Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Bezpečnost IoT

Bc. Adam Caha

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Adam Caha

Systémové inženýrství a informatika
Informatika

Název práce

Bezpečnost Internetu věcí

Název anglicky

Internet of things security

Cíle práce

Hlavním cílem diplomové práce je objasnit stav kybernetické bezpečnosti internetu věcí (IoT) na obecné rovině a zjistit stav a úroveň kybernetického zabezpečení zařízení, která jsou aktuálně prodávána na trhu s IoT produkty.
Dílčím cílem práce bude ověření míry inzerované bezpečnosti v reálném světě. Součástí práce bude také pokus o prolomení zabezpečení některých z volně dostupných produktů a případný návrh zvýšení zabezpečení tak, aby bezpečnost odpovídala aktuálním potřebám a zákonu o kybernetické bezpečnosti.

Metodika

První část diplomové práce bude založena na analýze pojmu „Internet věcí" a jeho bezpečnosti z hlediska pohledu laické veřejnosti v České republice.

Další částí bude rozbor zákona o kybernetické bezpečnosti v návaznosti na zabezpečení IoT, dále také analýza aktuální nabídky prodávaných IoT zařízení a úrovně jejich inzerované bezpečnosti. Tato část práce se bude zabývat teoretickou stránkou problematiky.

Praktická část práce bude zaměřena na otestování a pokusy o prolomení některých z volně prodejných IoT zařízení. Součástí testování bude i případný návrh, jak zabezpečení upravit, aby odpovídalo dnešním požadavkům na bezpečnost síťových prvků.

Doporučený rozsah práce

60-80 stran

Klíčová slova

IoT, internet věcí, kybernetická bezpečnost, sítě

Doporučené zdroje informací

SMITH, Ian G., ed. The Internet of Things 2012: new horizons. Halifax: IERC, 2012. 360 s. ISBN 9780955370793.

Technology classification, industry, and education for Future Internet of Things. International journal of communication systems. 2012, roč. 25, č. 9, s. 1230. ISSN 10745351.

The Internet Of Things. InformationWeek. 2016. ISSN 87506874.

WEBER, Rolf H a Romana WEBER. Internet of things: legal perspectives. Heidelberg: Springer, 2010, xxiv, 129 s. ISBN 9783642117091.

Předběžný termín obhajoby

2019/20 LS – PEF

Vedoucí práce

Ing. Petr Benda, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 30. 10. 2017

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 1. 11. 2017

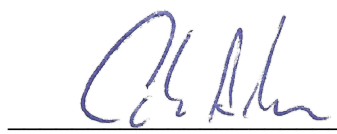
Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 28. 03. 2020

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Bezpečnost IoT" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 5. 4. 2020 

Poděkování

Rád bych touto cestou poděkoval Ing. Petru Bendovi, Ph.D. za vedení práce a především nezměrnou trpělivost. Poděkování patří i celé ČZU a také kolegům, kteří mi pomohli s vypracováním této závěrečné práce. V neposlední řadě poté patří velké díky mé rodině, která mě podporovala i v nelehkých chvílích a vždy mi dodávala další energii.

Bezpečnost IoT

Abstrakt

S ohledem na zvyšující se počet nabízených IoT zařízení si tato práce dává za cíl provést rešeršní analýzu pojmu IoT a následně otestovat bezpečnost prodávaných zařízení.

Podstatou diplomové práce je analýza vybraných IoT produktů dostupných na českém trhu, především s ohledem na jejich bezpečnost. Cílem je prozkoumat kvalitativní řešení zabezpečení prodávaných produktů, které mají zjednodušit chod či zvýšit bezpečnost našich domácností.

V úvodní části jsou vymezeny pojmy informační bezpečnost a Internet věcí a následuje souhrn teoretických východisek pro pochopení hlubší problematiky IoT. Dále se teoretická část věnuje návaznosti Zákona o kybernetické bezpečnosti na IoT ekosystém.

Součástí praktické části je dotazníkové šetření se zaměřením na informační bezpečnost, dále pak analýza vybraných zařízení na českém trhu. Hlavní částí výzkumu je praktické otestování bezpečnosti a zranitelností vybraných IoT produktů.

V poslední části práce jsou komparovány teoretická východiska s praktickými poznatky, vyhodnocené výsledky jsou interpretovány a zobecněny. Zásadním poznatkem je nepříliš dobrá kvalita hesel uživatelů a extrémní rozvoj IoT platformy v posledních letech. S rozšiřujícím se počtem IoT zařízení vzniká i větší míra a úroveň nebezpečí pro koncové uživatele.

Klíčová slova: IoT, Internet věcí, bezpečnost, Zákon o kybernetické bezpečnosti, kybernetika, šifrování

IoT Security

Abstract

In view of the increasing number of IoT devices offered, this these aims to research the concept of IoT and subsequently test the safety of the devices sold.

The essence of this thesis is the analysis of selected IoT products available on the Czech market, especially regarding their safety. The goal is to explore qualitative security solutions for products sold to simplify the operation or increase the security of our homes.

The introductory part defines the concepts of information security and Internet of Things and follows a summary of theoretical bases for understanding the deeper knowledge of IoT. Furthermore, the theoretical part deals with the link of the Cyber Security Law to the IoT ecosystem.

The practical part includes a questionnaire survey focusing on information security, as well as an analysis of selected devices on the Czech market. The main part of the research is practical testing of safety and vulnerability of selected IoT products.

The last part of the thesis compares the theoretical background with practical knowledge, the evaluated results are interpreted and generalized. The key knowledge is the poor quality of user passwords and the extreme development of the IoT platform in recent years. With the increasing number of IoT devices, a greater degree and level of danger for end users arises.

Keywords: IoT, Internet of Things, security, cyber law, cyber-tech, encrypting

Obsah

Seznam obrázků

Seznam použitých zkratek

IoT	Internet of Things (Internet věcí)
ISO	International Organization for Standardization (mezinárodní organizace pro normalizaci)
EDGE	Enhanced Data rates for GSM Evolution
GSM	Global System for Mobile Communications, také Groupe Spécial Mobile
IPv6	Internetový protokol verze 6
IPv4	Internetový protokol verze 4
IP	Internetový protokol
4G	Mobilní sítě 4. generace
5G	Mobilní sítě 5. generace
ČR	Česká republika
GPU	Graphics Processing Unit
SSL	Secured Sockets Layer
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
MD5	Message-Digest algorithm 5
MITM	Man-in-the-middle
ARPU	Average Revenue Per Customer – průměrná tržba na zákazníka
ROI	Return of investment – návratnost investice
IDC	International Data Corporation
GSM	Groupe Spécial Mobile
MHz	Mega-hertz – jednotka frekvence
A/D	Analogově digitální převodník
4K	Rozlišení 4K odpovídá přibližně 4096 (šířka) x 2304 (výška) bodů pixelů
LCD	Liquid Crystal Displej, displej založený na technlogii tekutých krystalů
MIT	Massachusetts Institute of Technology
M2M	Machine-to-machine
B	Byte (bajt), datová jednotka odpovídající 8 bitům
ISO/OSI	Referenční model ISO/OSI
OSI	Open Systems Interconnection
ISO	International Organization for Standardization
WiFi	Wireless fidelity – bezdrátová věrnost
6LoWPAN	IPv6 over Low-Power Wireless PAN
AES	Advanced Encryption Standard

PAN	Personal Area Network
IPsec	IP security
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
MQTT	Message Queuing Telemetry Transport
IEEE	Institute of Electrical and Electronics Engineers
SMB	Server Message Block
NFS	Network File Systém
DIY	Do It Yourself (udělej si sám)
SSL	Secure Sockets Layer
TLS	Transport Layer Security
IFTTT	If This Then That
AWS	Amazon Web Servicies
DPH	Daň z přidané hodnoty
WEP	Wired Equivalent Privacy
WPA	Wireless Protected Access
WPA2	Wireless Protected Access 2
SSID	Service Set Identifier
EAPOL	Extensible Authentication Protocol over LAN
AP	Access Point (přístupový bod směrovače)
MAC	Media Access Control (fyzická adresa)
ARP	Address Resolution Protocol
PIR	Passive infrared sensor (pasivní infračervené čidlo)
NIST	National Institute of Standards and Technology
IDS	Intrusion Detection System (systém pro detekci průniku)

1 Úvod

IoT, Internet of Things nebo také Internet věcí, je bezesporu následníkem dnešních technologií a automatizace. Několik let nazpět začalo IoT nabírat na objemu, dynamika tohoto oboru směle konkuruje dynamice celého odvětví a dříve nepředstavitelné vybavení našich domácností se stává běžnou realitou dostupnou každému. Otevření vstupních dveří telefonem či hodinkami je již nyní standardem, který stále více proniká do našich životů. Možnost zapnout alarm i ze vzdálenosti stovek kilometrů, zkontrolovat teplotu i na místech, kde není pokrytí rychlým internetem dnes není nedozírným ideálem, nýbrž standardem. Sítě čtvrté generace umožňují okamžitou kontrolu našeho majetku v reálném čase, zatímco společnosti jako je Sigfox nabízejí alternativní přístup k nízkoenergetickým sledovacím zařízením, díky kterým můžeme sledovat polohu našeho vozidla pomocí několika knoflíkových baterií dlouhé měsíce.

Automatizace domovních systémů je také součástí většiny nově vznikajících developerských projektů. Vývoj oboru je stále rychlejší, a ačkoliv jsme před několika lety používali mobilní telefony, díky kterým jsme byli schopni vstupní dveře otevřít, nyní se dveřní zámek odemkne automaticky při našem příjezdu domů. Sluneční rolety se zatáhnou, kdykoli slunce svítí příliš nebo teplota v interiéru přesáhne stanovenou teplotu.

Z pohledu technologické evoluce však nejde o žádný revoluční krok, jako tomu bylo při vytvoření skleněné baňky s odčerpaným vzduchem a napnutým zuhelnatělým bambusovým vláknem, jde spíš o postupnou miniaturizaci elektroniky a její zlevňování. Z technologického pohledu je velmi důležitým milníkem spuštění IPv6, nicméně větší část internetu stále používá IPv4 a IoT zařízení jsou v privátních rozsazích. V příštích letech se však dá očekávat masivní nástup dalších IoT zařízení a je pravděpodobné, že IPv6 bude důležitým stavebním kamenem této pomyslné revoluce.

Dalším důležitým prvkem je rozvoj cloudových služeb a snížení jejich cen, takže je možné je v některých případech začít využívat i bezplatně (Google, Amazon, Apple). Bez rozvoje cloudových služeb bude takřka nemožné sbíraná data zanalyzovat a společnosti, které nezaspí a budou schopny integrovat zanalyzovaná data do svých systémů, budou mít pravděpodobně rozdílový obchodní náskok.

Všechny doposud zmíněné informace ukazují, že IoT je na vzestupu a může přivést nejen do našich domácností před několika lety nepředstavitelné možnosti. Ať se již bude

jednat o chytrou domácnost nebo propracovaný systém řízení dopravy či kontejnery, které upozorní svozovou službu při svém naplnění, IoT nám změní život.

Avšak právě extrémně rychlý rozvoj zařízení připojených k Internetu, by měl znamenat i větší důraz na jejich zabezpečení. Zvlášť, když se nyní Internet věcí stává součástí každodenního života a už zdaleka se nejedná jen o rozsvícení žárovky, ale také o zasílání naší aktuální polohy nebo odemykání našeho domu či auta.

Výše uvedené důvody jsou hlavní motivací pro vznik této diplomové práce. Cílem práce je analyzovat pojem IoT, zjistit, jakým způsobem se vyvíjel a kam nyní IoT směřuje. Následně zanalyzovat trh s IoT produkty pro domácí použití se zaměřením na jejich bezpečnost.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavní cílem diplomové práce je objasnit stav kybernetické bezpečnosti Internetu věcí na obecné rovině a zjistit stav kybernetického zabezpečení zařízení aktuálně prodávaných na trhu s IoT.

Dílčím cílem bude ověření míry inzerované bezpečnosti v reálném světě. Součástí práce je pokus o prolomení zabezpečení některých z volně prodejných produktů a případný návrh způsobu zabezpečení tak, aby bezpečnost odpovídala aktuálním potřebám a zákonu o kybernetické bezpečnosti.

2.2 Metodika

První část práce bude založena na analýze pojmu „Internet věcí“ a jeho bezpečnosti a toho, jako ho chápe laická veřejnost v ČR.

Další částí bude rozbor zákona o kybernetické bezpečnosti v návaznosti na zabezpečení IoT, studium aktuální nabídky prodávaných IoT zařízení a jejich inzerované bezpečnosti. Tato část práce se bude zabývat teoretickou stránkou problematiky.

Praktická část práce bude zaměřena na otestování a pokusu prolomení některých z volně prodejných IoT zařízení. Součástí testování bude i případný návrh, jak zabezpečení upravit, aby odpovídalo dnešním požadavkům na bezpečnost síťových prvků.

3 Teoretická východiska

3.1 Vymezení pojmů

3.1.1 Bezpečnost

Hlavní myšlenkou práce má být bezpečnost IoT. Tento pojem je velmi obsáhlý, z toho důvodu budou před samotnou analýzou rizik a možných bezpečnostních incidentů vysvětleny jednotlivé aspekty, kroky a náležitosti kybernetické bezpečnosti.

Bezpečnost musí být komplexní, přičemž platí, že obrana neboli bezpečnost zařízení, je právě tak silná a dokonalá jako její nejslabší článek. Tím je poukázáno na skutečnost, že extrémní zaměření na jeden aspekt kybernetické bezpečnosti, zatímco ostatní budou opomenuty, je pravděpodobně ta největší chyba, které se výrobci IoT zařízení mohou dopouštět. Například, pokud se budeme bavit o zařízení chytrého zámku, který má substituovat klasickou cylindrickou vložku na kovový klíč a vnější část zámku bude z umělé hmoty, může být šifrování a komunikace chytrého zámku na sebelepší úrovni, nicméně pro útočníka, v tomto případě pravděpodobně zloděje, nebude nic lehčího, než plast rozbít a vstoupit navzdory asynchronní šifře s 4096 bitů dlouhým klíčem a čtečce oční sítnice.

Důležitým aspektem je rozdělení bezpečnosti z pohledu zákona a z pohledu laické veřejnosti. Zatímco pro koncového uživatele je důležitá funkční stránka zařízení a jeho ochrana soukromí, majetku, či dat, z pohledu zákona se jedná o státem stanovené postupy, rozdělení přístupu, dostupnosti dat v čase nebo nakládání s daty. Dynamika státem udávaných ustanovení zrcadlí nejnovější potřeby dané rychle se rozvíjejícím odvětím a snaží se konkretizovat obecná nařízení norem ISO 27000.

Z právního pohledu je aktuálně pravděpodobně nejřešenějším tématem otázka ochrany osobních údajů (Škorničková, 2017). Z pohledu bezpečnosti se však nejedná pouze o nakládání s osobními údaji, jak to vykládá Zákon o ochraně osobních údajů, ale i laický pohled na bezpečnost, který znamená problémy koncových uživatelů v běžném životě a může dramaticky ovlivnit jejich bezpečí a soukromí. Pokud například použije uživatel v dobré víře „chytré“ ovládání své garážové brány, nebo si nainstaluje „smart“ zámek na své vchodové dveře a zařízení nebude správně vyrobeno a chráněno proti zneužití, může útočník lehce obranný mechanismus zařízení překonat a zneužít. Druhým aspektem bezpečnosti je

samotná fyzická odolnost zařízení. Zde pochopitelně hrozí největší nebezpečí především u zařízení chránících majetek, jako například „chytrých“ zámků, které mohou být vyrobeny z nekvalitních plastů a útočník poté nemusí překonávat složité bezpečnostní kování, pokud dokáže překonat plastový kryt zámku.

Fyzická odolnost zařízení není součástí výzkumu této práce, nicméně kvalita některých zařízení není ani zdaleka dostatečná, jak se přesvědčil penetrační tester Andrew Tierney. Tierney testoval několik volně zakoupitelných zámků a jeden z testovaných visacích zámků (Obrázek 1) na sobě měl několik volně přístupných šroubků, po jejichž odstranění se zámek rozpadl. O to zarážející fakt se jedná, když Tierney uvádí, že mu výrobce odpověděl, že zámek chrání pouze proti útočníkům nemající šroubovák. (Ilascu, 2015) (High tech fingerprint, 2015)

Obrázek 1 - Visací zámek se špatnou mechanickou ochranou

Zdroj: (High tech fingerprint, 2015)

Bezpečnost cloudu

Nacházíme se v době, kdy cloud přebírá velkou část veškerých používaných služeb na internetu.[1] Úkol zajištění bezpečnosti tak přebírá za koncového zákazníka z určité části i společnost, která cloudové služby provozuje a kvalita poskytovaných služeb danou

[1] Více informací týkající se cloudových služeb bude uvedeno v příslušné kapitole (3.2.5) níže v textu

společností bývá pro koncového zákazníka jen velmi těžko ověřitelná. Především z důvodu chybějících informací jak používané či zakoupené zařízení funguje. Pokud dojde k bezpečnostnímu incidentu a společnost spravující daný cloud nebo službu nesídlí či nemá pobočky v Evropské Unii či České republice, nemusí koncového zákazníka o incidentu informovat. Právní vymahatelnost takových pochybení je mizivá. Respektive právní vymahatelnost na bezejmenné čínské společnosti bude pravděpodobně horší, než u společností jako je Google či Microsoft nebo český Jablotron, především z důvodu hledání zodpovědné osoby či dokonce sídla společnosti samotné.

Pokud tedy dojde například k odcizení dat o uživatelích včetně ukradení uživatelských jmen a hesel, mohou pak tyto údaje být lehce zneužity na jiných místech či serverech, a koncový uživatel se o celém problému ani nemusí dozvědět.

Data již nejsou lokálně uložena v našich počítačích, ale především v cloudu. Z pohledu bezpečnostního hlediska se jedná o velkou změnu, především z toho důvodu, že ochrana údajů koncových uživatelů či celých společností není tak zcela v jejich kompetenci. Je pravdou, že ne vždy to musí znamenat zhoršení původního stavu, ale velké databáze uživatelských dat se tak samovolně stávají honeypotem pro útočníky a data spotřebitelů, například fotografie z rodinné dovolené, které by jen stěží mohla zajímat jakéhokoli útočníka, se náhle mohou dostat do rukou útočníků spolu s informacemi, které prvořadě přišli na daný server odcizit.

Pravdou zůstává, že zabezpečení většiny renomovaných cloudových služeb je na vysoké úrovni, používá nejnovější způsoby šifrování s dlouhými klíči, v některých případech end-to-end šifrování i dvoufázové autentizace (Google 2-step Verification, 2020). Data jsou tak chráněna kvalitně, lépe než na domácí wifi, chráněné slabým, nebo lehce uhodnutelným heslem.

Vliv koncového uživatele

Velkou váhu má i přístup samotných zákazníků, kteří v libosti využívání služeb zadarmo svěřují zabezpečení svých domů jakékoli společnosti vyrábějící elektrické zařízení a nehledí přitom na ochranu svého soukromí a bezpečí. Nedá se to považovat za pochybení koncových uživatelů, kteří neměli dostatek času na přizpůsobení se změnám, které odvětví

informačních technologií doprovází, avšak určitá dávka nedůvěry by napomohla bezpečnosti celého Internetu a především samotných uživatelů.

Zabezpečení hesla

Dalším zásadním prvkem bezpečnosti IoT je heslo. Navzdory novým metodám používající biometrické ověřování je heslo stále zásadním prvkem bezpečnosti internetu. Jak uvádí servery *PCTuning* (PCTuning, 2018), *Security Portal* (Security Portal, 2009) nebo *Je Čas* (Je čas, 2014) v letech 2009, 2014, 2018, je nejpoužívanějším heslem 12346. Nedá se tedy říct, že by se kvalita hesel v čase zlepšovala.

Zabezpečení hesla musí probíhat jak na straně uživatele, jeho přenosu, tak i při uložení na straně databáze společnosti, u které je účet vytvořen.

Pokud bude uživatel vytvářet heslo, jeho délka a počet různých znaků určují náročnost jeho uhádnutí. Na jednoduchém příkladu lze ukázat, jak se počet možných kombinací zvětšuje exponenciální řadou.

