Spoofing
   - Zařízení se pro připojení k řídicí jednotce musí autentizovat.
2) Tampering
   - Zařízení je na bezpečném místě a je přístupné pouze oprávněným uživatelům.
3) Repudation
   - Řídicí jednotka loguje komunikaci zařízení, která jsou k ní připojená.
4) Information disclosure
   - Data ze zařízení jsou odesílána v nečitelné formě.
5) Denial of service
   - Síť pro komunikaci zařízení bude izolována od jiné komunikace.

6.2.3 Řídicí jednotka + router <-> Server + MQTT broker

1) Spoofing
   - Server a řídicí jednotka ověří navzájem svou identitu pomocí svých přidělených PSK (Pre-Shared Key).
2) Tampering
   - Řídicí jednotka musí být uložena na bezpečném místě, ke kterému mají přístup pouze oprávněné osoby, aby nemohla být poškozena nebo upravena.
   - Musí být zaručena integrita dat.
3) Repudation
   - Obě strany logují MQTT komunikaci.
   - Řídicí jednotka loguje vzdálený přístup k zařízení.
4) Information disclosure
   - Data při přenosu nesmí být odesílána v čitelné formě, data musí být šifrována nebo musí být ustanoven komunikační kanál, který se nedá odposlouchávat, např. pomocí technologie VPN, konkrétně IPsec tunel, díky kterému jsou data odesílána bezpečným komunikačním kanálem.
   - Bude nastaveno nedefaultní číslo portu pro komunikaci protokolem MQTT.
5) Denial of service
   - Díky technologii VPN bude řídicí jednotka dostupná pouze z virtuální lokální sítě.
6) Elevation of Privilege
   - Řídicí jednotka má účet administrátora pro vzdálenou správu a účet, který slouží pro kontrolu zařízení, ale nemá přístup k konfiguračním souborům nebo souborům s daty.

7) Lateral Movement

- Přístup k řídcí jednotce nesmí útočníkovi dovolit přístup k serveru, pro přístup ke každému zařízení je potřeba autentizace jinými přihlašovacími údaji.

6.2.4 Server + MQTT broker <-> Databáze s daty

1) Spoofing
   - Databáze je připojená přímo k serveru a ukládá data pouze od něj. Tato omezení mohou být zajištěna např. pomocí IP filtrů, nastavení práv pro práci s databází nebo autorizací serveru.
2) Tampering
   - Data v databázi jsou uložena v nečitelné formě. Přístup k nim mají jen ověřené osoby
   - Pouze oprávněný uživatel může měnit data v databázi a to pouze ta, která mu patří.
   - Server je uložen na bezpečném místě a fyzický přístup k němu mají pouze administrátoři.
3) Repudation
   - Databáze loguje ukládání nových dat.
4) Information disclosure
   - Data jsou ukládána v nečitelné formě.
5) Denial of service
   - Server by měl být schopný ukládat velké množství dat v reálném čase, i v případě zvýšeného množství ukládaných dat, než je běžné.
6) Lateral Movement
   - Přihlašovací údaje ostatních uživatelů a jiná citlivá data, která by mohla ohrozit další zařízení, jsou ukládána na jiném místě.

6.2.5 Zákazník <-> Databáze s daty

1) Spoofing
   - Uživatel se před přístupem k databázi musí autentizovat.
   - Hesla pro přístup k databázi musí být dostatečně silná.
2) Tampering
   - Uživatel, který si chce zobrazit data nemá povolen přístup ani není oprávněn měnit konfiguraci a jiná nastavení databáze.
3) Repudation
   - Databáze loguje uživatelské akce v databázi.
   - Databáze loguje přístup jednotlivých uživatelů do databáze.

4) Information disclosure
   - Pro přihlášení k webové aplikaci pro přístup k databázi musí být ustanoven bezpečný komunikační kanál, který nebude možný odposlouchávat a přihlašovací údaje budou přenášeny zašifrované.
5) Denial of service
   - Server po určitém počtu neúspěšných přihlášení nedovolí uživateli další pokusy a dovolí mu se přihlásit až po určité době.
6) Lateral Movement
   - Uživatel nesmí být schopen prohlížet data jiných uživatelů, jejichž data jsou v databázi taky uložena.

6.2.6 ADMIN <-> Databáze s daty

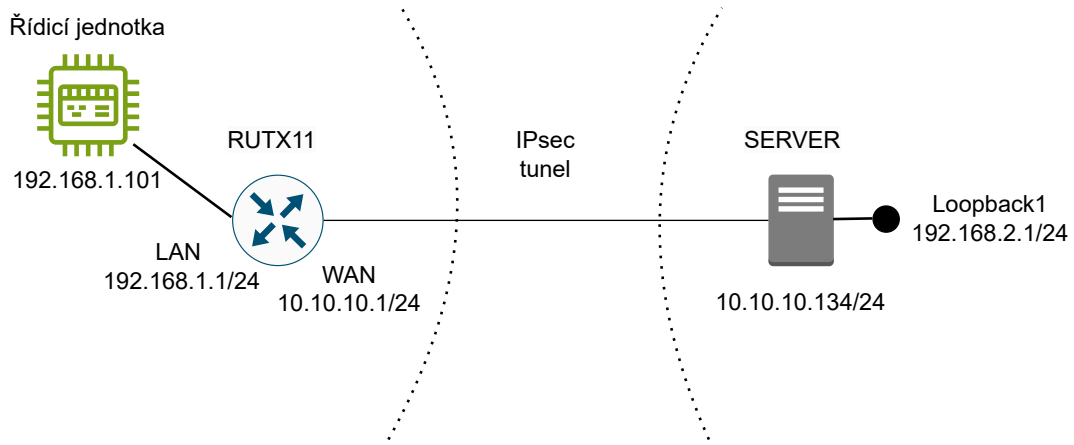
Pokud by útočník získal přístup k databázi pod účtem Admin, měl by přístup k datům všech uživatelům, mohl by měnit nastavení databáze a upravovat přístup jiných uživatelů k databázi. Je proto nesmírně důležité, aby se uživatel Admin přihlašoval přímo k serveru ze sítě, ve kterém se nachází a aby komunikace nešla vůbec mimo důvěryhodnou síť. Přihlašovací údaje musí být bezpečně skladovány, aby se nedostaly do rukou potencionálního útočníka.

7 Implementace bezpečnostních opatření

V teoretické části práce byly navrženy bezpečnostní opatření pro celý proces komunikace zařízení, která měří požadovaná data až po přístup dat ze serveru. Praktická implementace bezpečnostních opatření se primárně zaměřuje na komunikaci řídicí jednotky ESCON-C s routerem a následnou komunikací se serverem, který MQTT komunikaci zpracovává. Implementovány byly opatření pro řídicí jednotku, router a server, díky kterým může být simulováno nasazení a fungování MQTT komunikace. Jako bezpečný komunikační kanál byl zvolen IPsec tunel.

7.1 Schéma zapojení pracoviště pracoviště

Router RUTX11 přiděluje připojené řídicí jednotce IP adresu pomocí DHCP ze sítě 192.168.1.0/24, která je nastavena pro LAN rozhraní routeru. Server je k routeru připojen přímo do rozhraní WAN, které by ve skutečnosti bylo použito pro připojení routeru k internetu. V tomto experimentálním případě je internet nahrazen sítí 10.10.10.0/24, přes kterou budou data přenášena pomocí IPsec tunelu. Rozhraní *Loopback1* slouží jako cílová adresa pro MQTT komunikaci, na kterou klientské zařízení odesílá MQTT komunikaci. Komunikace probíhá mezi dvěma důvěryhodnými sítěmi, do kterých mají přístup pouze zařízení z těchto připojených sítí a jakýkoliv vnější přístup je silně omezen.



