Využití certifikátů pro bezpečnou komunikaci prvků IoT

Martin Mazal

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin Mazal**
Osobní číslo:	**A15141**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Využití certifikátů pro bezpečnou komunikaci prvků IoT.**
Téma anglicky:	**Using Certificates for Secure Communication of IoT (Internet of Things) Components**

Zásady pro vypracování:

1. **Seznamte se s problematikou zabezpečení smart prvků Internetu věcí a možných rizik z toho plynoucích.**
2. **Sestavte přehled aktuálně používaných řešení pro zabezpečení s ohledem na jejich výhody a nevýhody.**
3. **Vhodným způsobem vyberte konkrétní technologie a navrhněte strukturu zabezpečení založenou na systémových certifikátech.**
4. **Vytvořte funkční vzorek navrženého řešení za použití webových technologií a embedded systémů.**
5. **Ověřte a zhodnoťte sestavené zařízení, možnosti jeho využití a úroveň zabezpečení.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.**
2. **VOHNOUTOVÁ, Marta, Libor DOSTÁLEK a Miroslav KNOTEK. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 2. akt. vyd. Brno: COMPUTER PRESS, 2009, 542 s. ISBN 978-80-251-2619-6.**
3. **DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP: Bezpečnost. Brno: Computer Press, 2001, 566 s. ISBN 80-7226-513-X.**
4. **SHOVIC, John C. Raspberry Pi IoT projects: prototyping experiments for makers. New York: Apress, 2016. Technology in action series. ISBN 978-148-4213-780.**
5. **GREENGARD, Samuel. The internet of things. Cambridge, Massachusetts: MIT Press, 2015, 184 s. ISBN 978-026-2527-736.**

Vedoucí bakalářské práce: **Ing. Peter Janků**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **12. prosince 2017**

Termín odevzdání bakalářské práce: **24. května 2018**

Ve Zlíně dne 12. prosince 2017

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl jsem seznámen s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne …….

podpis diplomanta

ABSTRAKT

Tato práce se zabývá problematikou zabezpečení komunikace smart prvků Internetu věcí. Podává stručný přehled o současném stavu zabezpečení smart prvků Internetu věcí a použitých řešení s ohledem na výhody či nevýhody jejich využití. Problematika zabezpečení smart prvků Internetu věcí je aktuální téma, které se neustále vyvíjí na základě vývoje samotných technologií. Právě vývoj nových technologií a jejich velmi rychlé rozšíření a zavedení do procesů, vytváří potřebu zvýšení úrovně zabezpečení nejen smart prvků Internetu věcí, ale i komunikace jako takové. Jelikož žijeme v digitální době, kdy právě dochází ke spojení věcí a digitálních dat, musíme svoje digitální data chránit stejně, jako chráníme vlastní hmotné i nehmotné majetky v reálném světě. Vývoj nových technologií musí jít ruku v ruce s vývojem zabezpečení těchto technologií.

Klíčová slova: certifikační autorita, digitální certifikát, Internet věcí, šifra, zabezpečení

ABSTRACT

This thesis deals with the issue of security of the communication of smart elements of Internet of things. It provides a brief overview of the current state of security of the smart elements of the Internet of Things and of the solutions used, based on their advantages and disadvantages. The issue of securing smart elements of the Internet of Things is an up-to-date topic, that is constantly evolving on the basis of the development of the technologies themselves. Just the development of new technologies and their very rapid expansion and deployment into processes, creates a need to increase the security level not only of smart elements of the Internet of things, but also of communication itself. Because we live in a digital age, when things and digital data are being merged, we need to protect our digital data just as we protect our tangible and intangible assets in the real world. The development of new technologies should go hand in hand with the development of security for these technologies.

Keywords: certification authority, cipher, digital certificate, Internet stuff, security

Poděkování, motto a čestné prohlášení, že odevzdaná verze bakalářské práce a verze elektronická, nahraná do IS/STAG jsou totožné ve znění:

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Velmi děkuji vedoucímu své bakalářské práce Ing. Peteru Janků za jeho čas a rady při řešení dané problematiky.

OBSAH

ÚVOD

Lidstvo se již od počátku věků snaží zdokonalit a zjednodušit svůj život a zpříjemnit domov i jeho okolí. Nové technologie a technologické postupy ovlivňují životy většiny lidí, ať chceme nebo ne. Ať v práci nebo doma. Od vynálezu parního stroje jsme se dostali do věku digitální průmyslové revoluce, doby miniaturizace, doby Internetu věcí. Bezpečnostní technologie či systémy jsou nedílnou součástí každé komplexní technologie, se kterou se člověk může potkat. Největším problémem moderní doby digitalizace je právě sama digitalizace dat a bezpečné nakládání s digitálními daty od jejich vzniku a uložení přes přenos nejenom mezi dvěma zařízeními, ale i na dlouhé vzdálenosti pomocí Internetu a dalších sítí. Bezpečný přenos dat nyní závisí na míře a kvalitě veřejně známých a důvěryhodných zabezpečení. Je však zřejmé, že vývoj nových technologií přináší i potřebu vývoje nových technologií zabezpečení. První kapitola obsahuje seznámení s problematiku zabezpečení smart prvků Internetu věcí. Druhá kapitola popisuje aktuálně používaná řešení zabezpečení s ohledem na jejich výhody a nevýhody. Ve třetí kapitole je navržena struktura zabezpečení založená na kvalifikovaných systémových certifikátech. Praktická část je rozdělena do dvou kapitol. Čtvrtá kapitola se zabývá přípravou funkčního vzorku řešení za použití webových technologií a embeded systémů. Poslední pátá kapitola obsahuje ověření a zhodnocení sestaveného zařízení, možnosti jeho využití a úroveň zabezpečení. Záměrem bakalářské práce je seznámení se s aktuálním řešením zabezpečení komunikace Internetu věcí s ohledem na jejich výhody a nevýhody a využití těchto poznatků k navržení zabezpečení na základě kvalifikovaných systémových certifikátů ověřených důvěryhodnou certifikační autoritou s následným ověřením zabezpečení sestaveného funkčního návrhu.

I. TEORETICKÁ ČÁST

1 SEZNÁMENÍ S PROBLEMATIKOU ZABEZPEČENÍ SMART PRVKŮ INTERNETU VĚCÍ

Technologický vývoj nám přináší různé inovace usnadňující běžný či pracovní život. IoT (Internet věcí) jakožto množina všech adresovaných zařízení, která spolu komunikují, roste tak rychle, že každá technologie bude brzy potřebovat bezdrátové připojení k Internetu. Mezi tato zařízení již nyní patří například detektory kouře, pračky, chladničky, termostaty, inteligentní hodinky, monitory spánku, posilovací pásy, odpadkové koše a pouliční osvětlení se senzory pro sledování provozu, znečištění ovzduší, hluku a parkování, senzory pro hospodářská zvířata či senzory a čidla v průmyslu zajišťující automatizovanou výrobu. [1, 2, 3] Na základě analýz různých odborných firem bude k Internetu připojených zařízení extrémně narůstat. Společnost CISCO se například domnívá, že v roce 2020 bude k Internetu připojeno více než 50 bilionů zařízení. [4]

Obr. 1 Smart prvky Internetu věcí [5]

1.1 Speciální sítě pro provoz IoT

Pro účely propojení prvků IoT se využívají také speciální sítě navržené přímo k tomto účelu. Tyto sítě jsou odděleny od Internetu a jejich provoz je tak zcela izolován. Jedná se například o sítě Sigfox či LoRaWAN. Tyto sítě v České republice provozují významné společnosti z oboru telekomunikací. [6, 7]

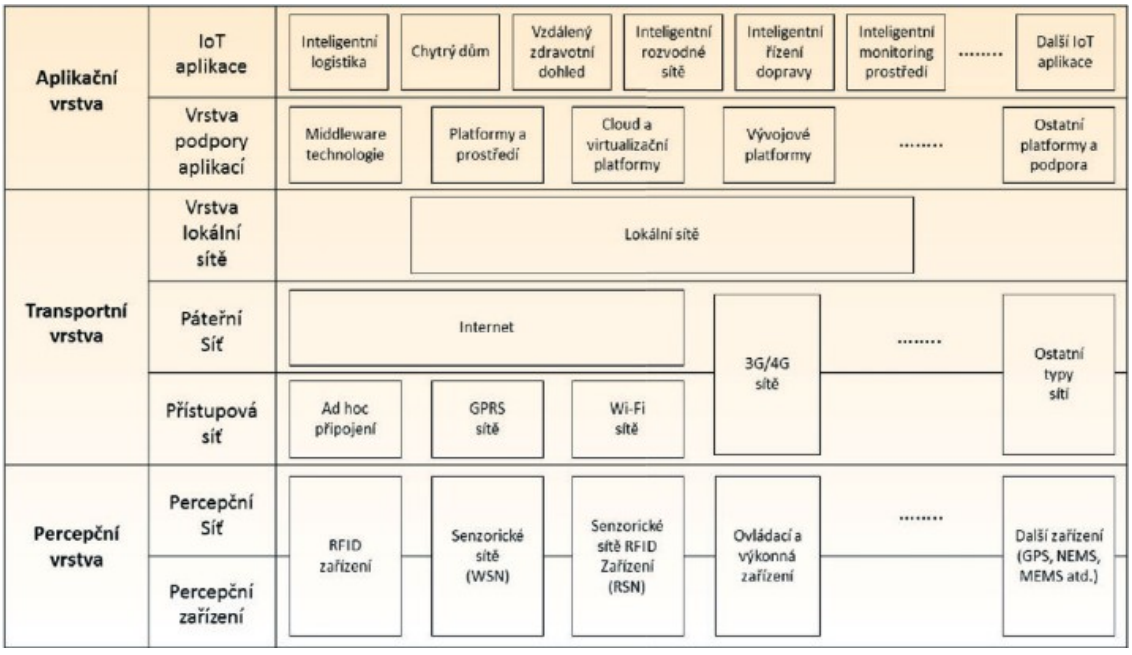
1.1.1 Sigfox

Komunikace je zcela izolovaná od sítě Internet a probíhá na frekvenci 868 MHz s omezením výkonu na 100mW. Velikost zprávy je omezená pouze na 12 bajtů při vysílání a 8 bajtů při

příjmu. Dále se používá omezení na počet zpráv (140 za den pro vysílání a 4 za den pro příjem). Tato omezení jsou použita pro minimalizaci spotřeby energie, a tak zařízení při napájení z baterií vydrží dlouhou dobu. Pokud zařízení nevysílá nebo nepřijímá data, je uvedeno do stavu hlubokého spánku a nespotřebovává téměř žádnou energii. Zabezpečení komunikace je založeno na vymezení časových intervalů pro komunikaci smart prvků. Typická doba přenosu a zpracování dat je 4-6 sekund při rychlosti komunikace 100b/s. Speciální síť Sigfox také využívá autentizaci smart prvků, jako další zabezpečení sítě. Sigfox provozují v České republice společnosti T-Mobile a SimpleCell. Tato síť se například využívá pro automatizované odpočty vody, elektřiny a plynu nebo monitoringu parkovacích automatů. Otevírá se tak prostor pro realizaci myšlenek Industry 4.0, Smart City a dalších aktuálních trendů. [6]

1.1.2 LoRaWAN (Long Range Wide Area Network)

Další ze speciálních sítí provozovaná společnostmi Things.cz a Českými radiokomunikacemi je síť LoRaWAN, také komunikující na frekvenci 868 MHz. Zabezpečení sítě je založeno na principu dvou na sobě nezávislých 128 bitových klíčů. Aplikační klíč zajišťuje šifrování obsahu zprávy a síťový klíč šifruje celou zprávu kromě identifikátoru. Data jsou zašifrována pomocí symetrické blokové šifry AES. Každý koncový bod má přidělený jedinečný 64 bitový identifikátor, což umožňuje řídícímu serveru směrovat komunikaci pouze určitému adresátovi. LoRaWAN se již v dnešní době používá například na zjišťování polohy nezávisle na GPS a GSM signálu (GEO Tracker) nebo pro sledování hlukové zátěže. [7]



Obr. 2 IoT komunikační model [8]

1.2 Bezpečnostní rizika Internetu věcí

Samotné propojení jakéhokoliv zařízení s komunikační sítí, přináší potenciální riziko krádeže dat, poškození dat, znepřístupnění dat nebo úplné ovládnutí zařízení či celé sítě. V případě smart prvků Internetu věcí je velkým rizikem zneužití samotného smart prvku jako přístupového bodu do lokální sítě za daným účelem či ovládnutí zařízení za účelem šíření útoku. Samozřejmostí je dostatečná ochrana zařízení před fyzickou manipulací či odcizením. [9, 10, 11, 12]

1.2.1 Typy koncových zařízení

Rozlišujeme tři základní typy podle jejich inteligence.