Při použití hesla o čtyřech znacích, přičemž znakem může být 0 nebo 1, budou jednotlivé možnosti 0000, 0001, 0011, …, 1110, 1111. Jedná se celkem o 16 kombinací a matematicky se jedná o exponenciální funkci

$$y = f(x) = a^x.$$

Z pohledu kombinatoriky se jedná o variace s opakováním. V uváděném příkladě proměnná *a* odpovídá množině znaků, které v hesle mohou být použity (0 a 1) a exponent *x* odpovídá počtu znaků v hesle. Matematicky vyjádřeno v uvedeném případě:

$$a^x = 2^4 = 16.$$

V případě použití 26 různých znaků, což je počet znaků anglické abecedy a délce hesla 6 znaků se jedná o $26^6 = 308\,915\,776$ kombinací. To sice vypadá jako velké číslo, ale s rychlostí dnešních počítačů se skutečně jedná o sekundy, než by stroj prošel všechny možné kombinace. Pokud ale uživatel využije znaků 11 a přidá například i speciální znaky dostane se tak na množinu znaků čítající znaků 96 (to jsou všechny standardní klávesy dostupné na rozložení americké klávesnici (Rainbow Crack, n. d.)). Rázem se jedná o

$96^{11} = 6\,382\,393\,305\,518\,410\,039\,296$ kombinací. A pokud bychom přidali ještě dva znaky, dostali bychom 58 820 136 703 657 666 922 151 936 kombinací. Na domácím počítači s dedikovanou GPU je možné zpracovat 10 000 000 kombinací za

sekundu (Lixie, 2019). Výpočet ukázkového hesla o 6 znacích zabere tedy v průměru 30 sekund, avšak v případě hesla nejsložitějšího by jeho prolomení trvalo velmi dlouho. Při použití hesla o 13 znacích a použití jednoho domácího počítače k jeho prolomení, by jeho uhádnutí trvalo přibližně 5 882 013 670 365 766 692 sekund.

Při přepočtení na roky se jedná o více jak 186 miliard let. Toto heslo už je tedy velmi bezpečné. Samozřejmě útočník může počet GPU znásobit, ale i tak bude takové heslo takřka nemožné uhádnout pomocí hrubé síly (z anglického brute-force), tedy zkoušením všech možností.

Z výpočtu výše se dá usoudit, že heslo o délce cca 9 znaků, které bude obsahovat i speciální znaky bude dostatečně silné. Role uživatele v procesu zpracování a nakládáním s heslem končí, nicméně nadále jeho zabezpečení není v jeho roli. Zbytek bohužel, není v jeho rukou, a to jakým způsobem a kde se heslo uloží už uživatel ovlivnit nemůže. Pokud tedy uživatel například zadá heslo do formuláře na stránce, která nebude používat SSL certifikát, a přenos nebude cestou asymetricky šifrován s využitím veřejného klíče z certifikátu, může útočník odchytit přenos od klienta na server a zprávu si (jelikož není šifrovaná) přečíst, odeslané heslo pak uvidí v prostém textu.

Od roku 2018 již tak například společnost Google a její prohlížeč Chrome upozorňuje uživatele na webové aplikace běžící na nešifrovaném HTTP protokolu slovem „nezabezpečeno“ (Root.cz, 2018). Z dnešního pohledu je výpočetní výkon a datový tok potřebný pro zabezpečení stránek téměř bezvýznamný, a tak není mnoho důvodů proč web nezabezpečit. Nicméně jen letmým pohledem na komentáře u citovaného článku se názory různí. Spousta uživatelů se domnívá, že šifrování blogů, kam uživatel nevkládá při jejich čtení žádné informace, je zbytečné. Například uživatel s přezdívkou martyd uvádí: „K bankovnímu účtu SSL patří a je nutné. Takových případů je ale velmi maličké minimum. Na 99% obsahu, který teče přes http je šifrování úplně zbytečné.“ (Root.cz, 2018)

Trend zabezpečení webu je pozitivní, v minulosti web s HTTPS byl spíše výjimkou, ty lepší jej používaly na stránkách s přihlášením. Citovaný článek uvádí, že již v době jeho psaní (začátek roku 2018) společnost Google uvádí, že 78 % navštívených webových stránek má podporu HTTPS. (Root.cz, 2018)

Podporu HTTPS dnes zjednodušuje i fakt, že dnes se dá získat webový SSL certifikát od důvěryhodné certifikační autority Let’s Encrypt zdarma. Společnost, která je spravována

ISRG, což je nezisková společnost podporovaná největšími IT společnostmi jako je Cisco, Google, Mozilla, Facebook, Red Hat (IBM), nebo například GitHub, nabízí webové certifikáty zdarma, pro desítky providerů dokonce s plně automatickou obnovou. Pokud tedy pro svůj nízkonákladový projekt budete potřebovat důvěryhodný certifikát, ani to není problém.

Podpora HTTPS by ještě měla být zajištěna proti útoku zvanému SSL Strip nebo také HTTP Downgrade. Jedná se o útok, kdy útočník stojící mezi klientem a zabezpečeným serverem zachytí veškerý obsah a přesměruje jej přes sebe a následně zamění šifrovanou verzi webu za web bez ochrany certifikátem. Pokud tak mezi klientem a útočníkem následně již není HTTPS, ale pouze HTTP, útočník může každý POST, který klient odešle pohodlně přečíst v prostém textu. Některé stránky již však HTTPS vynucují a prohlížeč na straně klienta, tak nemůže stránku v HTTP vůbec zobrazit. Pokročilejší metodou téhož útoku je využití vlastního certifikátu, který podstrčí místo původního a vzhledem k tomu, že od tohoto certifikátu má privátní klíč, uživatel sice data odešle zabezpečená, nicméně útočník s využitím privátního klíče data pohodlně přečte. Asi největší nebezpečí tkví v nevědomosti koncového uživatele, který, pokud nezaregistruje chybějící SSL zabezpečení (či neplatný certifikát), vůbec nezpozoruje, že se stal obětí útoku (Comodo, 2019).

Naštěstí většina dnešních prohlížečů a webových serverů již podporuje HSTS, což je zmíněný bezpečnostní mechanismus, který umožňuje vynucení komunikaci v HTTPS na straně prohlížeče / klienta (SecurityHeaders.cz, 2018).

Po vytvoření a bezpečném odeslání hesla následuje poslední část procesu – uložení samotného hesla v databázi.

Jelikož se tato práce dotýká metodiky ukládání hesel pouze okrajově, není cílem používat pro vysvětlení složitou matematiku, či vysvětlovat postupy algoritmů skrývající se v útrobách hashovacích funkcí. Základní myšlenkou hashovacích funkcí je zobrazení řetězce libovolné délky do řetězce znaků o vždy jasně stanovené délky. Základním i zcela zásadním předpokladem hashovací funkce je vytvoření unikátního výstupu pro unikátní vstup. Množina výstupních možností samozřejmě není nekonečná, nicméně počet možných kombinací je v závislosti na konkrétní hashovací funkci zpravidla velmi obsáhlá. Například u stále velmi používané funkce MD5 se jedná o $16^{32} = 2^{128} \approx 3{,}40 * 10^{38}$ možných výstupů. Hashovací funkce jsou zpravidla jednosměrné. Podmínkou pro kvalitní hashovací

funkci je extrémně náročný, či nemožný zpětný výpočet vstupního řetězce, pokud je znám řetězec výstupní. Porušení této podmínky je možné dosáhnout při 2^L výpočtech, kde L se rovná počtu bitů hashe (Hashovací funkce, n. d.).

U některých hashovacích funkcí, například zmíněné MD5 byly nalezeny kolize, nebo také pseudo-kolize, kdy pro stejný výstupní hash mohou být různé vstupy. Útočník pak nepotřebuje znát originální heslo, stačí mu vypočtená hodnota, mající stejnou hash. Jiným příkladem může být zneužití u zachování integrity souborů, kde i při zachování kontrolního hashe by mohl být vstupní soubor (řetězec) jiný – například soubor mohl být upraven, aniž by to bylo možné zjistit z kontrolního hashe.

Dnes je tedy doporučením využívání hashovacích algoritmů například z rodiny SHA, jejichž délka hashe se pohybuje standardně mezi 160 a 512 bity.

SHA šifrovací algoritmy se používají pro vytváření digitálních otisků dokumentů, kvůli zajištění jejich integrity, vytváření integrity digitálních souborů nebo databází, při ukládání hesel nebo například v kryptoměnách, kde celý blockchain je založen na hashovacích funkcích.

Dalším důležitým opatřením je takzvané solení ukládaného hesla. Ochrana solením přispívá především k bezpečnosti hesla z pohledu jeho ochrany před útokem využívajícího duhové tabulky. Ochrana spočívá v přidání soli, řetězce znaků, jako vstupního parametru do hashovací funkce k heslu uživatele. Zahashovaný řetězec uložený v databázi pak neodpovídá hashi hesla zadaného uživatelem, ale jeho „osolené“ formě. Sůl se může přidávat do různých částí, od přikládání na konec hesla, na jeho začátek, až po neelementární kombinace, kdy se například sůl vloží do středu řetězce hesla, zahashuje se, a teprve poté se zahashuje výsledný řetězec.

Další výhodou solení hesel je fakt, že pokud náhodou použijí dva uživatelé stejné heslo a nebude využito soli, jejich výsledné hashe po použití hashovací funkce budou stejná (Obrázek 2). Tato nevýhoda odpadá právě při využití hesla, na obrázku níže je možné vidět příklad, kdy dva uživatelé používají stejné heslo. V první případě sůl není použita a oba mají v databázi stejný výsledný hash – f4c31aa. Při použití soli je výsledný hash zcela rozdílný a pokud se podaří útočníkům odcizit prvnímu uživateli jeho heslo, je druhý uživatel v bezpečí.

Obrázek 2 - Využití soli při hashovaní

Zdroj: (Arias, 2018)

Navíc, jak již bylo řečeno, přidávání soli zásadním způsobem ztěžuje využití duhových tabulek.

Předcházející tvrzení je platné pouze v případě, že použitá sůl je v obou případech odlišná. Sůl by se určitě neměla opakovat, pakliže by došlo ke kompromitování databáze a s ní i hashů a soli, pro útočníka by poté bylo jednoduché vytvořit duhové tabulky s využitím známé soli. Aby tedy využití soli bylo správné, je zapotřebí, aby byla pro každého uživatele unikátní. Sůl by také měla být patřičně dlouhá, což opět znesnadňuje využití brute-force útoku (Arias, 2018).

Duhové tabulky

Duhové tabulky neboli rainbow tables, mající základy postaveny již v roce 1980, kdy Martin Hellman popsal kryptoanalytický mechanismus používající předpočítaná data uložena v paměti, vymyslel z upraveného algoritmu Louis-Paul Rivestem v roce 1982 až v roce 2003 Philippe Oechslin působící na univerzitě v Lausanne. Úpravou původních algoritmů dosáhl dvojnásobné rychlosti celkového výpočtu (Oechslin, 2003, s. 617-630). Navíc využitím různých redukčních funkcí bylo dosaženo ke snížení celkové velikosti generované tabulky, a právě využití různých redukčních funkcí v jednotlivých funkcích zadalo jméno duhovým tabulkám. Pro lepší znázornění využití různých redukčních funkcí v jednotlivých sloupcích byly využity různé barvy.

Jak tabulka vypadá, a jak by vypadala bez různých redukčních funkcí je uvedeno na následujících obrázcích (Obrázek 3, Obrázek 4). V první tabulce se hash SOOM objevuje v 6. a 8. řádku a z důvodu vždy stejné použité hashovací funkce se poté opakují i všechny následující hashe, tedy DOLY, KAVA, RUZE. Pokud by tabulka měla desetitisíce sloupců, a i takové tabulky se vytvářejí, docházelo by k redundantním výpočtům v celém řádku. Využitím různých redukčních funkcí se sice nezabrání možným kolizím, ale eliminuje se možnost duplicitních výstupů v celých řádcích (Soom.cz, 2015).

Obrázek 3 - Tabulka s redundantními hashi

AAAA	VODA	NERV	PUSA	MLHA	SMRK
ABCD	KOLO	SKLO	LAMA	PRSA	VLAS
AKVA	OKOV	HUSA	KRUH	HORY	ROPA
KOLO	SKLO	LAMA	PRSA	VLAS	MLOK
LODE	PAKO	ROTA	VAZA	SVET	HLAS
MOTO	SOOM	DOLY	KAVA	RUZE	KOSA
STUL	RUKA	PATA	KROV	KOST	HRON
WIFI	NOHA	SOOM	DOLY	KAVA	RUZE
...	...				
ZZZZ	SKOK	NOKY	MULA	KUZE	NUSE

Zdroj: (Soom.cz, 2015)

Obrázek 4 - Tabulka po použití různých redukčních funkcí

AAAA	VODA	NERV	PUSA	MLHA	SMRK
ABCD	KOLO	VOSA	MAMA	PAKO	LASO
AKVA	OKOV	HUSA	KRUH	HORY	ROPA
KOLO	SKLO	LAMA	PRSA	VLAS	MLOK
LODE	PAKO	ROTA	VAZA	SVET	HLAS
MOTO	SOOM	DOLY	KAVA	RUZE	KOSA
STUL	RUKA	PATA	KROV	KOST	HRON
WIFI	NOHA	SOOM	SLZA	BRKO	TRNY
...	...				
ZZZZ	SKOK	NOKY	MULA	KUZE	NUSE

Zdroj: (Soom.cz, 2015)

Důvodů, proč se neprovádí hashování přímo na straně klienta pomocí javascriptu, je několik:

- hashovací funkce nenahrazují asymetrické šifrování, takže by heslo nebylo odesláno v prostém textu. Neochránila by data před útoky Man-in-the-Middle (MITM). Při zachycení komunikace by útočník mohl upravit javascript a kód upravit tak, aby se heslo odeslalo nehashované.
- Nelze zaručit, že klient bude mít povolený javascript na své stanici, a tedy zdali bude schopen heslo skutečně hashovat. Musel by být tedy využit nějaký mechanismus na straně serveru, který by ověřil, zdali heslo mající být uložené do databáze již hashováním prošlo, či zdali je nutné to provést za klienta.
- Posledním a nejpádnějším důvodem je, že v případně kompromitování databáze s hesly (s hashi), není pak zapotřebí žádné kryptoanalýzy, protože k ověření se používá hash, který je dostupná již při odeslání od klienta. K ověření pak tedy postačuje serveru poslat kopii hesla/hashe z databáze a pokus o autentizaci je úspěšný. Hashování na straně uživatele může být provedeno, ale vždy by mělo být prováděno i na straně serveru, a to z důvodu výše uvedených podmínek. (CrackStation, 2019).

Pokud bylo vše uskutečněno správně na straně klienta i majitele serveru či služby, heslo je nyní uloženo v osolené a zahashované podobě v databázi, což výrazně zvyšuje jeho bezpečí.

Rychlost změn a tlak ceny

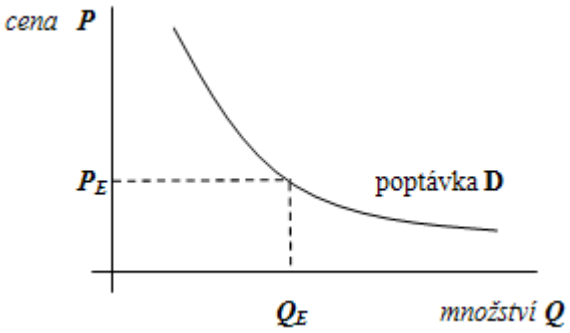
Trend vzniku nových technologií, a především jejich dostupnost, se v posledních letech zrychluje, ceny klesají, mediální kampaně cílí na „chytré“ domácnosti a největší prodejci elektroniky v České republice nabízejí produkty z této kategorie na předních stránkách svých e-shopů. Například společnost Alza v době psaní diplomové práce uvádí reklamu na Smart zařízení na jednom z šesti slidů na úvodním baneru svého e-shopu (Obrázek 5).

Obrázek 5 - Alza Smart domácnost

Zdroj: (Alza, 2020)

Jedním z prvků ovlivňující výši poptávky je i cena produktu (Obrázek 6).

Obrázek 6 - Graf poptávky



Zdroj: (Caha, 2020), vzor (Miras Lebl, n. d.)

Společnosti se snaží uspět na trhu také cenou a ceny produktu snižovat za účelem získání většího podílu na trhu, nechtějí zároveň snižovat počty dostupných funkcí, které mají nalákat zákazníky jejich služby využít. Dochází tak tedy k úbytku kvality na částech, který běžný zákazník na první pohled neuvidí. (Miras Lebl, n. d.)

Zabezpečení cloudů a databází s potenciálně citlivými údaji zákazníků pak bezejmenná společnost pravděpodobně nebere na příliš těžkou váhu. Zejména pokud sídlí v zemi, kde vymahatelnost zákonů je poněkud obtížnější.

Příkladem může být poměrně nedávný incident známé čínské společnosti Xiaomi, kdy se jednomu uživateli při používání napojení na Google Home zobrazovaly záběry z kamer jiných uživatelů. Obě společnosti postupovaly v rámci dané situace správně a řešení

incidentu trvalo pouze několik dní, avšak závažnost narušení osobního soukromí byla zcela zásadní. (Brown, 2020)

3.1.2 **Internet věcí**

Úvod a historie

Pojem internet věcí již nějakou dobu existuje, vysvětlení a přesná definice, co všechno Internet věcí (anglicky Internet of Things, dále jen IoT) obsahuje, zahrnuje a kde končí jeho hranice, lze nalézt jen stěží. Jako první promluvil o „internetu věcí" pravděpodobně Kevin Ashton, spoluzakladatel Auto-ID na MIT během své přednášky v roce 1999. (TechTarget.com, 2019). Jednou ze stále platných definic, která je již 11 let stará, nicméně stále velmi používaná je: „A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business processes. Services are available to interact with these „smart objects„ over the Internet, query their state and any information associated with them, taking into account security and privacy issues (Haller Stephan, 2009)." Odlišná, avšak stejně dobrá definice může ta, které je použita například na webu *techtarget.com*: „The internet of things, or IoT, is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. (TechTarget.com, 2019)" Volně přeloženo: Internet věcí je systém vzájemně propojených počítačových, mechanických a elektronických zařízení, objektů, zvířat a lidí, které jsou opatřeny unikátními identifikátory (UID), a schopností přenášet data přes síť, aniž by vyžadovaly jakoukoli akci mezi dvěma lidmi, či člověkem a zařízením.

IoT se vyvinulo z M2M, což je označení pro machine-to-machine komunikaci, kdy mezi sebou interagují zařízení bez vlivu člověka. IoT je dalším krokem M2M, kdy do komunikace zasahuje člověk za účelem získání informací poskytovaných připojenými zařízeními. (TechTarget.com, 2019)

Dle citovaného webu (TechTarget.com, 2019) může být onou *věcí* například člověk s implantátem srdce, zvíře, které má implantován čip pod kůží pro identifikaci nebo automobil, který má vestavěné sensory, pro upozornění řidiče ve chvíli, kdy má vůz nízký

tlak v pneumatikách. Onou *věcí* může být taktéž cokoliv, co může být připojeno do sítě a je schopno přenášet data po síti.

Jedním z prvních zařízení, které se podobalo dnešnímu pohledu na IoT byl univerzitní automat na Coca-Colu. Již okolo 1970 se na univerzitě Carnegie Mellon podařilo připojit k síti automat na Coca-Colu, který informoval pomocí sítě na aktuální zaplnění a díky zaznamenané době chlazení určit, zdali jsou láhve s nápojem dostatečně nachlazeny. Jelikož informaci o naplnění zprostředkovávaly senzory a automat byl připojen do sítě, dá se považovat Carnegieský automat na Coca-Colu za jedno z prvních IoT zařízení vůbec. (Carnegie Mellon University School of Computer Science, n. d.). Jednoduché rozhraní pro nápojový automat, který dostal uživatel při dotazu, zdali je nějaká láhev připravena k odebrání mohlo vypadat asi takto (Obrázek 7):

Obrázek 7 - Rozhraní jednoho z prvních IoT zařízení

```
EMPTY    EMPTY    1h 3m
COLD     COLD     1h 4m
```

Zdroj: (Carnegie Mellon University School of Computer Science, n. d.)

Další vývoj

Velmi aktuální a rozsáhlou studií, která byla uveřejněna společností Juniper Research v červnu roku 2019 je The Internet of Things: Consumer, Industrial & Public Services 2015-2020. Svým rozsahem zahrnujícím obchodní pohled desítek největších společností nemá příliš konkurenci. Kromě srovnání a analýzy trhu obsahuje i předpovědi dalšího vývoje týkajícího se IoT.

Tato studie uvádí, že v roce 2020 bude připojeno přes 38 miliard zařízení. V roku 2015 bylo připojeno k Internetu přes 13,4 miliard zařízení. Za posledních 5 let jde tedy o růst přes 285 %.

Studie dále uvádí, že ačkoliv titulky novin plní především zařízení sloužící přímo koncovým uživatelům, hlavním obchodním potenciálem je sektor průmyslových a veřejných služeb – jako je maloobchod, zemědělství nebo inteligentní budovy. Studie uvádí například společnosti John Deere nebo Michellin, které úspěšně změnily svůj hlavní předmět

podnikání a z dodavatelů a prodejců produktů se staly významné softwarové firmy, které se orientují na IoT podnikání.

Autor studie nadále uvádí, že jsme zatím stále v rané fázi IoT. Dle Sorrela nás nejtěžší úkol, a to najít ta správná data ke sběru a jejich následné zpracování, teprve čeká. Výzkum konstatuje, že internet věcí je proto stejně účinný jako součet jeho částí. Připojení zařízení k síti internetu vytváří data, nicméně informační a přidanou hodnotu data získávají až ve chvíli jejich shromáždění, analýzy a pochopení.

Mezi další zjištění analýzy patří, že IoT zaměřené na spotřebitele vyniká vysokým průměrem tržby na zákazníka (ARPU), zatímco průmyslový sektor může zajistit vysokou návratnost investic (Sorrell, 2020).