Obr. 7.1: Schéma zapojení pracoviště

7.2 Bezpečná hesla

Hesla, která jsou použita pro přístup do jednotlivých zařízení odpovídají minimálnímu bezpečnostnímu standardu, který vydal NÚKIB a který je platný ke dni 14. února 2023. Jelikož hesla spadají do kategorie tzv. Privilegované účty, musejí splňovat následující požadavky:

- Minimální délka hesla je sedmnáct znaků.
- Heslo musí obsahovat alespoň tři z těchto kategorií znaků:
  - Malé písmeno
  - Velké písmeno
  - Číslice
  - Speciální znak.
- Dále musí hesla splňovat následující:
  - Maximální doba platnosti hesla je osmnáct měsíců
  - Heslo nesmí být používáno opakovaně (posledních 12 hesel)
  - Heslo musí být platné alespoň jeden den
  - Při použití prvotního hesla musí být toto heslo změněno po prvním použití nebo musí být do 24 hodin zneplatněno [18].

7.3 Server

Počítač v roli serveru pro zpracování MQTT komunikace beží na operačním systému Debian. Na tomto počítači jsou důležité dva bežící procesy, Eclipse Mosquitto, který slouží jako broker pro MQTT komunikaci, a Strongswan, který slouží jako jeden z konců IPsec tunelu.

Důležité je také nastavení IPtables, aby server komunikoval pouze s řídicí jednotkou a nepřijímal jakoukoliv jinou komunikaci od cizích zařízení. Server přijímá pouze komunikaci se zdrojovou adresou 192.168.1.1, díky nastavení NAT na routeru, které je dále popsáno v kapitole 7.4.1.

7.3.1 Eclipse Mosquitto

Konfigurace Mosquitto serveru

Výpis 7.1: Obsah konfiguračního souboru mosquitto.conf.

```
listener 50000 192.168.2.1
password_file /etc/mosquitto/passwd
allow_anonymous false
```

Konfigurační soubor *mosquitto.conf* obsahuje následující tři parametry:

listener - parametr listener určuje, na jakém zdroji bude server hledat MQTT komunikaci. V tomto případě bude hledat komunikaci s portem 50000 a s cílovou IP adresou 192.168.2.1.

password_file - parametr ukazující na soubor obsahující přihlašovací jméno a heslo, kterými se klienti při připojení k serveru autentizují, uložený v adresáři /etc/mosquitto/passwd.

Výpis 7.2: Obsah souboru passwd.

```
ESCONC3S_PREDFLEX_1:$7$101$sCQGm5GsFN5alqhJ$mAuLer4ZmpkxY9m
INAvc7dSZMiesIZKOOiJ0t2ptcHDgJ3zNtx04U6uzKfy/nfmsr8OOoej20s
tKunpUW86ErQ==
```

Soubor *passwd* obsahuje kombinaci přihlašovacího jména a hesla, které má nakonfigurováno také klientské zařízení. Heslo je zde uchováno bezpečně pomocí hashovací funkce SHA256.

allow_anonymous - parametr určující, zda se k MQTT brokerovi mohou připojit i anonymní zařízení bez řádné autentizace. V tomto případě to není povoleno a klientské zařízení bude potřebovat přihlašovací jméno a heslo, které zná i MQTT broker (má ho uložené v souboru *passwd*).

7.3.2 Strongswan

Konfigurace Strongswan

Výpis 7.3: Obsah konfiguračního souboru ipsec.conf.

```
conn ipsec
    type=tunnel
    leftid=10.10.10.134
    left=10.10.10.134
    leftsubnet=192.168.2.0/24
    rightid=10.10.10.1
    right=10.10.10.1
    rightsubnet=192.168.1.0/24
    authby=secret
    keyexchange=ikev2
    ike=aes256-sha256-modp3072
    ikelifetime=3600s
    esp=aes256-sha256
    keylife=3600s
    auto=start
```

V souboru je nadefinováno spojení *ipsec* s následujícími parametry:

type - parametr určující typ spojení. Pro komunikaci mezi sítí, ve které se nachází řídicí jednotka a sítí, ve které je server, je využit tunelový mód, díky kterému jsou přenášené pakety včetně jejich IP hlaviček zapouzdřeny do nových packetů a mohou tak být bezpečně přenášeny přes nedůvěryhodnou síť. Posílaná data ani adresy obou komunikujících stran nemohou být ze zachycené komunikace vyčteny.

leftid - parametr identifikující lokální stranu komunikace (MQTT server). Může mít různé podoby: IP adresu, e-mailovou adresu, FQDN a musí být na obou koncích IPsec tunelu nakonfigurován stejně.

left - veřejná IP adresa lokální strany tunelu.

leftsubnet - IP adresa lokální sítě lokální strany tunelu.

rightid - parametr identifikující vzdálenou stranu IPsec tunelu.

right - veřejná IP adresa vzdálené strany tunelu.

rightsubnet - IP adresa lokální sítě vzdálené strany tunelu.

authby - metoda autentizace obou stran. Pro autentizaci byl použit PSK (Pre-shared Key), který znají obě strany a díky němu mohou ověřit, že navazují komunikaci se správným protějškem. [19] Svůj PSK má MQTT server nakonfigurován v souboru *ipsec.secrets*.

Výpis 7.4: Obsah souboru ipsec.secrets.

```
mqtt_server@lenovo_srv:/etc$ cat ipsec.secrets
10.10.10.134 10.10.10.1 : PSK "X6ert8+wryynoWQlP"
10.10.10.1 10.10.10.134 : PSK "X6ert8+wryynoWQlP"
```

keyexchange - parametr určující způsob ustanovení klíče, který následně bude použit pro šifrování komunikace. Využívá se protokol IKE (Internet Key Exchange), v dnešní době už pouze ve verzi 2, s vyšší úrovní bezpečnosti a větší efektivitou než její předchůdce. Verze 1 je již v dnešní době považována za zastaralou.

ike - určuje, jaké šifrovací a hashovací algoritmy a Diffie-Hellman skupiny se mají využít při ustanovení zabezpečeného komunikačního kanálu.

ikelifetime - určuje, po jaké době dojde k ustanovení nového šifrovacího klíče.

esp - šifrovací a hashovací algoritmy, které se využívají pro přenos dat.

keylife - určuje, po jaké době dojde k ustanovení nového klíče, který je používán pro šifrování dat.

auto - určuje, jakou operaci se má provézt okamžitě po zapnutí služby IPsec. Příznak *start* znamená, že okamžitě po zapnutí služby načte nakonfigurovaná připojení a začne ustanovovat připojení. [19]

Kryptografické algoritmy byly zvoleny podle doporučení NÚKIB platnému ke dni 1. července 2023. Pro algoritmy určené pro procesy k dohodě šifrovacích klíčů je doporučeno použití algoritmu Diffie-Hellman s minimální délkou klíče 3072 bitů.

Pro šifrování dat jsou použity kryptografické algoritmy AES256 a SHA256, které jsou považovány za bezpečné [20].

Výpis 7.5: Funkční IPsec tunel na straně serveru.

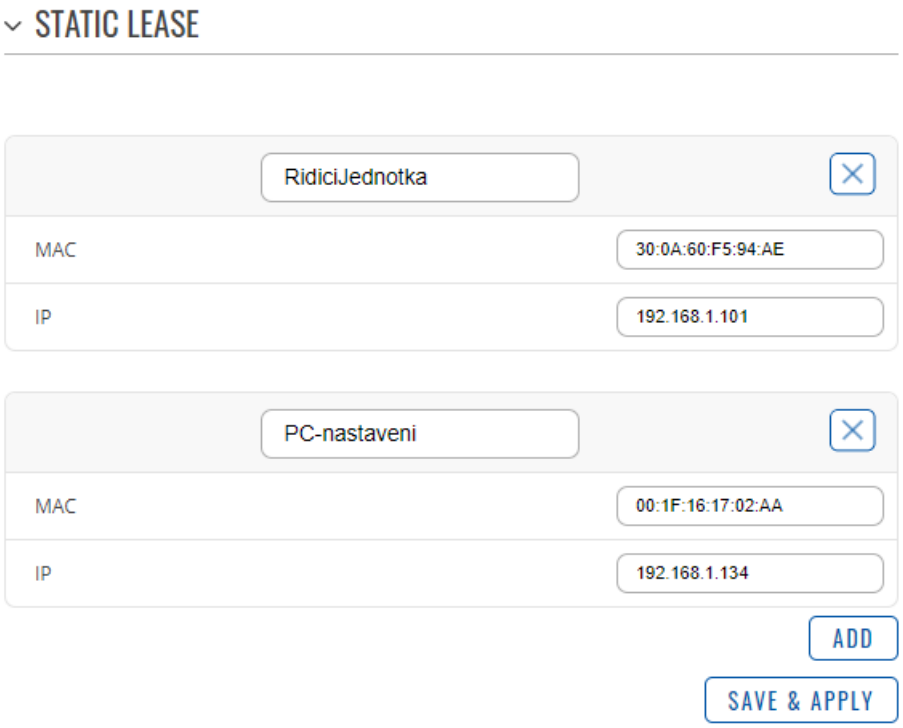
```
mqtt_server@lenovo_srv:~$ sudo ipsec status
Security Associations (1 up, 0 connecting):
       ipsec[1]: ESTABLISHED 16 minutes ago,
       10.10.10.134[10.10.10.134]...10.10.10.1[10.10.10.1]
       ipsec{1}:  INSTALLED, TUNNEL, reqid 1,
       ESP in UDP SPIs: c82f0527_i c1ee36e0_o
       ipsec{1}:   192.168.2.0/24 === 192.168.1.0/24
```