- *Zařízení "bez inteligence"*

Zařízení je schopno se autorizovat, autentifikovat, šifrovat komunikaci či monitorovat komunikaci.

- *Zařízení se základní inteligencí*

Takové zařízení je schopné řídit přístup, šifrovat data, používat firewall a detekovat průnik nebo spravovat vlastní aktualizace.

- *Inteligentní zařízení a ovladače*

Zařízení, které mají vlastní operační systém a mohou poskytovat další služby třetích stran pro zabezpečení komunikace. [8]

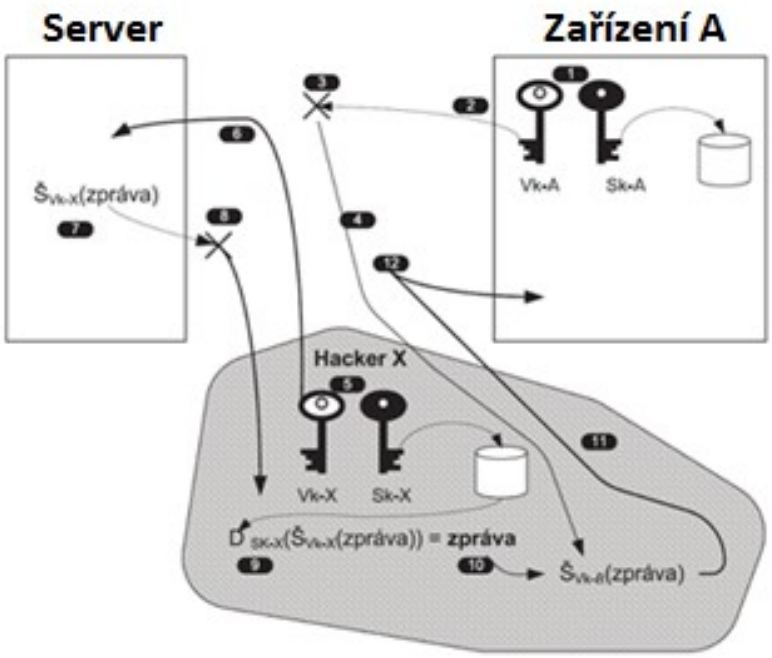
1.2.2 Typy a metody útoků IoT

Útoky můžeme rozdělit na základě původu útoku a provedení útoku. Původ útoku může mít zdroj vně či uvnitř bezpečnostního obvodu. Provedení útoku můžeme rozdělit na aktivní útok a pasivní útok. Aktivní útok se snaží ovlivnit systémové prostředky nebo provoz zařízení. Naopak pasivní útok se snaží naučit nebo využít informace ze systému, nemá však vliv na systémové prostředky nebo provoz zařízení. [13]

Jednou z metod útoků je Man in the middle útok, v překladu znamená muž uprostřed. Z názvu vyplývá, jak útok funguje. Útočník je schopen díky přesměrování veškeré komunikace přes svoje aktivní zařízení odposlouchávat komunikaci mezi účastníky nebo ji dokonce pozměnit či jinak kontrolovat. Cílem útoku může být například komunikace mezi serverem

a zařízením A, jak můžeme vidět na obrázku č. 3. Hacker X je schopen přesměrovat komunikaci, a tím získat veřejný klíč zařízení i serveru a kontrolovat celou komunikaci, aniž by byl odhalen. Tento útok je jednou z častých praktik útočníků. [12]

Další metodou je zahlcení pásma komunikace flood útokem či DDoS útokem. Velké množství komunikace na přenosové frekvenci koncového zařízení může způsobit znemožnění komunikace s tímto zařízením. [14]



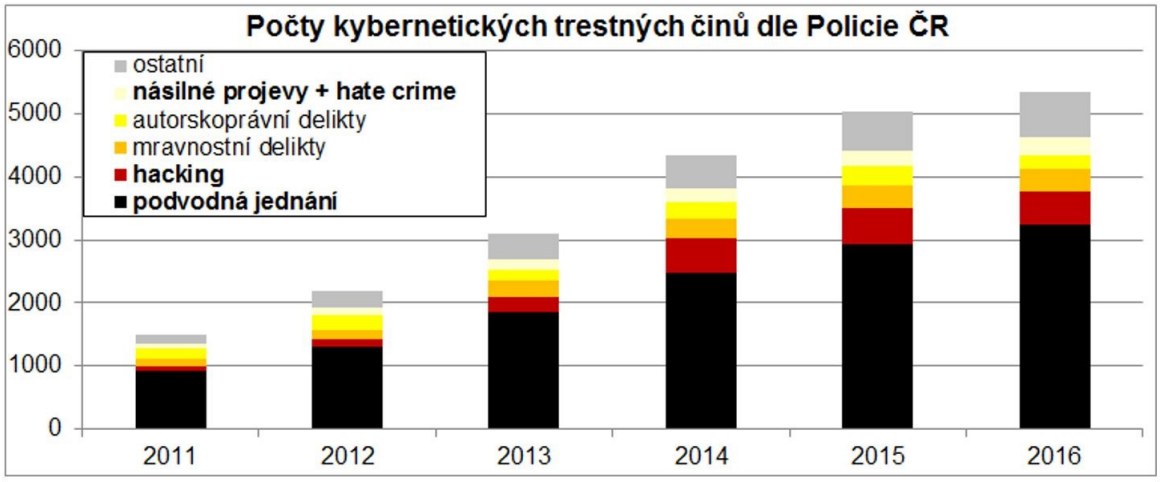
Obr. 3 Útok na distribuci veřejného klíče [13]

1.2.3 Ovládnutí smart prvku

Nepříjemnou situací pro uživatele IoT zařízení je ovládnutí zařízení útočníkem. Útočník využije slabinu v zabezpečení a může získat i plnou kontrolu nad smart prvkem. Pokud útočník získá kontrolu nad smart prvkem, může zařízení znefunkčnit a požadovat výkupné nebo může zařízení využít pro šíření útoku na síti či pro distribuované výpočetní operace. Rovněž může zneužít samotnou primární funkci smart prvku pro získání dat. Možnosti zneužití smart prvku jsou omezeny pouze útočníkovými schopnostmi. Uživatel většinou brzy rozpozná nefunkční smart prvek, a pokud útočník požaduje výkupné, ihned rozpozná, že jde o útok na jeho smart prvek. Často ani zaplacení požadované částky útočníkovi nestačí. Takové zařízení musíme neprodleně odpojit od sítě a nejlépe předat příslušným orgánům státní správy, případně odborné firmě. Pokud útočník zneužije smart prvek, aniž by znatelně ovlivnil jeho funkčnost, uživatel nemusí rozpoznat, že se stal cílem útoku. Zařízení funguje pořád stejně

a na první pohled není zřejmé, že zařízení je pod kontrolou útočníka. V takovém případě je zařízení nedobrovolně využito například pro šíření škodlivého kódu, jako přístupový bod pro útočníka do sítě nebo jinými způsoby a uživatel se o útoku dozví, až se nějakým způsobem projeví. [9, 10, 11, 14]

Mezi známé úspěšné útoky na IoT zařízení patří útoky na chůvičky pro odposlech domácností, dále útoky na smart TV s využitím integrované kamery televize a CCTV kamer pro krádež citlivých záznamů nebo útok na autonomní vozidlo. [10, 14]



Obr. 4 Graf kybernetických trestných činů dle PČR [14]

1.3 Shrnutí problematiky zabezpečení IoT

Technologie použité pro Internet věcí se vyvíjí společně s požadavky na funkční vlastnosti nových zařízení. Komunikace již neprobíhá pouze přes Internet, ale vznikly a vznikají speciální IoT sítě, právě za účelem uspokojení funkčních požadavků nových technologií. Každá ze speciálních sítí má svá specifika, výhody a nevýhody. V této bakalářské práci jsem se zaměřil na část IoT využívající pro svoji komunikaci veřejnou síť Internet a její zabezpečení.

2 PŘEHLED AKTUÁLNĚ POUŽÍVANÝCH ŘEŠENÍ PRO ZABEZPEČENÍ S OHLEDEM NA JEJICH VÝHODY A NEVÝHODY

Aktuální protokoly zabezpečení jsou založeny na dobře známém balíčku kryptografických algoritmů. Pro různé operace se používají různé algoritmy, například bloková šifra Advanced Encryption Standard (AES) pro šifrování dat, Rivest-Shamir-Adelman (RSA) asymetrický algoritmus pro digitální podpisy, Diffie-Helman (DH) asymetrický algoritmus pro výměnu klíčů a SHA-256 hash algoritmus pro zajištění integrity. Tato sada algoritmů se běžně doplňuje dalšími kryptografickými algoritmy a funkcemi. [16]

2.1 Hash algoritmy

Jednocestné matematické funkce schopné převodu libovolně velkého objemu dat na unikátní, konstantně dlouhé číslo v reálném čase, jsou ideální hash funkce respektive algoritmy. Samotné hash funkce jsou postaveny na nízkoúrovňových výpočetních operacích, tudíž jsou velice rychlé. Principem jednocestné funkce je efektivní výpočet otisku daných dat za použití především bitových operací a posunů. Vypočtený otisk daným algoritmem je unikátní pro daná data, a pokud se vstupní data nezmění, nezmění se ani vypočtený otisk. Vývoj kryptografie přinesl celou řadu hash algoritmů, doporučuje se však používat SHA-2 řada algoritmů a vyšší. [14, 17, 18]

2.1.1 Využití

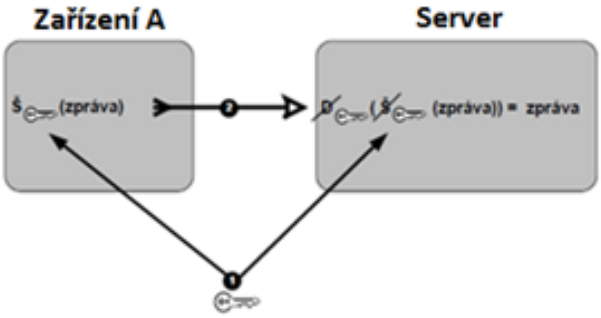
Při sebemenší změně vstupních dat dojde k vytvoření odlišného otisku. Tento princip tedy zajišťuje, že pokud máme k dispozici originální vstupní data a také vypočtený otisk, můžeme s jistotou prokázat opětovným výpočtem otisku a následným srovnáním obou otisků, že se vstupní data nezměnila. [14, 17, 18] Hash funkce se využívá pro ověření integrity dat, ukládání hesel a ochranu citlivých údajů. Dalším využitím je ověření správnosti přenosu dat při komunikaci.