Výše uvedené také směřuje k dalšímu velkému tématu, a to je pojem Big Data. Jde o logické spojení, které Sorrel uvádí ve své analýze, IoT nyní generuje neuvěřitelné množství informací a v budoucnosti právě schopnost tato data zpracovat může být rozdílovou konkurenční výhodou v daném segmentu.

Server HelpNetSecurity.com uvádí s odvoláním na společnost IDC (International Data Corporation), že v roce 2025 bude 41 miliard zařízení generovat téměř 80 zettabytů, což je 1 miliarda terabytů dat. Tento web však také poukazuje na možná bezpečnostní rizika hlavně s odkazem na ochranu osobních údajů. Píše, že s každým dalším připojením zařízením se zvedají požadavky na bezpečnost, a především zodpovědnost v otázce řešení nových bezpečnostních zranitelností a ochrany soukromí. Uvádí, že společnosti musí k těmto skutečnostem přihlížet se zvyšující se informovaností koncových uživatelů. Avšak dodává, že z dlouhodobého hlediska, se snižující se cenou videokamer a dronů a příchodem sítí 5G se počet zařízení sledujících naše životy pomocí videokamer rapidně zvýší (HelpNetSecurity.com, 2019).

Principy IoT

IoT zařízení jsou často zaměřeny na minimální velikost s možností komunikovat s dalšími zařízeními pomocí datových sítí. Často se klade důraz na možnost například vydržet po dlouho dobu pouze s napájením na baterii. Takové sítě a zařízení buduje například francouzská společnost Sigfox, založena teprve v roce 2009. Tyto zařízení povětšinou fungují na sítích velmi podobným 2G, které se stále využívají například pro GSM

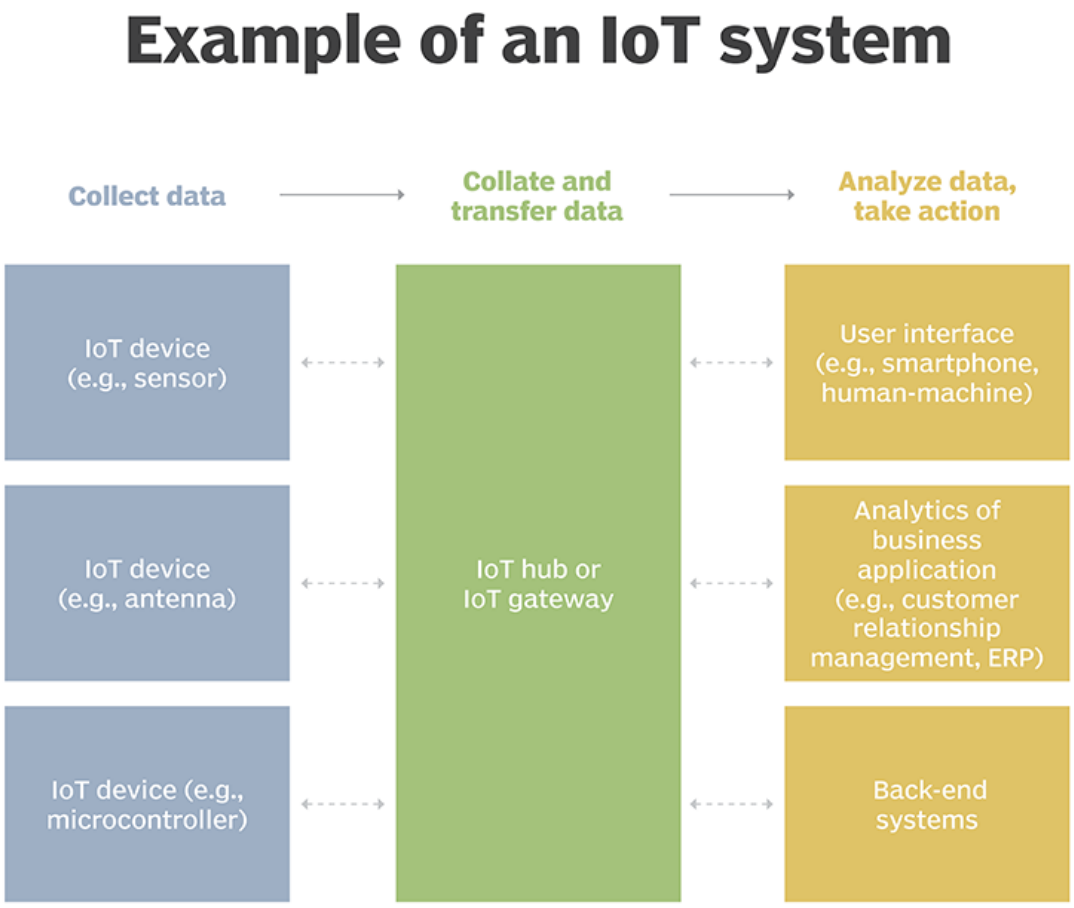
hovory. Výhodou těchto sítí je především jejich vysoká prostupnost krajinou díky poměrně nízkým hladinám frekvencí, na kterých fungují (800 – 1000 MHz v ČR) a to, že jejich pokrytí je dnes již dostupné prakticky po celém světě. Zásadní nevýhodou je pak nízká rychlost přenosu, která se, v závislosti na konkrétním typu sítě, pohybuje v desítkách až stovkách kilobitů za sekundu.

V závislosti na typu senzoru může buď senzor komunikovat s hubem, který data sbírá, analyzuje, zpracovává a dále posílá buď k lokálnímu využití nebo do cloudu, nebo senzor komunikuje s cloudem napřímo (především o těchto typech je tato práce). Pokud se jedná o zařízení, které je určeno pro sítě typu Sigfox jedná se o jednoduché, klidně analogové senzory, které následně pomocí jednoduchých A/D převodníků překládá signál na digitální, který pak pomocí datové sítě odesílá do cloudu, odkud jsou sbíraná data dostupná pomocí API rozhraní poskytovatele sítě. (SigFox.cz, 2020)

Takové typy senzorů mohou být nejrůznějších druhů – od primitivních teplotních senzorů založených na polovodičích, infračervených senzorů měřících vzdálenost (například využíváno ve smart městech pro kontrolu naplnění kontejnerových nádob na odpad) až po senzory měřící vlhkost půdy pro zavlažování. Jejich předností je provoz na baterie s několika měsíční výdrží. Zařízení sbírají data v čase a jednou za určitý interval se připojí ke cloudu a odešlou komprimovanou metodou svá data. Důraz je kladen na minimální datový objem odesílaných zpráv, tak aby energeticky náročné spojení s cloudem mohlo trvat co nejkratší dobu. Příkladem může být odesílání teploty za použití jediného čísla. Pomocí sítě Sigfox lze odesílat pouze zprávy do velikost 8 bajtů. V dnešním světě 4G a přicházejícím 5G a možností streamování videí ve 4K se jedná o těžce uvěřitelnou skutečnost, nicméně pro odeslání teploty je to hodnota dostačující. Jeden bajt odpovídá 256 bitům, v jedné zprávě tedy lze odeslat například teplotu, která odpovídá rozsahu 256 hodnotám. Při zaokrouhlení na 0,5 °C, lze pracovat v rozsahu od -64 °C po 64 °C, což pro venkovní teploměr bude naprosto dostačující. Hodnota 0 odpovídá -64 °C, hodnota 128 odpovídá 0 °C a hodnota 255 64 °C. Zaokrouhlení lze zajistit na straně mikrokontroleru postaveném například na oblíbeném Arduino Uno a zpracování hodnot, například zapsání do jednoduché webové aplikace ve stupních Celsia, pak opětovně na straně webového serveru. Při tomto přístupu byl využit 1 bajt. Vzhledem k tomu, že zpráva může být osm krát větší, lze například při zachování rozsahu zvýšit přesnost až osm krát. Výsledná teplota tedy nebude zaokrouhlena na 0,5 °C,

ale na 0,0625 stupně Celsia, což je přesnější hodnota, než nabízí většina domácích teploměrů (Čížek, 2016).

Obrázek 8 - Příklad IoT systému



Zdroj: (TechTarget.com, 2019)

Na obrázku (Obrázek 8) je zobrazeno schéma, které bylo popsáno výše a příklad systému, jak může IoT systém fungovat a být zapojen. Na levé straně v modrém sloupci jsou uvedeny zařízení, které mohou být nejrůznějších typů od jednoduchých senzorů měřící rychlost větru, až po složitější vypočítávající množství srážek a vlhkost za posledních 24 hodin postavených na mikrokontrolerech typu Arduino. Uprostřed – v zeleném může stát hub, či brána, která slouží pro komunikaci s (pravým sloupcem) cloudem, lokálním serverem, který data zobrazuje (displej našeho telefonu, nebo jednoduchý osmibitový LCD displej zobrazující naměřenou teplotu), komplexní robotické systémy fungující

v automobilovém průmyslu, až po pult centrální ochrany při detekci narušení zabezpečení chráněného objektu.

Výhody a nevýhody IoT

Internet věcí může přinášet společnostem a organizacím, které je začnou využívat mnohé výhody. Některé z nich se dají využít napříč všemi odvětvími, jiné jsou specifické pro určité druhy průmyslu. Patří mezi ně:

- sledování pracovních a výrobních procesů,
- zlepšení uživatelského prožitku (anglicky user nebo customer experience),
- úspora času a peněz,
- zvýšení produktivity zaměstnanců,
- integrace a adaptace byznys modelů,
- zjednodušení a zlepšení obchodních rozhodnutí,
- zvýšení celkových příjmů,
- možnost dosažení informací odkudkoli a kdykoli
- zlepšení a zjednodušení komunikace mezi propojenými IoT zařízeními,
- možnost automatizace procesů za účelem zvýšení kvality a úspory lidských zdrojů.

IoT nutí společnosti přemýšlet jiným způsobem o zájmech a objektech podnikání tak, aby byl maximalizován výnos z daného odvětví.

Přínosem poté nejčastěji budou pro výrobně, transportně a pomocně orientované společnosti, jimž se při využívaní senzorů a IoT zařízení usnadní práce pravděpodobně nejvíce, nicméně i například zemědělské závody mohou využít výhod, které IoT přináší. Kontrola vlhkosti, množství spadených srážek, množství soli či jiných prvků v půdě, napomůže optimalizaci výdajů, urychlí výrobní proces a maximalizuje výnosy, čímž zvýší celkové příjmy s ohledem na minimalizace nákladů.

Dalším případem může být stavebnictví, kdy se různé druhy sond mohou využívat například pro kontrolu statiky budov, či napomáhat v předcházení nešťastných událostí jako jsou požáry.

IoT se dotkne či již dotýká všech odvětví průmyslu od zdravotní péče začínaje až po obchod či výrobní procesy. (TechTarget.com, 2019)

Na druhou stranu server TechTarget (TechTarget.com, 2019) i zmiňuje různé nevýhody IoT, a to především s ohledem na možná bezpečností rizika:

- se zvyšujícím se počtem připojených zařízení a množstvím informací sdílených mezi zařízeními se zvyšuje i potenciál k úniku či krádeži informací,
- celkové množství IoT zařízení, které budou jednotlivé společnosti využívat se může zvýšit na nepředstavitelné množství, a z toho důvodu sběr dat a jejich vyhodnocení může být obtížené,
- pokud se v systému objeví chyba, pravděpodobně se může, vzhledem ke vzájemnému propojení systémů, dotknout i dalších závislých zařízení,
- vzhledem ke stálému vývoji, a tedy i chybějícímu mezinárodnímu standardu, zaštiťujícímu celé IoT odvětví, je obtížné integrovat navzájem komunikující zařízení od různých výrobců.

3.2 Technologické základy

3.2.1 IPv6

Jak bylo výše uvedeno, rozmach IPv6 protokolu byl jedním z milníků pro možnost integrovat miliony nových zařízení do sítě Internetu. Oproti protokolu IPv4, který je aktuálně používán do velké míry, nabízí především násobně větší adresní prostor. Zatímco IPv4 nabízí teoreticky 2^{32} adres, IPv6 protokol nabízí ve svém adresním prostoru 2^{128} adres. Díky této změně lze směle přemýšlet o připojení jakéhokoliv zařízení do sítě Internet na celém světě. Další změnou v IPv6 protokolu je vzhled IP datagramu, což je ovšem z pohledu IoT zanedbatelná výhoda. IP datagram byl upraven a hlavička zjednodušena. Odstraněny byly například kontrolní hlavičky, který se musely při každém průchodu směrovačem přepočítávat a komunikace zpomalovala. Díky těmto změnám se délka hlavičky prodloužila pouze na 40 B z 20 B, ačkoliv adresy mají čtyřnásobnou délku (12B oproti 4B u IPv4). (Satrapa, 2019, s. 26,112,345,346,348)

3.2.2 Komunikace a ISO/OSI

Komunikace je pro svět Internu věcí základním prvkem. Komunikační technologie, ať již drátové či bezdrátové, jsou pro funkčnost IoT systémů stěžejní, umožňují IoT

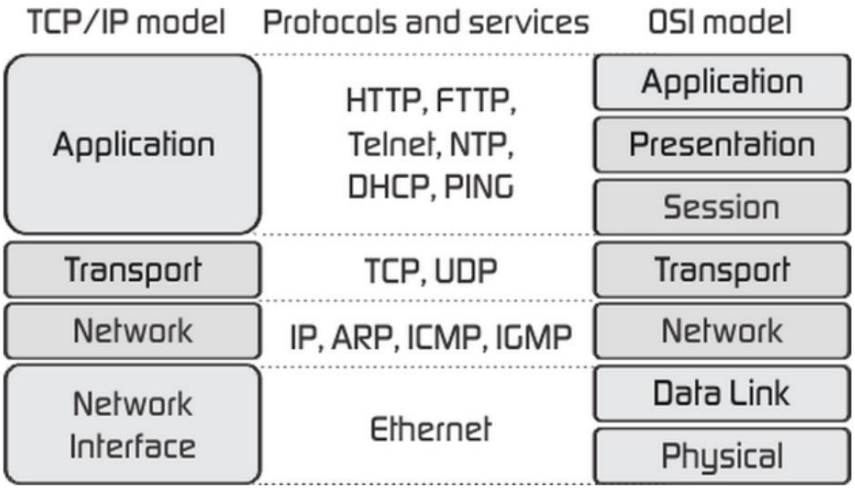
zařízením komunikovat s ostatními prvky IoT ekosystému, stejně tak interagovat s aplikacemi, službami běžícími v cloudu, ale i s uživateli. (Geber, 2018)

Kdykoliv během průchodu jednotlivými vrstvami ISO/OSI modelu – fyzickou (bezdrátových sítí jako je WiFi, 802.15.4 nebo drátovou verzí Ethernet), síťovou (např. IPv6 (Internet Protocol version 6), 6LoWPAN (IPv6 over Low-Power Wireless PAN, či IPsec)), transportní (např. UDP (User Datagram Protocol) či primární přenosový protokol (anglicky Transmission Control Protocol, dále jen TCP)) nebo aplikační vrstvou (např. MQTT (Message Queuing Telemetry Transport)) mohou být data odchycena a nebo komunikace přerušena a je tedy nutné zabezpečit všechny části naší komunikace.

OSI, česky také model otevřeného systému pro propojení, je abstraktní model ISO standardu (anglicky také International Organization for Standardization), který předkládá sedm vrstev, postavených na jednotlivých, vzájemně oddělených, nicméně spolupracujících protokolech. Pokud se na ISO/OSI podíváme od spodní vrstvy a budeme pokračovat směrem nahoru, pak je to: fyzická vrstva, vrstva spojová nebo také linková, síťová, transportní, relační, prezentační a nejvrchnějším vrstvou je stupeň aplikační.

V konkrétní realizaci ISO/ISO, v modelu TCP/IP, protokol síťové vrstvy a sada internetových protokolů nejvrchnější tři vrstvy modelu ISO/OSI, ty jsou základem pro Internet. Na obrázku (Obrázek 9) je znázorněn rozdíl mezi klasickým ISO/OSI modelem a jeho konkrétní realizace TCP/IP modelem.

Obrázek 9 - ISO/OSI a TCP/IP modely



Zdroj: (CliNetworking, 2018)

Nejspodnější, fyzická vrstva TCP/IP zajišťuje přístup k síti, fyzická, protože skutečně realizuje fyzikální přenos signálu – ať už kabelem či bezdrátovým médiem. Signál je realizován proudem bitů. Jedná se vlastně o první a druhou vrstvu OSI modelu. Metody přenosu dat mohou být různé – od využití optického kabelu, rádiových vln, až po bezdrátové sítě fungující na frekvencích od 700 do 2800 MHz jako je Wi-Fi (IEEE (Institute of Electrical and Electronics Engineers) 802.11 a, b, g, n, ac). Jedná o hardwarovou vrstvu.

Linková vrstva je také hardwarová a využívá fyzickou vrstvu pro přenos větších bloků dat – rámců (anglicky frames). Zajišťuje integritu dat při průchodu jednoho uzlu na druhý. Její součástí jsou například mosty a směrovače.

Třetí vrstvou modelu je vrstva síťová, zajišťuje adresaci a směrování. Směrováním je myšleno hledání vhodné cesty a zajištění správného předávání dat po cestě. Bloky dat se na úrovni síťové vrstvy nazývají pakety. Nejznámějším protokolem fungujícím na síťové vrstvě je Internet Protokol (IP).

Síťová vrstva dostává a reaguje na žádosti o služby ze čtvrté vrstvy ISO/OSI modelu – vrstvy transportní.

Transportní vrstva, na jejíž úrovni běží protokoly jako jsou TCP a UDP, zajišťuje transparentní, spolehlivý provoz určité kvality. Je využita k doručení dat k příslušnému procesu v hostitelském počítači. Rozděluje soubory (odesílaná data) na pakety a je softwarová.

Relační, 5. vrstva ISO/OSI modelu má na starost udržení spojení po dobu jeho trvání. Na této vrstvě pracují protokoly jako jsou SMB nebo NFS.

Prezentační vrstva udává, jakým způsobem budou data formátována, prezentována a kódována. Řeší například kódování textu a jedná se o softwarovou vrstvu.

Aplikační vrstva, která je nejvyšší vrstvou ISO/OSI modelu, definuje způsob, jak se sítí komunikují aplikace, databázové systémy, programy nebo například elektronická pošta (Mendelova univerzita v Brně, 1999).

3.2.3 **MAC a OUI**

MAC adresa neboli fyzická adresa se používá k jednoznačné identifikaci síťového zařízení. Jak bylo uvedeno výše, k jejímu využití dochází na úrovni druhé vrstvy ISO/OSI modelu, na vrstvě linkové (spojové). Využívají ji například směrovače pro jednoznačnou identifikaci odesílatele a příjemce rámce v dané části podsítě. V sítích TCP/IP je možné díky protokolům ARP (IPv4) či NDP (IPv6) získat fyzickou adresu díky znalosti IP adresy daného zařízení.

MAC adresa je 48bitové číslo, které se zapisuje zpravidla v hexadecimálním tvaru, například 48:E1:E9:39:40:11, přičemž prvních 6 hexadecimálních číslic (24 bitů) je u univerzálně spravovaných MAC adres identifikátor výrobce, který mu byl přidělen IEEE. Tato část adresy se jmenuje OUI (Organisationally Unique Identifier). Zbylých 6 hexadecimálních číslic je rozděleno výrobcem, dle jeho uvážení, ale měl by zachovat jedinečnost adres, tak aby při jejich využití nedocházelo k duplikacím v síti.

Většina moderních zařízení dovoluje MAC adresu upravit, čehož se hojně využívá u útoku známého jako MAC spoofing (Digital Guide, 2017), nicméně pokud nebyla fyzická adresa upravena, dá se z ní identifikovat výrobce zařízení.

3.2.4 **Platformy bezdrátové komunikace**

802.15.4

Norma IEEE 802.15.4 definuje rádiovou komunikaci pro sítě krátkého dosahu, jejím úkolem je popsat fyzickou a spojovou vrstvu komunikačního modelu. Jejím cílem je především komunikace malou rychlostí, v řádu desítek až stovek bitů za sekundu, se

zachováním vysoké spolehlivosti přenosu, jednoduché a levné implementace a zároveň s ohledem na omezení spotřeby připojených zařízení.

Komunikační model normy 802.15.4 je specifikován využitím komunikace v bezlicenčních pásmech 868 MHz, 915 MHz a 2,4GHz. Maximální rychlost přenosu je 250 kilobitů za sekundu a maximální velikost odesílaného rámce činí 127 bajtů. Norma používá různé modulace a s ohledem na druh využité modulace, počtu využitých kanálů a využité frekvenci se rychlost pohybuje od 20 kb/s až po již zmíněných 250 kb/s. Nejčastěji se používají vysokofrekvenční moduly pro komunikace na frekvencích 2,4 GHz. Důvodů je několik, zaprvé byly velmi brzy dostupné, jejich přenosová rychlost je až 12krát větší než v případě využití frekvence 868 MHz a disponují větším množstvím využití kanálů (až 16). Nevýhodou je sdílená frekvence s bezdrátovými sítěmi jako je WiFi, Bluetooth, atd., kdy může docházet k interferencím signálu, navíc propustnost vyšších frekvencí je oproti nízkofrekvenčním rádiovým vlnám nižší (Hynčica, 2006).