7.4 Router RUTX11

7.4.1 Bezpečnostní mechanismy nastavené na routeru

DHCP

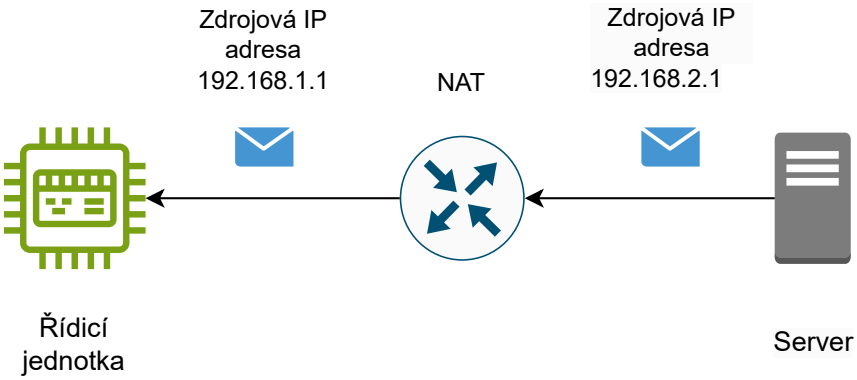
Zařízením připojeným k rozhraním LAN router přiřazuje IP adresy na základě nakonfigurovaného DHCP. Pokud by se útočník dostal k rozvaděči, mohl by se jednoduše připojit k routeru a pohybovat se ve stejné síti jako zařízení ESCON-C. Router však dokáže pomocí MAC adress whitelistu přiřazovat IP adresy jen těm zařízením, které mají namapované své MAC adresy ke konkrétním IP adresám v nastavení routeru. Útočník i tak při přístupu k zařízení nebude schopný se zařízeními komunikovat, jelikož jeho zařízení nebude přidělena IP adresa. Pro případ změny tohoto mapování je možné mapování upravit na dálku pomocí RMS, kterým router disponuje. To se bude provádět většinou v případě revizí nebo kontroly zařízení, když k němu bude potřeba připojit např. nějaké měřící zařízení, cizí a nebo nové počítače. Většinu čas však k routeru u zařízení ESCON-C bude připojena pouze řídicí jednotka a proto je toto statické mapování adres proveditelné a není náročné takto spravovat přístup nových zařízení do sítě.



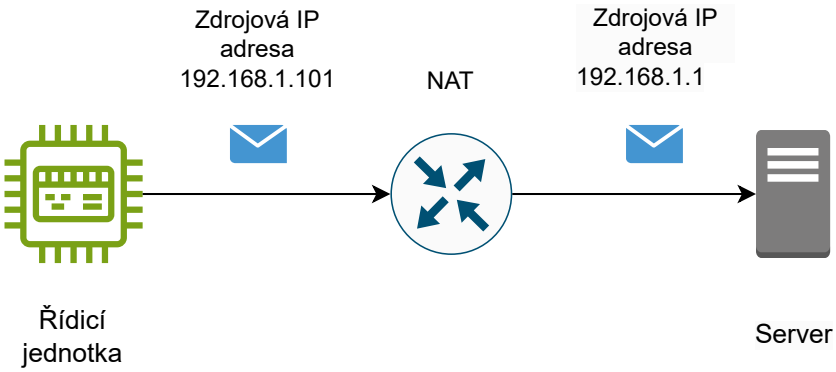
Obr. 7.2: Statické mapování MAC a IP adres.

NAT

Pro zvýšení bezpečnosti je na routeru nastaven NAT (Network Address Translation), který jakoukoliv komunikaci z adresy 192.168.2.1/24, která je použita jako zdrojová IP adresa serveru při komunikace s řídicí jednotkou, po příchodu na router přeloží na adresu 192.168.1.1, která odpovídá LAN rozhraní routeru. Při komunikaci serveru s řídicí jednotkou komunikuje řídicí jednotka pouze s routerem, který přijme komunikaci od serveru a se svou zdrojovou adresou ji přeposílá dál. V případě připojení cizího zařízení do sítě zabrání router pomocí NAT konfigurace komunikaci tohoto zařízení s řídicí jednotkou nebo serverem a správné fungování nebude moct být nijak narušeno a útočníkovi bude odepřen přístup k obou stranám komunikace.



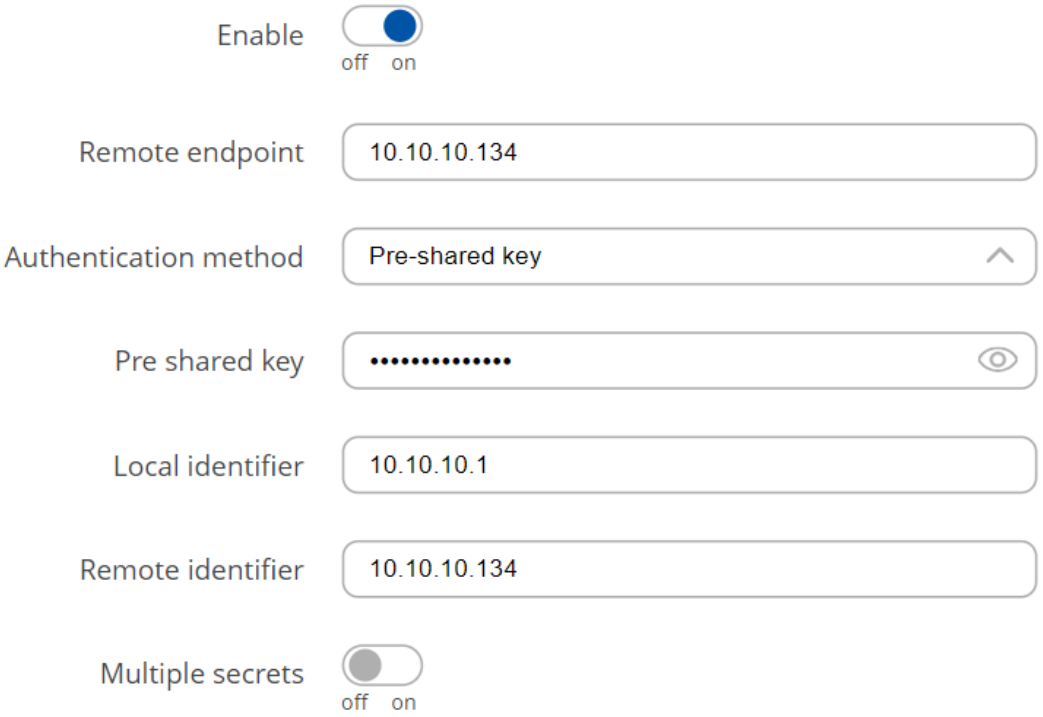
Obr. 7.3: NAT překlad zdrojové adresy ze serveru.