2.1.2 Výhody/Nevýhody

Přednosti hash funkcí jsou nepopiratelně jejich rychlost a efektivita, jelikož výsledný hash je konstantně velký na základě použitého algoritmu. Avšak hash je, jak bylo řečeno, pouze jednocestná operace a neslouží v kryptografické bezpečnosti pro šifrování, což je jeho nevýhoda. [14, 17, 18]

2.2 Symetrická šifra

Oproti hash algoritmu je symetrická šifra obousměrná, a tedy vstupní data jsou pozměněny určitým klíčem, pomocí kterého lze získat zpět vstupní data v původním tvaru. Význam symetrické šifry plyne z použití stejného klíče pro šifrování i dešifrování daných dat. Symetrické šifrování používá celá řada algoritmů, které jsou veřejně známé, protože bez znalosti klíče nejsme schopni běžně dostupnými prostředky data dešifrovat. [14, 17, 18]



Obr. 5 Symetrická šifra [14]

2.2.1 Využití

Samotné šifrování se využívá pro utajení informací před třetí stranou, která nemá klíč k dešifrování. Stejně jako speciální síť LoRaWAN využívá symetrické šifrování pomocí šifry AES 128, tak i některé digitální certifikáty využívají šifrování pomocí šifry AES 128. Smart prvkům sítě LoRaWAN je přiřazen symetrický klíč již při výrobě. Síť Internet využívá Diffie-Helman asymetrický algoritmus pro výměnu klíčů. [7, 14, 17, 18]

2.2.2 Výhody/Nevýhody

Symetrická šifra je velice rychlá, a lze tudíž použít pro šifrování velkých objemů dat. Rychlost šifrování a dešifrování závisí na výkonu šifrovacího stroje, ale i méně výkonný stroj zvládne velice rychle šifrovat či dešifrovat data na základě správného klíče. Nevýhodou symetrické šifry je samotný klíč, který musí být uchován v naprostém utajení před třetí stranou, ačkoli si klíč zároveň potřebujeme předat s druhou stranou. Nutnost předání klíče před zahájením komunikace je tedy hlavní nevýhodou. [14, 17, 18]

2.3 Asymetrická šifra

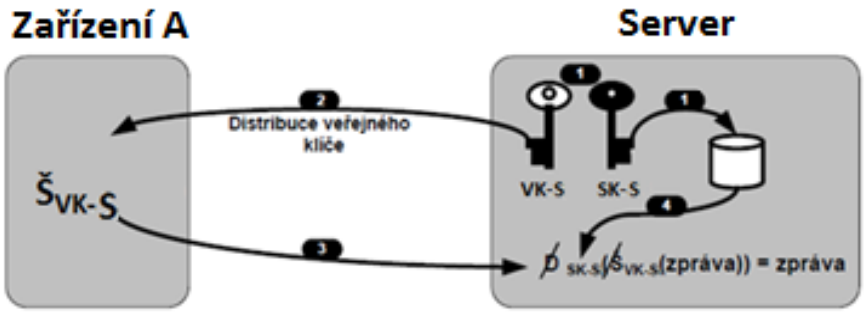
Asymetrická šifra je založena na základě použití šifrovacího páru klíčů, a ne jen jednoho klíče jako u symetrické šifry. Stejně jako u symetrických šifer je celá řada různých algoritmů

asymetrických šifer. Princip je však odlišný. Zvoleným algoritmem vygenerujeme párový klíč, tedy jeden soukromý klíč a jeden veřejný klíč. Veřejný klíč slouží pro šifrování a soukromý klíč pro dešifrování dat. Algoritmus šifrování je opět veřejně známý. [14, 17, 18]

2.3.1 Využití

Asymetrické šifrování dovoluje šifrovaně komunikovat bez nutnosti si předávat tajně klíč. Pro dosažení co největší efektivnosti šifrování je pro šifrování klíčů symetrických šifer využito asymetrické šifrování. Postup pro šifrování a odeslání citlivých informací mezi smart prvkem a dalšími zařízeními IoT (obrázek č. 6):

1. zařízení A si vyžádá veřejný klíč serveru;
2. zařízení A zašifruje zprávu symetrickou šifrou a klíč symetrické šifry zašifruje pomocí získaného veřejného klíče serveru;
3. zařízení A odešle zašifrovanou zprávu a zašifrovaný klíč po (ne)zabezpečené lince;
4. server dešifruje pomocí soukromého asymetrického klíče zašifrovaný klíč symetrické šifry, který poté využije pro dešifrování zprávy.



Obr. 6 Asymetrická šifra [14]

2.3.2 Výhody/Nevýhody

Asymetrické šifry pracují na principu bloků bitů a chrání proti frekvenční analýze a frázovým útokům, jelikož pro šifrování a dešifrování je použit vždy jiný klíč. Také není potřeba si klíč tajně vyměňovat. Bohužel generování párového klíče a šifrování asymetrickou šifrou je náročné na výkon šifrovacího stroje. V porovnání se symetrickou šifrou je asymetrická šifra pomalejší. Největší nevýhodou je však omezení velikosti šifrovaných dat pomocí asymetrické šifry v závislosti na délce klíče. Maximální velikost šifrovaných dat u algoritmu RSA při použití 2048 bitového klíče je 1960 bitů. [14, 17, 18]

2.4 Digitální certifikát

Jedním z typů asymetrické kryptografie je i digitální certifikát. Jedná se o digitálně podepsaný veřejný šifrovací klíč vydaný certifikační autoritou. Nejrozšířenější formát digitálního certifikátu je X.509, který obsahuje veškeré potřebné údaje o majiteli veřejného klíče a vydavateli certifikátu. [14, 17, 18]

2.4.1 Obsah certifikátu

- *Verze certifikátu*

  Verze certifikátu je odvozena od verze standardu X.509.

- *Sériové číslo certifikátu*

  Sériové číslo certifikátu je unikátní v rámci dané certifikační autority a napomáhá jasné identifikaci certifikátu.

- *Algoritmus podpisu certifikátu*

  Algoritmus použitý certifikační autoritou k vytvoření podpisu certifikátu.

- *Vydavatel certifikátu – Certifikační autorita*

  Identifikační údaje vydavatele certifikátu – jedinečný název certifikační autority.

- *Platnost certifikátu*

  Datum počátku a konce platnosti certifikátu.

- *Předmět certifikátu*

  Předmětem certifikátu jsou identifikační údaje majitele certifikátu.

- *Informace o veřejném klíči subjektu*

  Identifikátor použitého algoritmu a samotný veřejný klíč subjektu.

- *Rozšíření*

  Mezi rozšíření certifikátu patří všechny další důležité informace jako:

  - *Alternativní jméno subjektu certifikátu*
  - *Základní omezení certifikátu*
  - *Distribuční body CRL*
  - *Pravidla certifikátu*

- *Identifikační klíč certifikační autority*
- *Použití klíče certifikátu - (šifrování, ověřování nebo obojí)*
- *Rozšířené použití klíče*
- *Přístup k informacím autority*
- *Identifikátor objektu*
- *Doba platnosti soukromého klíče*
- *Biometrické informace*
- *Název šablony certifikátu a další*

- *Hodnota podpisu certifikátu*

  Samotný podpis digitálního certifikátu vytvořený certifikační autoritou. [14, 17, 18]

2.4.2 Druhy certifikátů

- *Self-signed certifikát*

Jedná se o certifikát podepsaný sám sebou. Při vygenerování klíčového páru je možné veřejný klíč podepsat daným privátním klíčem. Jelikož jde o certifikát podepsaný vlastním soukromým klíčem, nejde pro jeho ověření využít důvěryhodná a nezávislá certifikační autorita, a tudíž musíme v případě použití takového certifikátu složitě manuálně ověřovat jeho pravost a integritu. Právě proto jsou tyto certifikáty použity výhradně v lokálních sítích či pro testování. [14, 17, 18]

- *Komerční certifikát*

Nejrozšířenějším druhem digitálních certifikátů je právě komerční certifikát. Komerční certifikát vystavuje certifikační autorita dle interních směrnic a pravidel, přičemž žádný zákon nestanovuje způsob ověření takových certifikátů. Uplatnění mají široké a nejčastěji jsou použity pro autentizaci uživatelů pomocí certifikátů, pro zajištění šifrované komunikace nebo pro ověření elektronických podpisů. [14, 17, 18]

- *Kvalifikovaný certifikát*

Digitální certifikát vydaný akreditovanou certifikační autoritou je v České republice definován zákonem č. 297/2016 Sb., tzv. kvalifikovaný certifikát. [15] Kvalifikovaný certifikát je spíše znám jako elektronický podpis, se kterým se potkáme v elektronické komunikaci, kde je potřeba přiložit ověřený podpis, například v komunikaci s Českou správou sociálního zabezpečení, s některými zdravotními pojišťovnami, soudy. Kvalifikovaný osobní certifikát je

nepostradatelný při odesílání zpráv z datové schránky u společností s více jednateli nebo ze schránek orgánů veřejné moci. [14, 17, 18, 19]

- *Technologické (Serverové) certifikáty*

Definice podle První certifikační autority I.CA zní: *„Komerční technologické (serverové) certifikáty I.CA jsou určeny především pro vzájemnou zabezpečenou komunikaci serverů. Použití tohoto typu certifikátu není vhodné pro zabezpečení webových serverů. Tyto certifikáty jsou vydávány jak fyzickým, tak i právnickým osobám na základě řádné elektronické žádosti o certifikát (zpravidla vytvořené přímo příslušným serverem), kterou žadatel předloží společně s požadovanými doklady totožnosti na vybraných registračních autoritách I.CA.“* [20]

- *Kvalifikované systémové certifikáty*

Definice podle První certifikační autority I.CA zní: *„Systémový certifikát je speciální formou kvalifikovaného certifikátu. Společně s daty pro tvorbu elektronických značek slouží k bezpečnému vytváření a ověřování elektronických značek. Označujícím subjektem (tvůrcem elektronické značky) může být pouze právnická osoba nebo orgán státní správy či samosprávy. Systémový certifikát tedy slouží zejména pro automatizované systémy, které využívají technologii založenou na principech elektronického podpisu, bez součinnosti konkrétní fyzické osoby, například elektronická fakturace, hromadné zasílání e-mailů, doručenky e-podatelny.“* [21]

2.4.3 Fáze certifikátu

Stejně jako jiné doklady totožnosti, prochází digitální certifikát několika fázemi, a to:

1. Žádost o vydání certifikátu
2. Vydání certifikátu
3. Platnost certifikátu
4. Vypršení platnosti certifikátu
5. Odvolání certifikátu [14, 17]

2.5 Certifikační autorita

Digitální certifikáty generuje subjekt nazvaný certifikační autorita. Certifikační autorita potvrzuje pravdivost a platnost vydaných certifikátů a provádí další činnosti. Za předpokladu,

že je zvolená certifikační autorita důvěryhodná, můžeme díky ověřenému digitálnímu certifikátu důvěřovat uvedeným informacím v digitálním certifikátu, a také datům podepsaných daným digitálním certifikátem. [14, 17, 18]

2.5.1 Činnosti certifikační autority

- *Počáteční ověření identity žadatele o digitální certifikát*

Hlavní činností certifikační autority je samotné ověření žadatele o digitální certifikát. Žadatel musí na základě vybraného certifikátu splnit požadované podmínky pro jeho vydání, tím se prokázat před certifikační autoritou a ověřit svoji identitu. Fyzické i právnické osoby mají odlišné podmínky ověření, stejně jako různé druhy certifikátů vyžadují splnění různých podmínek pro jejich získání. [14, 17, 18]

- *Vydávání nových digitálních certifikátů*

Za všechny digitální certifikáty vydané certifikační autoritou ručí certifikační autorita. Po identifikaci a ověření žadatele vydá certifikační autorita digitální certifikát, který obsahuje ověřené údaje. Elektronický podpis ověřující autentičnost digitálního certifikátu je nedílnou součástí certifikátu. V případě pozměnění údajů třetí stranou by ověření certifikátu selhalo, a tím odhalilo útok. [14, 17, 18]

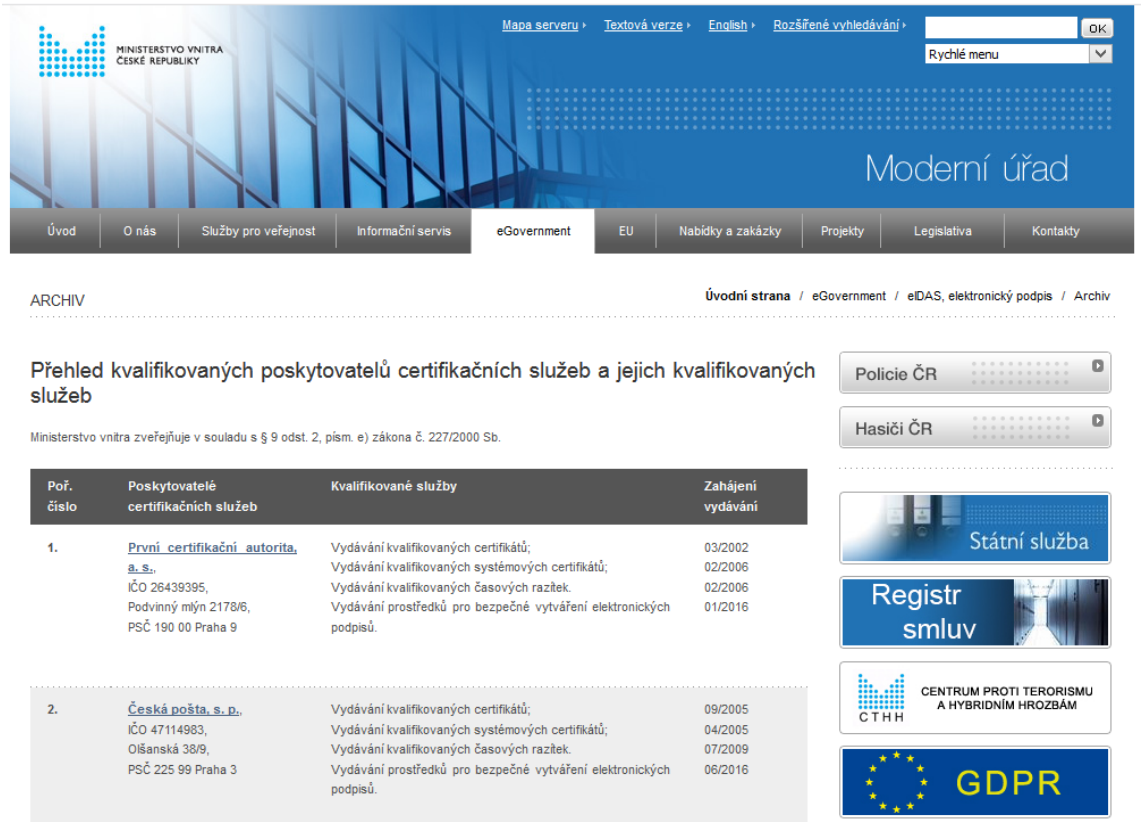
- *Zveřejňování seznamu neplatných digitálních certifikátů CRL*