Linková vrstva je založena na metodě náhodného přístupu k médiu CSMA-CA (Carrier Sense Multiple Access with Collision Avoidance). Dle této metody přistupují zařízení, které chtějí vysílat k médiu, náhodně. Hlavní výhodou je jednoduchá implementace a nasazení, hlavní nevýhodou je nedeterminismus metody, kdy skutečná doba přístupu k médiu se může značně lišit, v závislosti na čase a vytížení pásma. (Zheng, 2006, s. 218-237)

6LoWPan

6LoWPan je akronymem pro IPv6 over Low-Power Wireless Personal Area Networks. Hlavní myšlenkou dle Mulligana je, že IP protokol by měl být využitelný i pro nejmenší zařízení (Mulligan, 2007). Doplňují to Zach Shelby a Carsten Bormann, kteří o 6LoWPAN napsali, že i nízkoenergetické zařízení s omezeným výpočetním výkonem by měla být součástí Internetu věcí, a právě 6LoWPAN by k tomu mohlo být klíčem. 6LoWPAN je postaven na, jak již název napovídá, IPv6 protokolu a využívá již zmíněného standardu 802.15.4 (Zach, 2009).

EETimes server uvádí, že diverzita oboru IoT z důvodu naprosto rozlišných požadavků na zařízení, (systém sledující zdraví pacienta, či jeho srdce, přes chytrý zámek,

až po sondu kontrolující vlhkost půdy), vysvětluje odlišené standardy a různé možnosti implementací pro IoT, které vznikaly již od roku 2000 (EETimes, 2011).

6LoWPAN, což je množina standardů, navržených skupinou IETF (Internet Engineering Task Force), která zastřešuje i ostatní Internetové standardy a architekturu, definovala mechanismy zapouzdření a komprese záhlaví, které umožňují odesílání a přijímání paketů IPv6 přes sítě založené na IEEE 802.15.4.

6LoWPAN je speciálně navržen pro automatizaci domácnosti a budov. IPv6 poskytuje základní transportní mechanismus pro základ složitých řídicích systémů a pro efektivní komunikaci se zařízeními prostřednictvím nízkoenergetické bezdrátové sítě.

Pravděpodobně největší výhodou standardu 6LoWPAN je možnost propojení se zařízeními používající 802.15.4, ale zároveň i sítě využívající IP protokoly, například Internet.

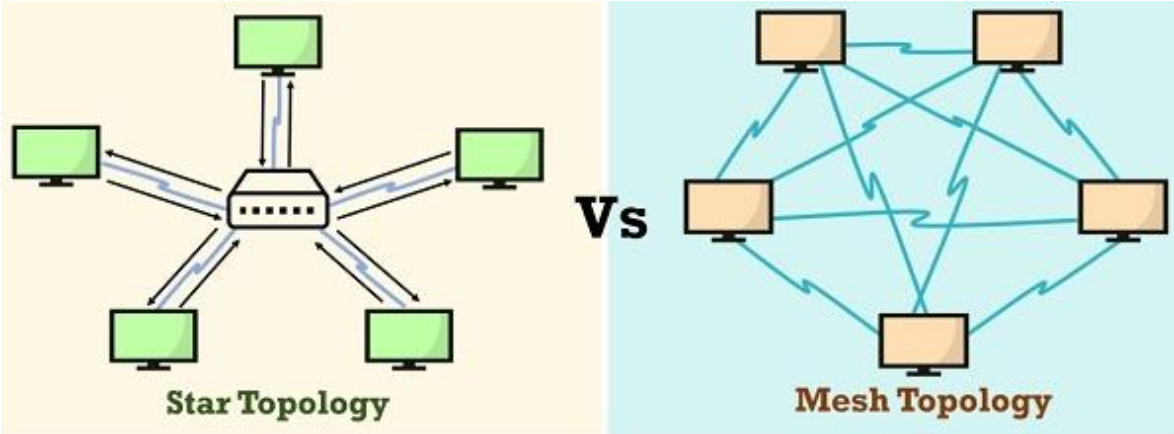
Tato výhoda se samozřejmě stává do určité míry i nevýhodou, například z pohledu bezpečnosti se určitá uzavřenost jiných platforem jako je ZigBee nebo Z-Wave hodí. (IoTbyHVM, 2019)

ZigBee a Z-Wave

Obě technologie ZigBee i Z-Wave používají nehvězdicovou mesh topologii sítě, která přináší v domácí automatizaci velkou výhodu ve smyslu dosahu sítě. Díky možnosti komunikace mezi jednotlivými nody sítě není zapotřebí přímý dosah k centrálnímu prvku systému – například routeru jako tomu je u hvězdicových sítí. Jednotlivé prvky je tak možné řetězit a v závislosti na konkrétní použité technologii využít i několikanásobného zřetězení. Mezi další výhody mesh sítí, je decentralizace, a tedy chybějící primární centrální prvek, který v případě výpadku postihne celý systém. Další výhodou je možná duplikace nejzásadnějších prvků a jejich možná libovolná míra redundance, kterou je možné dostáhnout požadované míry robustnosti systému. V mesh sítích chybí centrální prvek a síť tedy zůstává funkční i v případě výpadku libovolného z prvků.

Na obrázcích (Obrázek 10) vidíme příklad hvězdicové a mesh topologie.

Obrázek 10 - Hvězdicová a mesh topologie sítě



Zdroj: (TechDifferences, 2018)

Nevýhodou mesh sítí je nutné zajištění směrování a delší doby latence k IP bráně, je-li zapotřebí (například z důvodu ovládání přes Internet). Navíc při zapojení IP brány (hub) se stává následně prvkem nutným pro komunikaci pomoci IP protokolu, a i když síť zůstává funkční v případě výpadku tohoto prvku, systém přestává být pro uživatele dostupný mimo dosah samotné mesh sítě a ovládání přes internet přestává fungovat. (TechDifferences, 2018)

Pro připojování nových prvků domácí automatizace je tento způsob více než vhodný, čemuž napovídá i přístup společností, které se mesh routery a sítěmi, čím dále více zabývají. Většina společností vyrábějící běžně dostupné routery pro domácí využití začínají využívat i směrování pomocí mesh sítí. Hlavní nevýhodou zůstává pouze cena (Kuruc, 2019) (Trlica, 2019).

ZigBee, stejně jako 6LoWPAN, je navrženo pro zařízení, která nevyžadují vysokou rychlost přenosu dat a pracují často na baterii. V roce 2019 se dle Chewa ZigBee považovalo za nejoblíbenější nízkonákladový a nízkoenergetický bezdrátový standard na trhu, a vyspělejší z technologií ZigBee, 6LoWPAN. Obvykle je implementována pro osobní nebo domácí sítě nebo v bezdrátové síti pro sítě, které pracují na delší vzdálenosti.

Obrázek 11 - Zigbee alliance

Zdroj: (Digi, 2017)

ZigBee (Obrázek 11, Obrázek 12) IP je postaven na standardu IEEE 802.15.4, ale na rozdíl od 6LoWPAN nemůže snadno komunikovat s jinými protokoly. Rychlost sítě je 250 kb/s, poměrně vysoká rychlost ve spojení nízkého vyřazovacího výkonu jednotlivých prvků (z důvodu šetření energie) znamená nízký dosah sítě, proto ke správné funkčnosti je zapotřebí zajistit dostatečné množství uzlů v síti, či použít opakovače signálu. Připojení sítí ZigBee k IP protokolu je možné pomocí hubů. Tím se otevírá cesta k monitorování a kontrole ze zařízení, jako jsou smartphony a tablety v síti LAN nebo WAN včetně Internetu.

Jednou ze zásadních výhod ZigBee je možnost nechat uzly většinu času ve spánkovém režimu, což výrazně prodlužuje životnost baterie.

Protokol Zigbee 3.0 vychází ze stávajícího standardu ZigBee, ale sjednocuje aplikační profily specifické pro trh a druhy zařízení, aby umožnil bezdrátové připojení všech zařízení používajících Zigbee ve stejné síti bez ohledu na jejich označení a funkci. Navíc certifikační schéma ZigBee 3.0 zajišťuje interoperabilitu produktů od různých výrobců. Vzájemná nekompatibilita zařízení postavených na standardu ZigBee byla a stále je hlavní nevýhodou oproti konkurenční platformě Z-Wave. (Chew, 2018)

Obrázek 12 - ZigBee

Zdroj: (SmartRoom, 2018)

Mezi hlavní vlastnosti protokolu Zigbee patří:

- podpora více síťových topologií, jako je point-to-point, sítě typu point-to-multipoint a mesh,
- pomalý pracovní cyklus – zajišťující dlouhou životnost zařízení při provozu na baterie,
- nízká latence v případě dobře zpracovaného směrování a nepřetížení vysílacího pásma,
- až 65 000 vzájemně propojených zařízení v síti,
- 128bitové šifrování AES pro zabezpečená datová připojení,
- vyhýbání se kolizím, opakování a potvrzení – zajišťující kvalitu doručení zprávy.

Název vznikl podobností k pohybu včel při sběru medu. Stejně jako včely i data přeskakují ze zařízení na zařízení, než naleznou cestu k cíli, nejčastěji IP bráně, která zajišťuje komunikaci se sítí Internetu. (TheSmartCave, 2017)

Z-Wave (Obrázek 13) byl založen dánským startupem Zensys v roce 2004. V roce 2009 ho zakoupila společnost Sigma Designs. Jedná se o bezdrátovou síť, která propojuje zařízení domácí automatizace. Tato technologie, stejně jako předcházející ZigBee využívá mesh sítí. Dosah jednotlivých nodů má cca 100 metrů ve volném prostoru. Celkem může být do sítě připojeno až 232 zařízení, přičemž jejich zřetězení není technicky omezeno.

Obrázek 13 - Z-Wave certifikace vzájemné kompatiblity

(TheSmartCave, 2017)

V sítích Z-Wave, které využívají jiných frekvencí než Wifi, nedochází díky této skutečnosti k interferencím s ostatními bezdrátovými zařízeními. Každé zařízení v síti má svůj vlastní jedinečný identifikátor, který usnadňuje nastavení a napomáhá bezpečnosti sítě.

Stejně jako sítě ZigBee je možné využít některé z běžně dostupných hubů, například SmartThings od společnosti Samsung a ovládat tak Z-Wave zařízení přes IP protokol.

Hlavním rozdílem Z-Wave protokolu, které dává oproti ZigBee konkurenční výhodu, je certifikace poskytovaná Z-Wave Alliance. Díky této certifikaci, si může být uživatel jistý, že jím zakoupený modul bude plně podporovanými zařízeními z Z-Wave ekosystému. Tento rozdíl se pokouší ZigBee umazat standardem ZigBee 3.0, který by měl zajišťovat totéž. (TheSmartCave, 2017)

Z-Wave Plus je nový certifikát, který Z-Wave začala využívat. Jedná se o označení, především pro zákazníka, aby mohl jednoduše identifikovat zařízení, které podporuje nedávno zavedenou hardwarovou platformu Z-Wave „Next Gen“, známou také jako série 500, 5. generace, Z-Wave Pro Gen5 nebo Gen5. Řešení certifikovaná pro Z-Wave Plus obsahují vybranou sadu rozšířených funkcí, navýšení rychlosti a dosahu, snadnost instalace a nastavení systémů Z-Wave, prodloužení životnosti baterie a aktualizace OTA (Over The Air). Zásadním je i zachování zpětné kompatibility, a tím zachováním různorodosti ekosystému Z-Wave.

3.2.5 **Služby domácí automatizace**

Kapitola se věnuje rozdílům mezi nejprodávanějšími automatizačními systémy Google Home, Apple HomeKit a Amazon Alexa. Rozvoj platforem pro domácí automatizaci je však natolik rychlý, že jakékoliv srovnání je platné pouze v okamžiku daného testu. Během přípravy této práce bylo čerpáno z několika zdrojů, nicméně informace a názory uživatelů se lišily v závislosti na aktuálnosti daného článku, přičemž rozdíl mezi nejstarším a nejnovějším zdrojem byl tři roky.

Z pohledu bezpečnosti IoT zařízení se chytré reproduktory společností Amazon, Google nebo Apple na bezpečnosti nikterak nepodílí. Jedná pouze o rozšiřující možnost, jakým způsobem se dají vybraná IoT zařízení ovládat. Chytré reproduktory, které v sobě obsahují asistenty pro ovládání chytré domácnosti, nejsou prvkem zajišťujícím bezpečnost samotných zařízení. Možnost zneužití a útoku tak je z daných důvodů možná pouze v případě napadení cloudových služeb společností Apple, Google či Amazon. Vzhledem k robustnosti a rozdílnému zaměření se tato práce bezpečnosti systémů Amazon, Google či Apple nevěnuje.

Google Home (Assistant) a Amazon Alexa

Vzhledem k podobnosti obou systémů, jejich automatizace, jimi podporovaných modulů, seznamu podporovaných zařízení, jsou systémy podle Niedla zaměnitelné. Uvádí, že výběr vhodného nástroje pro automatizaci záleží primárně na aktuálně vlastněných zařízeních a jejich podpory danými asistenty.

Hlavní výhodou společnosti Google je pravděpodobně možnost využití Google Assitanta v mobilních telefonech, zatímco u Amazon Alexa systému musíme mluvit přímo k reproduktoru, jenž Alexu obsahuje. Výhodou řešení od společnosti od Amazon je implementace brány pro zařízení ZigBee, a tím i možnosti integrace ZigBee produktů bez nutnosti využití brány pro komunikaci s IP protokoly. (Nield, 2019)

Apple HomeKit

Apple HomeKit stojí v automatizaci dle dostupných informací o něco dále, především možnosti vytváření Routines (kapitola 3.2.7) je na pokročilejší úrovni a poskytuje možnosti takových podmínek, jako například „odchodu posledního člena domácnosti z domu“. Niedl toto považuje za jednu z klíčových podmínek v případě automatizace domácnosti z důvodu možnosti vytvoření akcí při odchodu všech členů domácnosti z domova. Navíc možnosti ovládání automatizace z počítače je něco, co konkurence od Amazanu či Googlu zatím neposkytuje.

Na druhou stranu počet modulů, které jsou v aktuální chvíli podporované ekosystémem Apple, je nižší než u zbývajících dvou konkurentů (Nield, 2019).

3.2.6 MQTT

Další velmi důležitý protokol z pohledu domácí automatizace a především DIY (Do it yourself) je MQTT. Jedná se o protokol využívaný pro komunikaci jednotlivých zařízení na aplikační úrovni ISO/OSI modelu využívající TCP.

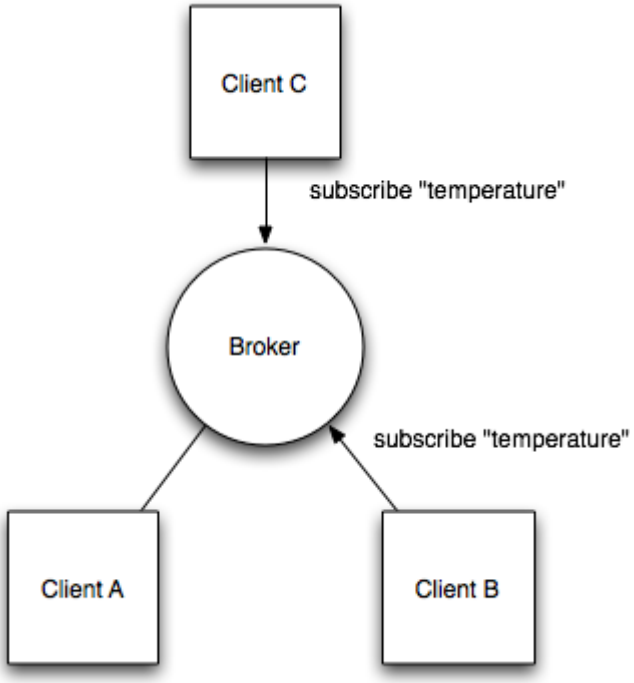
MQTT je protokol založený na publikaci a odběru zpráv. Byl vyvinut společností IBM pro komunikaci M2M zařízení. Nyní se jedná o otevřený standard. (Eclipse Foundation, 2014)

Architektura MQTT

Jedná se o architekturu, ve které se využívá model klient / server, kde každý senzor je klient a připojuje se k serveru, známému jako broker. MQTT je zprávami (eventy) řízený protokol. Každá zpráva obsahuje tzv. topic (téma) a vlastní zprávu – payload, která je pro broker nedostupná. Topic je naopak veřejný a broker ho používá, aby věděl, komu má delegovat zprávy, u nichž má přihlášen odběr. Každý klient se může přihlásit k odběru více témat a následně pak dostane každou zprávu publikovanou k danému tématu.

Níže je uveden příklad sítě se třemi klienty a centrálním serverem, brokerem. Po navázání TCP spojení s brokerem z jednotlivých nodů, se klienti B a C na obrázku níže (Obrázek 14) přihlásí k odběru tématu *temperature*.

Obrázek 14 - MQTT - odběr

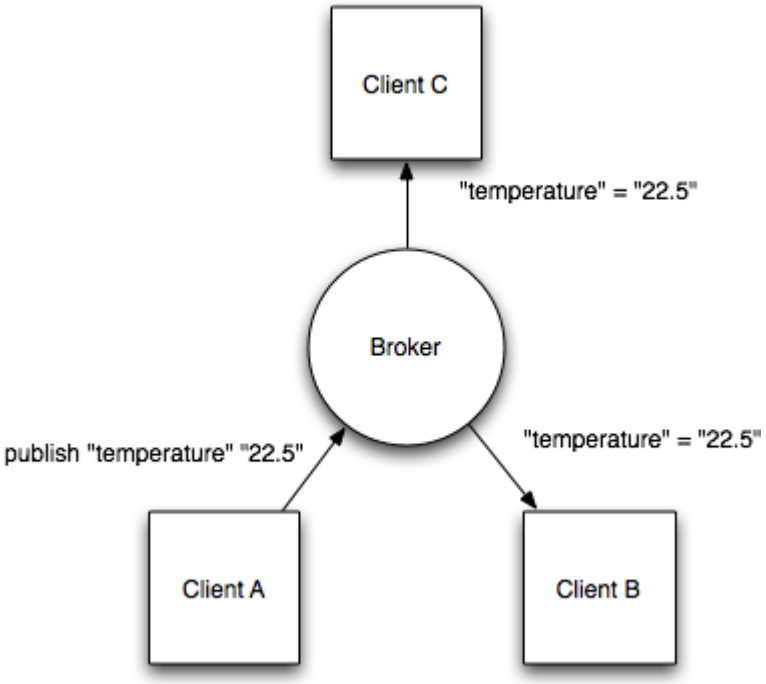


Zdroj: (Eclipse Foundation, 2014)

Dalším stavem (Obrázek 15), následujícím po předcházejícím obrázku může být publikování nové zprávy klientem A, jehož zprávu broker následně doručí všem klientům, kteří se přihlásili k odběru daného tématu – tedy teploty. Klient B a C tedy obdrží v daném příkladu zprávu z tématu *temperature* s vnitřní zprávou „22,5“. Tvar zaslané zprávy není

protokolem nikterak standardizován, nicméně se nejčastěji počítá s json formátem. (Eclipse Foundation, 2014)

Obrázek 15 - MQTT - publikace



Zdroj: (Eclipse Foundation, 2014)

Bezpečnost protokolu a její význam

Z pohledu bezpečnosti může být klient (pokud tak broker žádá) autentizován i autorizován jménem a heslem, možné je taktéž ověření SSL certifikátem a zabezpečení protokolu pomocí TLS. Implicitně však nejsou (například na rozdíl od výše uvedených komerčních protokolů ZigBee a Z-Wave) data symetricky či asymetricky šifrována. Implementace šifrování tak není vynucena a jedná se o jedno možných rizik MQTT protokolu.

Jelikož komunikace je řízena brokerem, je jeho zodpovědností šifrování komunikace vynutit a jedná se o místo, kde by měl uživatel zpozornět a případně zkontrolovat, zdali je šifrování umožněno a zapnuto.