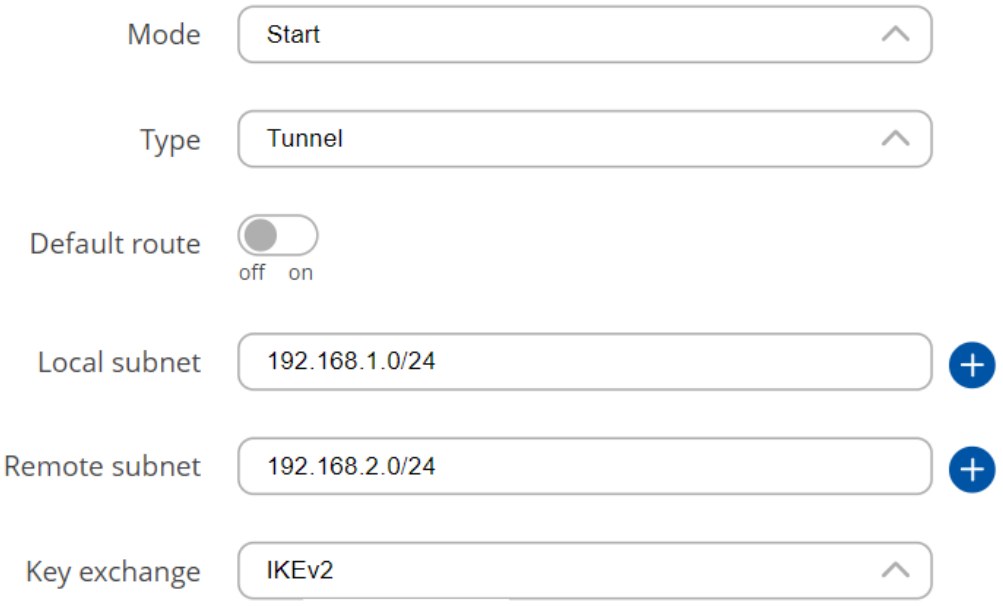
Obr. 7.4: NAT překlad zdrojové adresy z řídicí jednotky.

IPsec

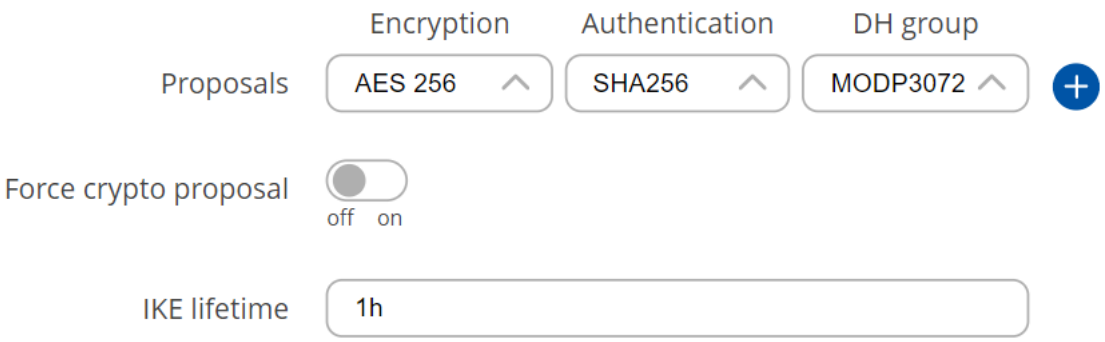
Ve firmwaru routeru je nastaven IPsec obdobně, jako na serveru, jen jsou prohozeny strany left a right podsítí a IP adresy konců tunelu. Nastavení všech parametrů musí přesně odpovídat tomu, jak jsou nastaveny na serveru. 7.3, jinak se nenaváže spojení IPsec tunelu.



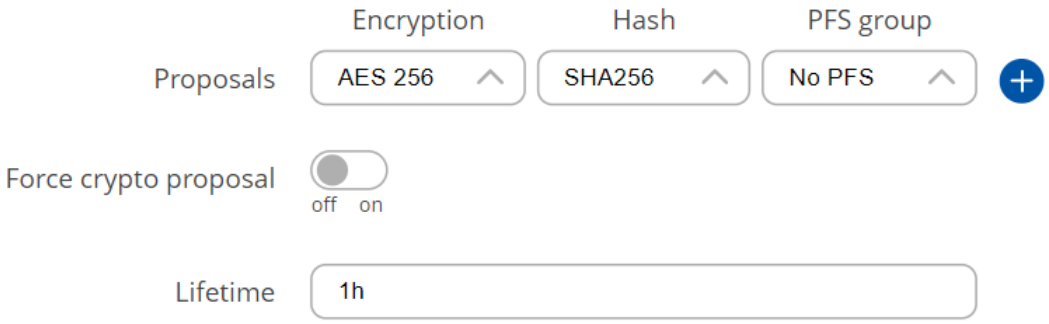
Obr. 7.5: IPsec - Nastavení koncových bodů IPsec tunelu.



Obr. 7.6: IPsec - Nastavení propojených sítí.



Obr. 7.7: IPsec - Nastavení algoritmů pro ustanovení šifrovacího klíče.



Obr. 7.8: IPsec - Nastavení algoritmů pro šifrování dat.

7.5 Řídicí jednotka

V řídicí jednotce zařízení ESCON-C je v příslušném konfiguračním souboru zařízení shodně nastaveno přihlašovací jméno a heslo, které se shoduje s nastavením v souboru *passwd* v nastavení Mosquitto serveru 7.2. Nastavena je taky IP adresa MQTT brokera a port, na kterém broker naslouchá, které odpovídá nastavení v souboru mosquitto.conf 7.1.

Řídicí jednotka má dále nastaveno pomocí IPtables blokování veškeré komunikace, která nemá zdrojovou IP adresu 192.168.1.1, viz podkapitola 7.4.1.

8 Experimentální testování opatření

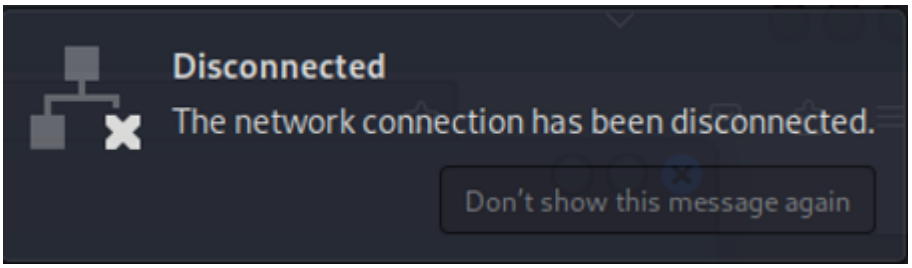
8.1 Potencionální útoky na zabezpečenou síť

Útočníci na takto zabezpečenou síť mají pouze několik možností, jak na síť zaútočit. Jako první krok se musejí připojit a být schopni komunikovat v síti, kde se nachází řídicí jednotka a poté mohou pohybovat v síti. Toto by pro ně měla být ta největší překážka, kterou by neměli být schopni obejít. Bez tohoto by neměli být žádné další útoky proveditelné.

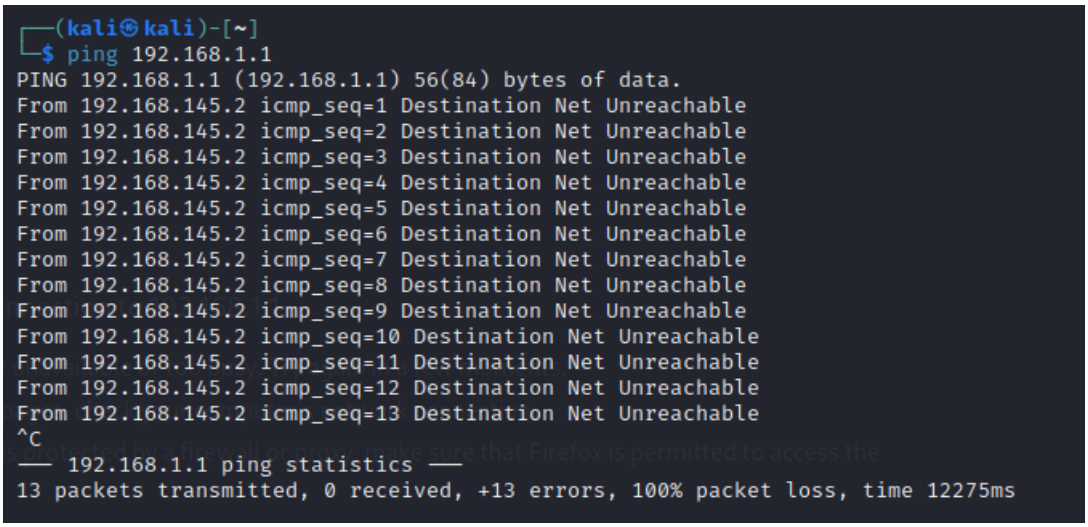
Následující čtyři scénáře popisují útoky, o které by se útočník mohl pokusit, aby narušil funkčnost služby a nebo mohl komunikaci odposlouchávat.