Stejně jako ověřování žadatelů nebo vydávání nových certifikátů, je neméně důležitou činností zveřejňování seznamu neplatných digitálních certifikátů CRL (Certificate Revocation List). Tento CRL seznam slouží k odvolání certifikátů před datem skončení jejich platnosti, a než datum platnosti digitálního certifikátu vyprší, musí být uveden na tomto seznamu. Tento seznam není určen pro manuální lidské ověřování, ale pro komunikaci a ověřování mezi stroji a zařízeními. Standart X.509 stanovuje formát CRL seznamu, který musí být aktualizovaný a dostupný. [14, 17, 18]

2.5.2 Kvalifikovaná certifikační autorita

Kvalifikovaná certifikační autorita je v rámci České republiky definována zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce a nařízením č. 910/2014 Sb., o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a zákonem na ochranu osobních údajů 101/2000 Sb. [19, 20]

Seznam akreditovaných certifikačních autorit vydávajících kvalifikované certifikáty zveřejňuje Ministerstvo vnitra České republiky. [20]



Obr. 7 Seznam kvalifikovaných certifikačních autorit [20]

3 NÁVRH STRUKTURY ZABEZPEČENÍ ZALOŽENÉ NA SYSTÉMOVÝCH CERTIFIKÁTECH

Struktura zabezpečení založená na kvalifikovaných systémových certifikátech využívá výhod všech dříve zmíněných technologií, jako jsou hash funkce, symetrické, asymetrické šifry a digitálního certifikátu ověřeného certifikační autoritou. Mnou navržená struktura zabezpečení komunikace mezi připojenými zařízeními je založená právě na kvalifikovaných systémových certifikátech generovaných důvěryhodnou certifikační autoritou, jelikož jsem se osobně nesetkal se zařízením IoT, které by využívalo tuto technologii zabezpečení. [14, 17, 18, 22]

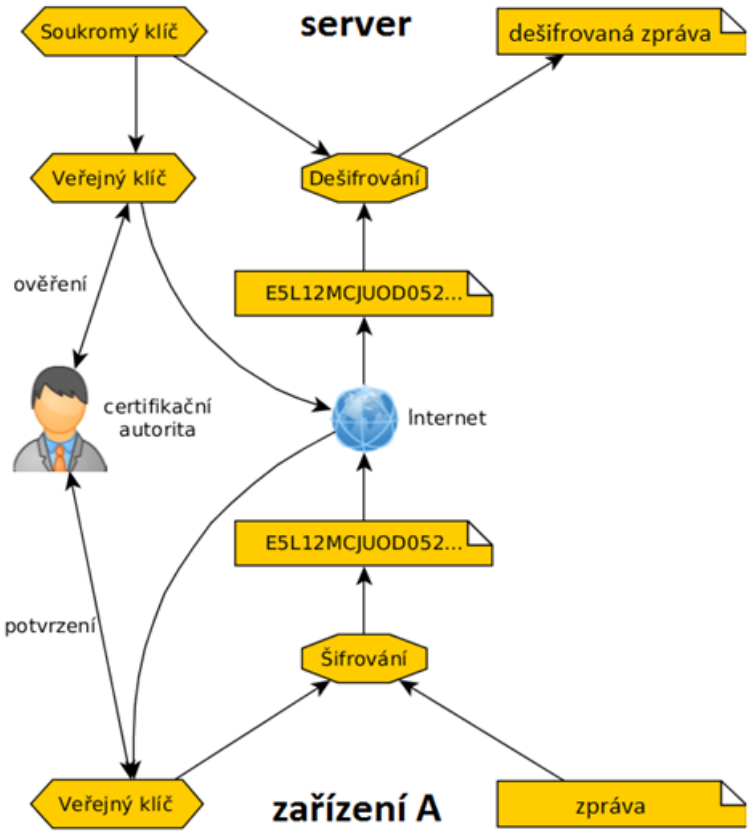
3.1 Certifikační autorita

Aktuálně jedna ze tří českých kvalifikovaných certifikačních autorit je První certifikační autorita a.s., která nabízí i kvalifikovaný systémový certifikát. [20] Definice systémového certifikátu První certifikační autority I.CA zní: *„Systémový certifikát je speciální formou kvalifikovaného certifikátu. Společně s daty pro tvorbu elektronických značek slouží k bezpečnému vytváření a ověřování elektronických značek. Označujícím subjektem (tvůrcem elektronické značky) může být pouze právnická osoba nebo orgán státní správy či samosprávy. Systémový certifikát tedy slouží zejména pro automatizované systémy, které využívají technologii založenou na principech elektronického podpisu, bez součinnosti konkrétní fyzické osoby, například elektronická fakturace, hromadné zasílání e-mailů, doručenky e-podatelny.“* [22]

Jak z definice vyplývá, systémové certifikáty slouží pro automatizované systémy, což je i předpoklad Internetu věcí. Schéma na obrázku č. 8 zobrazuje bezpečnou komunikaci s využitím digitálního certifikátu a šifrováním zprávy asymetrickou šifrou. Server nejprve vygeneruje párový klíč. Veřejný klíč s žádostí o digitální certifikát nechá ověřit certifikační autoritou a předá tento veřejný klíč zařízení A. Zařízení A ověří u certifikační autority, že veřejný klíč patří opravdu serveru, použije ověřený veřejný klíč k zašifrování zprávy a pošle ji serveru přes Internet. Server poté použije svůj soukromý klíč k dešifrování zprávy.

Zabezpečení na základě digitálního certifikátu jsem zvolil z několika důvodů. Jedním z důvodů je jeho snadná implementace. Dalším důvodem je jeho celosvětové rozšíření a používání mnoha institucemi, což dokumentuje spolehlivost tohoto řešení. Používání jednotné

formy X.509 a dalších obecně uznávaných protokolů zajišťuje kompatibilitu komunikace různých zařízení.



Obr. 8 Obecné schéma zabezpečené komunikace [23]

3.1.1 HTTPS vs MQTT

Protokol HTTPS je ve světě Internetu velmi rozšířený. Pro komunikaci mezi zařízeními Internetu věcí však není úplně ideální. MQTT (Message Queue Telemetry Transport) je protokol vytvořený pro komunikaci mezi klienty prostřednictvím centrálního bodu, tzv. brokeru. Tento protokol navrhla společnost IBM. Před nedávnem byla vydána specifikace OASIS. Zprávy jsou tříděny centrálním brokerem do témat s hierarchickou strukturou. Můžeme použít hvězdičkovou konvenci pro rozdělení do skupin koncových zařízení, například patro, místnost, svítidlo a další. Hierarchická struktura je zcela volná a závisí pouze na návrhu autora. Níže uvedená tabulka č. 1 nabízí souhrnné porovnání výsledků testů provedených mezi protokolem HTTPS a MQTT. Testy byly provedeny opakovaným odesláním a příjmem 1024 zpráv, každá o velikosti 1 bajtu. [24]

Tabulka 1 Porovnání výsledků testů mezi HTTPS a MQTT [24]

		3G		WiFi	
		HTTPS	MQTT	HTTPS	MQTT
Přijaté zprávy	Počet zpráv za hodinu	1 708	160 278	3 628	263 314
	Spotřeba baterie v procentech za hodinu	18.43%	16.13%	3.45%	4.23%
	Spotřeba baterie za zprávu	0.01709%	0.00010%	0.00095%	0.00002%
	Počet potvrzených přijatých zpráv	240/1024	1024/1024	524/1024	1024/1024
Odeslané zprávy	Počet zpráv za hodinu	1 926	21 685	5 229	23 184
	Spotřeba baterie v procentech za hodinu	18.79%	17.80%	5.44%	3.66%
	Spotřeba baterie za zprávu	0.00975%	0.00082%	0.00104%	0.00016%

Data z tabulky vypovídají následující:

1. HTTPS protokol je více náročný na baterii než MQTT protokol
2. HTTPS protokol je méně spolehlivý než MQTT protokol
3. HTTPS protokol je pomalejší než MQTT protokol

3.1.2 Graylog

Základem komunikace elektronických zařízení bylo zaslání příkazu odesílatelem a splnění příkazu přijímacím zařízením. Tento způsob komunikace není úplně vhodný pro IoT zařízení. Mnohem vhodnější je, když zařízení jako jsou senzory, snímače, čítače a další, pouze posílají informace naměřené nebo spočítané, ale samotné rozhodnutí o následně provedené či neprovedené akci je oddělené a nezávislé na samotných připojených zařízeních. Graylog je systém, který se zabývá zpracováním příchozích zpráv. Tento systém nahlíží na příchozí

zprávy jako na proudy, které si definuje uživatel. Proudy zpráv se mohou skládat ze zpráv jednoho či více zdrojů. Zprávy jsou ukládány do databáze pro jejich další použití. Indexováním zpráv v databázi docílíme rychlého vyhledávání. [25]

Obr. 9 Úvodní stránka systému Graylog 2 [25]

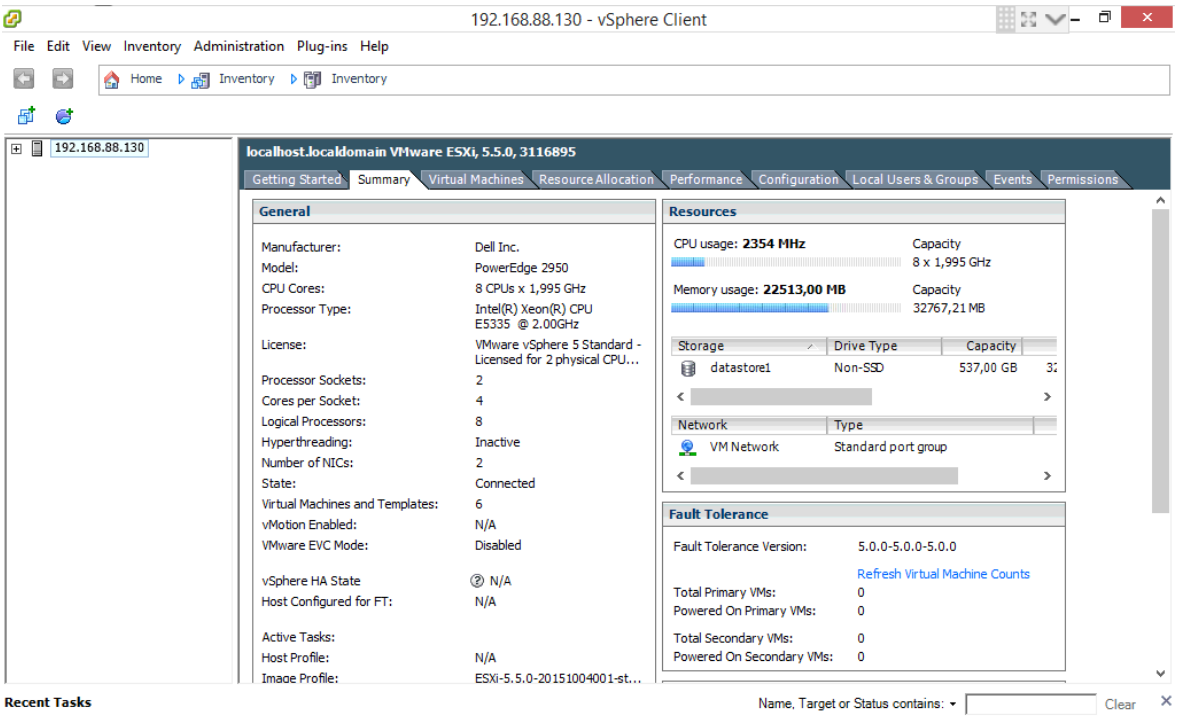
II. PRAKTICKÁ ČÁST

4 FUNKČNÍ VZOREK ŘEŠENÍ ZA POUŽITÍ WEBOVÝCH TECHNOLOGIÍ A EMBEDED SYSTÉMŮ

Zabezpečení komunikace za použití digitálních certifikátů jsem otestoval na sestaveném funkčním vzorku popsaném v této kapitole. Využil jsem webové technologie a embeded systémy.