Z pohledu bezpečnosti není MQTT protokol problém, pracuje na aplikační vrstvě, používá TCP umožňuje šifrování s ověřením na uživatele a heslo, či pomocí certifikátů. Možný problém se může skrývat pouze v nevynucenosti. (Eclipse Foundation, 2014)

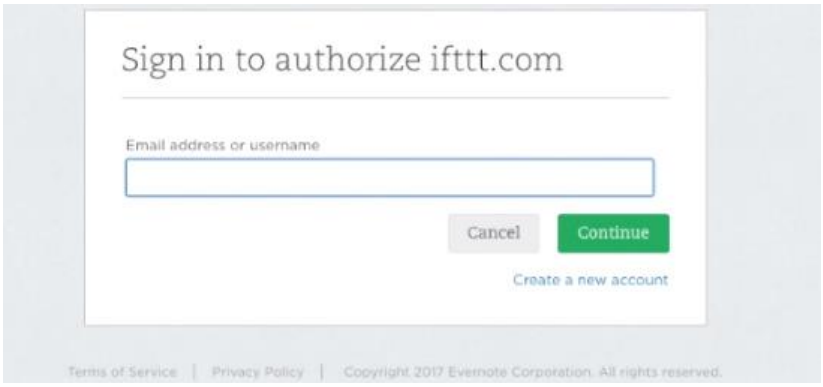
3.2.7 **IFTTT**

If This Then That neboli česky *pokud něco, pak něco* je platforma pro automatizaci domácích vzájemně navázaných procesů. Díky IFTTT se dají vytvářet automatické akce, které mohou spustit a vyvolat několik vzájemně propojených akcí. Díky vzájemné komunikaci všech komponent zapojených do domácí sítě IoT, je možné vytvářet sofistikovaná řešení automatizace. V případě uvedeném výše v kapitole 3.2.6 by se mohlo jednat například o teplotní čidlo a klimatizaci, která při odběru tématu *temperature* a zaznamenání vyšší teploty než 24 °C, sepne a začne klimatizovat místnost.

Z IFTTT se postupně stala platforma pro automatizaci i běžné práce či činností prováděných v online světě. Díky propojení různých služeb na internetu a stovkám předpřipravených procedur nazývaných Flow, je možné jednoduše automatizovat běžné činnosti. Příkladem může mít vytvoření Tweetu po vložení příspěvku na Instagramu. IFTTT přistupuje ke službám přes API a k ověření používá uživatelův účet.

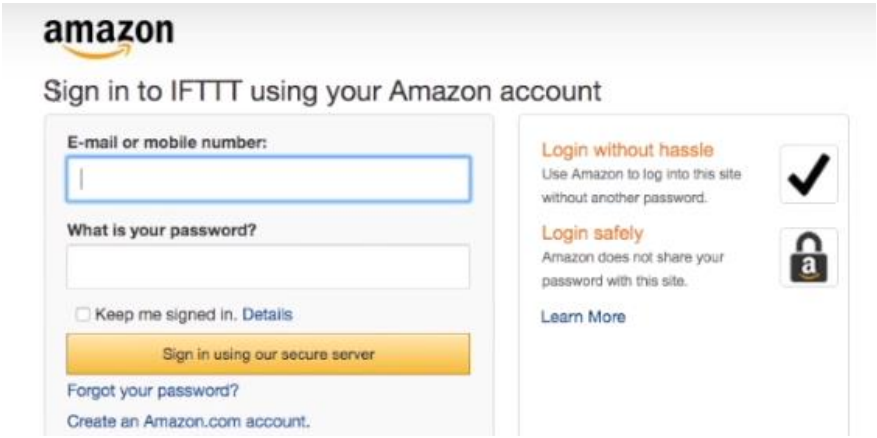
Ověřování k jednotlivým službám, probíhá, stejně jako u služeb od společností Google či Apple, pomocí uživatelského jména a hesla. Vzhledem k faktu, že IFFFT využívá k připojování k jednotlivým službám webových serverů konkrétních služeb, je z pohledu bezpečnosti většina zodpovědnosti na poskytovatelích jednotlivých služeb. Rozdíly v přihlašování k jednotlivým službám jsou zobrazeny na obrázcích níže (Obrázek 16, Obrázek 17), kde je předvedeno připojení ke služně Evernote a Amazon (IFTTT, 2019).

Obrázek 16 - Přihlášení ke službě Evernote z portálu IFTTT.com



Zdroj: (IFTTT, 2019)

Obrázek 17 - Přihlášení ke službě Amazon z portálu IFTTT.com



Zdroj: (IFTTT, 2019)

3.3 Zákon o kybernetické bezpečnosti

Tato část práce se zaměří na analýzu Zákona o kybernetické bezpečnosti a jeho využití při použití IoT prvků domácnosti.

Zákon, který je v platnosti od 29. srpna roku 2014 a účinnosti nabyl 1. ledna 2015 byl do dnešní doby upraven několika novelami a aktuálně je platná jeho 6. verze. Počet revizí a úprav dokazuje dynamiku potřebnou k zachování dostatečného pokrytí potřebné legislativy. Zákon vychází a částečně se odvolává na normu ISO/IEC 27001:2013, případně ČSN ISO/IEC 27001:2014, nicméně se nejedná o totéž. Především proto, že norma ISO definuje doporučení a best practice v oblasti informační bezpečnosti, zatímco Zákon, či Vyhláška o kybernetické bezpečnosti jsou legislativně vymahatelné. Tvůrci zákona tak

přesněji specifikovali požadavky, a díky tomu předcházejí nejasnostem v pohledu vykládání normy, která na rozdíl od zákona v České republice není právně vymahatelná, pokud na ní přímo neodkazuje zákon. Odkazy na ISO normu v samotném zákoně se mohl orgán, či subjekt domnívat, že nabývá všech zákonných náležitostí, které jsou popsány v Zákoně o kybernetické bezpečnosti. (Goll, 2019)

„Toto tvrzení bylo přinejmenším zavádějící, byť podložené ustanovením § 29 – Prokázání certifikace. Naštěstí se tento problematický paragraf v nové verzi vyhlášky o kybernetické bezpečnosti z roku 2018 již nevyskytuje, a tak i mizí důvod k tvrzení, že když mám zaveden ISMS (implementovaný systém řízení bezpečnosti informací), jsem v souladu i se ZoKB (Zákonem o kybernetické bezpečnosti)," (Goll, 2019) uvádí Jan Goll, senior Information Security Consultant ve společnosti Anect.

3.3.1 **Bezpečnost IoT z pohledu zákona**

Hned v první hlavě zákona je specifikován rozsah, pole působnosti a informace, koho se zákon týká. Ve § 3 je vypsán seznam orgánů a osob, jimž zákon ukládá povinnost se jím řídit. Patří mezi ně:

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),
b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),
c) správce a provozovatel informačního systému kritické informační infrastruktury,
d) správce a provozovatel komunikačního systému kritické informační infrastruktury,
e) správce a provozovatel významného informačního systému,
f) správce a provozovatel informačního systému základní služby, pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d),
g) provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f), a
h) poskytovatel digitální služby.

Přičemž digitální službou, které má z výše uvedeného nejblíže ke spotřebiteli se, dle § 2 písmene l) rozumí:

digitální službou služba informační společnosti podle zákona upravujícího některé služby informační společnosti, která spočívá v provozování:

1. on-line tržiště, které spotřebiteli nebo prodávajícímu umožňuje on-line uzavírat s prodávajícím podnikatelem kupní smlouvu nebo smlouvu o poskytnutí služeb, a to prostřednictvím internetové stránky on-line tržiště nebo prostřednictvím internetové stránky prodávajícího, který využívá službu poskytovanou on-line tržištěm,
2. internetového vyhledávače, který umožňuje provádět vyhledávání v zásadě na všech internetových stránkách, a to na základě dotazu uživatele na jakékoliv téma v podobě klíčového slova, sousloví nebo jiného zadání, přičemž služba poskytuje odkazy, na nichž lze nalézt informace související s požadovaným obsahem, nebo
3. cloud computingu, který umožňuje přístup k rozšiřitelnému a přizpůsobitelnému úložišti nebo výpočetním zdrojům, které je možné sdílet. (CZ, 2014)

Z výše uvedeného vyplývá, že výrobci, pokud nespadají pod dodavatele digitálních služeb, nebo jednu shora uvedených kategorií subjektů, nejsou kybernetickým zákonem nikterak ovlivněny.

Vzhledem k dynamice zákona v posledních letech (a například přidáním odstavce h) do paragrafu 3) se dá sledovat snaha o přiblížení zákona ke koncovým uživatelům za účelem poskytnutí co největšího stupně jejich ochrany.

Zákon je koncipován k ochraně infrastruktury státu, avšak s přibývajícími zařízeními úzce souvisejícími s našimi životy bude zapotřebí, čím dál větší zákonná ochrana – a to nejenom z pohledu záruční doby zakoupených výrobků, což již dnes z důvodu všudypřítomných cloudových služeb začíná být problém – tak především z důvodu ochrany zdraví, života a majetku spotřebitele.

4 Vlastní práce

4.1 Úvod

Vlastní práce je vymezena především na otestování různých zařízení a zmapování trhu s ohledem na propagovanou a reálnou skutečnost bezpečnosti produktů se zaměřením na bezpečnost komunikace.

Modelovým příkladem může být zakoupení produktu ve známém českém internetovém obchodě. Jedním ze zásadních kritérií výběru je zcela logicky vždy cena a poměr nabízených funkcionalit daného produktu. Bohužel, především z důvodu tlaku výrobců na cenu a zatím stále nedostatečné informovanosti běžných uživatelů (viz kapitoly 3.1.1 a 4.2), ve spojení s mediálním tlakem pro „chytré domácnosti“, se může uživatel dobrovolně stát obětí koupí nekvalitního produktu, jehož bezpečnost je na velmi nízké úrovni.

Práce cílí na zařízení, u kterých je očekávána větší míra možného pochybení, či nedostatečnost ze strany výrobce. Je zaměřena primárně na zařízení nepracující na ZigBee ani na Z-Wave, které by ve svém standardu měly obsahovat AES šifrování.

Cílem testování nejsou ani po domácku vytvořená zařízení postavená na mikročipech či mikropočítačích typu Arduino, ani zařízení koupitelná na e-shopech typu AliExpress. To z důvodu, že typický zákazník, který je nejzranitelnější a nemá hlubší znalost IoT zařízení pravděpodobně nepůjde na čínský e-shop nakupovat chytré žárovky a zásuvky a ani nebude mít tendence sám něco vyvíjet. Naopak je možné, že půjde na stránky e-shopu Alza a nakoupí nejlevnější osvětlení a do své nově zakoupené, na dálku ovládané zásuvky na elektřinu zapojí rychlovarnou konvici, či si dokonce zakoupí externí ovládání pro svá garážová vrata. To vše bez předchozí znalosti, odborné montáže do domácí wifi sítě, aniž by očekával jakékoli problémy.

Poslední řádky jsou hlavní motivací pro tvorbu této práce, autor jako zaměstnanec společnosti zabývající se bezpečnostním monitoringem využívající pokročilé systémy pro sledování sítě, netflow, ale zároveň i využívající bezpečnostních logů z produkčně používaných přepínačů, IDS či IPS systémů, je denně svědkem pokusů nejrůznějších útoků, ale i dopadu, který vzniká na sítích, které nejsou správným způsobem monitorovány. Jedná

se o nejrůznější prostředí, avšak spojuje je společný jmenovatel, kterým je jmenovaný kybernetický zákon. Autor vychází z předpokladu, že právě u společností, kterých se dotýká kybernetický zákon se dá očekávat největší míra zabezpečení, avšak i tak se denně setkává s nejrůznějšími typy incidentů, které jsou zapříčiněny ať již pochybením jedince, špatným návrhem nebo jen útokem zvenčí.

Pokud se tedy lze setkat i ve státem sledovaných systémech s bezpečnostními problémy, zůstává otázkou, na jaké úrovni se dá očekávat zabezpečení dat klientů například u společnosti, jejímž hlavním předmětem podnikání byla donedávna výroba plastových hraček. Tyto společnosti, navíc pokud nevyužívají data spadající pod zákon o ochraně osobních údajů, nejsou nikterak sledovány a forma uložených dat může být zvolena naprosto nevhodným způsobem. Taková data pak mohou být zneužita a jediným možným následkem pro danou společnost se stává mediální tlak v případně odhalení problému či úniku a zneužití informací. Můžeme se pouze domnívat, jak a co se s daty děje při jejich skladování, či jakým dalším způsobem je dané společnosti využívají.

Vše uvedené umocňuje již zmíněný tlak na cenu, rychlost rozvoje tohoto průmyslu, který znamená minimálně absolutní nedostatek dostatečně kvalifikované pracovní síly, a především chybějící tlak na potřebu maximálního úsilí pro zabezpečení zpracovávaných dat.

Investigace, jak jsou data ukládána a jak je s daty nakládáno na straně serverů je velmi náročné a většina společností tyto informace neuvádí, ať již z důvodu minimalizace možných cílených útoků, nebo to považují za know-how, či nechtějí dané informace poskytovat. Nicméně o tom, jakým způsobem se s daty nakládá můžeme ověřit již na straně klienta při záchytu komunikace ze zařízení do routeru. Pokud komunikace nebude zabezpečena, nedá se očekávat ani vyšší úroveň ochrany na straně serveru, databáze apod. I kdyby data na straně serveru byla uchována kvalitně a správným způsobem, bezpečnost je právě tak silná, jako její nejslabší článek, takže v případně odhalení pochybení již zde, je celkový výsledek špatný.

Další způsob bude analýza dostupných zdrojů se známými zranitelnostmi.

4.2 Dotazníkové šetření – kvalita zabezpečení účtu

V rámci práci byl provedl krátký výzkum, jehož zobecněné závěry potvrzují informace získané v teoretické části práce. Kvalita hesel zůstává i pro rok 2020 nedostatečná,

uživatelé často nevyužívají dvoufaktorového ověřování a nechrání informace dostupné na svých sítích.

Výzkum o 30 respondentech, z neuceleného demografického vzorku společnosti, nelze brát jako statistický významný vzorek, nicméně výsledky odpovídají skutečnostem uváděným v teoretické části práce a podtrhují problémy s informační bezpečností.

Dotazník ochrany účtu

1. Nechali byste kolemjdoucího v případě jeho potřeby připojit na Vaší domácí WiFi?
    a. Ano – 23
    b. Ne – 7
    c. Neodpovím – 0
2. Používáte oddělenou síť pro rodinu a návštěvníky?
    a. Ano – 2
    b. Ne – 28
    c. Neodpovím – 0
3. Obsahuje Vaše heslo do domácí Wifi sítě více jak 8 znaků?
    a. Ano – 2
    b. Ne – 25
    c. Neodpovím – 3
4. Obsahuje jiné znaky než číslice a písmena?
    a. Ano – 6
    b. Ne – 20
    c. Neodpovím – 4
5. Kolik různých hesel používáte ke svým účtům (e-maily, webové účty, Facebook, …)
    a. Používám jedno heslo všude – 3
    b. Používám pět a méně hesel, které opakuji – 17
    c. Používám více jak 5 hesel – 3
    d. Používám správce hesel jako je Keepass nebo 1Password – 2
    e. Neodpovím – 5

6. Používáte dvoufázové ověření pro přístup do Vašeho e-mailového účtu? Pokud nikoli tak proč?
    a. Ne, nepoužívám
        i. Nevím, o co se jedná – 16
        ii. Nemyslím si, že to je potřeba – 4
        iii. Zdržovalo by mě to – 2
    b. Ano – 6
    c. Neodpovím – 2

Zdroj: (Caha, 2020)

Ochota sdělovat informace o používaných heslech je stejně tak zarážející jako nechat připojit cizího člověka do soukromého virtuálního prostoru. Nic z toho nesnižuje fakt, že respondenti sice znali důvod vzniku dotazníku a že výsledky budou použity pro vznik diplomové práce, přesto jsou výsledky velmi nepříznivě jednoznačné. Kuriozní byla situace, kdy byl během dotazníku položen konkrétní dotaz ze strany respondenta, zdali jím používané heslo je dostatečně bezpečné, přičemž ho nahlas vyslovil.

Určitou výhodou pro české uživatele může být používání neanglických slov v běžně používaných heslech pro zabezpečení účtů a dalších. Hesla známá z databází nejčastěji používaných hesel jsou standardně v anglickém jazyce a útočník by tak musel primárně cílit na českého uživatele, pokud by používal slovníkový útok, nebo duhové tabulky (TeamsID, 2019).

4.3 Nabízené typy řešení

4.3.1 Zámky

Chytré zámky jsou jedním z nejnabízenější artiklů mezi IoT zařízeními. Jejich přidanou hodnotou je dle výrobců především:

- možnost ovládat a kontrolovat vstup na úrovni osob,
- vysoká úroveň bezpečnosti,
- dlouhá výdrž provozu na baterie díky využití low-power protokolů.

Příklady

Danalock V3, zástupce dražšího řešení, balení za cca 6 500,- Kč obsahuje bezpečností cylindrickou vložku. Komunikuje na různých protokolech, podle nabízeného typu – ZigBee, Z-Wave, nebo s podporou Apple Homekit. Zámek lze používat i bez hubu, po nainstalování aplikace pro ovládání díky Bluetooth rozhraní. Zámek podporuje AES šifrování a je napájen pomocí baterií.

Obrázek 18 - Danalock V3

Zdroj: (Alza, 2020)

Dalším zástupcem z řady chytrých zámků, je řešení, na které je upozorněno v teoretické práci (Obrázek 1 - Visací zámek se špatnou mechanickou ochranou) s naprosto nevyhovujícím mechanickým řešením.

Zhodnocení

Testováním chytrých zámků se tato práce nezabývá z důvodu nabídky dostupných produktů na českém trhu. Všechny nabízené produkty na e-shopu společnosti Alza.cz nabízejí šifrování AES, které by mělo zajišťovat dostatečnou ochranu provozu. Na druhé straně spektra, zámek zmíněný výše není dostupný na českém trhu a šance jeho pořízení laickou veřejností České republiky, je tedy výrazně snížena.

4.3.2 **Osvětlení**

Chytré osvětlení patří mezi nejprodávanější kategorie chytrých IoT zařízení, alespoň společnost Alza.cz má v této kategorii nejvíce produktů. Důvodů může být několik, zcela jistě mezi ně patří finanční dostupnost, a především jednoduchost instalace.

Příklady

Některé žárovky dostupné na Českém trhu stačí pouze našroubovat do standardní objímky, nastavit Wifi připojení a žárovka může být ovládána z dodané aplikace. Mezi tento typ patří i jedno z testovaných zařízení SONOFF B1. Jedná se o žárovku, která podporuje komunikaci přes Wifi sítě, a díky aplikaci eWeLink či integraci přes například Google Assistant může být hlasově či na dálku ovládána z mobilního zařízení. Cena za žárovku je dle cen českých obchodů mezi 346,- Kč a 549,- Kč (Heureka, 2020)

V nabídce jsou i zařízení, které komunikují přes IoT protokoly ZigBee či Z-Wave, příkladem mohou být zařízení Philips Hue, která nabízejí velký výběr svítidel s běžně dostupnými paticemi. Jedna z nabízených žárovek, *Philips Hue White and Color ambiance 9W E27* (Obrázek 19) s cenou 1319,- Kč (Alza.cz 29. 2. 2020) sice nabízí ovládání přes Bluetooth protokol po připojení k mobilnímu zařízení, nicméně pro využití všech funkcí – scény, ztlumení, ovládání po internetu, apod. je zapotřebí zařízení Hue Bridge, který slouží jako brána pro „překlad“ ZigBee protokolu, který Philips Hue zařízení využívají do standardu 802.11.

Obrázek 19 - Philips Hue

Zdroj: (Alza, 2020)

Dalším z praktických zástupců, které lze zařadit do kategorie osvětlení, je zařízení společnosti Sonoff. Sonoff Mini umožňuje zapojení pod vypínač do standardní evropské montážní krabice o průměru 68 mm. Díky zapojení, které Sonoff Mini (Obrázek 20)

umožňuje, je i po zapojení nadále možné využívat vypínač na zdi. Navíc není zapotřebí měnit stávající žárovku, ovládání přes hlasové asistenty zůstává zachováno, stejně tak možnosti automatizace. Nevýhodou je obtížnost montáže, kterou by z bezpečnostních důvodů měl provádět profesionál.

Obrázek 20 - Sonoff Mini

Zdroj: (chytrevypinace.cz, 2020)

Zhodnocení

Společnost Sonoff nabízí především zařízení, která komunikují pomocí Wifi, inzeruje, že používá AWS cloud k běhu svých serverů, na nichž běží i eWeLink cloud. Níže v praktické části jsou dostupné výsledky testování.

Jelikož se výrobky společnosti Philips zaměřují na ZigBee protokol, nejsou cílem dalšího zkoumání.

4.3.3 **Kamery**

V teoretické části byla zmíněna pasáž týkající společnosti Xiaomi, která se v nedávné době dopustila závažné bezpečností chyby způsobující streamování obrazu z bezpečnostních videokamer jiným uživatelům. Zařízení *Xiaomi Mi Home Security Camera*, které společnost Alza.cz (29. 2. 2020) nabízí za 1399,- Kč včetně DPH, disponuje rozlišením 1920 x 1080 pixelů, noční režim, vestavěný mikrofon i reproduktor a připojení přes Google Assistant a Amazon Alexa.

Po připojení se videokamera připojí ke cloudu společnosti Xiaomi a její uživatelské rozhraní je dostupné přes aplikaci Mi Home, která je dostupná pro operační systémy Android i iOS. Díky detekci pohybu v automatickém režimu nahraje 15 sekund záznamu (3 před a 12 sekund po zaznamenání pohybu) uloží ho do cloudu.

Právě tato kamera způsobila popisovaný problém a níže v práci bude otestována.

Z důvodu nízké přenosové rychlosti nejsou často u kamer využívány protokoly Z-Wave ani ZigBee a využívá se bezdrátových sítí s vyšší přenosovou rychlostí jako Wifi či jiných proprietárních protokolů. Pokud videokamery podporují Z-Wave, je to z důvodu možnosti komunikace s jinými IoT zařízeními (například senzory) fungujícími na tomto protokolu. Příkladem zařízení mohou být zařízení společnosti Arlo, vyrábějící videokamery, které používají proprietární protokol ke komunikaci, nicméně pro zapojení do ZigBee či Z-Wave ekosystému deklaruje výrobce podporu dalších zařízení fungujících na ZigBee a Z-Wave protokolech.

Zařízení společnosti Arlo zatím nejsou v České republice dostupné, a tak nebylo možné zařízení otestovat, proto se jimi práce nadále nebude zabývat.

4.3.4 **Ostatní**

Mezi další výrobky, dnes běžně dostupné na českých e-shopech jsou senzory nejrůznějších druhů, termostaty, zvonky, požární hlásiče nebo chytré ovladače garážových vrat. Zařízení *Meross Smart Wi-Fi Garage Door Opener* dostupný na e-shopu Alza.cz za cenu 1259,- Kč s DPH (29. 2. 2020) nabízí možnost ovládání garážových vrat díky vlastní aplikaci, stejně jako připojení pomocí Wifi k Amazon Alexa či Google Assistant. Zařízení je kompatibilní s běžně dostupnými motory a jeho výhoda je možnost instalace k již zapojené bráně či vratům. Podmínkou zapojení je přítomnost volných pinů na ovládací jednotce motoru, u kterých při zkratování dojde k impulsu pro uzavření či otevření brány do koncových poloh.

Zařízení bude otestováno níže v práci.

4.4 **Metodický postup testování**

Testování bude probíhat pomocí volně dostupných zdrojů a software. Cílem je zachytit komunikaci jednotlivých zařízení a následně ji analyzovat. Určitým předpokladem u levnějších zařízení, které nedeklarují šifrování komunikace, je, že se může jednat o slabý článek v jejich zabezpečení, a z toho důvodu se může jednat o celkově zranitelné, či nedostatečně chráněné zařízení. Navíc pokud se podobná pochybení budou objevovat již v komunikaci, nelze se spoléhat ani na kvalitativní pojetí s nakládáním sbíraných dat.

V kapitole 4.5.2 bude ověřeno, zdali některé z testovaných, či případně jiné podobné zařízení, mají bezpečnostní problémy zaznamenané v některé z databází zranitelností.

Záchyt komunikace

Záchyt komunikace je proveden pomocí USB Wi-fi adaptéru Tenda W311M. Jedná se o základní WiFi USB dongle, který používá čipset Ralink RT3370, pracuje 2,4 GHz, podporuje WEP, WPA, WPA2 a Kali Linux disponuje ovladačemi pro tento čipset.

Zařízení bylo zakoupené jako druhé, po nefunkčním pokusu s TP_ LINK TL_WN722N, pro který pro Linux nebyly ovladače. Operační systém Windows standardně podporuje většinu Wi-Fi adaptérů, nicméně monitorovací a promiskuitní mód se nepodařilo s dostupnými ovladači použít.

Dále je využit operační systém Linux Kali, který disponuje předinstalovanou sadou nástrojů pro odposlech síťového provozu a program Wireshark, pro analýzu protokolů a paket sniffingu.

Aplikovány jsou nástroje z rodiny airdump, mimo jiné airmon-ng pro zapnutí monitorovacího módu na síťovém rozhraní, airodump-ng pro odposlech provozu a zároveň paketový záchyt konkrétního zařízení a přístupového bodu. Z důvodu napodobení podmínek skutečného provozu, je použita síť WiFi s WPA2 zabezpečením. Protokol 802.11 používá blokové AES šifrování a k dešifrování je tedy zapotřebí použití klíče a SSID sítě, na které provoz probíhá. Vzhledem k předpokladu, že IoT prvky domácí automatizace budou připojeny na zabezpečených sítích a útočník s největší pravděpodobností nebude mít možnost drátového připojení do sítě, byl útok nasimulován taktéž na zabezpečené bezdrátové síti. Pro tento typ útoku je zapotřebí znát heslo bezdrátové sítě.

Heslo sítě je možné zjistit ze záchytu komunikace. Při zachycení WPA handshaku, který je v 802.1x komunikace zajištěn pomocí EAPOL protokolu, je možné ho po rozšifrování hashe hesla získat.

U několika předem vybraných zařízení jsou zachyceny komunikační pakety s cílem zjistit, jak zařízení komunikují, případně kam a kolik dat zasílají, či zdali jsou otevřeny nějaké porty, které by potenciálně mohly být zneužity.

4.5 Testování

4.5.1 Záchyt provozu a skenování portů

Meross Smart Wi-Fi Garage Door Opener

Prvním testovaným zařízením byl chytrý ovladač garážových vrat od společnosti Meross, který umožňuje pro většinu dostupných motorů garážových vrat či vjezdových bran díky zkratování dvojice z dostupných pinů na kontrolní jednotce motoru změnit stav brány – otevřít a zavřít bránu, či vrata.

Technologicky zařízení napřímo komunikuje přes IP protokoly a je připojeno k WiFi směrovači pomocí 2,4 GHz bezdrátové 802.11 sítě. Dle dostupné oficiální dokumentace používá cloudových služeb AWS (Amazon Web Services), zde je hostované API rozhraní, které zařízení používá a díky němuž je možné z mobilní aplikace přepínat stav otevření či zavření garážových vrat. V balení je i magnetický senzor indikující aktuální stav.

Díky integraci s Google Assistant a asistenty domácí automatizace je možné garážová vrata ovládat i pomocí chytrých reproduktorů. Aplikace se ověřuje stejně jako asistenti chytré domácnosti pomocí uživatelského jména a hesla. Následně využívá API k ovládání a zjištění stavu zařízení.

Následující postup byl proveden pro všechna testovaná zařízení, detailní postupy jsou uvedeny v příloze (Přílohy).

Po instalaci systému a detekci USB rozhraní s připojenou Wifi kartou bylo nejprve zapotřebí nastavit síťové rozhraní a přepnout jej do monitorovacího módu (Obrázek 22, Obrázek 23), jelikož po zapnutí se rozhraní automaticky detekuje v řízeném režimu (Obrázek 21) pro obvyklé použití karty.

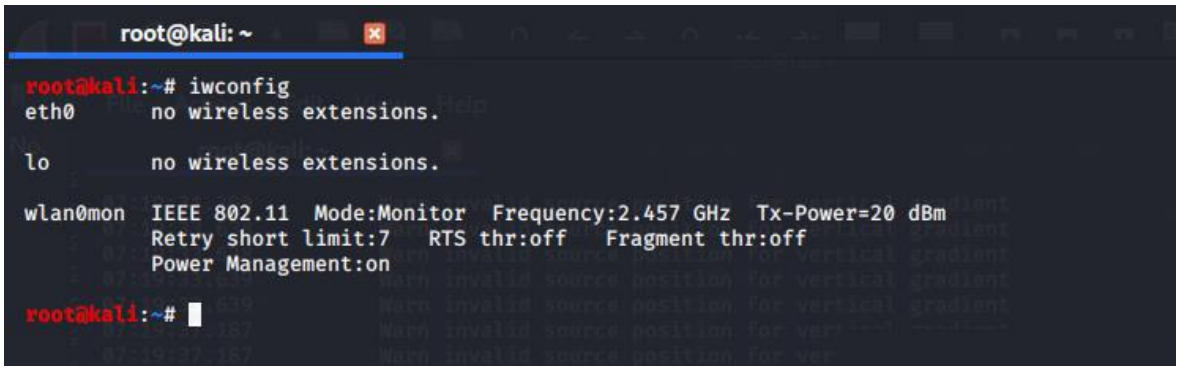
Obrázek 21 - Konfigurace rozhraní – managed

Zdroj: (Caha, 2020)

Obrázek 22 - Zapnutí monitorovací módu na rozhraní wlan0

Zdroj: (Caha, 2020)

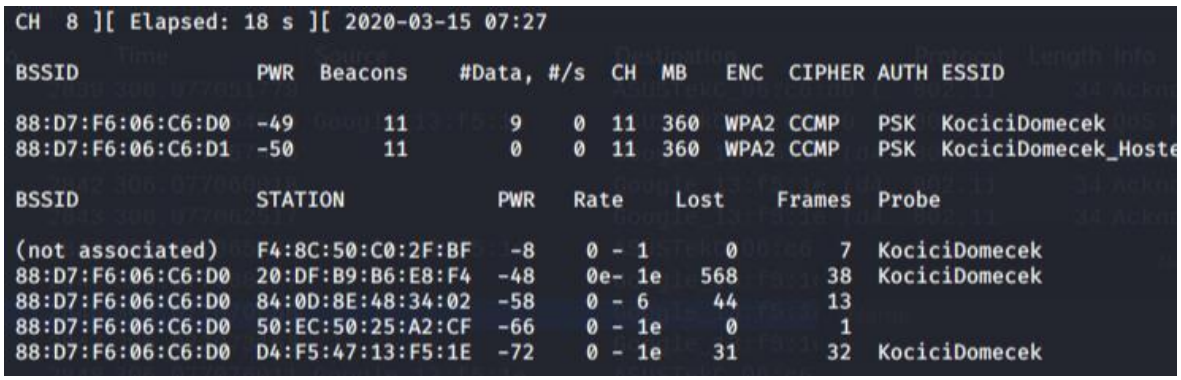
Obrázek 23 - Zapnutý monitorovací režim



Zdroj: (Caha, 2020)

S využitím příkazu *airodump-ng* je následně možné provést záchyt provozu. Díky zapnutému monitorovacímu režimu odposlouchává síťová karta veškerý provoz, který zachytí (Obrázek 24).

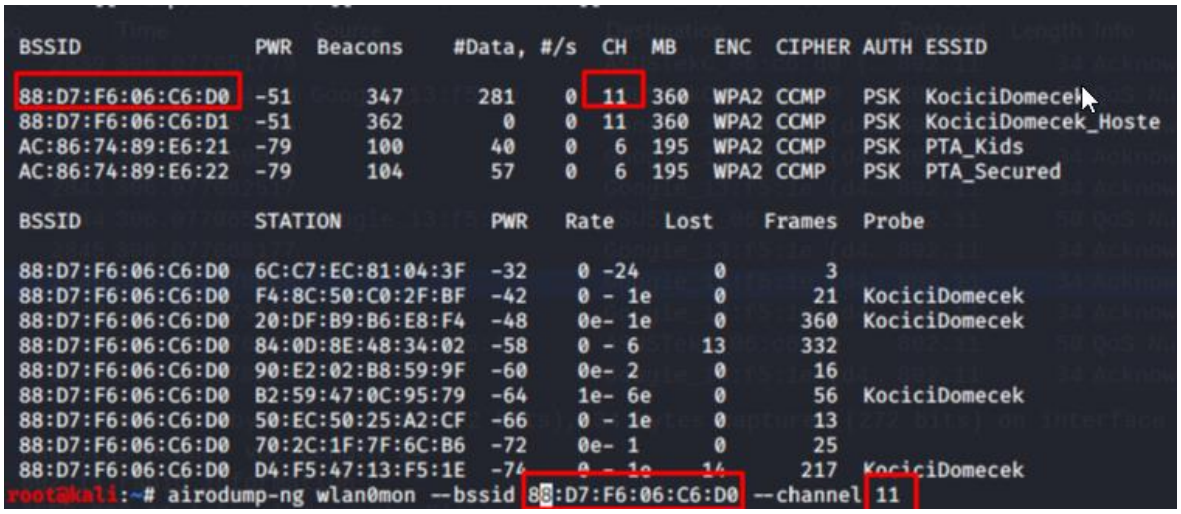
Obrázek 24 - Airodump - 18 sekund



Zdroj: (Caha, 2020)

Množství zachycených paketů se zvedá s časem, proto při delším běhu *airodump-ng*, je možné zachytit i komunikaci s AP vysílající SSID *PTA_Secured* a *PTA_kids* (Obrázek 25),

Obrázek 25 - Airodump - 2 minuty

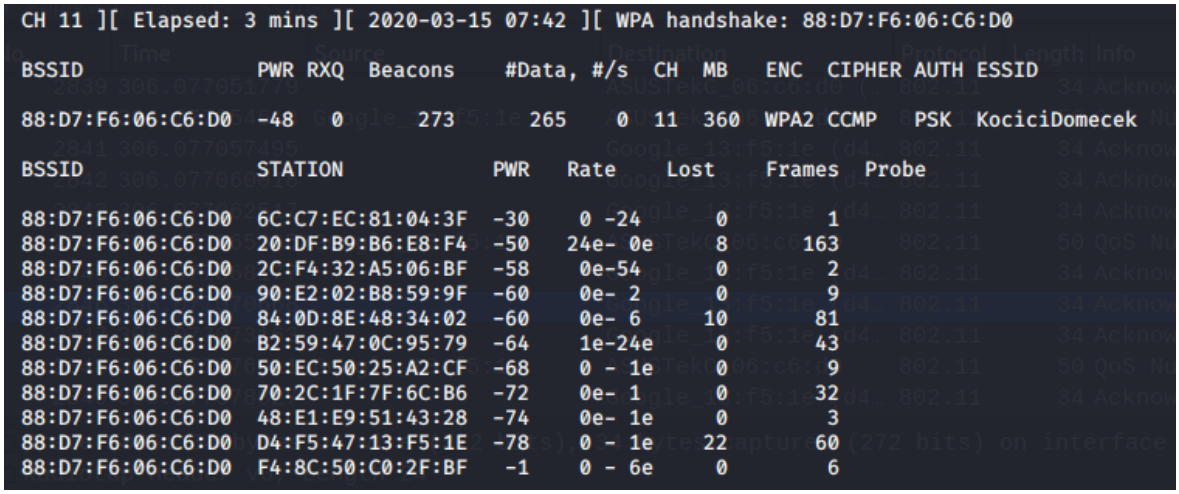


Zdroj: (Caha, 2020)

který je vzdálen od stanice, na které záchyt probíhal přibližně 30 metrů.

Pro další analýzu provozu byl sledován pouze provoz vybraného AP (BSSID) a kanálu, na kterém AP běží. Příkaz, který byl použit je vidět na spodní části obrázku výše (Obrázek 25) (*airodump-ng wlan0mon --bssid 88:D7:F6:06:C6:D0 --channel 11*). Po spuštění filtrování sledování provozu pouze daného kanálu je možné dostat data podobným těm na následujícím obrázku (Obrázek 26):

Obrázek 26 - Airodump na konkrétní kanál a BSSID



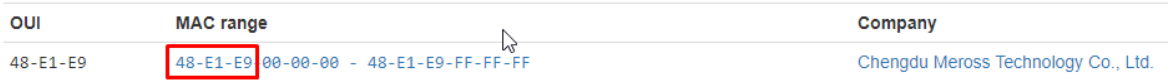
Zdroj: (Caha, 2020)

Horní část výše uvedeného obrázku (Obrázek 26) zobrazuje MAC adresu AP, kterou sledujeme (BSSID), v dolní části jsou zobrazeny ve sloupci STATION MAC adresy jednotlivých zařízení, které s AP komunikují. Kromě síly signálu, je zde vidět i počet zachycených rámců.

Pro zjištění příslušných MAC adres a jejich přiřazení konkrétním zařízením je možné využít administrátorského rozhraní směrovače (pokud má útočník k tomuto zařízení přístup) nebo lze prostá analýza zařízení provést rozkladem fyzické adresy.

S využitím některého z online nástrojů, například https://macaddress.io/ je možné zjistit výrobce. Tyto veřejné databáze pracují s OUI identifikátory a pokud je v síti pouze jedno zařízení daného výrobce, jeho identifikace je triviální. Na obrázku níže (Obrázek 27)

Obrázek 27 - OUI 48-E1-E9



Zdroj: (Caha, 2020)

je identifikováno zařízení od společnosti Chengdu Meross Technology Co., Ltd.. Jedná se o výrobce vybraného zařízení pro vzdálené ovládání garážových vrat.

Vzhledem k tomu, že na obrázku výše (Obrázek 26) je možné pozorovat, že komunikace dané BSSID používá zabezpečení WPA2 PSK, bude zachycená komunikace šifrována. WPA2 používá symetrickou blokovou šifru AES Rijndael a k jejímu dešifrování

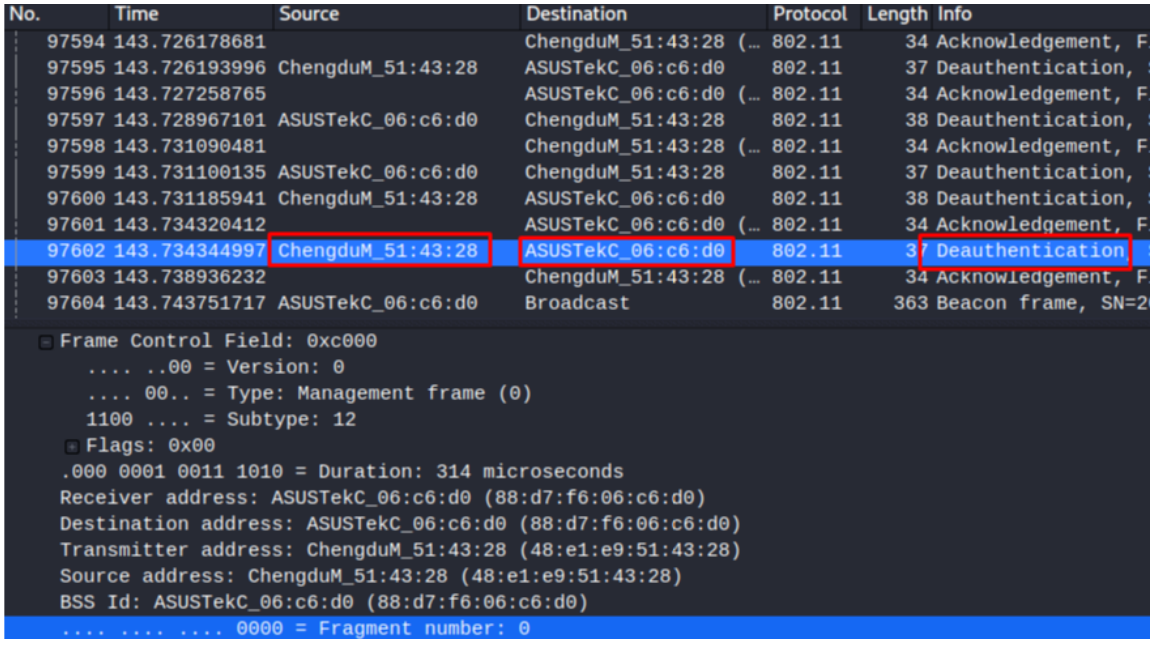
je nutný klíč. Na dobře zabezpečené síti by nyní nebylo možné pokračovat, nicméně nástroje Aircrack umí zaslat deautentizační pakety, které přimějí klienta se od daného AP odpojit a následně, při opětovném navázání spojení mezi klientem a AP, zachytit WPA handshake, z něhož je možné získat hash používaného hesla. Za pomoc technik uvedených v teoretické části práce je následně možné heslo získat. Zaslání deautentizačních paketů je zachyceno na obrázku (Obrázek 28) níže.

Obrázek 28 - Zaslání deautentizačních paketů

```
root@kali:~# aireplay-ng --deauth 5 -c 20:DF:B9:B6:E8:F4 -a 88:D7:F6:06:C6:D0 wlan0mon
12:31:01  Waiting for beacon frame (BSSID: 88:D7:F6:06:C6:D0) on channel 11
12:31:05  Sending 64 directed DeAuth (code 7). STMAC: [20:DF:B9:B6:E8:F4] [26|60 ACKs]
12:31:06  Sending 64 directed DeAuth (code 7). STMAC: [20:DF:B9:B6:E8:F4] [11|61 ACKs]
12:31:06  Sending 64 directed DeAuth (code 7). STMAC: [20:DF:B9:B6:E8:F4] [23|57 ACKs]
12:31:07  Sending 64 directed DeAuth (code 7). STMAC: [20:DF:B9:B6:E8:F4] [ 2|56 ACKs]
12:31:07  Sending 64 directed DeAuth (code 7). STMAC: [20:DF:B9:B6:E8:F4] [ 0|62 ACKs]
```

Na následujícím obrázku (Obrázek 29) jsou vyobrazeny deautentizační pakety, jak jsou interpretovány na straně programu Wireshark.

Obrázek 29 - Deautentizační pakety interpretovány programem Wireshark

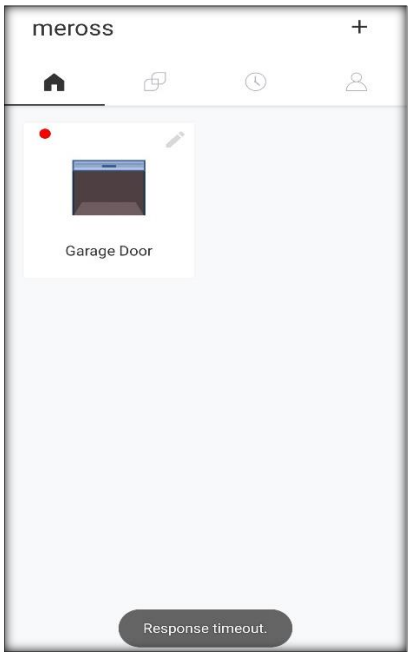


Zdroj: (Caha, 2020)

Zdali se zařízení skutečně odpojuje bylo otestováno pomocí pokusu spustit akci (otevřít / zavřít garážová vrata) z aplikace, kterou se zařízení ovládá. Při zasílání

deautentizačních paketů zařízení neodpovídalo na dotazy a žádosti o změnu stavu (Obrázek 30). Po zastavení zasílání paketů způsobující odhlašování od sítě, se spojení opětovně navázalo.

Obrázek 30 - Meross – výpadek při zasílání deautentizačních paketů



Zdroj: (Caha, 2020)

Po identifikaci zařízení Meross byl spuštěn program Wireshark, program s grafickým uživatelským prostředím, který dokáže analyzovat síťový provoz na úrovni jednotlivých paketů.

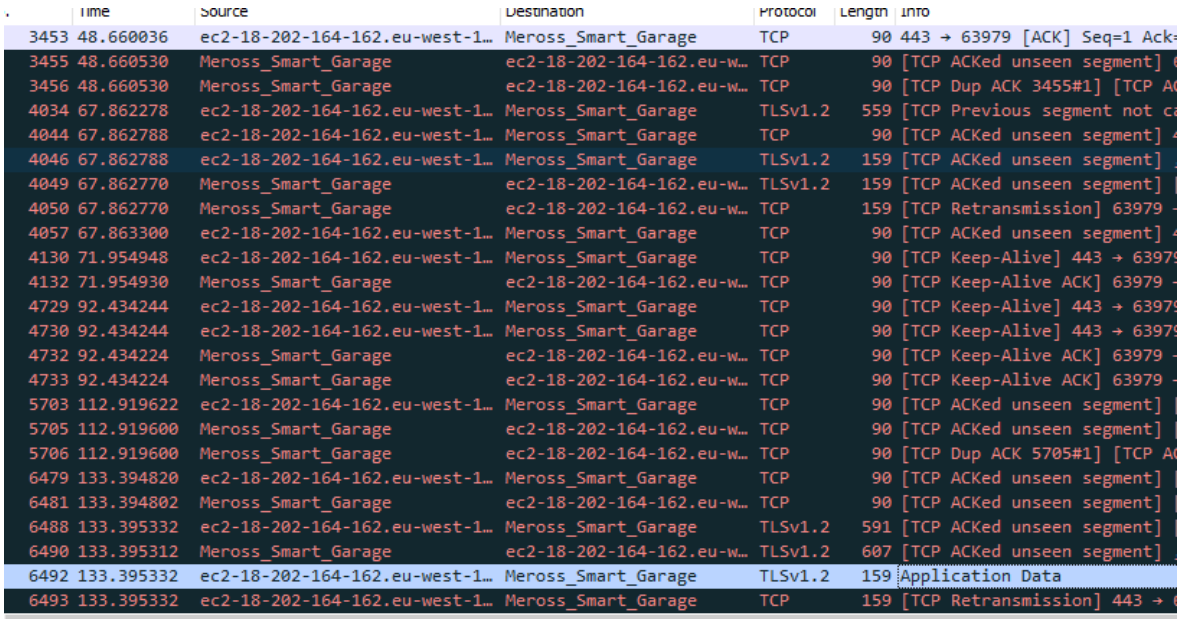
Jelikož byl provoz odposloucháván základní síťovou kartou, která navíc pracovala v monitorovacím režimu a byla poměrně vzdálená od AP a daného zařízení, není záchyt úplný, nicméně pro zběžnou představu, jakým způsobem a kam zařízení komunikuje, je záchyt plně dostačující.

Záchyt událostí běžel několik minut, během této doby bylo, stejně jako i pro ostatní testovaná zařízení, zachyceno stovky až tisíce paketů.

Na obrázku (Obrázek 29) lze pozorovat, že veškeré pakety mají protokol 802.11, je to z důvodu šifrování provozu pomocí WPA2. S využitím znalosti klíče a zachycení čtyřcestného handshaku (díky deautentizačním paketům) můžeme provoz na protokolu 802.11 zpětně dešifrovat.

Po zadání šifrovacího klíče v programu Wireshark bylo detekováno TCP spojení mezi zařízením a IP adresou, která odpovídá AWS cloudu, kde běží infrastruktura společnosti Meross. Meross zařízení komunikuje s cloudovou službou, využívá protokol MQTT over HTTP a MQTT broker běžící ve společnosti Amazon. Po jeho zapnutí bylo možné detekovat pokusy o spojení na servery Amazonu. Spojení mezi zařízením a cloudem probíhá šifrovaně, MQTT využívá TLSv1.2 (Obrázek 31).

Obrázek 31 - Šifrovaná komunikace mezi zařízením Merros a AWS

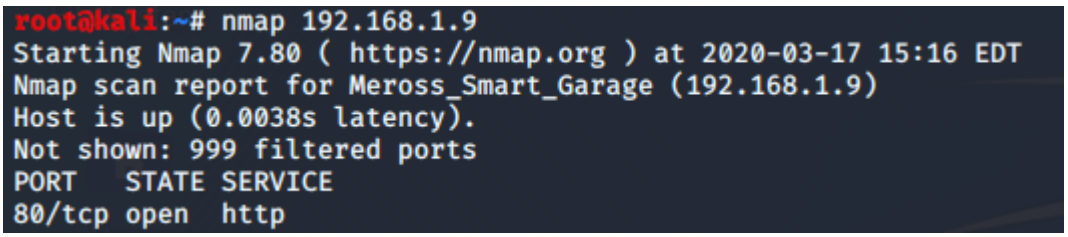


.	Time	Source	Destination	Protocol	Length	Info
3453	48.660036	ec2-18-202-164-162.eu-west-1…	Meross_Smart_Garage	TCP	90	443 → 63979 [ACK] Seq=1 Ack=
3455	48.660530	Meross_Smart_Garage	ec2-18-202-164-162.eu-w…	TCP	90	[TCP ACKed unseen segment]
3456	48.660530	Meross_Smart_Garage	ec2-18-202-164-162.eu-w…	TCP	90	[TCP Dup ACK 3455#1] [TCP A
4034	67.862278	ec2-18-202-164-162.eu-west-1…	Meross_Smart_Garage	TLSv1.2	559	[TCP Previous segment not c
4044	67.862788	ec2-18-202-164-162.eu-west-1…	Meross_Smart_Garage	TCP	90	[TCP ACKed unseen segment]
4046	67.862788	ec2-18-202-164-162.eu-west-1…	Meross_Smart_Garage	TLSv1.2	159	[TCP ACKed unseen segment]
4049	67.862770	Meross_Smart_Garage	ec2-18-202-164-162.eu-w…	TLSv1.2	159	[TCP ACKed unseen segment]
4050	67.862770	Meross_Smart_Garage	ec2-18-202-164-162.eu-w…	TCP	159	[TCP Retransmission] 63979
4057	67.863300	ec2-18-202-164-162.eu-west-1…	Meross_Smart_Garage	TCP	90	[TCP ACKed unseen segment]
4130	71.954948	ec2-18-202-164-162.eu-west-1…	Meross_Smart_Garage	TCP	90	[TCP Keep-Alive] 443 → 6397
4132	71.954930	Meross_Smart_Garage	ec2-18-202-164-162.eu-w…	TCP	90	[TCP Keep-Alive ACK] 63979
4729	92.434244	ec2-18-202-164-162.eu-west-1…	Meross_Smart_Garage	TCP	90	[TCP Keep-Alive] 443 → 6397
4730	92.434244	ec2-18-202-164-162.eu-west-1…	Meross_Smart_Garage	TCP	90	[TCP Keep-Alive] 443 → 6397
4732	92.434224	Meross_Smart_Garage	ec2-18-202-164-162.eu-w…	TCP	90	[TCP Keep-Alive ACK] 63979
4733	92.434224	Meross_Smart_Garage	ec2-18-202-164-162.eu-w…	TCP	90	[TCP Keep-Alive ACK] 63979
5703	112.919622	ec2-18-202-164-162.eu-west-1…	Meross_Smart_Garage	TCP	90	[TCP ACKed unseen segment]
5705	112.919600	Meross_Smart_Garage	ec2-18-202-164-162.eu-w…	TCP	90	[TCP ACKed unseen segment]
5706	112.919600	Meross_Smart_Garage	ec2-18-202-164-162.eu-w…	TCP	90	[TCP Dup ACK 5705#1] [TCP A
6479	133.394820	ec2-18-202-164-162.eu-west-1…	Meross_Smart_Garage	TCP	90	[TCP ACKed unseen segment]
6481	133.394802	Meross_Smart_Garage	ec2-18-202-164-162.eu-w…	TCP	90	[TCP ACKed unseen segment]
6488	133.395332	ec2-18-202-164-162.eu-west-1…	Meross_Smart_Garage	TLSv1.2	591	[TCP ACKed unseen segment]
6490	133.395312	Meross_Smart_Garage	ec2-18-202-164-162.eu-w…	TLSv1.2	607	[TCP ACKed unseen segment]
6492	133.395332	ec2-18-202-164-162.eu-west-1…	Meross_Smart_Garage	TLSv1.2	159	Application Data
6493	133.395332	ec2-18-202-164-162.eu-west-1…	Meross_Smart_Garage	TCP	159	[TCP Retransmission] 443 →

Zdroj: (Caha, 2020)

Následně byl proveden test otevřených portů pomocí programu nmap (Obrázek 32). Zařízení má otevřen pouze port 80, na kterém běží při prvním zapojení webový server, který slouží pro konfiguraci. Poté se zařízení restartuje, port 80 zůstává otevřen i nadále, nicméně již na něm žádná aplikace neběží.

Obrázek 32 - Sken portů pro zařízení Meross



(Caha, 2020)

Zařízení Sonoff

Zařízení Sonoff, stejně jako Meross, dle dokumentace uvádí, že používají servery společnosti Amazon a dle provedeného záchytu je možné tuto informaci potvrdit. Smart žárovka B1 i chytrý vypínač osvětlení Sonoff Mini používají ke svému chodu servery společnosti Amazon. Během testování bylo zařízení odpojeno od napájení, následně restartováno, byla použita aplikace eWeLink i Google Assistant k jejich spínání, avšak nepodařilo se zachytit komunikaci k žádným jiným serverům.

Společnost Sonoff používá k výrobě svých zařízení ESP moduly, což je často používaný WiFi modul, který do jisté míry pomohl rozmachu IoT, nejen na poli hobbistů, ale vzhledem k nízké ceně i na profesionální úrovni (SOS Distribuce elektronických součástek, 2017).

Právě díky využití často používaného modulu od společnosti Espressif je možné využít alternativní software Tasmota (GitHub, 2020), díky čemuž je možné zařízení přeinstalovat a využívat alternativní firmware. Následně je možné využít alternativní MQTT broker, a vyhnout se tak komunikaci zařízení do Internetu a na servery společnosti Sonoff. Společnost Sonoff v nově vyráběných verzích svých zařízení dokonce umožňuje přehrání firmware zařízení nikoli přes připojení přes sériovou linku, ale přes webové rozhraní. DYI možnost uvádí i jako oficiální cestu na svých webových stránkách. Dle některých uživatelů je cesta stále poněkud obtížná (DrZss, 2019), ale alternativní přístup s nevynucováním využití serverů výrobce je z pohledu bezpečnosti správná cesta. Navíc pro společnost Sonoff odpadá nutnost udržování cloudových služeb.

Záchyt je uveden v příloze (Příloha A).

Sken portů odhalil na zařízení Sonoff Mini otevřený TCP port 8081, který pravděpodobně slouží pro službu iotbrokeru. Ačkoliv nmap jej detekoval jako

blackice-icecap, IDS od společnosti ICE Network se již dlouhou dobu nepoužívá a běh na ESP čipech je nepravděpodobný. Při analýze, jaké služby port 8081 v prostředí IoT používají bylo zjištěno, že port 8081 používá administrátorské rozhraní ioBrokeru (ioBroker, 2020). Nepodařilo se ověřit, zdali port 8081 je skutečně připraven pro využití ioBrokeru v režimu DIY, ale funkční předpoklady k tomu jsou.

Xiaomi Mi Home Security Camera

Z pohledu závažnosti bezpečnostního incidentu se narušení soukromí při problémech s kamerovým systémem může rovnat problémům s ovládáním garážových vrat či dveřních zámků. Ať bude kamera používána jako domácí chůvička, k dozoru starších osob nebo pro ochranu majetku, možné zneužití získaných dat je nebezpečné a závažné.

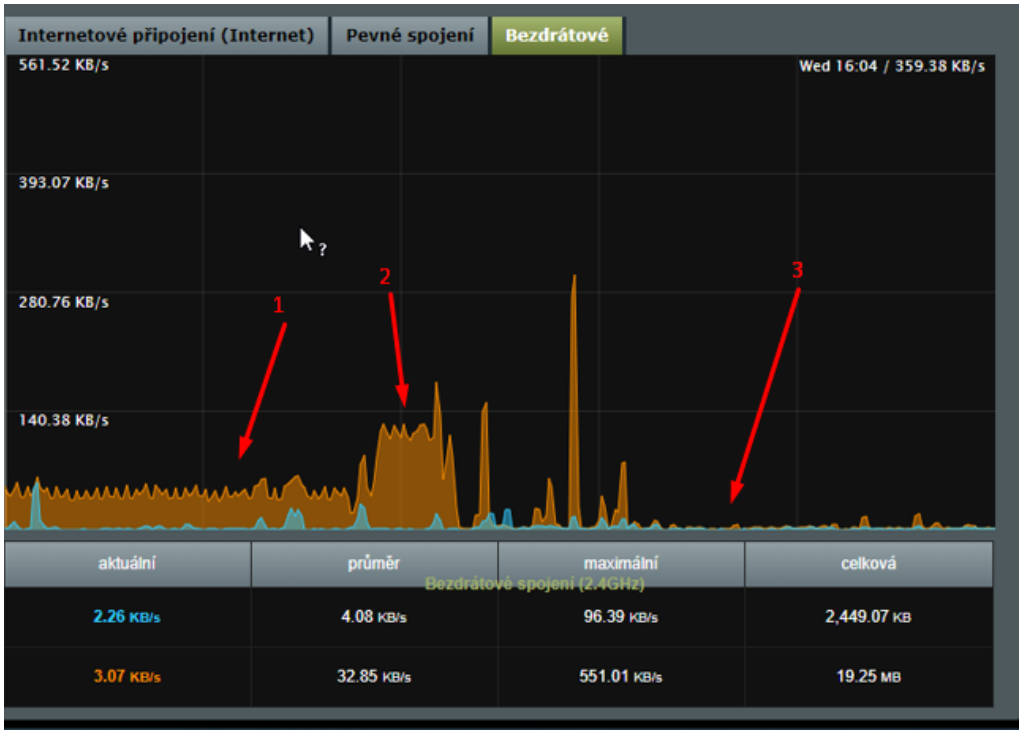
Během testování se bohužel z neznámého důvodu nepodařilo odchytit provoz Xiaomi kamery. Pomocí paket sniffingu nebyly zachyceny pakety přicházející do či ze zařízení, jako v předcházejících případech. Stejně jako v předchozích případech byla kamera během testování restartována, byly prováděny změny konfigurace, byl streamován kamerový záběr, avšak přes veškeré úsilí se žádný provoz zachytit nepodařilo.

Pomocí analyzátoru provozu na použitém směrovači Asus RT-AC58U, byla ověřena z pohledu bezpečnosti patrně nejdůležitějších informace, zdali kamera někam neustále streamuje snímaný záznam či nikoli. Dle výsledků se zdá, že kamera neposílá téměř žádná data v době, kdy obraz z ní není aktivně sledován. Dle dostupných informací na oficiálních stránkách výrobce a provedené analýzy provozu, kamera ukládá záznam lokálně a při zaznamenání pohybu pomocí PIR čidla dojde k vyvolání dat z lokálního úložiště kamery, čímž se minimalizuje datový tok a data zůstávají uložena lokálně bez nutnosti je kamkoli odesílat. Data jsou tak ze zařízení odesílána pouze v případě zapnutí aplikace pro sledování záznamu či po zaznamenání pohybu, aby se uložila do cloudu společnosti Xiaomi.

Při testování byly odzkoušeny i různé režimy rozlišení, které kamera nabízí – v případě použití rozlišení 1920 * 1080 pixelů odpovídá datový tok na obrázku níže (Obrázek 33) v grafu pozici 2, při přepnutí do nízkého rozlišení (640 * 480) pozici 1 a při vypnutí streamování do mobilního telefonu pozici 3.

Kameru Xiaomi lze využívat i bez připojení ke cloudu, lokálně. Nicméně uživatel tím ztrácí některé výhody, které kamera nabízí (například online úložiště zaznamenaných nahrávek) a také možnost sledovat přenos z Internetu.

Obrázek 33 - Datový tok při použití kamery Xiaomi



Zdroj: (Caha, 2020)

Obrázek 34 - Nmap sken Xiaomi kamera

```
Nmap scan report for chuangmi_camera_ipc009 (192.168.1.150)
Host is up (0.034s latency).
All 1000 scanned ports on chuangmi_camera_ipc009 (192.168.1.150) are closed
MAC Address: 50:EC:50:25:A2:CF (Beijing Xiaomi Mobile Software)
```

Zdroj: (Caha, 2020)

Sken portů (Obrázek 34) neodhalil žádné otevřené porty na kameře.

4.5.2 **Kontrola z databází zranitelností**

Ke kontrole zranitelností je využito databáze NIST (National Institute of Standards and Technology), institut stojící při americkém ministerstvu obchodu vydává mimo jiné

standardy ohledně šifrování a bezpečnosti internetu (National Institute of Standards and Technology, 2020). Další testované databáze zranitelností dostupné na internetu CVE (https://cve.mitre.org/index.html) nebo CVEDetails.com (https://www.cvedetails.com/) obsahovaly pro vybraná zařízení stejné zranitelnosti.

Meross Smart Wi-Fi Garage Door Opener

Zařízení Meross Garage Door Opener v databázích žádnou zranitelnost nemá, nicméně chytrá zásuvka Smart Plug od téže společnosti byla zranitelná v roce 2018 dvěma způsoby. První zranitelnost se týká možnosti přihlášení se do administrátorského rozhraní bez nutnosti ověření přes telnet na portu 23. Druhá zranitelnost popisuje možnost získání admin.htm rozhraní bez nutnosti jakéhokoli ověření. Zranitelnosti byly s aktualizací firmware odstraněny. Port 23, který byl u první jmenované zranitelnosti využit pro telnet připojení a dle technické dokumentace byl otevřený i na dalších zařízeních společnosti Meross, již na testovaném Garage Openeru otevřen není.

Ani jedna dostupná zranitelnost se netýkala testovaného zařízení, nicméně jednalo se o problémy, které jsou obecného charakteru a mohly by se objevovat i na dalších zařízeních od stejného výrobce.

Zařízení Sonoff

V době přípravy této závěrečné práce nebyly známy žádné zranitelnosti na zařízeních Sonoff. Výjimku tvoří popsaná XSS zranitelnost (CVE-2020-7470) uveřejněná na konci ledna 2020. V tomto případě se však jedná pouze chybu v alternativním firmware Tasmota, o kterém byla řeč v teoretické části práce.

Analýzu zařízení Sonoff Switch provedl i Dennis Henke a výsledky uvedl na serveru *IoTTests.org* (Henke, 2018). Uvádí problém především v detailním logováním do souboru, který je uložen v adresáři, kam má přístup běžný uživatel. V souboru jsou ve formě prostého textu uloženy i senzitivní data jako jsou uživatelská jména a hesla, klíče API a tokeny. Uvádí taky zaznamenanou nešifrovanou komunikaci po ukončení aplikace.

V rámci testování aplikace se podobné chování nasimulovat nepodařilo, ale vzhledem k tomu, že článek je starý přibližně dva roky a Henke neuvádí verzi firmware ani aplikace, je možné, že výrobce v některé z následných aktualizací chyby odstranil.

Xiaomi Mi Home Security Camera

Během testování zranitelností se nepodařilo objevit žádné oficiálně zaznamenané zranitelnosti, nicméně veřejně dostupná zranitelnost na této kameře byla motivací k této práci. Detaily ohledně zranitelnosti jsou uvedeny v teoretické části této práce.

Dohledatelných zranitelností pro zařízení Xiaomi je velká řada, nicméně většina z nich se týká mobilních telefonů.

5 Závěr

Hlavním cílem této závěrečné práce bylo analyzovat na jaké úrovni se nachází stav kybernetické bezpečnosti Internetu věcí, především produktů, které jsou aktuálně prodávány v České republice na trhu s IoT.

Dílčím cílem bylo porovnání inzerované bezpečnosti IoT produktů se zkušenostmi reálných uživatelů a databázemi zranitelností. Posledním cílem bylo prozkoumání Zákona o kybernetické bezpečnosti v návaznosti na problematiku informační bezpečnosti Internetu věcí.

V teoretické části se práce věnuje vymezení pojmu informační bezpečnost, ochraně a bezpečnosti hesla a postupům, jak správně postupovat při odesílání a ukládání osobních či citlivých dat jako jsou uživatelská jména či hesla do databází. V další části je objasněn pojem Internet věcí. V této části se mimo historie IoT věnuje práce i principům IoT, je vysvětlena podstata IoT ekosystému a jsou předneseny hlavní výhody a nevýhody využití IoT, jak v domácnosti, tak v průmyslovém nasazení. Ze zjištěných informací vyplývá, že mezi hlavní výhody se řadí například úspora času a peněz, zjednodušení a zlepšení obchodních rozhodnutí či zvýšení produktivity zaměstnanců. Mezi zjištěné nevýhody patří otázka bezpečnosti. S narůstajícím počtem zařízení komunikujících po síti se zvedá i pravděpodobnost s problémy týkající se nejen bezpečnosti.

V další části práce přibližuje technologické základy, které napomohly k rychlému rozvoji IoT, či objasňují fungování některých částí IoT ekosystému. Technologickým milníkem v rozvoji Internetu věcí byl příchod protokolu IPv6, který zásadním způsobem rozšiřuje adresovatelný prostor IP protokolu. Teoretická část nadále vysvětluje pojmy MQTT a IFTTT. MQTT je protokol pro komunikaci IoT zařízení, který funguje na modelu klient a server. IFTTT je zkratkou *If This Then That*, jedná se o platformu sloužící pro automatizaci projektů. API nejrůznějších služeb umožňuje jejich zprostředkování přes platformu IFTTT, a díky tomu je možné automatizovat procesy nejen IoT zařízení.

Jeden z dílčích cílů této práce byl výklad Zákona o kybernetické bezpečnosti v souvislosti s používáním IoT. Během analýzy však bylo zjištěno, že Zákon má jasně definovanou množinu subjektů, které jsou jím řízeny a výrobci IoT zařízení k těmto subjektům převážně nepatří. Z toho důvodu nebyl nadále Zákon v této práci diskutován.

Praktická část obsahuje dotazník, na který odpovědělo 30 respondentů a výsledky šetření se shodují s poznatky z teoretické rešerše. Kvalita hesla se v posledních 10 letech nezlepšila a nejpoužívanějším heslem je nadále 123456. 25 z 27 dotazovaných odpovědělo, že heslo na jejich domácí WiFi síť je tvořeno méně než 9 znaky, 3 se zdrželi. Dvě třetiny všech respondentů odpověděly, že jejich heslo je tvořeno pouze písmeny a čísly. 16 dotázaných odpovědělo, že neví, co znamená dvoufaktorové ověřování a pouze 5 dotázaných odpovědělo, že jej používá.

Další část praktické části je zaměřena na průzkum českého trhu se zaměřením na IoT zařízení. Jsou představeni zástupci jednotlivých kategorií z opačných stran cenového portfolia. Následně jsou vybrány zástupci z kategorií osvětlení, kamer a zařízení k ovládání garážových vrat, kteří jsou otestovány.

Testování zařízení je provedeno pomocí záchytu a analýze jejich datového provozu a oskenování portů zařízení. Druhá část spočívala ve vyhledání známých zranitelností ve veřejných databázích jako CVEDetails či NIST na testovaných a podobných zařízeních.

Ačkoliv u žádného z testovaných zařízení nebyla zjištěna zásadní bezpečnostní pochybení a výrobci se drží deklarovaných informací o produktu, všechna testovaná zařízení či jejich předchůdci nebo podobné výrobky se bezpečnostních pochybení čas od času dopouštějí. Ta bývají méně či více závažná a mohou či nemusí způsobovat problémy pro koncové uživatele.

Jedno z nejzávažnějších pochybení, kterých se však výrobci IoT zařízení v posledních letech dopustili, způsobila společnost Xiaomi s testovanou kamerou. Jeden z uživatelů reportoval závažné pochybení, ovlivňující zásadním způsobem soukromí uživatelů. Jednalo se o přenos videozáznamu jiným uživatelům.

Informační bezpečnost je rychle rozvíjející se obor, který stínuje a doprovází obor informačních technologií, avšak dle nabytých a získaných informací týkajících se bezpečnosti Internetu věcí, lze prohlásit, že bezpečnost IoT zařízení neodpovídá vždy očekávané a potřebné kvalitě. U testovaných zařízení sice nebyly objeveny žádné aktuální problémy, nicméně dle veřejně dostupných informací, u IoT zařízení k méně či více závažným bezpečnostním incidentům dochází. Obecně se za největší problém dá považovat nedostatečná míra aktualizací odstraňující objevené incidenty, a především nejistota dalších aktualizací poskytovaných výrobcem po dobu delší, než je záruční doba produktu.

Výzkum potvrzuje názor, že s příchodem nových zařízení se bude měnit svět, množství vyráběných druhů IoT zařízení neustále roste a dle zjištěného, bezpečnost není vždy ideální, ba dokonce dostatečná. V příštích letech bude muset být otázka bezpečnosti soukromí a integrity dat řešena s čím dál větším důrazem, jinak může dojít k zásadním problémům s ochranou soukromí a bezpečnosti koncových uživatelů.

V následujících letech je plánem závěrečnou práci rozšířit o otestování dalších prvků a provedení kompletního paketového záchytu a následné analýzy pomocí nástrojů společnosti IBM QRadar Incident Forensics a pomocí specializovaného nástroje na analýzu síťového provozu od společnosti Flowmon.

6 Seznam použitých zdrojů

100 Worst Passwords of 2019 is now available! [online]. 2019. [cit. 2020]. Dostupné z: https://www.teamsid.com/100-worst-passwords/

40 nejpoužívanějších hesel [online]. 2014. [cit. 2020]. Dostupné z: https://jecas.cz/nejcastejsi-hesla

41.6 billion IoT devices will be generating 79.4 zettabytes of data in 2025. 2019. In: *HelpNetSecurity.com* [online]. [cit. 2020]. Dostupné z: https://www.helpnetsecurity.com/2019/06/21/connected-iot-devices-forecast/

6LoWPAN | ZigBee | 6LoWPAN Vs ZigBee [online]. 2019. [cit. 2020]. Dostupné z: https://iotbyhvm.ooo/6lowpan-zigbee/

6LoWPAN: The wireless embedded Internet [online]. 2011. [cit. 2020]. Dostupné z: https://www.eetimes.com/6lowpan-the-wireless-embedded-internet-part-2-6lowpan-history-market-perspective-applications/?utm_source=eetimes&utm_medium=networksearch

Auth0 [online]. 2018. [cit. 2020]. Dostupné z: https://auth0.com/blog/adding-salt-to-hashing-a-better-way-to-store-passwords/

BROWN, Scott. 2020. *Xiaomi fully resolves its creepy security cam bug (Updated)* [online]. [cit. 2020]. Dostupné z: https://www.androidauthority.com/google-nest-hub-security-bug-1070840/

CAHA, Adam. 2020. *Vlastní zdroj vytvořen za účelem diplomové práce Bezpečnost IoT*.

Compare and contrast OSI and TCP/IP models [online]. 2018. [cit. 2020]. Dostupné z: https://clinetworking.files.wordpress.com/2018/06/tcp-ip-model-vs-osimodel.png

ČESKO. 2014. *Zákon č. 181/2014 Sb.*. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

ČÍŽEK, Jakub. 2016. *Pojďme programovat elektroniku: Pošleme zprávu na desítky kilometrů daleko díky síti Sigfox* [online]. [cit. 2020]. Dostupné z: https://www.zive.cz/clanky/pojdme-programovat-elektroniku-posleme-zpravu-na-desitky-kilometru-daleko-diky-siti-sigfox/sc-3-a-185097/default.aspx

Difference Between Star and Mesh Topology [online]. 2018. [cit. 2020]. Dostupné z: https://techdifferences.com/difference-between-star-and-mesh-topology.html

DRZSS. 2019. *Sonoff NEW DIY Mode easier Tasmota flashing | home automation* [online]. [cit. 2020]. Dostupné z: https://www.youtube.com/watch?v=fsrT5o1C1w0

GEBER, Anna. 2018. *Connecting all the things in the Internet of Things* [online]. [cit. 16]. Dostupné z: https://developer.ibm.com/articles/iot-lp101

GOLL, Jan. 2019. *Zákon o kybernetické bezpečnosti versus ISO 27001* [online]. [cit. 2020]. Dostupné z: http://m.systemonline.cz/sprava-it/zakon-o-kyberneticke-bezpecnosti-versus-iso-27001.htm

HALLER STEPHAN a A KOL.. 2009. *The Internet of Things in an Enterprise Context.* [online]. [cit. 2020]. Dostupné z: https://papers.duckdns.org/files/2008_FIS2008.pdf

Hashovací funkce [online]. n. d. [cit. 2020]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7029

HENKE, Dennis. 2018. *Sonoff Basic WiFi* [online]. [cit. 2020]. Dostupné z: https://www.iot-tests.org/2018/06/sonoff-basic-wifi/

Heureka Sonoff B1 [online]. 2020. [cit. 2020]. Dostupné z: https://www.heureka.cz/?h%5Bfraze%5D=SONOFF+B1&min=&max=&o=3

High tech fingerprint lock is, and I quote: "invincible to the people who do not have a screwdriver.." [online]. 2015. [cit. 2020]. Dostupné z: https://imgur.com/gallery/MPOlwkp

HTTP Strict Transport Security (HSTS) [online]. 2018. Dostupné z: https://securityheaders.cz/hsts

https://www.security-portal.cz/clanky/50-nejpou%C5%BE%C3%ADvan%C4%9Bj%C5%A1%C3%ADch-hesel-pro-web-v-%C4%8Dr [online]. 2009. [cit. 2020]. Dostupné z: https://www.security-portal.cz/clanky/50-nejpou%C5%BE%C3%ADvan%C4%9Bj%C5%A1%C3%ADch-hesel-pro-web-v-%C4%8Dr

HYNČICA, Ondřej a Karel PAVLATA. 2006. Bezdrátové komunikační systémy založené na IEEE 802.15.4 v procesní automatizaci. . Dostupné z: http://www.odbornecasopisy.cz/res/pdf/43411.pdf

CHEW, Daniel. 2018. *The Wireless Internet of Things*. IEEE Press, 48-65. ISBN 978-1119260578.

Chrome bude HTTP označovat jako „nezabezpečené“ od července [online]. 2018. Dostupné z: https://www.root.cz/zpravicky/chrome-bude-http-oznacovat-jako-nezabezpecene-od-cervence/

ILASCU, Ionat. 2015. *Smart locks flunk the physical security test* [online]. [cit. 2020]. Dostupné z: https://www.bitdefender.com/box/blog/iot-news/smart-locks-flunk-physical-security-test

ioBroker Automate your Life [online]. 2020. [cit. 2020]. Dostupné z: https://www.iobroker.net/

IoT Agenda - internet of things (IoT) [online]. 2019. [cit. 2020]. Dostupné z: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

Jaká jsou nejpoužívanější hesla na internetu? [online]. 2018. [cit. 2020]. Dostupné z: https://pctuning.tyden.cz/index.php?option=com_content&view=article&id=49949&catid=1&Itemid=57

Jak doma vylepšit signál Wi-Fi: Pomůže repeater, více routerů, ale nejlépe systémy mesh Více na: https://www.zive.cz/clanky/jak-doma-vylepsit-signal-wi-fi-pomuze-repeater-vice-routeru-ale-nejlepe-systemy-mesh/sc-3-a-200720/default.aspx [online]. 2019. [cit. 2020]. Dostupné z: https://www.zive.cz/clanky/jak-doma-vylepsit-signal-wi-fi-pomuze-repeater-vice-routeru-ale-nejlepe-systemy-mesh/sc-3-a-200720/default.aspx

LIXIE. 2019. *How brute-force cracking might reveal your password* [online]. [cit. 2020]. Dostupné z: https://www.expressvpn.com/blog/how-attackers-brute-force-password/

MQTT and CoAP, IoT Protocols [online]. 2014. [cit. 2020]. Dostupné z: https://www.eclipse.org/community/eclipse_newsletter/2014/february/article2.php

MULLIGAN, Geoff. 2007. The 6LoWPAN architecture. [online]. č. 07, s. 78-82 [cit. 2020]. Dostupné z: https://doi.org/10.1145/1278972.1278992

Nabídka, poptávka, cena [online]. n. d. [cit. 2020]. Dostupné z: https://www.miras.cz/seminarky/mikroekonomie-n02-nabidka.php

How to Choose the Right Platform to Run Your Smart Home [online]. 2019. [cit. 2020]. Dostupné z: https://gizmodo.com/how-to-choose-the-right-platform-to-run-your-smart-home-1834808865

NIST [online]. 2020. [cit. 2020]. Dostupné z: https://www.nist.gov/

OECHSLIN, Philippe. 2003. *Making a Faster Cryptanalytical Time-Memory Trade-Off*. Dostupné z: https://lasec.epfl.ch/pub/lasec/doc/Oech03.pdf

První celorepublikový mobilní operátor pro internet věcí [online]. 2020. [cit. 2020]. Dostupné z: https://sigfox.cz/cs

Rainbow Crack - charset. n. d. In: *Rainbow Crack* [online]. [cit. 2020]. Dostupné z: https://project-rainbowcrack.com/charset.txt

Rainbow tables tajemství zbavené [online]. 2015. [cit. 2020]. Dostupné z: https://www.soom.cz/clanky/1165--Rainbow-tables-tajemstvi-zbavene

Referenční model ISO/OSI [online]. 1999. [cit. 2020]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=10010

Salted Password Hashing - Doing it Right [online]. 2019. [cit. 2020]. Dostupné z: https://crackstation.net/hashing-security.htm

SATRAPA, Pavel. 2019. *IPv6*. CZ.NIC. ISBN 978-80-88168-43-0.

Skutečně revoluční IoT moduly ESP od Espressif [online]. 2017. [cit. 2020]. Dostupné z: https://www.soselectronic.cz/articles/espressif/skutecne-revolucni-iot-moduly-esp-od-espressif-1956

Smart Home [online]. 2020. [cit. 2020]. Dostupné z: https://i.alza.cz/Foto/ImgGalery/bannery/v2/ddafe465-dbe3-4bcc-a51f-dff8c72bdca1.jpg

Sonoff Mini [online]. 2020. [cit. 2020]. Dostupné z: https://www.chytrevypinace.cz/Sonoff-Mini-d126.htm

SORRELL, Steffen. 2020. The Internet of Things: Consumer, Industrial & Public Services 2015-2020. In: *Juniper Research* [online]. [cit. 2020]. Dostupné z: https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020

Stronger security for your Google Account [online]. 2020. [cit. 2020]. Dostupné z: https://www.google.com/landing/2step/

ŠKORNIČKOVÁ, Eva. 2017. *Obecné nařízení o ochraně osobních údajů prakticky* [online]. [cit. 2020]. Dostupné z: https://www.gdpr.cz/gdpr

Tasmota [online]. 2020. [cit. 2020]. Dostupné z: https://github.com/arendst/Tasmota

The "Only" Coke Machine on the Internet. n. d. In: *Carnegie Mellon University School of Computer Science* [online]. [cit. 2020]. Dostupné z: https://www.cs.cmu.edu/~coke/history_long.txt

Google WiFi recenze: Rychlý mesh router se skvělým výkonem a jednoduchou obsluhou [online]. 2019. [cit. 2020]. Dostupné z: https://www.svetandroida.cz/google-wifi-recenze/

What is IFTTT? [online]. 2019. [cit. 2020]. Dostupné z: https://help.ifttt.com/hc/en-us/articles/115010325748-What-is-IFTTT-

What is MAC spoofing? [online]. 2017. [cit. 2020]. Dostupné z: https://www.ionos.com/digitalguide/server/know-how/what-is-mac-spoofing/

What is SSL Stripping? A Beginner's Guide to SSL Strip Attacks [online]. 2019. Dostupné z: https://comodosslstore.com/blog/what-is-ssl-stripping-beginners-guide-to-ssl-strip-attacks.html

Z Wave Vs ZigBee: Which Is Better For Your Smart Home? [online]. 2017. [cit. 2020]. Dostupné z: https://thesmartcave.com/z-wave-vs-zigbee-home-automation/

ZACH, Shelby a Bormann CARSTEN. 2009. *6LoWPAN: The Wireless Embedded Interne*. IEEE. ISBN 9780470747995.

ZHENG, J. a J. LEE. 2006. Sensor Network Operations. *A comprehensive performace study of IEEE 802.15.4.* Wiley-IEEE Press. ISBN 0-471-71976-5.

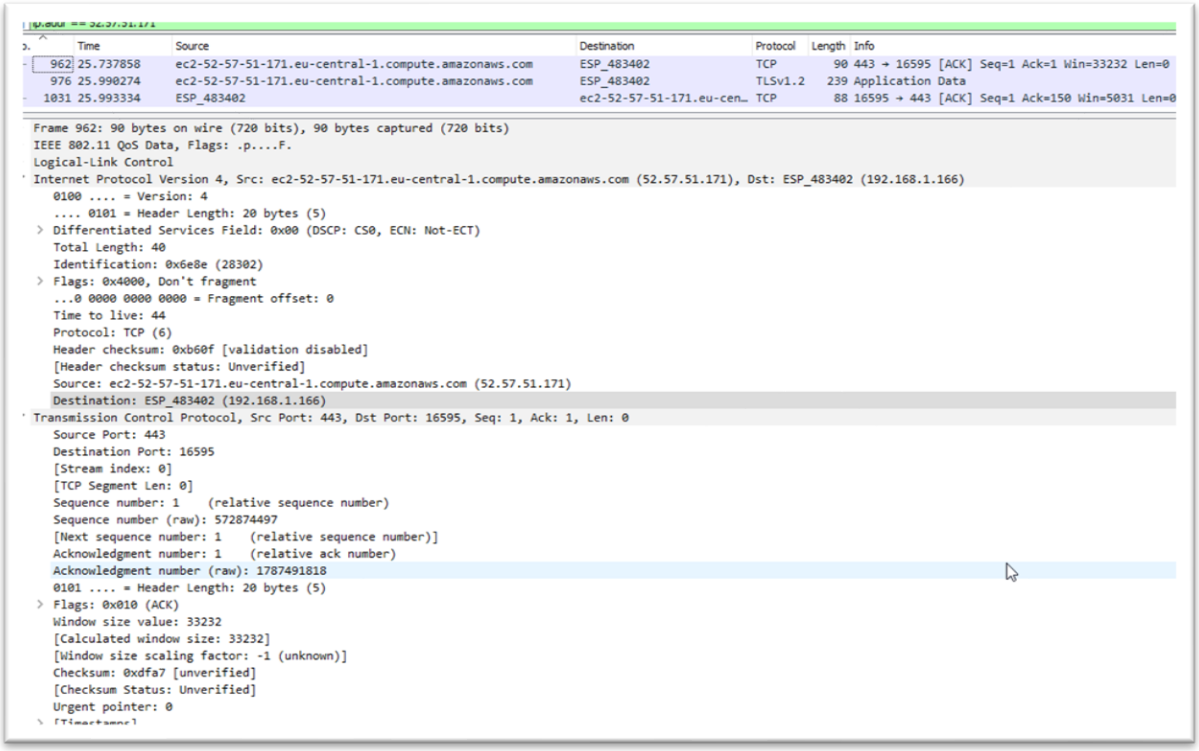
ZibBee [online]. 2018. [cit. 2020]. Dostupné z: https://www.smartroom.cz/zigbee/

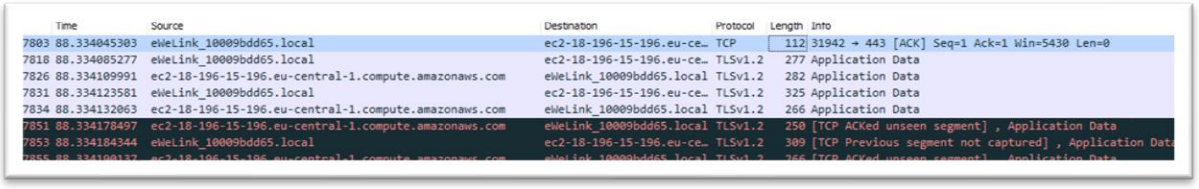
Zigbee Wireless Mesh Networking [online]. 2017. [cit. 2020]. Dostupné z: https://www.digi.com/resources/standards-and-technologies/zigbee-wireless-mesh-networking

7 Přílohy

Příloha A – Záchyt zařízení Sonoff

Příloha A - Záchyt paketů, tcpstream a nmap na zařízení Sonoff






```
Nmap scan report for ESP_A506BF (192.168.1.96)
Host is up (0.025s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
8081/tcp open  blackice-icecap
MAC Address: 2C:F4:32:A5:06:BF (Espressif)
```

```
Nmap scan report for ESP_483402 (192.168.1.166)
Host is up (0.018s latency).
All 1000 scanned ports on ESP_483402 (192.168.1.166) are closed
MAC Address: 84:0D:8E:48:34:02 (Espressif)
```