8.2 Scénář 1

Útočník snaží připojit přímo kabelem k routeru zařízení ESCON-C do LAN rozhraní a chce se pokusit komunikovat se zařízením ESCON-C. Toto by mu otevřelo možnost dalších útoků na zařízení ESCON-C samotné nebo také na útok na router, u kterého by se mohl pokusit vypnout nakonfigurovaná zabezpečení a služba MQTT komunikace by tak nemusela být bezpečná. Díky nastavení statického mapovaní IP adres pro zařízení nedostane útočníkův počítač přidělenou IP adresu od DHCP, které běží na routeru. Útočník není schopen komunikovat s routerem, řídicí jednotkou ani serverem.



Obr. 8.1: Útočníkův počítač nebyl připojen k síti.



Obr. 8.2: Útočníkův počítač není schopen komunikovat s routerem.

Pro připojení do sítě by musel útočník vypnout bezpečnostní opatření, která cizím počítačům zabraňují připojení k síti. Pro to by se musel dostat do routeru, který je chráněn uživatelským jménem a heslem. Další možnost by bylo ukrást a změnit MAC adresu zařízení, k té se však dostane pouze po připojení k řídicí jednotce, nutná autentizace přihlašovacím jménem a heslem, nebo pokud se mu do rukou dostane jiné zařízení, které má přístup povoleno, to je však velmi nepravděpodobné, protože takové zařízení na místě bude pouze řídicí jednotka, které svou MAC adresu nemá nikde z venku na zařízení čitelnou. Další překážkou by bylo nastavení NAT, jelikož řídicí jednotka ani server by komunikaci se zdrojovou IP adresou útočníkova počítače nepřijalo.

8.3 Scénář 2

Útočník chce odposlouchávat naměřená data přenášena na server. Útočník může zachytit komunikaci po cestě, ta je však pomocí IPsec zapouzdřená a není navenek nijak čitelná. Data i informace o IP adresách jsou útočníkovi skryty. Pro zachycení komunikace útočník použil program Wireshark pro analýzu síťového provozu. V pravém sloupci obrázku 8.3 můžeme vidět hodnotu SPI (Security Parameter Index) = 0xc1ee36e0. Jedná se o identifikátor IPsec tuenlu, který protistraně říká, kterou konfigurací má toto zapouzdření dešifrovat. Vzniká při ustanovení IPsec tunelu, když se vybírají šifrovací algoritmy. Je shodný jako identifikátor v nastaveném IPsec tunelu běžícím na serveru 7.5. Při zobrazení obsahu, obrázek 8.4, komunikace útočník uvidí pouze to, že jsou data šifrována a hodnoty SPI.

Time	Source	Destination	Protocol	Lengtl	Info
436.00005…	10.10.10.134	10.10.10.1	ESP	178	ESP (SPI=0xc1ee36e0)
437.02416…	10.10.10.134	10.10.10.1	ESP	178	ESP (SPI=0xc1ee36e0)
695.35124…	10.10.10.134	10.10.10.1	ESP	178	ESP (SPI=0xc1ee36e0)
696.35206…	10.10.10.134	10.10.10.1	ESP	178	ESP (SPI=0xc1ee36e0)
697.38016…	10.10.10.134	10.10.10.1	ESP	178	ESP (SPI=0xc1ee36e0)
698.40416…	10.10.10.134	10.10.10.1	ESP	178	ESP (SPI=0xc1ee36e0)
699.42816…	10.10.10.134	10.10.10.1	ESP	178	ESP (SPI=0xc1ee36e0)
700.44813…	10.10.10.134	10.10.10.1	ESP	178	ESP (SPI=0xc1ee36e0)
701.47606…	10.10.10.134	10.10.10.1	ESP	178	ESP (SPI=0xc1ee36e0)
702.50016…	10.10.10.134	10.10.10.1	ESP	178	ESP (SPI=0xc1ee36e0)
703.52415…	10.10.10.134	10.10.10.1	ESP	178	ESP (SPI=0xc1ee36e0)
704.54412…	10.10.10.134	10.10.10.1	ESP	178	ESP (SPI=0xc1ee36e0)

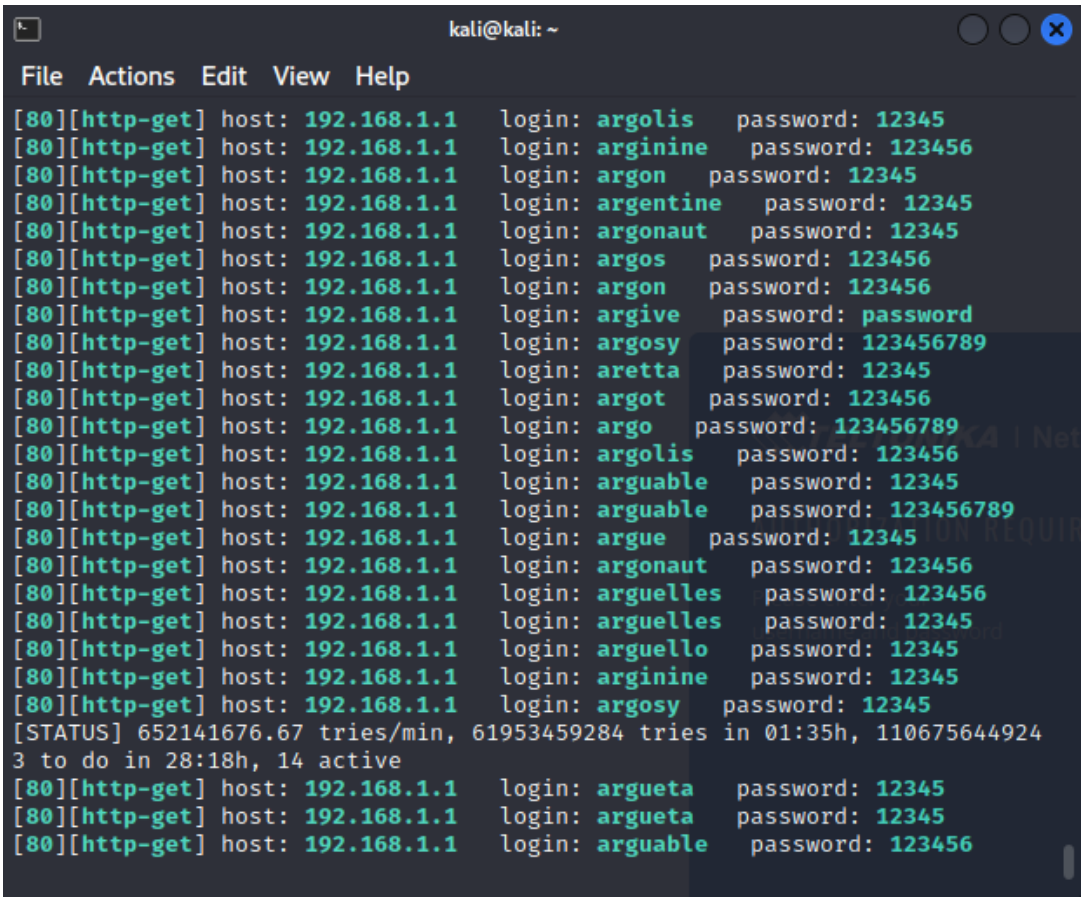
Obr. 8.3: Zapouzdřená komunikace pomocí protokolu IPsec.

```
> Frame 1141: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits)
> Ethernet II, Src: Teltonik_0f:94:7e (20:97:27:0f:94:7e), Dst: Wistron_17:
> Internet Protocol Version 4, Src: 10.10.10.1, Dst: 10.10.10.134
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
  UDP Encapsulation of IPsec Packets
v Encapsulating Security Payload
    ESP SPI: 0xc5a86981 (3316148609)
    ESP Sequence: 17
```

Obr. 8.4: Zašifrovaná data komunikace.