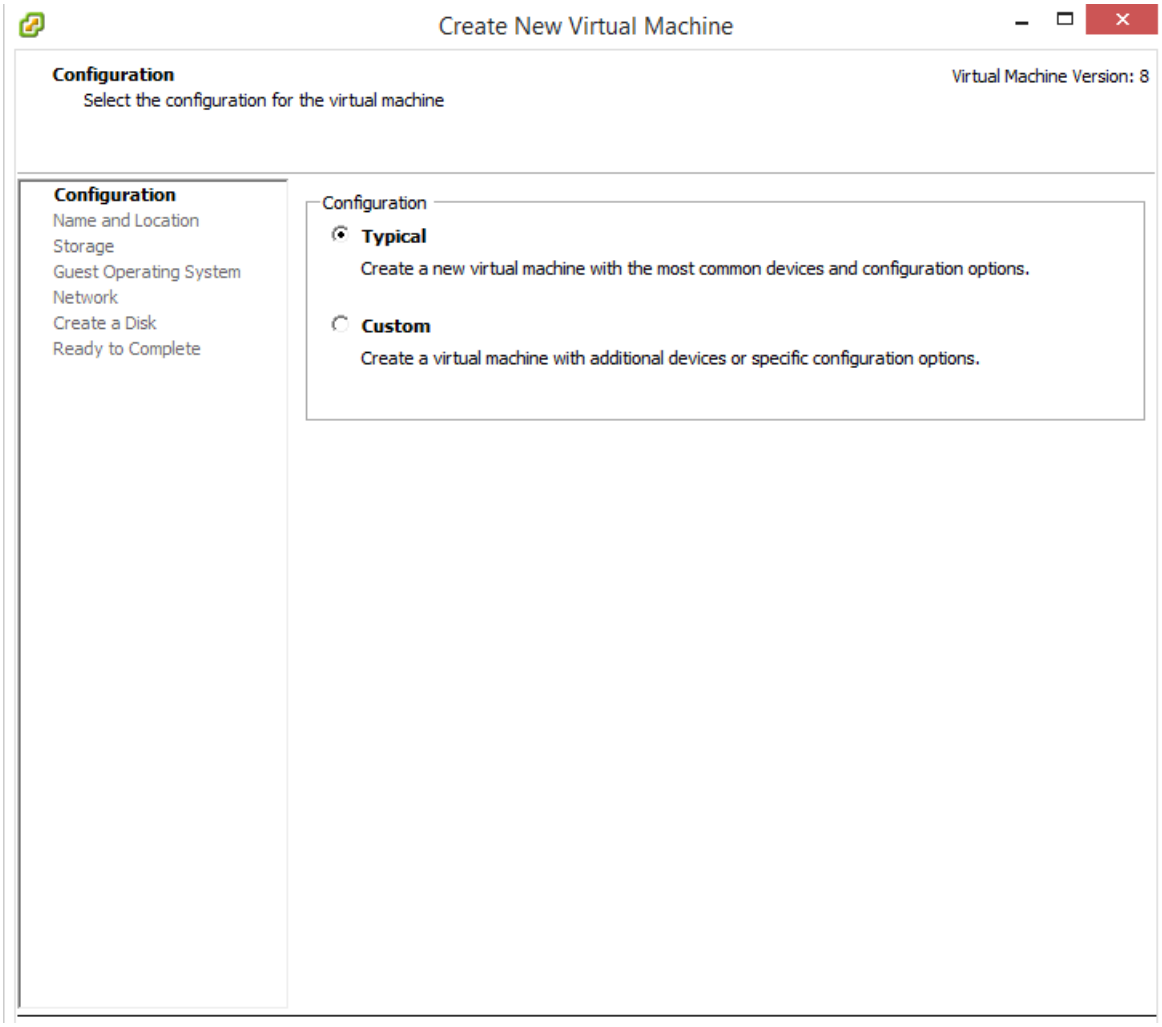
4.1 Instalace serverů

Abychom mohli sestavit funkční vzorek, musíme nejprve připravit několik serverů. Pro servery využijeme virtualizaci od společnosti VMware. Na obrázku č. 10 je vyobrazen vSphere client, což je administrativní prostředí pro virtualizaci VMware.



Obr. 10 Správa virtuálního prostředí VMware

Dále použijeme průvodce vytvořením virtuálního serveru VMware, jak je vyobrazeno na obrázku č. 11. Zvolíme operační systém Linux a vybereme připravený soubor pro instalaci operačního systému.



Obr. 11 Průvodce vytvořením virtuálního serveru

4.1.1 Instalace a nastavení MQTT serveru

Pro MQTT server jsem použil OS Linux Debian 9. Po instalaci serveru je potřeba provést update a upgrade systému Linux a můžeme pokračovat s instalací MQTT serveru. Pro otestování funkčnosti navrženého řešení využijeme MQTT server Mosquitto a kvalifikovaný systémový certifikát. Postup pro vydání systémového certifikátu je detailně popsán na webových stránkách První certifikační autority. [22, 26]

Instalace se provádí příkazem: *apt-get install mosquitto*

dále nainstalujeme CertBot příkazem: *apt-get install certbot*

povolíme v Linux Firewall port 8883 příkazem: *ufw allow 8883*

Nastavíme CertBot příkazem:

certbot certonly --standalone --standalone-supported-challenges -d mazalholding.cz -x509 -new -nodes -key /etc/ssl/private/rootCA-Development.key -sha256 -days 3650 -subj "/C=CZ/ST=Olomouc/L=Olomouc/O=Development" -out /etc/ssl/certs/rootCA-Development.pem

nastavíme heslo pro MQTT příkazem: *mosquitto_passwd -c /etc/mosquitto/passwd HESLO*

provedeme příkaz: *nano /etc/mosquitto/conf.d/default.conf* a vložíme:

```
1 allow_anonymous false
2 password_file /etc/mosquitto/passwd
```

Provedeme restart MQTT serveru příkazem: *systemctl restart mosquitto* [27]

4.1.2 Embedded zařízení

Pro testování bylo použito zařízení Raspberry Pi pro jeho dostupnost a cenu. V každém případě námi zvolené technologie zabezpečení komunikace lze implementovat na všechny kompatibilní zařízení s procesorem schopným šifrovat, interní pamětí pro uložení programu a certifikátu.

Nejdříve musíme nainstalovat OS také na Raspberry Pi. Použil jsem nativní OS Raspbian Stretch Lite. Po instalaci OS, jsem nakonfiguroval WiFi a povolil SSH připojení příkazy:

sudo systemctl enable ssh

sudo wpa_supplicant -iwlan0 -Dwext -c/etc/wpa_supplicant.conf -B -N \ -ieth0 -Dwired -c/etc/wpa_supplicant.conf

spustíme příkaz: *sudo nano /etc/wpa_supplicant.conf*

obsah souboru upravíme na:

```
1 network={
2     ssid="NAZEV SITE"
3     proto=WPA
4     key_mgmt=WPA-EAP
5     pairwise=TKIP
6     group=TKIP WEP104 WEP40
7     eap=PEAP
8     identity="USER@NAZEV DOMENY.cz"
9     password="HESLO"
```

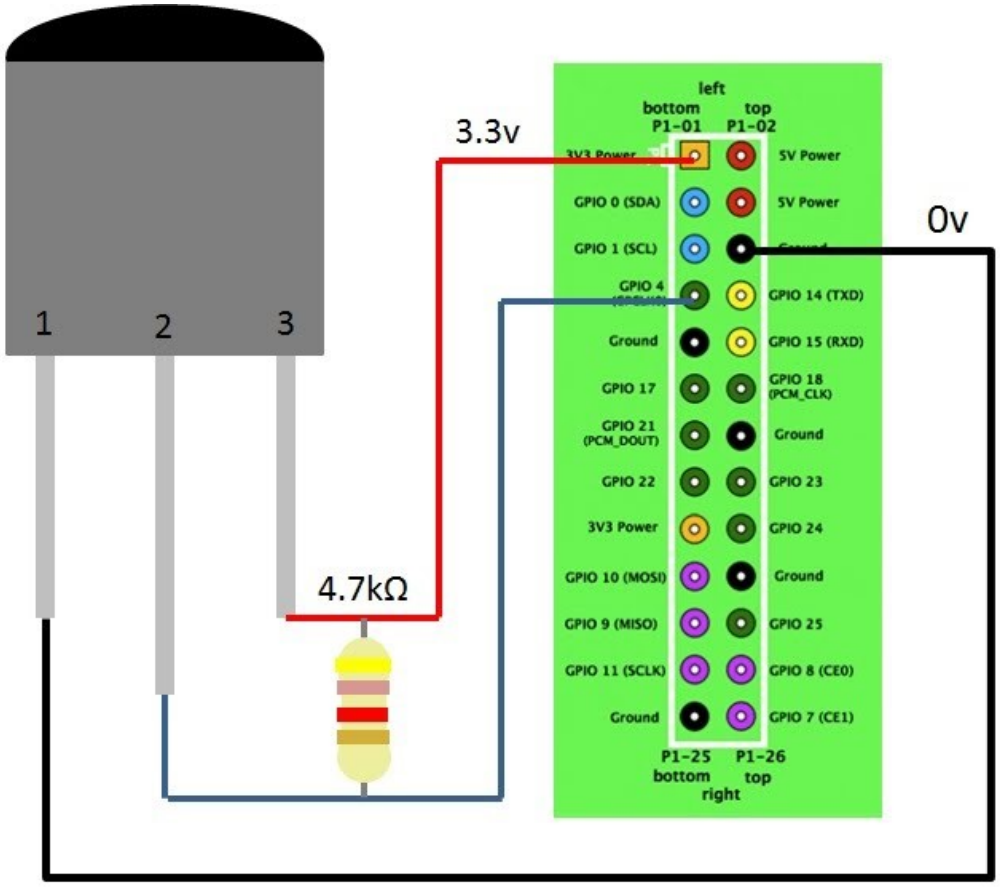
```
10    ca_cert="/etc/1x/CERTIFIKAT.pem"
11    phase2="auth=PAP" }
```

dále provedeme příkaz: *sudo nano /etc/network/interfaces*

obsah souboru upravíme na:

```
1 auto lo
2 iface lo inet loopback
3 allow-hotplug eth0
4 iface eth0 inet dhcp
5 wpa-conf /etc/wpa_supplicant.conf
6 allow-hotplug wlan0
7 iface wlan0 inet dhcp
8 wpa-conf /etc/wpa_supplicant.conf
```

Nyní máme nastavenu WiFi síť a můžeme připojit připravený senzor teploty a vlhkosti. Senzor zapojíme dle nákresu na obrázku č. 12.



Obr. 12 Schéma zapojení senzoru teploty a vlhkosti [28]

Vytvoříme nový skript v jazyce python, který bude číst data ze senzoru a bude je odesílat na MQTT server. Komunikace je zabezpečená digitálním certifikátem. Pro vytvoření skriptu použijeme příkazy:

sudo apt-get install build-essential python-dev python-openssl paho-mqtt

cd /home/pi

sudo wget https://github.com/adafruit/Adafruit_Python_DHT

cd Adafruit_Python_DHT

sudo python setup.py install

sudo nano TEMPaHUM.py

obsah souboru upravíme na:

```
1 import sys
2 import Adafruit_DHT
3 import paho.mqtt.client as mqtt
4 import time
5 import json
6 import ssl
```

Vytvoření mqtt klienta:

```
7 client = mqttClient.Client()
```

Nastavení připojení:

```
8 client.username_pw_set(USER, HESLO)
9 client.tls_insecure_set(False)
10 client.tls_set(ca_certs="cert.pem", certfile=None, key-
file=None, cert_reqs=ssl.CERT_REQUIRED,
tls_version=ssl.PROTOCOL_TLSv1_2, ciphers=None)
11 tls.connect("mazalholding.cz", 8883, 60)
12 client.loop_start()
```

Kontrola vstupních parametrů:

```
13 while True:
14     sensor_args = {'22': Adafruit_DHT.DHT22}
15     if len(sys.argv) == 3 and sys.argv[1] in sensor_args:
16         sensor = sensor_args[sys.argv[1]]
17         pin = sys.argv[2]
18     else:
19         print('Špatně zadané vstupní parametry!')
20                 sys.exit(1)
```

Čtení dat ze senzoru a jejich poslání na MQTT server:

```
21     hum, temp = Adafruit_DHT.read_retry(sensor, pin)
22     hostname = 'Pi home'
23     text = "Teplota a Vlhkost"
24     data = {
25         'host'      : hostname,
26         'short_message' : text,
27         'Teplota'   : temp,
28         'Vlhkost'   : hum }
29     if hum is not None and temp is not None:
30         client.publish("TEMPaHUM", json.dumps(data))
31     else:
32         print('Nelze načíst hodnoty senzoru.')
33         sys.exit(1)
34     time.sleep(10) [27, 28]
```

4.1.3 Instalace webové technologie Graylog

Graylog server lze instalovat několika způsoby. Jedním ze způsobů je instalace připraveného virtuálního stroje. Jelikož jde o testovací prostředí, využijeme tuto možnost a do virtuálního prostředí importujeme stažený virtuální stroj graylog-2.4.4-1.ova. [25]

Po úspěšném importování Graylog 2 serveru do VMware prostředí musíme provést nastavení a doinstalovat MQTT plugin. [29]

Nejdříve je potřeba nastavit heslo pro administrátora webového rozhraní. Připojíme se na Graylog server a v příkazové řádce spustíme příkaz:

echo -n AdminHeslo | sha256sum

Výstupem bude heslo v hash tvaru:

68sd4df613fdf156fdf98df8d9g91hghg9j4k1dd2a116bf235e943771ad16c4e88

Dále je nutné vygenerovat tajné heslo příkazem:

pwgen -N 1 -s 96

Výstupem bude řetězec znaků:

vHjldsdoinklkPc0YKySXhkebfwUYvW2dQz7kD1GxBKljidre1eIAySsUUJkadloP58IHImk-pTswvc3MFSVDrwn5AmdwOSMrikl85

Takto vytvořené hashe vložíme do konfiguračního souboru Graylog serveru:

nano /etc/graylog/server/server.conf

Upravíme řádky:

```
1 password_secret = vHjldsdoinklkPc0YKySXhkebfwUYvW2dQz7kD1G-
xBKljidre1eIAySsUUJkadloP58IHImkpTswvc3MFSVDrwn5AmdwOSMrikl85
2 root_username = admin
3 root_password_sha2
= 68sd4df613fdf156fdf98df8d9g91hghg9j4k1dd2a116bf235e943771a-
d16c4e88
```

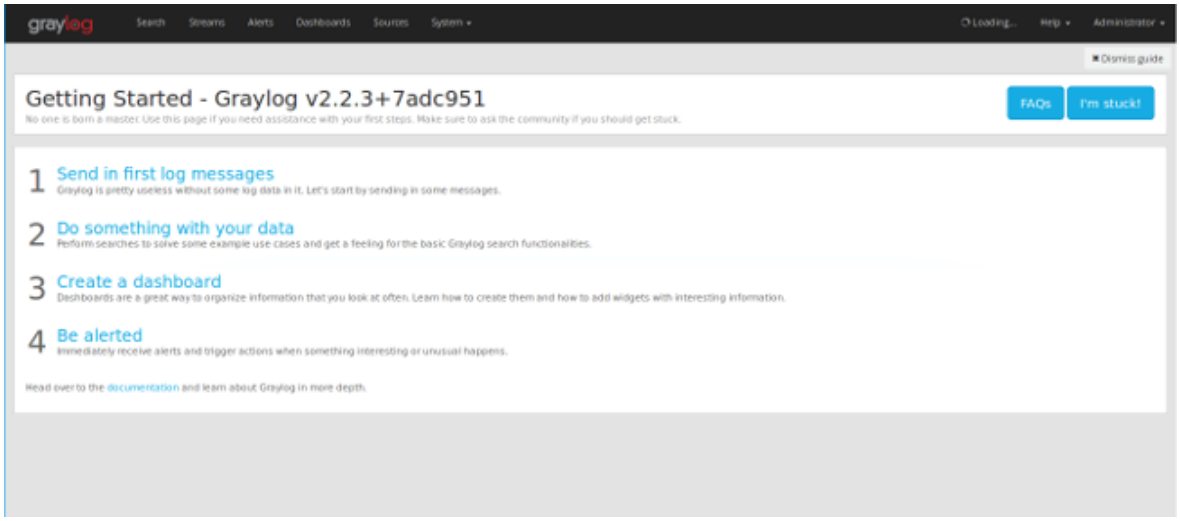
Po změně konfiguračního souboru musíme restartovat Graylog server příkazem:

systemctl restart graylog-server

Nyní je webové rozhraní Graylog serveru dostupné na portu 9000, viz obrázek č. 9 a 13:

192.168.88.153:9000

Přihlášení je nyní možné za pomocí uživatele ‚admin' a hesla ‚AdminHeslo'.



Obr. 13 Úvodní stránka po prvním přihlášení

Následně musíme stáhnout MQTT plugin pro logování zpráv z MQTT serveru. Použijeme připravený plugin dostupný na adrese *https://github.com/graylog-labs/graylog-plugin-mqtt.*

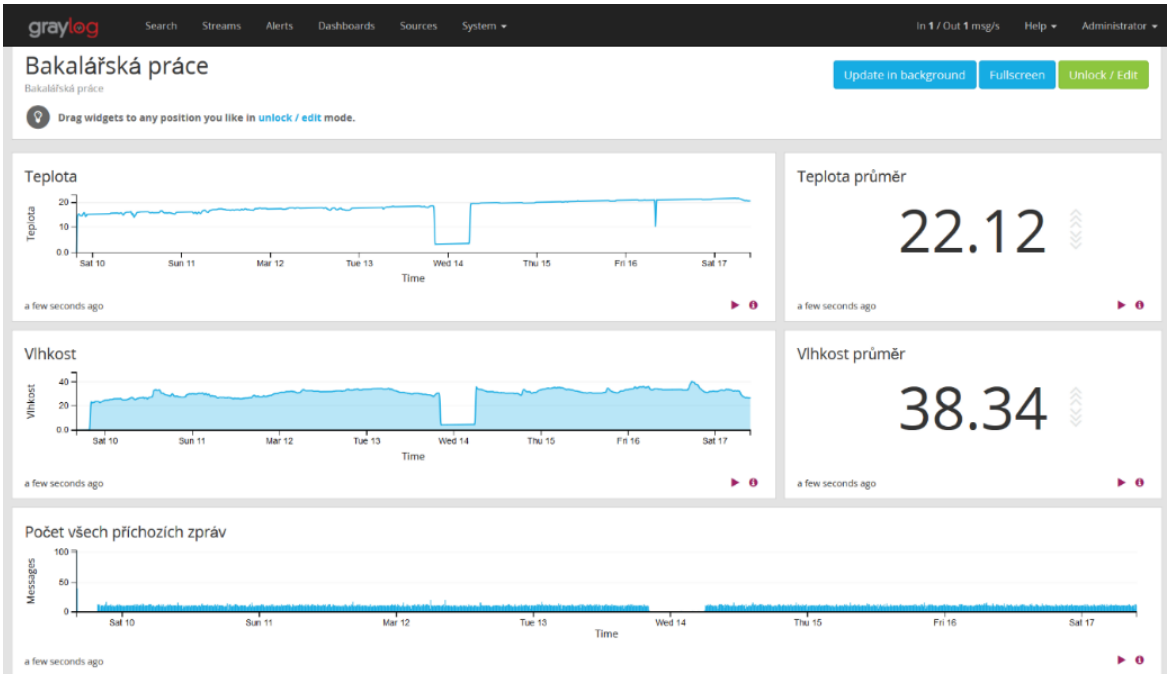
Stažený soubor s příponou jar uložíme na Graylog server do složky */usr/share/graylog-server/plugin.* Provedeme restart Graylog serveru příkazem:

systemctl restart graylog-server

Nyní v menu System -> Inputs vybereme nově přidaný MQTT plugin, potvrdíme tlačítkem Launch new input a nastavíme, viz obrázek č. 14.

Obr. 14 Nastavení MQTT pluginu

Nyní Graylog server zpracovává zprávy zaslané na MQTT server a ukládá je do databáze, která umožňuje další zpracování zpráv ve formě statistik s možností přehledných grafů, viz obrázek č. 15.



Obr. 15 Zobrazení statistik pomocí Graylog 2

5 OVĚŘENÍ A ZHODNOCENÍ SESTAVENÉHO ZAŘÍZENÍ, MOŽNOSTI JEHO VYUŽITÍ A ÚROVEŇ ZABEZPEČENÍ

5.1 Ověření a zhodnocení sestaveného zařízení

Ověření zabezpečení sestaveného zařízení jsem provedl za použití penetračních testů projektu Nessus společnosti Tenable a online testovacích nástrojů Pentest-Tools. Software Nessus Proffesional lze zdarma stáhnout z webových stránek společnosti Tenable na 7 dní. Zmíněný sofware obsahuje balíčky přednastavených testů od skenovnání otevřených portů, až po kontrolu na přítomnost virů. Online testovací nástroj Pentest-Tools umožňuje zdarma použít některé penetrační testy jako například SSL Heartbleed Scan, jak je zobrazeno na obrázku č. 16. Navržené zabezpečení odolalo použitým balíčkům penetračních testů i pokusu o odposlechnutí komunikace či použitých klíčů, jak je vidět na obrázku č. 16 a v tabulce č. 2. Následně jsem provedl test pomocí BullGuard IoT Scanner, abych zjistil, zda není zařízení vedeno na seznamu zranitelných zařízení, jak je vidět na obrázku č. 17. [30, 31, 32]

Tabulka 2 Seznam použitých testů nástrojů Nessus a Pentest-Tools [30, 31]

Název testu	Popis testu	Výsledek testu
Network Scan	Test skenuje základní charakteristiky a nastavení sítě.	0 kritických zranitelností
Advanced Scan	Test skenuje otevřené porty a jejich zranitelnosti.	0 kritických zranitelností
Badlock Detection	Testování CVE-2016-2118 a CVE-2016-0128.	0 kritických zranitelností
Bash Shellshock Detection	Testování CVE-2014-6271 a CVE-2014-7169.	0 kritických zranitelností
DROWN Detection	Testování CVE-2016-0800.	0 kritických zranitelností
Shadow Brokers Scan	Test skenuje zranitelnosti popsané skupinou The Shadow Brokers.	0 kritických zranitelností

Spectre and Meltdown	Testování CVE-2017-5753, CVE-2017-5715 a CVE-2017-5754.	0 kritických zranitelností
OpenSSL Heartbleed Scan	Testování CVE-2014-0160.	0 kritických zranitelností

5.1.1 Použité testy

Penetrační testy použité pro otestování zabezpečení se zaměřují na známé zranitelnosti zabezpečení. Známé zranitelnosti jsou uvedeny v seznamu CVE (Common Vulnerabilities and Exposures). [33]