8.4 Scénář 3

Útočník se snaží přihlásit k routeru a měnit jeho nastavení. Tím by se mohl vypnout zabezpečení a komunikovat v síti. (Předpokládejme, že se útočník dokázal připojit k síti a je schopný komunikovat se zařízeními v síti). Pro útok bude využit nástroj Hydra, který je součástí operačního systému Kali Linux. Útočník zvolil slovníkový útok, jelikož nezná ani přihlašovací jméno, ani heslo pro přístup do routeru.

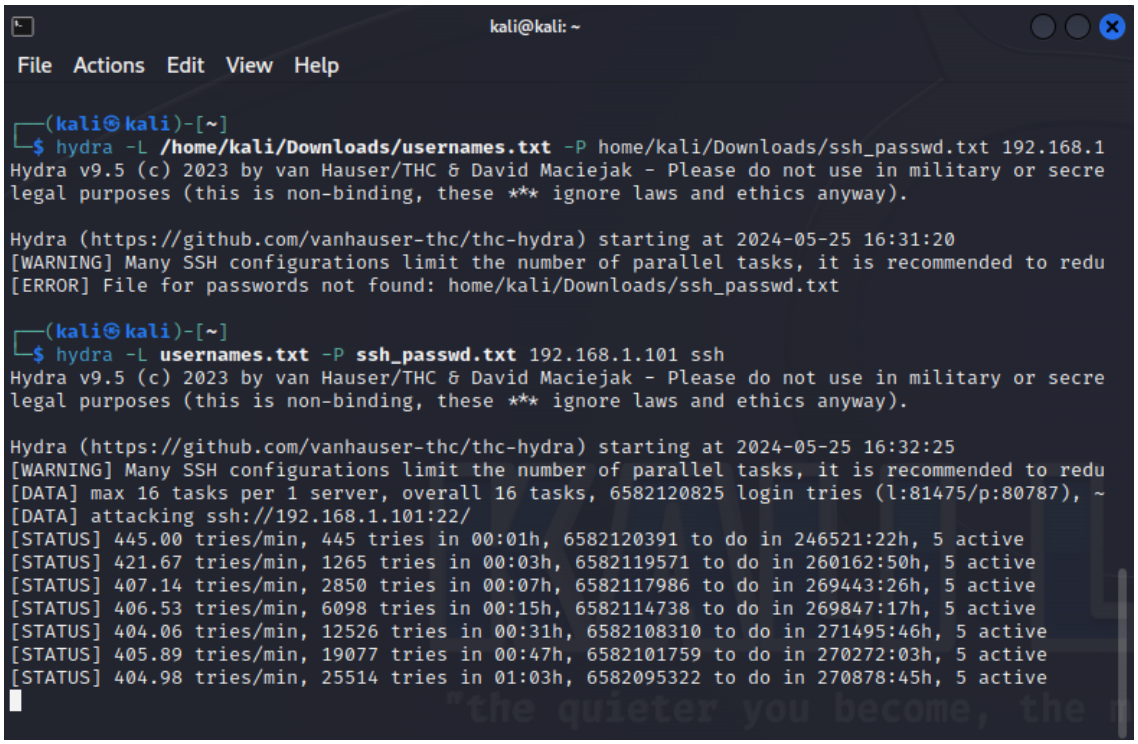


Obr. 8.5: Útok na login stránku routeru.

Z obrázku 8.5 můžeme vidět, že slovníkový útok (rozsáhlé slovníky, volně dostupné na https://github.com/jeanphorn/wordlist) ani po hodině a půl není schopný správné přihlašovací jméno a heslo najít a celková doba, kterou útok s touto kombinací slovníků, může trvat dalších 30 hodin a více. Výsledek však ani tak není zajištěn, jelikož se komplexní heslo použito pro přihlášení k routeru nemusí ve slovníků vůbec nacházet. V reálném provozu není možné, aby útočník jen tak nechal běžet počítač, případně u něj byl v místnosti se zařízením ESCON-C, do které by měl být přístup omezen pouze na vybrané pracovníky.

8.5 Scénář 4

Útočník se snaží slovníkovým útokem přihlásit k zařízení ESCON-C přes SSH (Předpokládejme, že se útočník dokázal připojit k síti a je schopný komunikovat se zařízeními v síti). Pro útok bude využit nástroj Hydra, který je součástí operačního systému Kali Linux. Útočník zvolil slovníkový útok, jelikož nezná ani přihlašovací jméno, ani heslo pro přístup k řídicí jednotce.



Obr. 8.6: Probíhající slovníkový útok na SSH přihlášení.

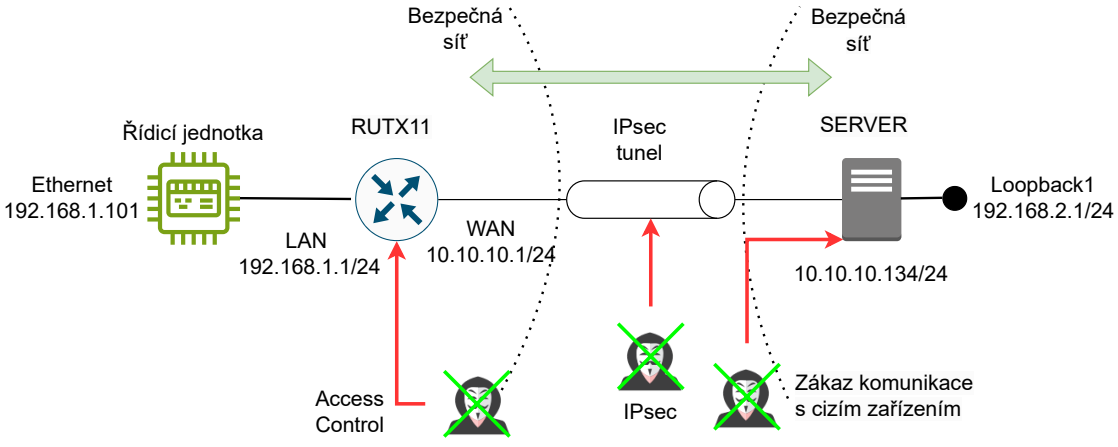
Jedná se o slovníkový útok pomocí slovníků *usernames.txt* a *passlist.txt* (volně dostupné z https://github.com/jeanphorn/wordlist), který zkouší náhodné kombinace uživatelských jmen a hesel, aby se vzdáleně přihlásil k řídicí jednotce. Díky dodržení politiky o bezpečných heslech popsaných v kapitole 7.2 není útok úspěšný, jelikož se jedná o extrémně komplexní heslo a šance jeho výskytu ve slovníku je minimální. Také šance na úspěch útoku hrubou silou je téměř minimální, jelikož postupně generovat heslo, které je dlouhé 17 znaků by trvalo v řádech tisíců hodin a celkový počet kombinací nutných pro vytvoření takového hesla při použití malých, velkých písmen, číslic a speciálních znaků by bylo 94^{17} kombinací, to je rovno cca. $3.49 * 10^{33}$. Útočník není schopen být takto dlouho v reálném provozu u řídicí jednotky v prostorách, kde je omezený přístup. Další možnost, jak útočníkovi udělat útok těžší je použití přihlašovacího jména s např. s identifikačním číslem nebo jiným náhodným nebo polo náhodným identifikátorem. Takovéto uživatelské jméno se s největší pravděpodobností nebude vyskytovat v žádném slovníku a útok tak zase selže.