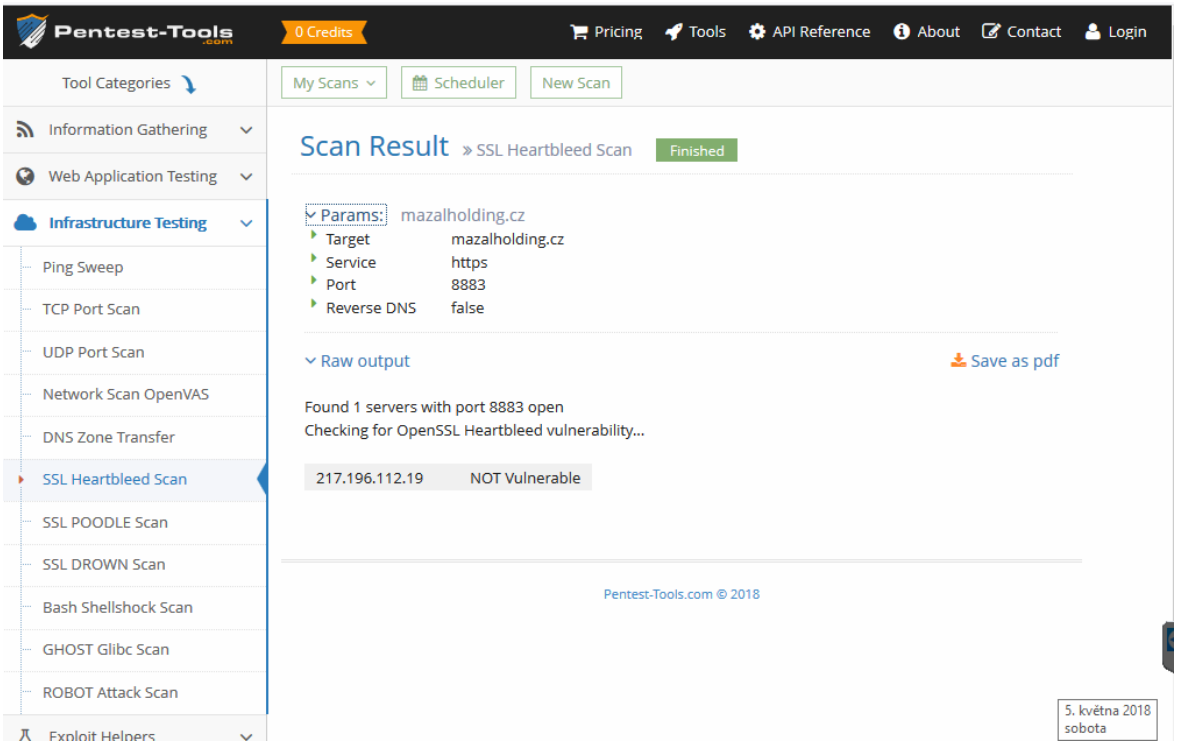
Badlock Detection test se zaměřuje na zranitelnosti popsané v CVE-2016-2118 a CVE-2016-0128. Tyto zranitelnosti umožňují podvrhnutí verze komunikačního protokolu s cílem odposlechnout komunikaci. Takový útok je jedním z typů MITM útoků. [33]

Bash Shellshock Detection testuje zranitelnosti popsané v CVE-2014-6271 a CVE-2014-7169. Zranitelnost umožňuje útočníkovi přes definice funkcí proměnných prostředí zapisovat do souborů, či jinak ovlivnit prostředí. [33]

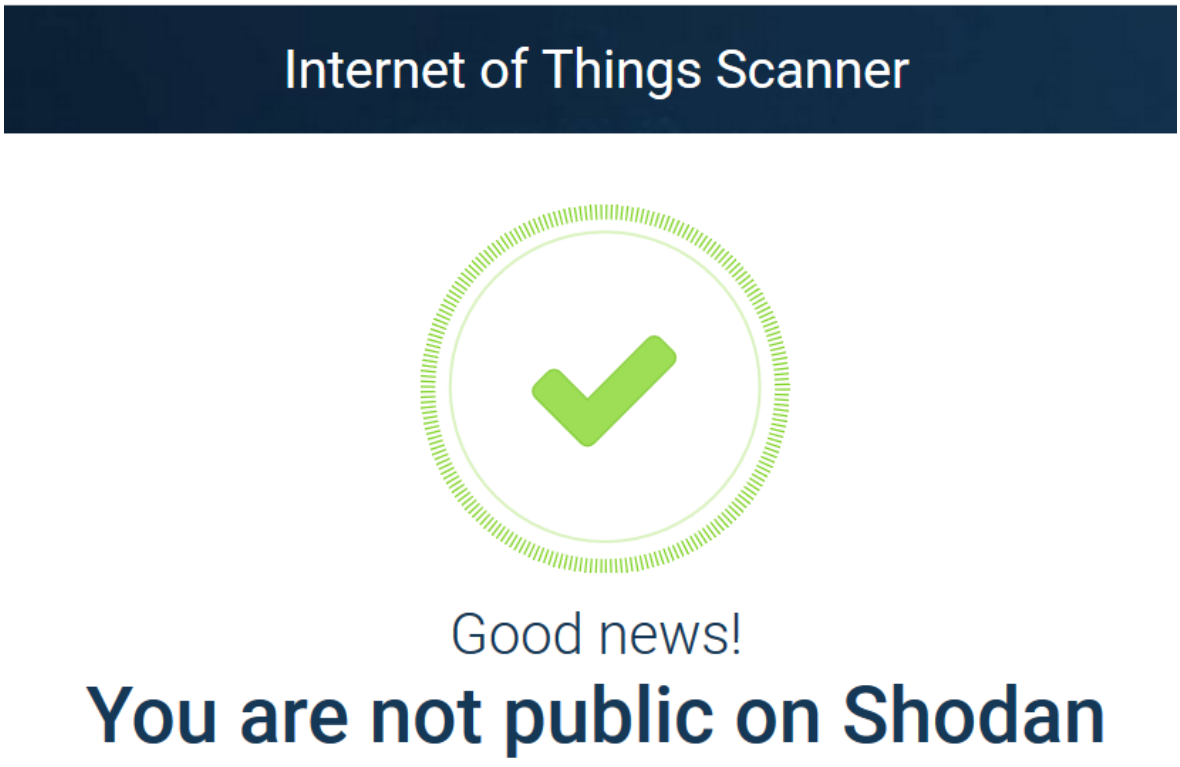
DROWN Detection zkoumá zranitelnosti popsané v CVE-2016-0800. Zranitelnost umožňuje útočníkům snadněji dešifrovat šifrovaná data. [33]

Spectre and Meltdown test se zaměřuje na zranitelnosti popsané v CVE-2017-5753, CVE-2017-5715 a CVE-2017-5754. Systémy s mikroprocesory využívajícími spekulativní provádění a predikce větví mohou umožnit neoprávněnému odhalení informací útočníkovi s místním uživatelským přístupem prostřednictvím analýzy postranních kanálů. [33]

OpenSSL Heartbleed Scan testuje zranitelnosti popsané v CVE-2014-0160. Zranitelnost umožňuje útočníkovi získat citlivé informace z procesní paměti prostřednictvím vytvořených paketů, které spouštějí přečtení vyrovnávací paměti. Takto lze získat například soukromé klíče. [33]



Obr. 16 Výsledek penetračního testu



Obr. 17 Výsledek BullGuard IoT Scanner testu

5.2 Možnosti využití sestaveného zařízení

Sestavené zařízení využívá bezpečnostní technologie zajišťující integritu a autentičnost zpráv ověřenou na základě kvalifikovaného systémového certifikátu. Komunikaci zajišťuje MQTT protokol, který je oproti HTTPS protokolu mnohem vhodnější, což jsme probrali v kapitole 3.1.1. Zprávy zpracovává Graylog 2 systém, který data ukládá do databáze pro další zpracování. Použité bezpečnostní, komunikační a webové technologie jsou využitelné pro průmysl i komerční sféru Internetu věcí. Avšak většina uzavřených systémů nepodporuje jakoukoliv modifikaci, a z toho důvodu není možné implementovat navržené řešení dodatečně.

5.3 Úroveň zabezpečení

Zabezpečení sestaveného zařízení je potřeba rozdělit do více úrovní, jelikož existuje několik úrovní potenciálního rizika zabezpečení Internetu věcí, stejně jako existuje několik typů zařízení. Zabezpečení zajišťuje ochranu dat těch nejzákladnějších úrovní (systému) až po ta nejsložitější (transakce). Využití více vrstev zabezpečení snižuje míru rizika proniknutí k chráněným datům. [34]

5.3.1 Zabezpečení serverů a embeded zařízení na úrovni systému

Základem zabezpečení serverů i použitého embeded zařízení je systémový firewall, který zajišťuje zabezpečení serverů MQTT i Graylog 2, stejně jako Raspberry Pi. Konfiguraci portu a povolení komunikace v systémovém firewallu jsme provedli v kapitole 4.1.1. Rozdělení typů koncových zařízení je uvedeno v kapitole 1.2.1.

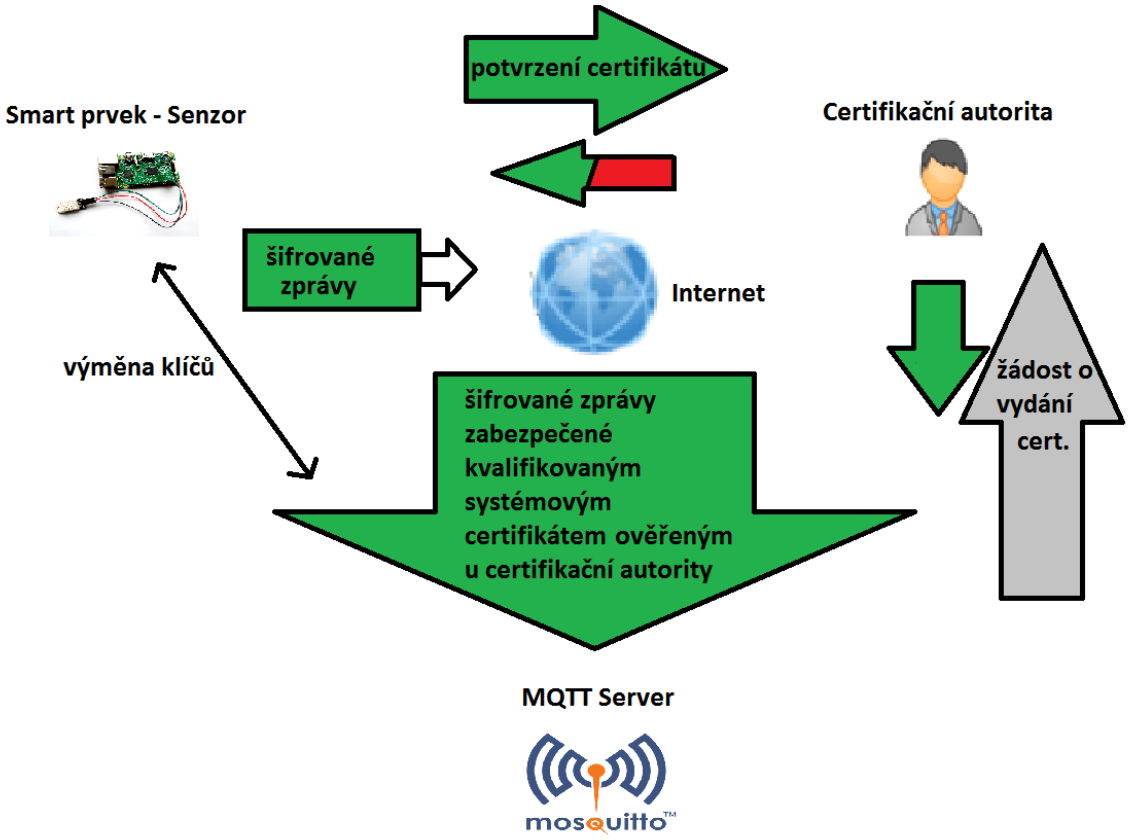
5.3.2 Zabezpečení na úrovni sítě

Zabezpečení na úrovni sítě je především zajištěno poskytovatelem služeb sítě Internet. Poskytovatel zajišťuje ochranou bariéru například ve formě různých pravidel filtrování na směrovačích nebo opatření pro služby jmen domény (DNS). [34]

5.3.3 Zabezpečení komunikace na úrovni přenosu

Veřejná síť Internet je nedůvěryhodná a nejsme schopni ovládat postup přenosu zaslaných dat. Přenášená data musíme zabezpečit proti odposlechnutí nebo modifikaci. Zabezpečení poskytuje kvalifikovaný systémový certifikát ověřený u důvěryhodné certifikační autority, který zajišťuje zabezpečenou komunikaci mezi smart prvkem Internetu věcí a serverem

MQTT, který si ověří u certifikační autority, že daný certifikát patří smart prvku a přijme zprávu, se kterou lze dále pracovat. [34]



Obr. 18 Schéma navrhnutého zabezpečení komunikace

ZÁVĚR

Zabezpečení komunikace mezi uživateli, zařízeními či servery využívajících systémových certifikátů generovaných nezávislými certifikačními autoritami, je stejně spolehlivé, jako je spolehlivé zabezpečení všech prvků a protokolů použitých pro komunikaci. Kovový řetěz je také tak silný, jako je silné jeho nejslabší kolečko. Jelikož je mnoho způsobů a úrovní jak útočník může napadnout svůj cíl a získat přístup k požadovaným datům, je potřeba se chránit všemi dostupnými způsoby, které nám bezpečnostní technologie nabízejí. V současné době existuje mnoho různých smart zařízení připojených k Internetu, které však nejsou dostatečně zabezpečené. Již mnoho úspěšných útoků nám toto tvrzení dokladuje.