9 Vyhodnocení bezpečnostních opatření

Bezpečnostní opatření implementována při přenosu dat mezi dvěma důvěryhodnými sítěmi útočníkovi zabrání v jakékoliv škodlivé aktivitě, která by mohla komunikaci zařízení a funkčnost služby narušit. Tento přístup k zabezpečení je výhodný v tom, že komunikace je zabezpečena jak v případě narušení cizím zařízením útočníka, tak v případě selhání některé ze služeb a je také odolná vůči jakémukoliv selhání bezpečnostních mechanismů nebo chybné implementace samotného protokolu MQTT. Uvnitř sítě může bez problémů probíhat jakákoliv komunikace s použitím libovolného protokolu, protože útočník není schopný do sítě vstoupit. S dostatečně silným šifrováním použitým s protokolem IPsec je komunikace bezpečná i po cestě mezi sítěmi, jelikož je odesílána v šifrované podobě a data ani detaily pro útočníka nejsou ze zachycené komunikace čitelné. Čitelné jsou pouze detaily o adresování v části sítě, kde útočník zrovna komunikaci naslouchá.

Zajištěna je v síti komunikace pouze mezi serverem a zařízením ESCON-C pro bezchybný chod služby odesílající MQTT data na server.

Toto je možné díky nastavení pravidla pro překlad síťových adres NAT na routeru, které jakoukoliv komunikaci se zdrojovou adresou 192.168.2.1 na serveru překládá na adresu 192.168.1.1. Pro zvýšení bezpečnosti a zaručení komunikace pouze mezi zařízením ESCON-C a serverem pro bezchybnou MQTT komunikaci mají zařízení nastavena pomocí IPtables pravidla, které jim umožňují komunikovat pouze se svým protějškem.



Obr. 9.1: Schéma bezpečné MQTT komunikace mezi bezpečnými sítěmi.

Blokací veškerého cizího provozu serveru nehrozí, že by na něj mohl přijít DoS útok mimo bezpečnou síť, protože taková komunikace by byla hned při doručení

na server zahozena. Uvnitř sítí by takový útok možný byl, ovšem až po překonání všech ostatních bezpečnostních zařízení.

9.1 Aktualizace STRIDE analýzy

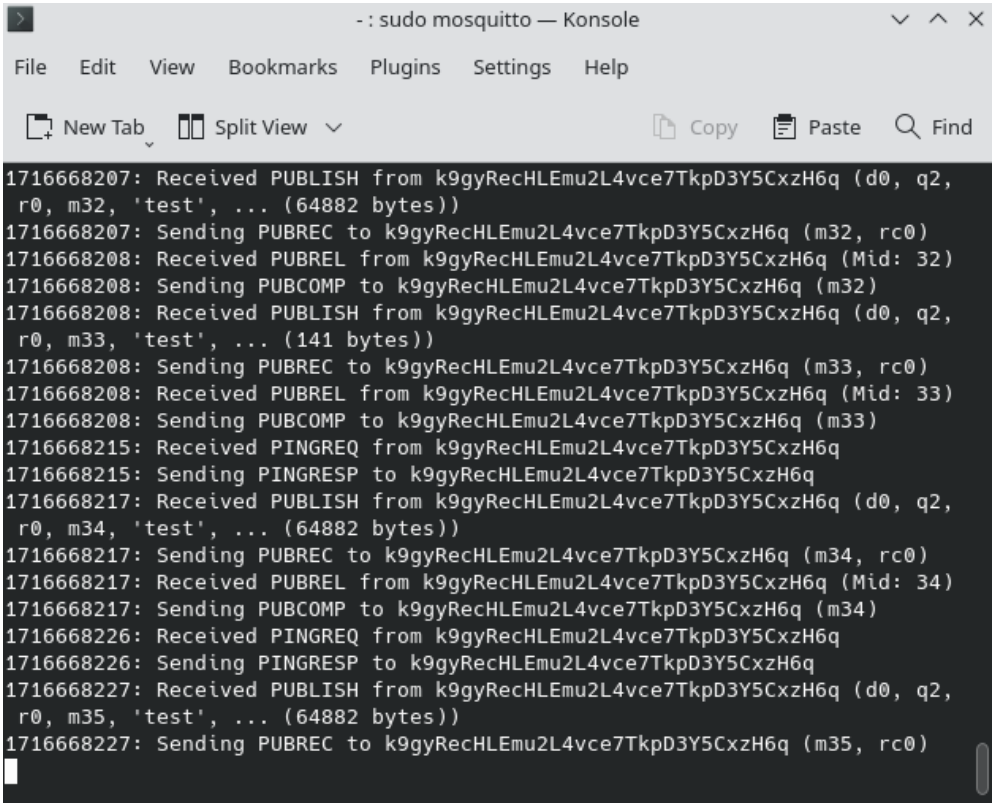
Po implementaci bezpečnostních opatření je možnost útoku na zabezpečený systém silně omezena. Zařízení nejsou dostupná pro síťovou komunikaci zvenčí, útočník bez přístupu do sítě není se zařízeními schopný komunikovat. Útočníkovi tak zbývá pouze jediná možnost, a to fyzický destruktivní útok na samotné zařízení, který by zařízení poškodil nebo by způsobil kompletní vyřazení služby, případně útok na zařízení, která jsou k zařízení ESCON-C připojená, pro manipulaci výsledků naměřených hodnot.

K celkovému navýšení bezpečnosti by podnik s nainstalovaným zařízením ESCON-C měl implementovat opatření, které omezují přístup osob k zařízení a chrání fyzickou celistvost zařízení ESCON-C:

- Omezený přístup k zařízení – zařízení umístěno v místnosti přístupné pouze pro některé pověřené osoby, zabezpečeno klíčem, čipovou kartou nebo jiným způsobem
- Monitoring umístění zařízení ESCON-C – vybavení místnosti a chodby a místa kolem místnosti kamerovým systémem

Při implementaci těchto bezpečnostních opatření se možnost zásahu útočníka do správného chodu zabezpečeného systému stává téměř nulovou.

10 Demonstrace funkčnosti MQTT



Obr. 10.1: Probíhající MQTT komunikace na serveru.

Výpis 10.1: Log MQTT komunikace na řídicí jednotce.

```
21-May-24 18:40:43:938547 - Sending PINGREQ[192.168.2.1]
21-May-24 18:40:44:136983 - Received PINGRESP[192.168.2.1]
2024-05-21 18:40:50.602696 [3591]: INFO - Publishing message
{"client_name": "k9gyRecHLEmu2L4vce7TkpD3Y5CxzH6q",
"device_id": 1, "message_id": "a8868ff15db64021be95b0892ce85
138", "message_type": "ping"}
21-May-24 18:40:50:615683 - Sending PUBLISH (d0, q2, r0, m46),
'b'test'', ... (141 bytes)[192.168.2.1]
21-May-24 18:40:50:760701 - Received PUBREC (Mid: 46)
[192.168.2.1]
2024-05-21 18:40:50.758155 [3591]: INFO - Publish message
results rc(0) mid(46))
21-May-24 18:40:50:776794 - Sending PUBREL (Mid: 46)
[192.168.2.1]
21-May-24 18:40:50:812478 - Received PUBCOMP (Mid: 46)
[192.168.2.1]
```

Závěr

Cílem bakalářské bylo rešerše na téma bezpečnost protokolu MQTT, návrh bezpečnostních opatření pro konkrétní případ užití protokolu MQTT a jejich následná implementace na zařízení ESCON-C od firmy Easycon Solutions s. r. o. a jejich následné testování. Teoretická část práce popisuje fungování a architekturu protokolu MQTT a principy komunikace pomocí protokolu MQTT. Dále popisuje slabiny a zranitelnosti protokolu MQTT, které vycházejí z jeho vlastností a možnosti mitigace těchto zranitelností. Součástí je také analýza zranitelností z databáze CVE, které se týkají protokolu MQTT a kategorizace těchto zranitelností. Součástí teoretické části je taky popis analýzy rizik a popis STRIDE analýzy, která byla použita pro identifikaci možných typů útoku na zabezpečovaný systém a následný popis možných útoků na interakce jednotlivých zařízení a služeb, které by útočník mohl proti jednotlivým zařízením a službám v systému použít. Součástí je také popis zařízení následně používaných v praktické části a návrh strategie a bezpečnostní opatření na základě jednotlivých interakcí vycházejících ze vstupní STRIDE analýzy.

Praktická část práce obsahuje implementaci řešení pro bezpečnou komunikaci založenou na principu komunikace mezi dvěma bezpečnými sítěmi skrz IPsec tunel. Na úvod bylo popsáno zapojení experimentálního pracoviště a způsob způsob zabezpečení komunikace mezi zařízením ESCON-C a serverem zpracovávajícím data.

Dále jsou popsány jednotlivé metody zabezpečení pro každé zařízení experimentálního pracoviště, způsob implementace těchto zabezpečení a popis těchto metod zabezpečení. V další části bylo toto zabezpečení testováno způsoby, jakými by se útočník mohl pokusit funkčnost služby a bezpečnost jednotlivých prvků komunikace narušit. Popsány jsou zde i důvody, proč útočník nebyl úspěšný a pokus o narušení služby by selhal.

Poslední část demonstruje funkčnost komunikace, shrnuje princip jednotlivých metod zabezpečení a vyhodnocení funkčnosti jednotlivých dílčích prvků zabezpečení.

V oblasti kybernetické bezpečnosti je nutné sledovat aktuální vývoj hrozeb, systematicky na ně reagovat na a neustále bezpečnost zlepšovat. S vývojem nových technologií se i toto zabezpečení a šifrování stane zastaralým a bude nutné patřičně reagovat a zabezpečení zvýšit. Stavu kybernetické bezpečnosti se nedá nikdy dosáhnout na 100 procent.

Literatura

[1] YUAN, Michael. *Getting to know MQTT.* Online. 2017, 2021. Dostupné z: https://developer.ibm.com/articles/iot-mqtt-why-good-for-iot/. [cit. 2023-11-19].

[2] LIGHT, Roger. *MQTT man page.* Online. 2018. Dostupné z: https://mosquitto.org/man/mqtt-7.html. [cit. 2023-11-21].

[3] OASIS OPEN. *MQTT Version 5.0.* Online. 2019. Dostupné z: https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.html#_Toc3901033. [cit. 2023-11-21].

[4] HIVEMQ. *MQTT Publish, MQTT Subscribe & Unsubscribe – MQTT Essentials: Part 4.* Online. 2015, 2023. Dostupné z: https://www.hivemq.com/blog/mqtt-essentials-part-4-mqtt-publish-subscribe-unsubscribe/. [cit. 2023-11-24].

[5] HIVEMQ. *MQTT 5 Vs. MQTT 3 – MQTT 5 Essentials Part 2. Online.* 2018, 2023. Dostupné z: https://www.hivemq.com/blog/mqtt5-essentials-part2-foundational-changes-in-the-protocol/.[cit. 2023-11-24].

[6] HIVEMQ. *What is MQTT Quality of Service (QoS) 0,1, & 2? – MQTT Essentials: Part 6.* Online. 2015, 2023. Dostupné z: https://www.hivemq.com/blog/mqtt-essentials-part-6-mqtt-quality-of-service-levels/. [cit. 2023-11-24].

[7] OWASP. *OWASP Internet of Things Project.* Online. 2018. Dostupné z: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Main. [cit. 2023-12-03].

[8] CVE MITRE. *CVE - Search Result.* Online. C1999-2023. Dostupné z: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=mqtt. [cit. 2023-12-08].

[9] THILAKARATHNE, Navod Neranjan. *Security and Privacy Issues in IoT Environment.* International Journal of Engineering and Management Research, Volume-10, Issue-1. Online. 2020. Dostupné z: https://deliverypdf.ssrn.com/delivery.php?ID=060100116086004028114092092107064076000050041076022024096096090109098086118076064127048021127015040030058021019030000093117100126094082050028021030004005118001122077009082021110007096123080122125110075109007016113115120009117106027085070084008024026001&EXT=pdf&INDEX=TRUE. [cit. 2023-12-03].

[10] SYAIFUL, Andy; BUDI, Rahardjo a HANINDHITO, Bagus. *Attack Scenarios and Security Analysis of MQTT Communication Protocol in IoT System.* Online. 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Yogyakarta, Indonésie, 2017. Dostupné z: https://doi.org/10.1109/EECSI.2017.8239179. [cit. 2023-12-06].

[11] OPENVPN. *Creating a Secure IoT Private Network.* Online. [2019], [2023]. Dostupné z: https://openvpn.net/blog/iot-secure-network/. [cit. 2023-12-06].

[12] EMQX. *Fortifying MQTT Communication Security With SSL/TLS.* Online. 2023. Dostupné z: https://www.emqx.com/en/blog/fortifying-mqtt-communication-security-with-ssl-tls. [cit. 2023-12-06].

[13] SANOJA, Damaso. *IPsec Tunnel Mode vs. Transport Mode.* Online. 2021. Dostupné z: https://www.twingate.com/blog/ipsec-tunnel-mode. [cit. 2023-12-13].

[14] HIVEMQ. *MQTT Message Data Integrity - MQTT Security Fundamentals.* Online. 2015. Dostupné z: https://www.hivemq.com/blog/mqtt-security-fundamentals-mqtt-message-data-integrity/. [cit. 2023-12-07].

[15] CONKLIN, Larry. *Threat Modeling Process.* Online. [2022] Dostupné z: https://owasp.org/www-community/Threat_Modeling_Process#stride. [cit. 2023-12-08].

[16] CSF-TOOLS. *STRIDE-LM Threat Model - CSF Tools.* Online. C2020-2023. Dostupné z: https://csf.tools/reference/stride-lm/. [cit. 2023-12-11].

[17] EASYCON SOLUTIONS S. R. O. *Technická specifikace rozvaděče ESCON.* Nezveřejněno. [cit. 2024-04-13].

[18] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Minimální bezpečnostní standard: podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti.* Online. 2. aktualizované vydání. 2023. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf. [cit. 2024-04-28].

[19] STRONGSWAN.ORG. *Ipsec.conf: conn Reference.* Online. C2006-2019, aktualizováno 24.7.2019. Dostupné z: https://wiki.strongswan.org/projects/strongswan/wiki/Connsection. [cit. 2024-04-13].

[20] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Doporuční v oblasti kryptografických prostředků.* Online. 3. aktualizované vydání. 2023. Dostupné z: https://nukib.gov.cz/cs/infoservis/doporuceni/1988-doporuceni-v-oblasti-kryptografickych-prostredku-verze-3-0/. [cit. 2024-04-27].

Seznam symbolů a zkratek

CVE	Common Vulnerability and Exposures
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DDoS	Distributed Denial of Service
ESP	Encapsulating Security Payload
FQDN	Fully Qualified Domain Name
HMAC	Hash-based Messasge Authentication Code
IoT	Internet of Things
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP Security
LAN	Local Area Network
MAC	Media Access Control
MAC	Message Authentication Code
NAT	Network Address Translation
MQTT	Message Queuing Telemetry Transport
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OWASP	The Open Web Application Security Project
PSK	Pre-shared Key
QoS	Quality of Service
RMS	Remote Management System
SPI	Security Parameter Index
SSH	Secure Shell

STRIDE Spoofing; Tampering; Repudation; Information disclosure; Denial of Service; Elevation of Privilege

STRIDE-LM Spoofing; Tampering; Repudation; Information disclosure; Denial of Service; Elevation of Privilege – Lateral Movement

TCP Transmission Control Protocol

TCP/IP Transmission Control Protocol/Internet Protocol

TLS Transport Layer Security

VPN Virtual Private Network

WAN Wide Area Network

A Seznam zranitelností CVE aktuální ke dni 11. 12. 2023

Soubor CVE 12-11-2023.xsl obsahuje tabulku zranitelností z databáze CVE [8], která byla vyhledána pomocí klíčového slova MQTT. Soubor obsahuje dva listy. List CVE výsledky vyhledávání obsahuje seznam zranitelností z databáze CVE, ty jsou označené jejich unikátním kódem a přiložen je i jejich detailní popis. List Jednotlivé výskyty kategorií obsahuje tabulku výskytu jednotlivých typů zranitelností, tabulku výskytu jednotlivých typů v určených časových rozmezích a vytvořený graf, který je také součástí této práce, Obr. 2.1.