Seznámení s problematikou zabezpečení smart prvků Internetu věcí včetně speciálních sítí jsem provedl v první kapitole. Pro vypracování této práce jsem vybral síť Internet a seznámil jsem se s aktuálně používanými řešeními zabezpečení s ohledem na jejich výhody a nevýhody, které jsem rozebral v druhé kapitole. Ve třetí kapitole jsem navrhl strukturu zabezpečení komunikace IoT zařízení založené na kvalifikovaných systémových certifikátech ověřených u důvěryhodné certifikační autority.

Na základě porovnání komunikačních protokolů HTTPS a MQTT jsem zvolil vhodnější MQTT protokol pro IoT, který je méně náročný na spotřebu baterií než HTTPS. Osobně jsem se nesetkal se zařízením využívající kvalifikovaný systémový certifikát a MQTT protokol pro bezpečnou komunikaci pomocí veřejné sítě Internet. Navrženou strukturu jsem zrealizoval a popsal ve čtvrté kapitole. Použil jsem embeded systém s vlastním operačním systémem, komunikující protokolem MQTT, zabezpečený kvalifikovaným systémovým certifikátem. Veškerou komunikaci přijatou MQTT serverem jsem dále zpracoval systémem Graylog 2. Tento systém ukládá zprávy do databáze pro jejich další statistické zpracování a vizualizaci.

Následně jsem navržený funkční vzorek podrobil penetračním testům. Využil jsem projektu Nessus společnosti Tenable, online testovacích nástrojů Pentest-Tools a BullGuard IoT Scanner. Všemi provedenými testy navržený vzorek prošel bez jediné kritické zranitelnosti. Mnou navržené praktické řešení kombinuje známé technologie a využívá jejich výhod pro dosažení minimální náročnosti na baterie koncových zařízení s důrazem na zajištění integrity, autentičnosti a nepopiratelnosti komunikace, a je tedy vhodnější než řešení komunikující protokolem HTTPS.

SEZNAM POUŽITÉ LITERATURY

[1] GREENGARD, Samuel. *The internet of things.* Cambridge, Massachusetts: MIT Press, 2015, 184 s. ISBN 978-026-2527-736.

[2] IoT - význam zkratky. *IT SLOVNÍK.CZ* [online]. Praha: IT SLOVNÍK.CZ, 2015, [cit. 2017-12-08]. Dostupné z: https://it-slovnik.cz/pojem/iot

[3] VOJÁČEK, Antonín. Základní úvod do oblasti internetu věcí (IoT). *Automatizace.HW.cz* [online]. Praha: Automatizace.HW.cz, 2016, 16.9.2016 [cit. 2017-12-11]. Dostupné z: https://automatizace.hw.cz/zakladni-uvod-do-oblasti-internetu-veci-iot.html

[4] How Many Internet Connections are in the World? Right. Now. *Cisco Blogs: Executive Platform* [online]. USA, 2013 [cit. 2017-12-11]. Dostupné z: https://blogs.cisco.com/news/cisco-connections-counter

[5] IoT. In: *Campus Tecnológico Madrid* [online]. Madrid: Campus Tecnológico Madrid, 2017 [cit. 2017-12-11]. Dostupné z: http://campustecnologicomadrid.com/wp-content/uploads/2017/09/iot.png

[6] Technologie Sigfox. *SimpleCell Networks* [online]. Praha: SimpleCell Networks, 2016 [cit. 2017-12-11]. Dostupné z: https://simplecell.eu/technologie-sigfox/

[7] Technické aspekty technologie LoRa. *#PRIPOJME* [online]. Praha: ČESKÉ RADIOKOMUNIKACE, 2017 [cit. 2017-12-11]. Dostupné z: https://pripoj.me/technicke-aspekty-technologie-lora/

[8] SEDLÁK, Jiří. Jak posílit bezpečnost Internetu věcí. *O2 IT Services* [online]. Praha: O2 IT Services, 2016 [cit. 2017-12-11]. Dostupné z: http://www.o2its.cz/wp-content/uploads/2015/05/DSM_Jak-pos%C3%ADlit-bezpe%C4%8Dnost-internetu-v%C4%9Bc%C3%AD.pdf

[9] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.

[10] Bezpečnostní problémy přicházejí s nástupem tzv. Internetu věcí (IoT)?. *TZB-info* [online]. Praha: redakce podle Lupa.cz a Consumerist, 2016, [cit. 2017-12-12]. Dostupné z: https://elektro.tzb-info.cz/120002-bezpecnostni-problemy-prichazeji-s-nastupem-tzv-internetu-veci-iot

[11] BUNTZ, Brian. 8 IoT security trends to look out for in 2018. *IoT Institute* [online]. USA: IoT Institute, 2017, [cit. 2017-12-13]. Dostupné z: http://www.ioti.com/security/8-iot-security-trends-look-out-2018

[12] MITM (Man In The Middle): Co je MITM (Man In The Middle). *ManagementMania.com* [online]. Praha: ManagementMania.com, 2016, [cit. 2017-12-14]. Dostupné z: https://managementmania.com/cs/mitm-man-in-the-middle

[13] Počítačový útok. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 23. 9. 2017 [cit. 2018-05-15]. Dostupné z: https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_%C3%BAtok

[14] DOSTÁLEK, Libor, Marta VOHNOUTOVÁ a Miroslav KNOTEK. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. 2., akt. vyd. Brno: COMPUTER PRESS, 2009, 542s. ISBN 978-80-251-2619-6.

[15] Kybernetických útoků přibývá. Pouze technické zabezpečení nestačí. *OPojištění.cz* [online]. Praha: VIZUS.CZ, 2018 [cit. 2017-12-17]. Dostupné z: http://www.opojisteni.cz/res/archive/084/009096_05_109849.jpg?seek=14948645

[16] AZAMUDDIN. Survey on IoT Security. In: *Washington University in St. Louis - Computer Science & Engineering at WashU* [online]. Washington: Washington University in St. Louis, 2012 [cit. 2017-12-20]. Dostupné z: https://www.cse.wustl.edu/~jain/cse570-15/ftp/iot_sec2.pdf

[17] JAŠEK, Roman. *Informační a datová bezpečnost*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. ISBN 80-731-8456-7.

[18] DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP: Bezpečnost*. Praha: COMPUTER PRESS, 2001, 566 s. ISBN 80-722-6513-X.

[19] Kvalifikovaný certifikát pro elektronický podpis. *První certifikační autorita, a.s.*[online]. Praha: První certifikační autorita, 2006 [cit. 2017-12-28]. Dostupné z: http://www.ica.cz/kvalifikovany-certifikat-pro-ePodpis

[20] Přehled kvalifikovaných poskytovatelů certifikačních služeb a jejich kvalifikovaných služeb. *Ministerstvo vnitra České republiky* [online]. Praha: Odbor eGovernmentu, 2018 [cit. 2018-04-08]. Dostupné z: http://www.mvcr.cz/clanek/prehled-kvalifikovanych-poskytovatelu-certifikacnich-sluzeb-a-jejich-kvalifikovanych-sluzeb.aspx

[21] Technologický (komerční serverový) certifikát. *První certifikační autorita a.s.* [online]. Praha: První certifikační autorita, 2015 [cit. 2017-12-13]. Dostupné z: http://www.ica.cz/Technologicke-certifikaty

[22] Systémový certifikát. *První certifikační autorita a.s.* [online]. Praha: První certifikační autorita, 2015 [cit. 2017-12-13]. Dostupné z: http://www.ica.cz/systemovy-certifikat

[23] HLADKÁ, Eva a Jan FOUSEK. Šifrování emailu. *Základy IT gramotnosti* [online]. Brno: Servisní středisko pro podporu e-learningu na MU, 2016 [cit. 2017-12-13]. Dostupné z: https://is.muni.cz/do/1492/el/sitmu/law/html/sifrovani-emailu.html

[24] DUTTA, Aditya a Cristiane KARASIEWICZ. The Mobile Frontier: Why HTTP is not enough for the Internet of Things. *IBM Community* [online]. India: IBM Community, 2013 [cit. 2017-12-15]. Dostupné z: https://www.ibm.com/developerworks/community/blogs/mobileblog/entry/why_http_is_not_enough_for_the_internet_of_things?lang=en

[25] Graylog for Compliance & Audit. *Graylog* [online]. Houston: Graylog, 2009 [cit. 2017-12-15]. Dostupné z: https://www.graylog.org/

[26] BEATON, Wayne. Eclipse Mosquitto. *Eclipse* [online]. Ottawa. Kanada: Eclipse Foundation, 2018 [cit. 2018-02-15]. Dostupné z: https://projects.eclipse.org/projects/technology.mosquitto

[27] MQTT Mosquitto broker: Client Authentication and Client Certificates. *Primal Cortex's Weblog* [online]. Lisbon, Portugal: PrimalCortex, 2017 [cit. 2018-02-15]. Dostupné z: https://primalcortex.wordpress.com/2016/11/08/mqtt-mosquitto-broker-client-authentication-and-client-certificates/

[28] SHOVIC, John C. *Raspberry Pi IoT projects: prototyping experiments for makers*. New York: Apress, 2016. Technology in action series. ISBN 978-148-4213-780.

[29] SCHALANDA, Jochen. MQTT Plugin for Graylog. *GitHub* [online]. Germany: GitHub, 2016 [cit. 2018-02-15]. Dostupné z: https://github.com/graylog-labs/graylog-plugin-mqtt

[30] Nessus Professional™ Vulnerability Scanner. *Tenable™* [online]. Maryland: Tenable™, 2018 [cit. 2018-04-16]. Dostupné z: https://www.tenable.com/products/nessus/nessus-professional

[31] OpenSSL Heartbleed vulnerability scanner. *Pentest-Tools.com* [online]. San: Pentest-Tools.com, 2018 [cit. 2018-04-16]. Dostupné z: https://pentest-tools.com/network-vulnerability-scanning/openssl-heartbleed-scanner

[32] Internet of Things (IoT) Scanner. *BullGuard* [online]. London: BullGuard, 2017 [cit. 2018-04-16]. Dostupné z: https://iotscanner.bullguard.com/

[33] Search CVE List. *CVE - Common Vulnerabilities and Exposures* [online]. McLean, Virginia: The MITRE Corporation, 2018 [cit. 2018-04-16]. Dostupné z: https://cve.mitre.org/cve/search_cve_list.html

[34] Metoda zabezpečení ochrany dat pomocí vrstvené obrany. *IBM Knowledge Center* [online]. Praha: IBM Knowledge Center, 2017 [cit. 2018-04-16]. Dostupné z: https://www.ibm.com/support/knowledge-center/cs/ssw_ibm_i_71/rzaj4/rzaj40a0internetsecurity.htm

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

3G	Třetí generace mobilních telekomunikačních technologií.
AES	Advanced encryption standard. Standard pokročilého šifrování.
b/s	Bitů za sekundu.
CCTV	Closed circuit television. Uzavřený televizní okruh.
CRL	Certificate revocation list. Seznam zneplatněných certifikátů.
CVE	Common vulnerabilities and exposures. Obecné zranitelnosti a ohrožení.
DDoS	Distributed denial of service. Distribuované odepření služby.
DH	Diffie-Helman algoritmus.
DNS	Domain name systém. Systém doménových jmen.
GEO	Geostationary Earth orbit. Geostacionární dráha.
GPS	Global positioning system. Globální polohový systém.
GSM	Groupe spécial mobile. Globální systém pro mobilní komunikaci.
HTTPS	Hypertext transfer protocol secure. Bezpečná verze hypertextového přenosového protokolu.
I.CA	První certifikační autorita.
IBM	International business machines. Mezinárodní technologická společnost.
IoT	Internet of things. Internet věcí.
LoRaWAN	Long range wide area network. Širokopásmová rozsáhlá síť.
MHz	Mega hertz. Jednotka frekvence.
MITM	Man in the middle. Muž uprostřed.
MQTT	Message queue telemetry transport. Přenosový protokol telemetrie fronty zpráv.
mW	Miliwatt. Jednotka výkonu.
OASIS	Organization for the advancement of structured information standards. Organizace pro rozvoj strukturovaných informačních standardů.

OS	Operating systém. Operační systém.
PČR	Policie České Republiky.
RSA	Rivest-Shamir-Adelman algorithm. Rivest-Shamir-Adelman algoritmus.
SHA-256	Secure hash algorithm. Rozšířená hash funkce.
SMART TV	Smart television. Chytrá televize.
SSH	Secure shell. Zabezpečený kryptografický síťový protokol.
SSL	Secure sockets layer. Zabezpečený kryptografický síťový protokol.
WiFi	Wireless fidelity. Bezdrátové připojení k síti.
X.509	Standard pro systémy založené na veřejném klíči.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK