Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Bezpečnostní hrozby Internet of Things

Pavel Fól

Bakalářská práce
2016

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2015/2016**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Pavel Fól**
Osobní číslo:	**I13119**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Bezpečnostní hrozby internet of things**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Cílem práce je představit modely a přístupy k řešení Internet of things a provést analýzu možných bezpečnostních hrozeb internetu věcí. V teoretické části autor provede rešerši problematiky zabezpečení a bezpečnostních rizik internetu věcí a podrobně představí aktuální modely a řešení oblasti. V praktické části autor provede analýzu možných bezpečnostních rizik systému Internet of things a u vybraných rizik navrhne možnosti jejího řešení.

Rozsah grafických prací:

Rozsah pracovní zprávy: **50**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

*** BEHMANN, Fawzi a Kwok WU. Collaborative internet of things (C-IoT): for future smart connected life and business. 1st edition. Hoboken: John Wiley and Sons, Inc., 2015, pages cm. ISBN 978-111-8913-741.**
*** GEIR, M Koien. Journal of Cyber Security and Mobility 4-1 : Resilient and Trustworthy Iot Systems. 1. United States: River Publishers, 2015. ISBN 9788793237667.**

Vedoucí bakalářské práce: **Mgr. Josef Horálek, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **31. října 2015**
Termín odevzdání bakalářské práce: **13. května 2016**

Univerzita Pardubice Česká republika

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Mgr. Josef Horálek, Ph.D.
vedoucí katedry

V Pardubicích dne 31. března 2016

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 13. 5. 2016 Pavel Fól

Poděkování

Děkuji Mgr. Josefu Horálkovi, Ph.D. za pomoc a cenné rady při zpracování této práce. Dále děkuji mé rodině a blízkým přátelům za trpělivost a podporu při studiu.

ANOTACE

Tato práce se zabývá představením modelů a přístupů k Internet of Things, a to zejména se zaměřením na možnosti zabezpečení. V teoretické části práce je popsáno co je to IoT, jsou představeny vybrané pozitivní i negativní dopady a je provedeno rozdělení na jednotlivé stavební části. Tyto části jsou podrobně rozepsány a pro každou je provedena analýza možností zabezpečení. Na základě zjištěných bezpečnostních hrozeb je v praktické části navrženo zabezpečení komunikační sítě pro chytrou domácnost.

KLÍČOVÁ SLOVA

Internet of Things, bezpečnostní hrozby, bezdrátové sítě, IEEE 802.15.4, zabezpečení

TITLE

Threats to the Internet of Things Security

ANNOTATION

This work deals with various models of and approaches to the Internet of Things, primarily with regards to available security options. The theoretical part describes the IoT itself; furthermore, it details some of its positive and negative impacts and individual types (categories) of devices. These types are then explored in more detail and an analysis of possible security options is carried out for each one of them. Security threats discovered in this section are then used in the practical part to design a secure communication network for a smart home.

KEYWORDS

Internet of Things, Security Threats, Wireless Networks, IEEE 802.15.4, Security

OBSAH

SEZNAM TABULEK, GRAFŮ A ILUSTRACÍ

SEZNAM ZKRATEK A ZNAČEK

IoT	Internet of Things
IoE	Internet of Everything
RFID	Radio-frequency Identification
NFC	Near Field Communication
GSM	Global System for Mobile Communications
GPRS	General Packet Radio Service
3G	Third generation of mobile telecommunications technology
LTE	Long-Term Evolution
GPS	Global Positioning System
IP	Internet Protocol
CIDR	Classless Inter-Domain Routing
IANA	Internet Assigned Numbers Authority
APNIC	Asia Pacific Network Information Centre
RIR	Regional Internet Registry
NAT	Network Address Translation
RFC	Request for Comments
MTU	Maximum Transmission Unit
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, Scientific and Medical
IBSG	Internet Business Solutions Group
ACL	Access Control List
Bluetooth LE	Bluetooth Low Energy
RFC	Request For Comments
RADIUS	Remote Authentication Dial In User Service
HTTP	Hypertext Transfer Protocol

TLS	Transport Layer Security
AES	Advanced Encryption Standard
SDK	Software Development Kit
CAN	Controller Area Network

Úvod

Za posledních několik let je možné pozorovat velký technologický pokrok, který přináší nespočet možností, jak využít všechny nové technologie a případně je i kombinovat. Od doby sálových počítačů již uběhla řada let a aktuálně jsou k dispozici různé počítače, které již nyní při velikosti kreditní karty nabízejí velký výkon a hlavně potenciál, jak je využít. Tyto miniaturní počítače lze nasadit i do míst, kde by to bylo dříve těžce představitelné a realizovatelné.

Různá elektronická zařízení tu však jsou již několik let a nemusí se jednat pouze o počítač, na kterém člověk zpracovává dokumenty do práce, nebo telefon, který kromě volání a odesílání textových zpráv již nějakou dobu dokáže člověka zabavit i jinak a obsahuje mnoho rozšiřujících senzorů. Příležitosti, kdy se člověk setkává s nějakou technologií, jsou na denním pořádku. Například automatické otevírání dveří, digitální termostat nebo váha. Jednoúčelová zařízení, která v podnětu na nějakou akci vyvolají předem definovanou reakci. Dveře se při příchodu otevřou, termostat dá při poklesu teploty pokyn k vytápění a váha při zatížení váží. Nejsou připojena nikam do internetu, nekomunikují s nikým jiným a nesbírají žádná data.

Dnešní technologie již dovolují levně rozšířit i tato jednoúčelová zařízení na chytrá, která dokáží komunikovat s okolním světem a hlavně s ostatními zařízeními. Obecně se trend připojených zařízení do sítě nazývá „Internet of Things“. Výše uvedená zařízení pak mohou fungovat různě. Po příjezdu k domu komunikuje jednotka vozu s vraty a ty se automaticky otevřou. Vrata o této skutečnosti informují termostat a ten se přepíná do optimálního režimu. Po průchodu dveřmi do domu je člověk zvážen integrovanou váhou a ta zasílá naměřené hodnoty do cloudu ke zpracování. Díky tomu je ale nutné čelit novým hrozbám, které se do této doby týkaly pouze osobních počítačů. Zabezpečení samotných zařízení před průnikem je jedna věc. Druhá věc je otázka soukromí a to hlavně toho, jaká data (a o kom) mohou tyto zařízení získávat.

Tato práce se ve svém začátku zabývá představením toho, co to vlastně IoT je, jak je možné tento model využít v různých odvětvích a také jsou uvedeny přínosy, ale i negativa. Dále se zabývá analýzou prvků, které jsou nutné k vytvoření IoT řešení s důrazem zjistit, jaké možnosti zabezpečení nabízí. To vyústí v uvedení bezpečnostních hrozeb, které reálně IoT ohrožují. Nakonec následuje praktická ukázka toho, jak zabezpečit síťovou komunikaci v modelové chytré domácnosti a jaké zásady dodržovat.

1 LITERÁRNÍ REŠERŠE

Obsah této kapitoly se snaží shrnout problematiku samotného Internet of Things (dále IoT) se stručným pohledem na všechny související věci a v neposlední řadě také na bezpečnost. Většina termínů je v detailnější podobě popsána v následujících kapitolách.

Slovní spojení „Internet of Things“ obsahuje hlavně slova „Internet“ a „Things“. Je tedy jasné, že je to spojení Internetu a věcí. Příkladem mohou být fyzické věci, jako jsou zařízení se senzory (snímající teplotu, vlhkost), které získávají různé informace o stavu domácnosti. Pro získání informace z těchto senzorů kdekoliv na světě je potřeba, aby toto zařízení bylo připojeno k internetu a bylo schopné poskytnout data kdykoliv se na ně druhé zařízení dotáže. Pro tyto objekty je možné použít název „smart object“, jak ho používá Kopetz ve své publikaci (2011, s. 307). Samozřejmě řešení je sofistikovanější a mezičlánek mezi konečnými senzory a koncovou aplikací tvoří zařízení, které je schopno data shromažďovat, zpracovávat a poskytovat dále.

Jak by se mohlo zdát, IoT vypadá celkem jako aktuální a nové téma. Opak je však pravdou. Koncept IoT byl popsán již v 90. letech. Termín „Internet of Things“ byl zpopularizován hlavně výrokem, který pronesl Kevin Ashton (FRIEDEMANN, 2010). V této době byly stále ještě technologie dost omezené, proto je možné se domnívat, že za aktuálním rozmachem stojí hlavně technologický pokrok a s tím spojené odstranění bariér pro připojení miliardy nových zařízení.

V dnešní době se předpokládá, že do roku 2020 bude připojeno 50 miliard inteligentních zařízení k síti. Společnosti se zaměřují hlavně na kompletní řešení postavené na chytrých zařízeních. Internet věcí se stává součástí našeho běžného života, kdy vlastníme věcmi ovládaný dům. Nejedná se však pouze o domácí využití. Velký rozmach chytrých řešení je vidět také v některých velkých městech. Toto řešení se pak nazývá „smart cities“, kterým se zabývá například společnost Cisco (MITCHELL, 2013).

Jak již bylo řečeno, pro splnění konceptu IoT je potřeba, aby zařízení komunikovala s okolním světem. V dnešní době již máme na výběr, jak se o to postarat. Díky plynulému přechodu na IPv6 je odbourán nedostatek volných adres, který zde byl díky nedostatečnému adresnímu prostoru v IPv4. Dle firmy Micrium a jejich článku, věnovanému IoT, je dnes stále nejvíce používané připojení hlavně pomocí technologie Ethernet, WiFi a další (2015c). Stejně tak tato firma srovnává nejpoužívanější protokoly užívané pro komunikaci a snaží se o objektivní porovnání. Za zmínku také určitě stojí snažení firmy T-Mobile, která v České republice pilotně

otestovala „SÍŤ PRO INTERNET VĚCÍ“ založenou na přenosu informací pomocí radiových vln v pásmu 868 MHz (T-Mobile, 2015).

Miliardy zařízení aktuálně zapojených do sítě a jejich rychlé rozšiřování by však potřebovalo jednotný standard pro komunikaci mezi sebou. Jak je již běžné, ve světě existuje konkurence v každém odvětví. V odvětví IoT, který má obrovský potenciál, cítí hlavně velké IT společnosti obrovskou příležitost prosadit svá řešení a získat tak většinový podíl na trhu. V této době tedy proti sobě stojí hlavně dvě aliance: Open Connectivity Foundation[1] (OCF) a AllSeen Alliance. Za první zmíněnou aliancí stojí velcí hráči na poli IT a to Intel, Broadcom a Samsung. Spolu s dalšími spojenci, kterými jsou například Cisco, Samsung, Dell, IBM a další, se snaží prosadit své standardy. Zveřejnili přitom první verzi své softwarové základny, která nese název „IoTivity“, je šířená pod open source licencí a poskytuje framework pro poskytování připojení k síti. Za druhou zmíněnou aliancí – AllSeen Alliance – stojí firmy jako Qualcomm, LG, Microsoft, Sharp a další. Stejně jako konkurent, i AllSeen Alliance zveřejnila své vlastní softwarové řešení, kterému dala název AllJoyn. Tento Framework také cílí na zařízení, jejich připojení do sítě a hlavně komunikaci mezi ostatními zařízeními. Ač mají obě dvě aliance podobný záměr a jejich řešení jsou cílena na stejný segment trhu, bude to právě uživatel, který bude trpět. Ten bude nucen při výběru nového zařízení čelit rozhodnutí, zda vybere zařízení, které podporuje jeden anebo druhý standard. Nutno dodat, že většina velkých společností z tohoto důvodu podporuje obě aliance.

Každá technická inovace je většinou přínosná do té doby, dokud nám slouží a dělá to, co chceme my. Zatímco politici a bezpečností experti stále varují před hrozbou kybernetických útoků, jen okrajem (a pokud vůbec) zmiňují hrozby spojené s IoT. Globální spojení mezi všemi zařízeními však přináší nová bezpečnostní rizika. Nejednomu z nás tak určitě v hlavě proběhla otázka „Jak bezpečný je IoT?“. Touto otázkou se zabývá i Nermin Hajdarbegovic, který sepsal článek, kde shrnuje a popisuje všechny aspekty bezpečnosti a některá řešení problémů IoT (HAJDARBEGOVIC, 2015). Samozřejmě i samotné firmy mají zájem, aby jejich zařízení byla dobře zabezpečena. Firma Cisco, která je jedna z největších hráčů na poli síťových prvků, se ve svém kurzu „Introduction to the Internet of Everything“, který je součástí portálu „Cisco Networking Academy“, věnuje mimo jiné i bezpečnosti IoT a popisuje, jaké hrozby existují a možnosti, jak se jim bránit. Bezpečnost v IoT bude přiblížena a analyzována v následujících kapitolách.

[1] Dříve „Open Interconnect Consortium“

2 ÚVOD DO IOT

Hned v úvodu je potřeba upřesnit, co vlastně IoT znamená. Nejedná se o výsledek vývoje jedné jediné technologie, je to spíše pojem, který je výstupem spojení několika různých technologických aspektů dohromady. Ty pak tvoří celek, který je schopen nabídnout spojení mezi virtuálním a fyzickým světem. Definic existuje více, většinou je jejich myšlenka podobná a jedná se pouze o jinou interpretaci. Jednou z možných definic je i tato: „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.“[2] (HALLER, 2009).

2.1 Z ČEHO SE SKLÁDÁ

Jak již název vypovídá, jedním z hlavních prvků jsou věci. IoT popisuje systém, kde jsou prvky fyzického světa a jejich integrované nebo přidané senzory připojovány do Internetu pomocí bezdrátového a drátového připojení. Senzory mohou používat různé typy připojení. Pro lokální připojení se využívá například RFID, NFC, Wi-Fi, Bluetooth a nebo ZigBee. Pro připojení na velké vzdálenosti se využívají technologie GSM, GPRS, 3G, LTE a další. Dále existují různé další proprietární protokoly (FRIEDEMANN, 2010).

2.2 PŘÍKLADY

Příkladů zařízení, která se dají zařadit pod označení IoT je spousta. Následuje rozdělení do několika kategorií, pro které jsou uvedeny příklady komerčních zařízení od osobních nositelných věcí přes domácí zařízení až po několik rozsáhlých řešení.

2.2.1 NOSITELNÁ ZAŘÍZENÍ

Pojem nositelná zařízení na první pohled nemusí vyjadřovat nic moc nového. Pro představu může jít o různé druhy hodinek nebo sluchátek. Nová doba však přináší i nové možnosti a i tak všední věci jako uvedené hodinky mohou být doplněny o různé senzory. Mezi přidané senzory lze zařadit například: senzor srdečního tepu, akcelerometr, gyroskop, magnetometr, senzor okolního osvětlení, senzor pro určení aktuální geografické polohy (GPS) a mnoho dalších.

[2] Svět, ve kterém jsou fyzické objekty bezproblémově integrovány do informační sítě a kde se tyto fyzické objekty mohou stát aktivními účastníky obchodních procesů. Služby mohou komunikovat s těmito chytrými objekty přes internet, mohou požadovat jejich stav a jakékoliv informace, které jsou s nimi spojeny, s ohledem na bezpečnost a ochranu osobních údajů.

Všechny tyto zmíněné senzory je možné již nyní integrovat do těla velikosti hodinek nebo různých náramků. Ovšem takováto nositelná zařízení se všemi možnými senzory by byla k ničemu, pokud by nedocházelo k produkci, přenosu a zpracování získaných dat. Proto jsou tato zařízení vybavena schopností komunikovat s dalšími zařízeními s využitím bezdrátových sítí. Angličtina pak pro označení nositelných zařízení používá slovo „wearables“, ovšem s tímto pojmem je možné se setkat i v české literatuře. Existuje mnoho různorodých zařízení, které spadají pod taktovku „wearables“. Jsou jimi například chytré náramky, hodinky, bezdrátová sluchátka, brýle nebo i chytré oblečení (WEARABLE DEVICES, 2014).

V následujících odstavcích budou popsána alespoň první dvě zmíněná zařízení.

Chytré náramky (Fitness trackers)

Zpravidla se jedná o náramek, který je vybaven různými senzory, které monitorují aktivity svého nositele. Dokáží však i upozornit na příchozí hovor nebo odemknout zamčený telefon (pokud je s náramkem spárovaný a tuto funkci podporuje). Zařízení může být buď přímo integrováno do náramku, nebo může být vyjímatelné a nositel si tak může měnit typ a barvu náramku. Na trhu existuje velké množství zařízení, které se liší hlavně počtem senzorů, jež poskytují různé údaje. Počet senzorů a funkcí se odvíjí od ceny. Většina výrobců poskytuje mobilní aplikace, které po spárování náramku s telefonem dokáží nejen v reálném čase zobrazovat aktuální informace získávané z náramku, ale dokáží také zpětně analyzovat získaná data a nositeli dát informace o tom, jak si přes den vedl v různých činnostech. Propojení s dalšími zařízeními probíhá převážně pomocí technologie Bluetooth. Na obrázku 1 je zobrazena část chytrého náramku s detailem na senzor srdečního tepu.

Obrázek 1: *Senzor srdečního tepu na chytrém náramku*[3]

[3] Zdroj: vlastní

Chytré hodinky (Smartwatches)

Další ze zástupců nositelných prvků jsou chytré hodinky. Nosí se na zápěstí a jejich potenciál je využit nejvíce po propojení s telefonem. Stejně jako chytré náramky i hodinky jsou vybaveny několika senzory a funkcemi. Oproti náramkům většinou obsahují větší displej, který se dá považovat za okno do digitálního světa. Dokáží upozornit na příchozí hovor, zobrazují zprávy, emaily nebo nové příspěvky na sociálních sítích. Dalo by se říci, že zobrazování času je spíše až druhotná požadovaná vlastnost.

Pro propojení s chytrým telefonem je využíváno převážně technologie Bluetooth.

2.2.2 CHYTRÁ DOMÁCNOST

Rozmach zažívají také zařízení, která tvoří chytrou domácnost. Následující odstavec na začátek uvádí, co je to inteligentní dům tak, jak ho popisuje Valeš ve své knize (2006):

„Inteligentní dům v nejširším možném smyslu slova je budova vybavená počítačovou a komunikační technikou, která předvídá a reaguje na potřeby obyvatel s cílem zvýšit jejich komfort, pohodlí, snížit spotřebu energií, poskytnout jim bezpečí a zábavu pomocí řízení všech technologií v domě a jejich interakcí s vnějším světem. Často se jako vzájemně zaměnitelné pojmy používají termíny „chytrý dům“, „digitální dům“, „domácí automatizace“, „inteligentní elektroinstalace“ a „domotika“. Hlavním cílem inteligentního domu je usnadnit a zpříjemnit uživatelům bydlení. Alespoň bez základní elektroniky, jako jsou termostaty pro řízení topení, osvětlení a zabezpečovací systém, se dnes neobejde žádný dům. V mnoha domech k tomu přibude počítačová síť, řízení rolet a žaluzií, klimatizace, kamerový systém, v neposlední řadě domácí kino a ozvučení alespoň některých prostor. Inteligentní dům dokáže všechnu techniku propojit a integrovat mezi sebou a sjednotit její ovládání, a to jak z hlediska vzhledu vypínačů a displejů na zdi, tak především poskytnout jednotný způsob ovládání přizpůsobený na míru pro konkrétní dům a jeho obyvatele.“

Pokud má být dům vybaven inteligentními zařízeními, existuje několik možností jak toho docílit. Na trhu existuje mnoho koncových zařízení, které stačí rozbalit, připojit k síti a téměř ihned začít využívat. Takto jednoduše lze rozšířit dům například o termostat, světla, elektrické zásuvky, robotické vysavače nebo třeba kamerový systém. Je již samozřejmostí, že vše lze ovládat vzdáleně pomocí aplikace pro chytrý telefon nebo přes webové rozhraní odkudkoliv na světě, kde je přístup k internetovému připojení. Jako nevýhoda takto hotových řešení se jeví hlavně to, že každý výrobce pro správu svého zařízení používá své aplikace a tyto zařízení také nedokáží, nebo jen omezeně, komunikovat se zařízeními jiných výrobců. V tomto případě

se pak může stát, že se spíše člověk stane otrokem chytré domácnosti, kdy bude nucen pro nastavení teploty otevřít aplikaci jednoho výrobce, zatímco pokud bude chtít zobrazit přehled rozsvícených světel, bude nucen otevřít aplikaci jinou.

Není nutné se omezovat pouze na již hotové produkty. Inteligentní dům lze vybavit dle vlastního uvážení a schopností. Na trhu jsou dostupné různé otevřené elektronické platformy, například Arduino[4], ke kterým je možné pořídit již od několika málo korun různé senzory a rozšiřující desky. Poté stačí jen autorova fantazie a zkušenosti s programováním k tomu, aby si upravil svůj dům na inteligentní podle svých požadavků. Na trhu však existuje mnoho firem, které se specializují na úpravu domů pomocí svých řešení, která dokáží upravit přesně na míru potřebám zákazníka. Výhoda těchto řešení je ta, že se jedná o komplexní systém spolupracujících zařízení a senzorů, které lze ovládat z jednoho řídícího panelu nebo aplikace. Zpravidla jde o to, že firmy staví svá řešení na jednom vybraném komunikačním protokolu. Tyto komunikační protokoly a standardy budou probrány dále.

2.2.3 CHYTRÁ MĚSTA

Takto definuje chytré město Yakovlev (2015):

„Když některé město označíme jako chytré, neznamená to, že ostatní města jsou hloupá. Každé moderní velkoměsto je složitý systém, který se skládá z mnoha komplexních dílů. Jedná se ale obvykle o pevně zaběhnutý systém, ve kterém každá změna čelí odporu tradičních a prověřených postupů. Chytrá města se ale naopak snaží kombinovat nové technologie z různých oblastí a tímto způsobem lidem usnadňovat život. Každé město by se dalo označit jako chytré, některá jsou ale v tomto ohledu úspěšnější než jiná a taková pak označujeme jako „chytrá města“, zatímco o ostatních mluvíme pouze jako o „městech“. Vezměme si například japonské město Fujisawa, které bylo v roce 2010 vybudováno v místě původní továrny Panasonic. Na 19 hektarech plochy již bylo postaveno a prodáno přibližně 100 domů. Každý dům je vybaven solárními panely a generátory na zemní plyn, které využívají energii s maximální efektivitou. Všechny domy jsou propojeny společnou rozvodnou sítí, která mezi nimi přenáší energii automaticky. Předpokládá se, že pokud by toto město bylo odpojeno od vnějších sítí, dokáže přežít tři dny jen s využitím vlastních ekologických zdrojů.“

Například společnost Cisco používá spojení „Internet of Everything“ (dále IoE), kterým označuje propojení lidí, dat, procesů a věcí. IoE je pak podle nich tvořeno několika

[4] Arduino je otevřená platforma, která se využívá k budování elektronických projektů.

technologiemi, mezi které patří právě IoT (CISCO). Podle průzkumu pak bude do roku 2050 žít 60 % populace ve městech. Díky tomu je nutné změnit aktuální pohled na město a je nutné začít přemýšlet o městech budoucnosti. Některá velká města již aplikují moderní technologie. Například město Amsterdam využívá pro veřejné osvětlení LED lampy, které jsou připojeny k síti (MITCHELL, 2013).

2.3 VELIKOST

Trh s IoT je již nyní velký a dále roste neuvěřitelným tempem. To je možné přičíst hlavně tomu, že najde uplatnění v každém průmyslovém odvětví a nejen tam. Díky příchodu IPv6 odpadá bariéra s nedostatečným počtem adres, který byl u IPv4. Adresa tak může být přiřazena miliardám zařízení. Se stále zlepšujícím se pokrytím planety připojením k Internetu zase lze dostat zařízení i do takových míst, kde by to dříve nebylo možné kvůli absenci připojení. To jde ruku v ruce s vývojem a miniaturizací síťových čipů, které jsou nezbytné pro připojení a to nejen pevné, ale hlavně bezdrátové. Společnost ABI Research odhadovala, že už v roce 2013 bude prodáno přes 5 miliard bezdrátových čipů (ABI RESEARCH, 2012). Technologie je vyvíjena v zájmu snížit energetickou náročnost, což je také jedním z hlavních pilířů rozmachu IoT. Díky těmto novým technologiím je možné napájet připojená zařízení jen s pomocí bateriových článků po několik stovek dní.

V roce 2003 bylo na světě skoro 6,3 miliardy lidí a 500 miliónů připojených zařízení do Internetu. Podle definice od Cisco IBSG, lze IoT chápat jako bod, kdy je k Internetu připojeno více zařízení než lidí. V roce 2003 tak tedy podle této definice ještě IoT neexistoval. Obrovský nárůst chytrých telefonů a tabletů zapříčinil, že v roce 2010 bylo k Internetu připojeno již 12,5 miliard zařízení, každopádně počet lidí na světě se zvýšil jen na 6,8 miliard. Nyní stačí vydělit počet zařízení počtem lidí na světě. Výsledkem je číslo, které udává počet připojených zařízení na osobu. Výsledek je v tomto případě větší než 1 a dle uvedené definice lze říci, že zde již IoT existoval. Kdy však došlo ke zlomu a IoT vznikl? Na základě dostupných dat Cisco IBSG odhaduje, že k tomuto milníku došlo někdy mezi lety 2008 a 2009 (EVANS, 2011).

Budoucnost dozajista patří IoT. Například společnost Cisco předpokládá, že do roku 2020 bude 50 miliard zařízení připojeno k sítí (EVANS, 2011). V jednom z prohlášení společnosti Gartner se uvádí, že trh s IoT v roce 2020 dosáhne hodnoty 26 miliard instalovaných a připojených věcí. Nutno dodat, že z výzkumu byly vyloučeny počítače, tablety a chytré telefony (GARTNER, 2013). Je tedy možné říci, že takto rozdílná čísla jsou dána právě danou metodikou průzkumu, kdy Cisco počítá se vším, co se k sítí připojí, kdežto společnost Gartner některá zařízení

vylučuje. Tak či tak, jedná se o opravdu vysoká čísla, která zajisté přináší mnoho otazníků. Takto velký počet zařízení vygeneruje značný objem dat, ze kterých bude potřeba vyfiltrovat relevantní data a ty pak správně analyzovat a vyhodnotit. S nárůstem připojených zařízení a jejich integrací i do méně běžných odvětví zase bude potřeba specialistů, kteří se budou zaměřovat právě na správu těchto zařízení. To je velice důležité i z hlediska bezpečnosti, protože s novými technologiemi také přichází nové bezpečností výzvy. Je svět na rozmach IoT připraven? Odpověď zní „Ano, ale…“. Při rozvoji IoT je totiž možné těžit z již dostupných technologií a to hlavně z vývoje chytrých telefonů. Na druhou stranu IoT je nové odvětví, ve kterém je nutné počítat s novými bezpečnostními hrozbami.

2.4 PŘÍNOSY

Tak jako masivní rozvoj počítačů na konci minulého století dovolil nahradit některé procesy, které dříve muselo dělat několik lidí, tak se děje i s příchodem IoT. Tento jev lze zaznamenat téměř v jakémkoliv odvětví. Příchod samotných věcí a konektivity je však pouze jedna strana mince. Druhá strana mince je ta, jak tyto možnosti efektivně využít. Věci mohou generovat nejrůznější důležitá data z různých procesů, ty je potřeba někde ukládat a následně analyzovat. Pro optimalizaci těchto procesů je nutné zvolit vhodnou cestu, jak s daty zacházet. A to se nemusí týkat pouze procesů automatizovaných systémů, ale i činností, které jsou vykonávány lidmi. Díky tomuto pak lze očekávat přínosy v oblasti produktivity, snížení nákladů, snížení dopadů na životní prostředí a další.

Následují reálné příklady z některých odvětví a jejich přínosy.

Doprava

Integrace do dopravy přinese zvýšení bezpečnosti díky tomu, že jednotlivé dopravní prostředky budou vzájemně komunikovat nejen mezi sebou, ale také mezi dalšími prvky dopravní infrastruktury. Na základě této komunikace bude možné zvýšit plynulost a bezpečnost provozu. Plynulá doprava zajistí snížení spotřeby automobilů a ušetří tak nemalé peníze. Další částí mohou být takzvaná „chytrá parkovací místa“, která v reálném čase poskytují uživatelům informace o jejich obsazení. To může být například efektivně využito k plánování rezervací tohoto místa a také k rychlejšímu parkování ve městech (MITCHELL, 2013).

Průmysl

V průmyslu se firmy snaží o různou automatizaci už velice dlouho. Ještě před příchodem moderních standardů a technologií firmy využívaly různé senzory a vzdálená ovládaní, které

však byla většinou postavena na proprietárních protokolech a hardwaru. Tato zařízení byla dříve velice drahá, neúsporná a měla omezenou výpočetní kapacitu. Proto bylo vždy těžké provádět různá rozšiřování o nové systémy a integrátoři měli problémy s integrací nových systémů tak, aby komunikovaly se systémy původními. To však již v dnešní době neplatí a v průmyslu se nasazují IoT řešení snad nejrychleji, protože dokáží ušetřit mnoho peněz a firmy tak stojí o jejich aplikaci. Snížení nákladů je zapříčiněno hlavně inteligentním řízením různých průmyslových systémů: vzduchotechnika, světla, chytré ovládání výtahů a další (ACCENTURE, 2015).

Člověk

O lidech se dá získávat mnoho informací. Monitorování zdravotního stavu, údaje o poloze, denní návyky nebo třeba informace o tom, jací jsou řidiči. K čemu by mohlo být monitorování chování řidiče? Pojišťovny by tyto informace určitě uvítaly. Na základě vyhodnocení těchto údajů by mohly jednotlivci nabídnout snížení ceny pojištění za předpokladu, že jezdí plynule a bezpečně. Na druhou stranu by takové informace pro někoho naopak mohly znamenat zvýšení jeho nákladů na pojistné.

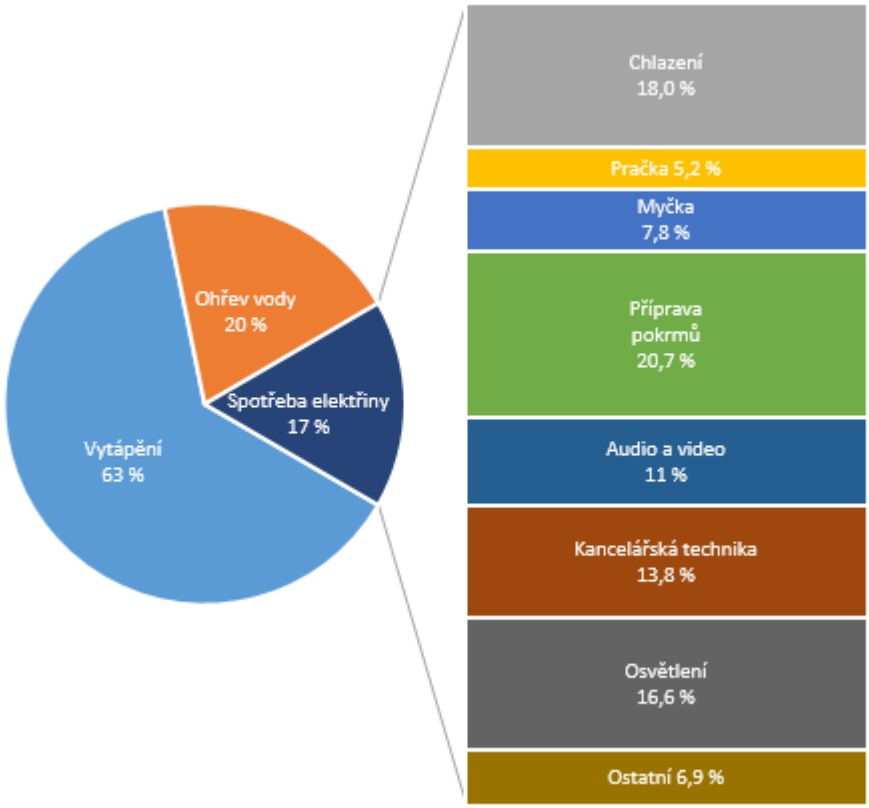
Zdravotnictví

Mnoho lidí v dnešní době již používá chytrý telefon. Ten je sám o sobě napěchován senzory. Je možné si zobrazit, kolik kilometrů a kolik výškových metrů jeho uživatel během dne zdolal. Mobilní telefon může být rozšířen, případně i nahrazen, některým ze specializovaných nositelných zařízení. Ty dokáží sledovat i další informace, jako jsou: srdeční tep, teplota atd. Všechny tyto informace dohromady o uživateli vytvoří jakýsi přehled, který může být přínosný nejen pro něj jako přehled a motivace, ale například i pro praktického lékaře. Ten si před návštěvou stáhne elektronickou zdravotní kartu pacienta, do které zařízení zasílá naměřené údaje. Dle toho pak dokáže snadněji a lépe určit zdravotní stav a případně upozornit na anomálie. V případě komunikace v reálném čase mezi zařízením a zdravotnickým střediskem může být uživatel bezprostředně pod dohledem lékařské péče. Toto středisko pak může automaticky v případě nutnosti naplánovat návštěvu u lékaře. A ještě lépe v případě ohrožení života automaticky vyšle záchrannou službu do naší lokace (TECHTARGET, 2015).

Domácnost

Chytré domácnosti mohou usnadnit a zpříjemnit život. Automatizované osvětlení domácnosti, automatizovaná vzduchotechnika a řízení rolet je jen část systémů, které přináší mimo jiné také

úsporu financí. Tyto systémy, které spolu komunikují, dokáží optimalizovat chod domácnosti. Rolety se automaticky zatáhnou, pokud svítí přímé slunce na stranu domu, kde jsou okna. Tím tak prodlouží dobu ohřevu domácnosti a klimatizace se zapne až po delší době. Při pohledu na následující graf 1 je vidět, jak je v české domácnosti rozložena spotřeba energie.



Graf 1: *Rozložení spotřeby v modelové domácnosti*[5]

Celkově dokáže inteligentní domácnost zajistit úsporu až 31 % nákladů. To je již znatelný přínos (HALUZA, 2012).

2.5 NEGATIVA

S nástupem IoT je však potřeba počítat i s možnými problémy. Těchto problémů je zatím celkem mnoho, což naznačuje, že internet věcí je stále ve svém počátečním stádiu. Otázky nastávají primárně v tématech bezpečnosti a soukromí. Je nutné si při nasazování uvědomit pár věcí. Pokud je zařízení připojeno k síti a je možné ho vzdáleně ovládat, pak je jisté, že tuto možnost může mít za jistých okolností i někdo další. To je hlavně v kritických odvětvích

[5] Zdroj: HALUZA, M., MACHÁČEK, J. *Spotřeba elektrické energie domácností, predikce a potenciální úspory pomocí BACS* [online]. 2012 [cit. 2016-04-19]. ISSN 1801-4399. Dostupné z: http://elektro.tzb-info.cz/8570-spotreba-elektricke-energie-domacnosti-predikce-a-potencialni-uspory-pomoci-bacs

absolutně nežádoucí a je potřeba se s tím vypořádat. V případě absence dostatečného zabezpečení by napadení a převzetí kontroly nad zařízením mohlo mít různé následky a v některých odvětvích by mohl být dopad fatální. Takový záškodník by mohl typicky měnit nastavení vytápění, nastavení regulace dopravy nebo měnit informace o pacientově zdravotním stavu a vznikl by tak chaos. Ale nemusí se jednat pouze o aktivní[6] narušení bezpečnosti. Získání přístupu k nezabezpečeným datům může být pro nějaké záškodníky dostatečné. V případě získání přístupů k datům o domácnosti pak nebude problém na základě informací zaznamenaných z různých čidel zjistit přítomnost obyvatel v domě v návaznosti na čase a vytipovat si tak vhodný čas na vloupání. Tento typ narušení se označuje jako pasivní útok[7].

Bezdrátové připojení sice dovoluje dostat zařízení do různých míst, kde není možné se připojit pomocí kabelu, avšak zařízení stále vyžadují napájení. Vývoj přinesl energeticky nenáročné protokoly na přenos, jako je například Bluetooth LE nebo ZigBee. U zařízení využívajících tyto protokoly je potřeba, dle nastavení četnosti odesílání zpráv a dalších parametrů přenosu, měnit baterii přibližně po dvou letech používání (LESWING, 2014).

Vyprodukovaná data jsou pak typicky přenášena do data center a cloudů ke zpracování. Tato data, jejich analýza a interpretace může mít velice lukrativní hodnotu pro obchodníky, reklamní agentury a další zástupce zprostředkovatelů služeb. Může se tedy stát, že budou odcizena, případně se s nimi bude obchodovat. V případě odcizení citlivých dat (čísla platebních karet, hesel atd.) pak nastává problém (MARR, 2015).

2.6 ZASTŘEŠUJÍCÍ ORGANIZACE

Čím více se ve světě začíná řešit IoT a jeho standardy, mnoho firem se snaží spojit a vytvořit tak své vlastní skupiny, aliance a konsorcia. Mezi hlavní patří hlavně Open Connectivity Foundation a AllSeen Aliance. Uskupení jsou tvořena mezinárodně známými firmami, které pak doplňují další více nebo méně známe firmy. Mezi těmito firmami jsou výrobci elektroniky, automobilové společnosti, poskytovatelé cloud úložišť, inovativní startupy, výrobci čipových sad, poskytovatelé služeb, prodejci a vývojáři software. Cílem je, co nejjednodušeji a nejefektivněji propojit miliardy zařízení na světě tak, aby spolu mohla bezpečně komunikovat. Obě zmíněné organizace pak podporují nebo samy vyvíjejí framework, který právě toto propojení mezi zařízeními umožní. Frameworky budou dále popsány v kapitole 3.3.

[6] Snaha změnit systémové zdroje nebo ovlivnit jejich funkce.
[7] Systém je monitorován a skenován. Cílem je vytěžit co nejvíce informací. Při tomto útoku nejsou ovlivněny systémové prostředky.

Open Connectivity Foundation

Jedná se o nadaci, která je nástupcem Open Interconnect Consortium (dále OIC) a byla založena v roce 2014. Nejznámějšími členy jsou Cisco, Intel, Samsung, Microsoft, Qualcomm, Dell a mnoho dalších. Mezi cíle patří zejména snaha o připojení dalších 25 miliard zařízení. Dále také snaha o bezpečné a spolehlivé vyhledání zařízení a jejich propojení napříč operačními systémy a platformami (FOX RUBIN, 2014). Na tyto cíle se snaží dosáhnout vydáváním specifikací a jejich implementací do open source projektu IoTivity. Zatím poslední zveřejněné specifikace, konkrétně „OIC SPECIFICATION 1.0“, jsou z roku 2015 a rozdělují se na několik jednotlivých částí (OPEN CONNECTIVITY FOUNDATION, 2016b):

- Core framework,
- Security,
- Smart Home Device,
- Resource Type,
- Remote Access.

AllSeen Aliance

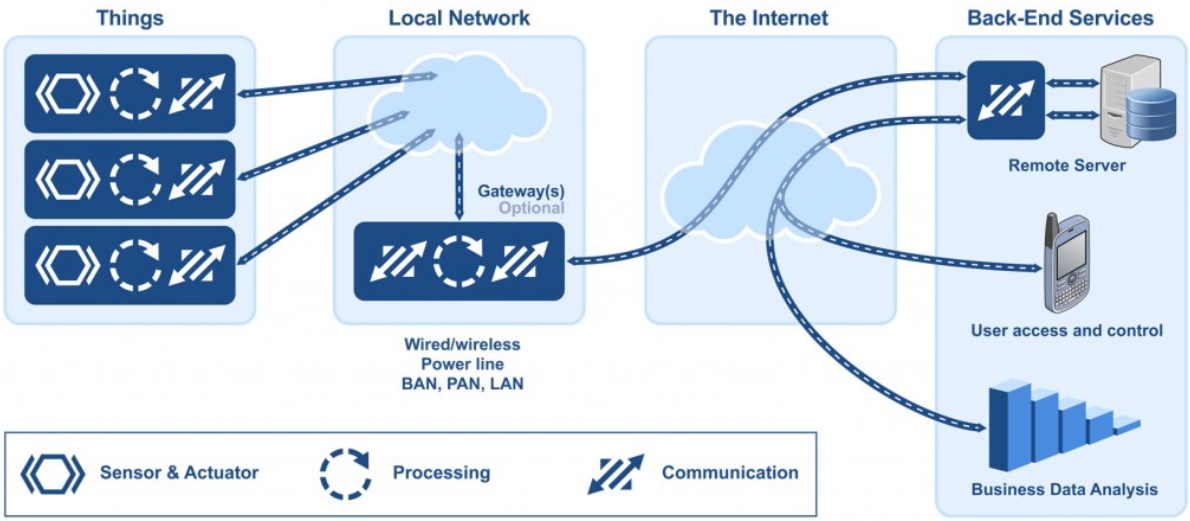
Na konci roku 2013 oznámila nezisková organizace „The Linux Foundation“ vznik AllSeen Aliance. Jedná se o konsorcium, jehož cílem je umožnění propojení a spolupráce miliard zařízení, služeb a aplikací v různých průmyslových odvětvích, které jsou součástí IoT. Mezi zakládající členy patří známé firmy, které podnikají v různých odvětvích, jako je spotřebitelská elektronika, služby pro spotřebitele, výrobci čipových sad nebo i různé startupy. AllSeen Aliance rozděluje své členy do tří skupin: Premier Members, Community Members a Sponsored Members. Mezi firmy, které spadají do první zmíněné skupiny, patří například: Qualcomm, Sony, Microsoft, LG, Sharp. Všichni členové AllSeen Aliance přispívají svým softwarem a zdroji při spolupráci na vývoji open source frameworku, který umožňuje výrobcům hardwaru, poskytovatelům služeb a vývojářům softwaru vytvářet zařízení a služby, které mezi sebou spolupracují (LINUX FOUNDATION, 2013). Tento Framework je pojmenován AllJoyn a bude probrán v kapitole 3.3.

3 ANALÝZA MOŽNOSTÍ PŘIPOJENÍ A BEZPEČNOSTI

Vývoj jde mílovými kroky kupředu a IoT je dozajista milník, který přináší mnoho benefitů v různých odvětvích a dotkne se každého. Předchozí kapitola poskytla hlavně abstraktní informace o tom, co to vlastně IoT je, z čeho se skládá a jaké může mít dopady – a to jak pozitivní tak negativní. Tento abstraktní pohled je nutný pro pochopení koncepce IoT. V této kapitole budou analyzovány stavební prvky IoT, mezi které patří různá zařízení, standardy, protokoly a také frameworky. Během analýzy bude probrán techničtější pohled na věc a také provedena analýza možností, které lze využít při integrování IoT do běžného života. U probíraných témat, u kterých je to možné, bude uvedeno, jaké nabízejí možnosti zabezpečení. V neposlední řadě bude také zmíněno, jaké hrozby aktuálně IoT ohrožují.

V této kapitole je potřeba lehce pozměnit pohled na IoT. Již bylo uvedeno, že základní myšlenkou je propojení věcí, v širším smyslu také propojení všeho ostatního, co může být připojeno – věci, lidé, zvířata atd. Pilíře, které tvoří IoT, jsou znázorněny na obrázku 2 a je možné je rozdělit do následujících 4 hlavních skupin (MICRIUM, 2015b):

- věci,
- lokální síť (zde může být zahrnuta i výchozí brána, která překládá komunikaci z proprietárních protokolů na IP protokol),
- samotný Internet,
- koncová zařízení, cloudové služby a další.



Obrázek 2: *Příklad pohledu na to, z čeho se skládá IoT*[8]

[8] Zdroj: MICRIUM. *Designing the Internet of Things - IoT Devices and Local Networks*. 2015 [online]. [cit. 2016-04-28]. Dostupné z: https://www.micrium.com/iot/devices/

Systémy IoT nejsou komplikované, ale jejich návrh a tvorba může být komplexní úloha. IoT je také možné rozdělit na dvě skupiny podle typu zaměření:

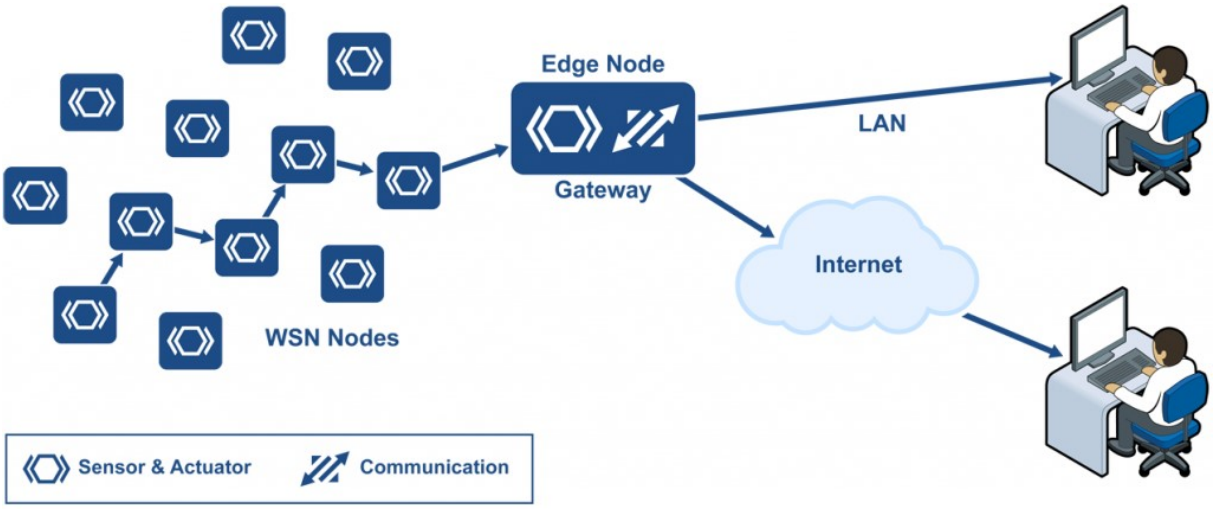
- **průmyslové IoT** – v lokální síti se typicky střetává několik různých technologií,
- **komerční IoT** – pro lokální komunikaci obecně převládá Bluetooth nebo Ethernet.

3.1 WIRELESS SENSOR NETWORK

Jak bylo uvedeno, IoT se skládá z několika částí. Je nutné si krok po kroku popsat, co tyto části obsahují. V této části bude kladen důraz na představení modelů a technik využívaných pro komunikaci věcí mezi sebou a okolním světem.

Výběr komunikační technologie závisí na několika faktorech a přímo ovlivňuje požadavky na hardware, a tak i cenu. Jaká technologie je nejlepší pro připojení? Vzhledem k tomu, že IoT zařízení mohou být součástí různých systémů – v oblečení, domech, budovách, továrnách, vozech a dokonce i v lidských tělech – nelze tedy jednoznačně určit, která technologie je nejlepší pro všechny. Pro každé řešení je tedy třeba vybrat takovou technologii, která nejlépe pokryje tyto specifické požadavky.

Jako modelový příklad je možné zmínit výše uvedenou továrnu. Tato továrna bude potřebovat velký počet koncových čidel a akčních členů roztroušených na velké ploše. V takovémto případě je nezbytné vybrat některou z bezdrátových technologii.



Obrázek 3: *Síť senzorů*[9]

[9] Zdroj: MICRIUM. *Designing the Internet of Things - IoT Devices and Local Networks*. 2015 [online]. [cit. 2016-04-28]. Dostupné z: https://www.micrium.com/iot/devices/

Obrázek 3 výše znázorňuje takzvané „Wireless sensor network“ (dále WSN). Tento typ sítě se skládá z jednotlivých vestavěných systémů (WSN Nodes). Ty jsou schopny interakce s jejich okolním prostředím díky různým senzorům. Díky těmto senzorům dokáží měřit různé parametry, jako je například teplota, vlhkost vzduchu, atmosferický tlak a mnoho dalších. Naměřené hodnoty jsou po lokálním zpracování odesílány distribuovaně do centrálního řídícího uzlu (WSN Edge Node), také nazývaný jako výchozí brána (AKYILDIZ, 2010).

3.1.1 WSN NODES

Jedná se o levná zařízení obsahující různé senzory, která tvoří zmíněnou WSN a jsou mezi sebou propojena. Vzhledem k nízké ceně mohou být nasazována ve velkém počtu. Pro svoji práci potřebují velice málo energie, a proto je možné je napájet pomocí baterie případně i pomocí externích zdrojů. Pod externími zdroji si lze představit například napájení pomocí solární, termální nebo větrné energie. V nejlepším případě jde o kombinaci baterie a externího zdroje. Pokud to podmínky dovolí, zařízení je napájeno pomocí externího zdroje, který zároveň dobíjí baterii. V případě nepříznivých podmínek je zařízení napájeno baterií a v závislosti na použité technologii může takto fungovat až několik let. Tyto uzly se typicky skládají ze tří částí (AKYILDIZ, 2010):

- bezdrátový modul,
- deska se senzory,
- programovatelná základní deska.

3.1.2 WSN EDGE NODES

Samotné uzly v síti WSN mohou pracovat s jiným než IP protokolem, proto je potřeba zařízení, které nabízí IP konektivitu a tím je zpravidla právě okrajový uzel. Ten se chová jako výchozí brána mezi sítí WSN a mezi IP sítí. Mimo jiné také může provádět lokální zpracování dat, nabízet lokální úložiště a mít uživatelské rozhraní. Nemusí se však jednat pouze o přechod z proprietárního protokolu na IP protokol (MICRIUM, 2015c). Obecně se dají tyto okrajové uzly popsat jako statické senzorové uzly, které distribuují data v překrývajících se oblastech mezi dvěma PAN (DONG, 2014).

3.1.3 WSN TECHNOLOGIE

Pro propojení těchto zařízení je nutné využít některou z bezdrátových technologií přenosu. V této kapitole jsou popsány ty nejzásadnější. Je nutné zmínit, že boj o upřednostňovaný protokol zdaleka není u konce. Existuje více kandidátů, mezi kterými je možné vybírat.

Wi-Fi

Pokud je řeč o bezdrátových sítích nejednoho jistě napadne jako první kandidát pro síť IoT využít právě Wi-Fi, a to hlavně z toho důvodu, že se může jevit jako všudypřítomná. V roce 2011 bylo zjištěno, že penetrace domácností těmito sítěmi je v řádech desítek procent. S 80,3 % patřila Severní Korea k zemi s největší penetrací sítí Wi-Fi v domácnostech. V České republice bylo v této době zjištěno pokrytí 31,6 % domácností (BUSINESS WIRE, 2012). Statistická data naznačují, že problém s pokrytím není až tak závažný. Nejlevnější zařízení pro pokrytí domácnosti Wi-Fi připojením se pohybují v řádech stovek korun a tak je velice dostupné domácnost o toto Wi-Fi připojení rozšířit. Problém je však v tom, že Wi-Fi potřebuje značné množství energie a pro většinu zařízení, které jsou napájeny bateriemi, je tedy nereálné tuto technologii použít. Proto jako kandidát přímo pro koncové prvky IoT není vhodná. Avšak pro připojení výchozí brány WSN, která je napájena pomocí elektrické sítě, je možné této technologie využít. Pro Wi-Fi existují různé verze standardu 802.11, nejčastěji se pak právě ve zmíněných domácnostech je možné setkat s IEEE 802.11b/g/n. Různé verze se liší například ve využívaném spektru a rychlostech (EPRIN, 2015). Sítě Wi-Fi obsahují prvky bezpečnosti, mezi které patří autentizace a šifrování. Autorizaci je však nutné provádět externím mechanizmem pro řízení přístupu (např. RADIUS). Mezi známé útoky na Wi-Fi sítě patří (PUŽMANOVÁ, 2005):

- instalace falešného zařízení (rogue AP),
- útok typu man-in-the-middle,
- útok typu DoS (odmítnutí služby).

IEEE 802.15.4

Jedná se o jeden z nejdůležitějších standardů, který pomohl rozvoji IoT. Definuje komunikaci pro bezdrátové sítě malého rozsahu s velice nízkými přenosovými rychlostmi. Tím je docíleno vysokých výdrží zařízení na baterii a to v řádech měsíců až roků. Pracuje v různých mezinárodních bezlicenčních pásmech. Tento standard specifikuje první a druhou vrstvu

ISO/OSI modelu pro takzvané „low-rate WPANs“. Tvoří základ například pro 6LoWPAN, ISA100 a známý ZigBee. Toto je výčet některých funkcí tohoto standardu (IEEE, 2016):

- rychlosti přenosu 250 kbps, 40 kbps a 20 kbps,
- zabezpečení linkové vrstvy pomocí šifrování 128 bit AES,
- dva módy adresace: 16 bitová a 64 bitová,
- přístup ke sdílenému médiu pomocí CSMA-CA,
- hvězdicová nebo peer-to-peer topologie,
- automatické navázání spojení pomocí koordinátora,
- zajištění nízké spotřeby energie,
- 16 kanálů v 2,4 GHz ISM pásmu (celý svět), 10 kanálů v 915 MHz (Severní Amerika) a jeden kanál v pásmu 868MHz (Evropa).

Jak bylo právě uvedeno, standard toho nabízí opravdu mnoho a to i na poli bezpečnosti. Aplikace různých úrovní bezpečnosti však záleží na povaze systému. Jiné zabezpečení (typicky nižší) bude nastaveno u systémů, které nevyžadují takovou míru zabezpečení (monitorování teploty bazénu nebo vláhy půdy na zahradě). To bude mít za následek také prodloužení výdrže na baterii, protože nebude docházet k náročným výpočtům šifry a také přenášená data budou menší. Na druhou stranu pro kritické systémy nabízí širokou škálu možností.

6LoWPAN

Pro zařízení s nároky na vysokou výdrž baterie je zásadní, aby jejich přenášené zprávy byly co nejkratší, proto většina řešení nepoužívá IP protokol ve své implementaci. Díky této skutečnosti byla navržena síťová technologie 6LoWPAN. Jedná se o akronym pro „IPv6 over Low power Wireless Personal Area Networks“ a jak už název napovídá, jedná se o vysílání a příjem IPv6 paketů přes sítě postavené na standardu IEEE 802.15.4. Výhoda 6LoWPAN je v tom, že dokáže komunikovat jak s ostatními bezdrátovými zařízeními na 802.15.4 sítích, tak i se zařízeními na jakékoliv další IP síti (Ethernet nebo Wi-Fi). Problém, který bylo nutné vyřešit, je ten, že velikost MTU u IPv6 je 1280 bajtů a limit velikosti rámce u IEEE 802.15.4 je 127 bajtů a také jsou zde limitní hodnoty rychlosti přenosu. Tento problém je vyřešen pomocí komprese hlavičky (standardizováno v RFC 6282) a fragmentace. Velice důležitou roli nejen v IoT zastává bezpečnost. Pro zabezpečení linkové vrstvy využívá 6LoWPAN výhod silného šifrování AES-128, které je definováno v IEEE 802.11.5. Zabezpečení linkové vrstvy zahrnuje jak autentizaci, tak i šifrování (OLSSON, 2014).

Bluetooth

Bluetooth LE je verze, která byla vytvořena přímo pro potřeby IoT. Jedná se o verzi Bluetooth, která je energeticky nenáročná a tak je možné zařízení napájet po dlouhou dobu jen s pomocí baterie. Nejčastější využití nachází v konzumních IoT zařízeních, jako jsou chytré náramky a hodinky nebo v různých měřících zařízeních, například zařízení na měření srdečního tepu. Bezpečnost je řešena pomocí párování, při kterém si komunikující strany vymění své identifikační údaje a připraví šifrovací klíče pro budoucí přenos informací. K šifrování dat je použito AES-128. Díky pokročilému systému párování je Bluetooth LE odolné proti útoku typu Man-in-the-Middle.

V tabulce 1 je uvedeno srovnání některých bezdrátových technologií, které se využívají v IoT.

Tabulka 1: *Porovnání bezdrátových technologií*[10]

Standard	IEEE 802.15.4	Bluetooth LE	Wi-Fi (802.11n)
Frekvence	868/915 MHz, 2,4 GHz	2,4 GHz	2,4 GHz, 5,8 GHz
Rychlost	Až 250 Kb/s	260 Kb/s	Přes 100 Mb/s
Dosah	10 až 300 m	Až 150 m	70 až 250 m
Nároky na napájení	Velice nízké	Nízké	Vysoké
Životnost baterie	Měsíce až roky	Dny až týdny	Hodiny

3.2 PŘECHOD Z IPV4 NA IPV6

Pro komunikaci end-to-end je stěžejní, aby jakékoliv zařízení bylo možné v síti jednoznačně identifikovat. To je díky IPv6, vzhledem k počtu adres, možné.

Pokud bude záměrem pouze lokální IoT síť, pak je možné použít kterýkoliv proprietární protokol, který bude nejvýhodnější. Naopak, pokud je cílem mít vzdálený přístup ke kterémukoliv zařízení, a také přenos dat přes internet, je nutností využít nejlépe protokolu IPv6 (v případě IoT pak implementace 6LoWPAN). Přechod na tento nový protokol je, nejen pro IoT, velice stěžejní (IOT6, 2014).

[10] Zdroj: TENGYUEN, N. *5 Wireless Wifi 802.11 a, b, g, n, ac, ad, ah, aj, ax, ay Router Range and Distance Comparison*. GeckoandFly. 2016 [online]. [cit. 2016-04-28]. Dostupné z: http://www.geckoandfly.com/10041/wireless-wifi-802-11-abgn-router-range-and-distance-comparison/

IPv4

Protokol IPv4 je čtvrtá verze Internet Protokolu a byla popsána již v roce 1981. V této době bylo těžko představitelné, jak se bude vývoj posouvat dále a kolik bude potřeba adres. Protokol IPv4 využívá pro adresaci 32 bitů. Poskytuje tak 2^{32} adres, tedy přibližně 4 miliardy adres. To bylo v době jeho vzniku naprosto dostačující. Časem se zjistilo, konkrétně v devadesátých letech, že takový počet adres stačit nebude. To dalo za vznik několika studiím a bylo jen otázkou času, kdy vznikne protokol nový. V roce 1995 tak vzniká sada RFC, která definuje první IPv6 specifikaci. Označení je RFC 1883 - Internet Protocol, Version 6 (IPv6) Specification (DEERING, 1995). Mohlo by se zdát, že problém nedostatku adres byl zažehnán. Bohužel opak je pravdou. Využívat IPv4 bylo snadnější a stále výnosnější. Proti nasazení IPv6 stálo také zavedení adresace CIDR a zavedení NAT (UNIVERZITA PARDUBICE, 2014). To je mechanizmus převodu IP adres z jednoho adresního prostoru do jiného, při kterém se modifikuje informace o síťové adrese. To se zpravidla děje při průchodu směrovačem, kde je NAT aktivní. Přínos tohoto mechanizmu představuje hlavně snížení spotřeby IPv4 adres. Na druhou stranu jeho zápor je ve složitém, a za určitých podmínek nemožném (bez použití kontaktního serveru), navázání komunikace mezi dvěma zařízeními. V takovém případě, pokud bude IoT zařízení v oddělených sítích a tyto sítě budou využívat NAT, je nemožné navázat přímé spojení mezi zařízeními bez prvku, který by se choval jako kontaktní server (JENNINGS, 2007).

<table>
<tr><td>Version</td><td>IHL</td><td>Type of service</td><td colspan="2">Total length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment Offset</td></tr>
<tr><td colspan="2">Time to live</td><td>Protocol</td><td colspan="2">Header Checksum</td></tr>
<tr><td colspan="5">Source address</td></tr>
<tr><td colspan="5">Destination address</td></tr>
<tr><td colspan="4">Options</td><td>Padding</td></tr>
</table>

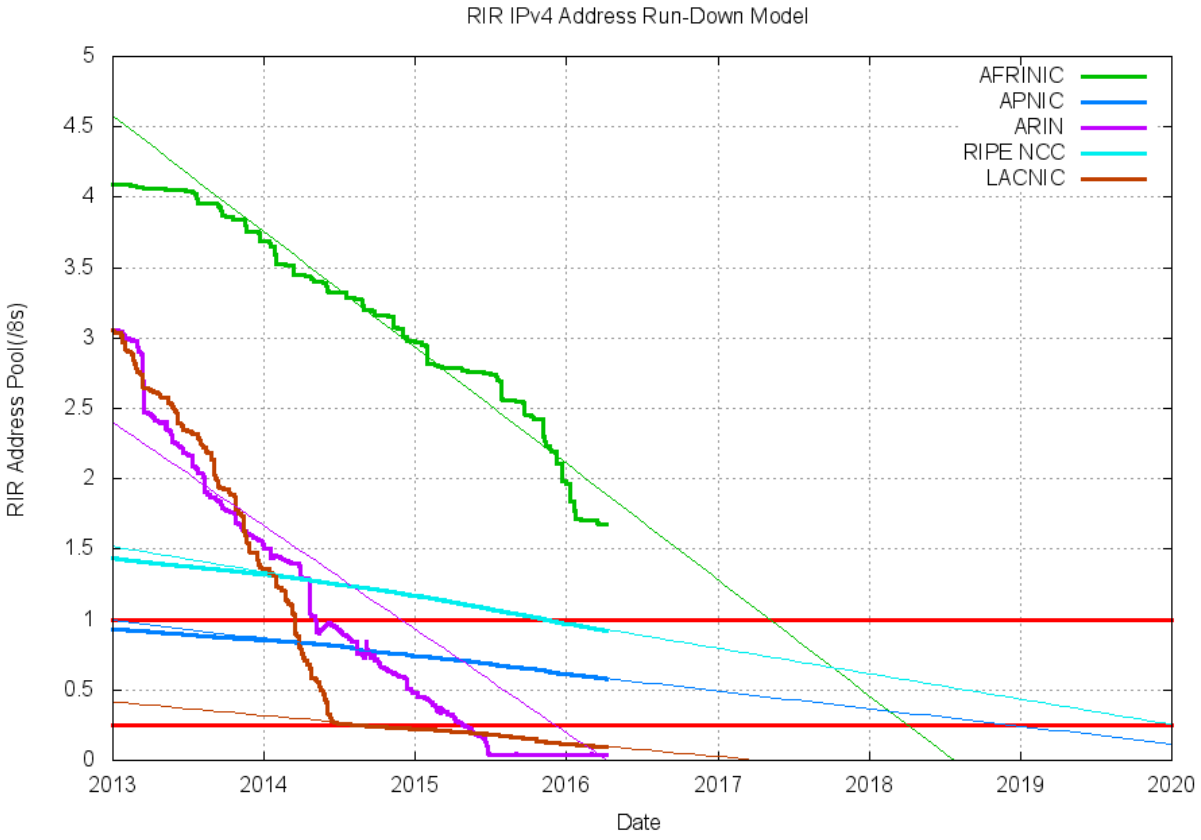
Obrázek 4: *Hlavička protokolu IPv4*[11]

V jakém stavu jsou zásoby IPv4 adres a jak je to s jejich vyčerpáním? Takto situaci popisuje Satrapa ve své knize (SATRAPA, 2011, str. 19):

„Aktuálně se nacházíme v situaci, kdy je vyčerpána centrální zásoba IANA a jednotlivé regionální registry (RIR) postupně spotřebovávají své zásoby. Nejrychleji rostoucí APNIC skončil s adresami velmi brzy po IANA, vyčerpání ostatních registrů je očekáváno během

[11] Zdroj: UNIVERZITA PARDUBICE. *IPv4 (Internet Protocol version 4)*. 2014 [online]. [cit. 2016-04-28]. Dostupné z: https://wiki.upce.cz/fei/studijni-materialy/ipv4_internet_protocol_version_4

několika let – evropský RIPE NCC kolem poloviny roku 2012, zbývající tři zhruba o rok až dva později. Vyčerpání registru neznamená, že v dané oblasti nelze získat IPv4 adresu. Ale místní poskytovatelé Internetu (v roli lokálních registrů, LIR) už nedostanou žádný větší blok. V režimu po vyčerpání regionální registry přidělují jen velmi omezené množství adres – každý lokální registr může získat jen jeden malý blok. Oficiálně jsou tyto adresy určeny pro přechodové mechanizmy.“



Obrázek 5: *Znázornění spotřeby zbývajících RIR adresních poolu*[12]

IPv6

Protokol, který eliminuje nedostatky svého předchůdce a zároveň přináší další různá vylepšení, to je IPv6. Jak již bylo zmíněno, jeho počátky se datují od devadesátých let, kdy vznikl první RFC definující základ IPv6. Nedostatek adres u tohoto protokolu nehrozí. Délka adresy IPv6 je totiž 128 bitů a díky tomu máme přibližně $3{,}4 \times 10^{38}$ adres. Jedná se o obrovské číslo, které je těžké si představit. Porovnání počtu adres je uvedeno v tabulce 2. Následující dvě definice se snaží přiblížit, o jak velké číslo se jedná:

[12] Zdroj: Geoff Huston. *IPv4 Address Report* [online]. 2016 [cit. 2016-04-29]. Dostupné z: http://www.potaroo.net/tools/ipv4/index.html

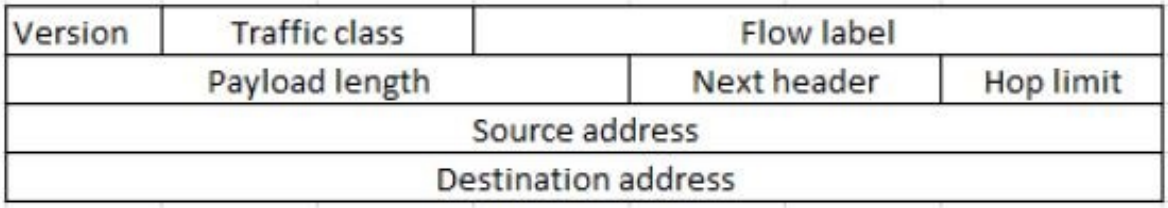
„IPv6's addressing scheme provides more addresses than there are grains of sand on Earth"[13] – (MICRIUM, 2015c).

„Povrch zeměkoule činí přibližně půl miliardy kilometrů čtverečních. To znamená, že na jeden čtvereční milimetr zemského povrchu připadá 667 × 10^{15} adres. Ano, řeč je o milionech miliard." – (SATRAPA, 2011).

Tabulka 2: *Porovnání počtu adres IPv4 a IPv6*[14]

Počet IPv4 adres (2^{32})	4 294 967 296
Počet IPv6 adres ($3{,}4\times10^{38}$)	340 000 000 000 000 000 000 000 000 000 000 000

Není možné ze dne na den přejít z IPv4 na IPv6, proto existují různé nástroje, které umožňují zároveň komunikaci mezi těmito protokoly. Jedná se o Dual Stack, mechanizmy tunelování nebo NAT64. Poslední zmíněný se pak stará o překlad IPv4 na IPv6 a naopak (UNIVERZITA PARDUBICE, 2014).



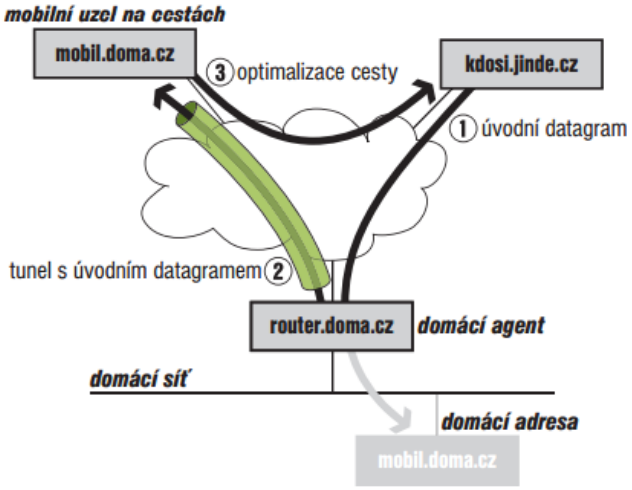
Obrázek 6: *Hlavička protokolu IPv6*[15]

Na obrázcích 4 a 6 jsou ilustrovány hlavičky obou protokolů. Jak je na první pohled zřejmé, IPv6 má hlavičku mnohem jednodušší a tak je zpracování ve směrovači rychlejší a jednodušší. Zároveň přináší i mnoho bezpečnostních vylepšení, mezi které například patří (THE GOVERNMENT OF THE HONG KONG SPECIAL ADMINISTRATIVE REGION, 2011):

- vzhledem k obrovskému množství adres je skenování otevřených portů velmi obtížné (vlastnost),
- k IPv6 adrese je možné přiřadit veřejný klíč, tato adresa se pak nazývá Cryptographically Generated Address (CGA),
- IP Security (dále IPsec) ve dvou rozšiřujících hlavičkách AH (Authentication Header) a ESP (Encapsulating Security Payload).

[13] Adresní schéma IPv6 nabízí více adres než je na světě zrnek písku.
[14] Zdroj: vlastní výpočet
[15] Zdroj: UNIVERZITA PARDUBICE. *IPv6 (Internet Protocol version 6)*. 2014 [online]. [cit. 2016-04-28]. Dostupné z: https://wiki.upce.cz/fei/studijni-materialy/ipv6_internet_protocol_version_6

IPv6 zároveň myslí i na mobilitu zařízení, její poslední podoba je definována v dokumentu RFC 6275 (PERKINS, 2011). To znamená, že každé mobilní zařízení má nějakou svoji domácí síť, ve které má svoji domácí adresu (dále HA), ta se nemění a je pro zařízení zaregistrována v DNS. Pokud je zařízení v pohybu a zpravidla dostává další dočasné adresy (dále CoA), stále je dostupné přes svoji HA. Aby však toto fungovalo, musí mít zařízení zvoleno domácího agenta – to je směrovač v domácí síti – ten předává všechny datagramy, které jsou směrovány na HA pomocí tunelu do zařízení. Díky tomuto systému je dále možné použít optimalizaci cesty. To znamená, že se korespondent dozví CoA mobilního zařízení a může s ním tak komunikovat napřímo, jak je vidět na obrázku 7 (SATRAPA, 2011).



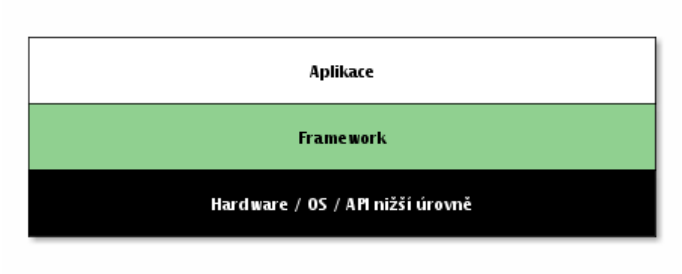
Obrázek 7: *Postup navázání spojení s mobilním zařízením*[16]

3.3 PŘEHLED FRAMEWORKŮ

Po výběru technologií pro zajištění bezdrátové konektivity je nutné začít přemýšlet o tom, jak zajistit vzájemnou komunikaci a interakci mezi všemi připojenými věcmi. Programování aplikace od začátku by určitě zabralo nemálo času. Naštěstí v dnešní době existuje mnoho frameworků, a některé jsou i open source, které lze použít a volně je upravovat. AllJoyn, IoTivity, Thread nebo HomeKit – toto je jen malý výčet ze všech dostupných frameworků.

Co si představit pod pojmem framework (také na obrázku 8) definuje Majda (2009) jako: „ucelený soubor tematicky zaměřených knihoven + policy decisions“.

[16] Zdroj: SATRAPA, Pavel. *IPv6: internetový protokol verze 6*. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC, 2011. CZ.NIC. ISBN 978-80-904248-4-5.



Obrázek 8: *Framework jako mezičlánek mezi hardwarem a aplikací*[17]

3.3.1 IOTIVITY

Tento open source projekt je vyvíjen pod záštitou „The Linux Foundation“, což je neziskové konsorcium, jehož účelem je podpora vývoje Linuxu. Informace o prvním vydání IoTivity byla zveřejněna v roce 2015, tedy rok po tom, co vznikla skupina OIC. Od této skupiny přejímá a implementuje vydané standardy a specifikace (LINUX FOUNDATION, 2015). Znění přesné definice je (OPEN CONNECTIVITY FOUNDATION, 2016a):

„IoTivity is an open source software framework enabling seamless device-to-device connectivity to address the emerging needs of the Internet of Things.“[18]

Hlavní jádro IoTivity je napsané v programovacím jazyce C a většina jeho funkcionalit je dostupná v C i v C++. Je dostupný také pro Android (Java) a pracuje se na podpoře pro JavaScript. Framework staví na čtyřech základních blocích (IOTIVITY, 2016a):

- objevování (zařízení a zdrojů),
- přenos dat,
- správa dat,
- správa zařízení.

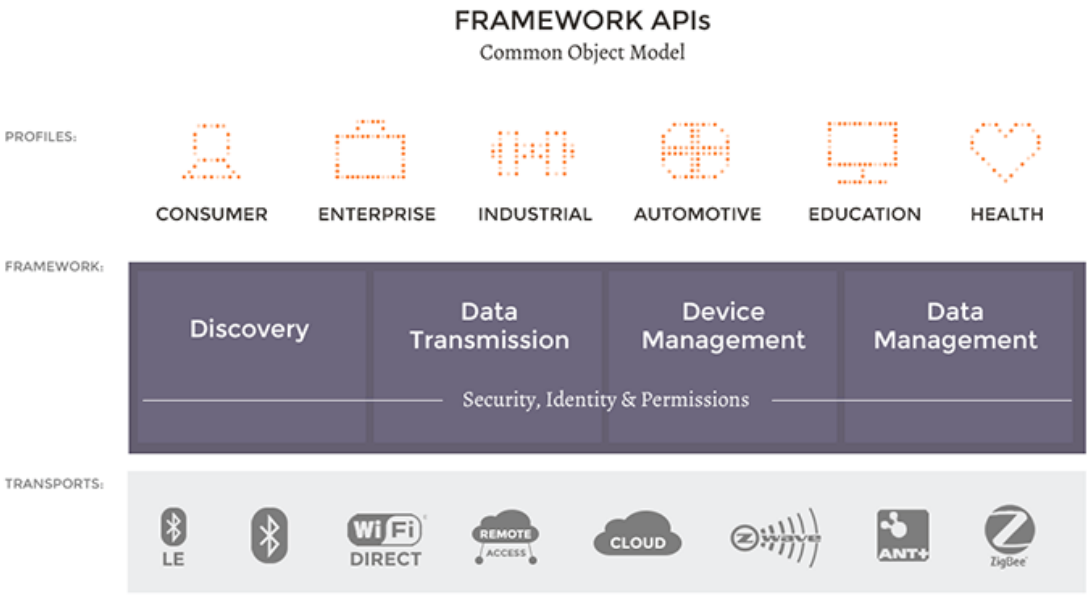
Velice důležitá je bezpečnost. Ta je zde vyřešena pomocí vrstvy „Secure Resource Manager“ a je implementována přímo v jádře, jak je znázorněno na obrázku 9. Tato vrstva má dva hlavní úkoly (IOTIVITY, 2016b):

- Filtruje požadavky přístupu ke zdrojům. Přístup k nim buď uděluje nebo ho zamítá. Filtrování je založeno na nastavené politice přístupu.

[17] Zdroj: MAJDA, D. *Knihovny vs. Frameworky*. 2009 [online]. [cit. 2016-04-30]. Dostupné z: http://majda.cz/blog/265

[18] IoTivity je open source software framework umožňující bezproblémové připojení mezi zařízeními (zařízení-do-zařízení) řešící vznikající potřeby internetu věcí.

- Spravuje materiály související s bezpečností. Tím jsou například správa pověření, načtení a udržování ACL (Access control list).



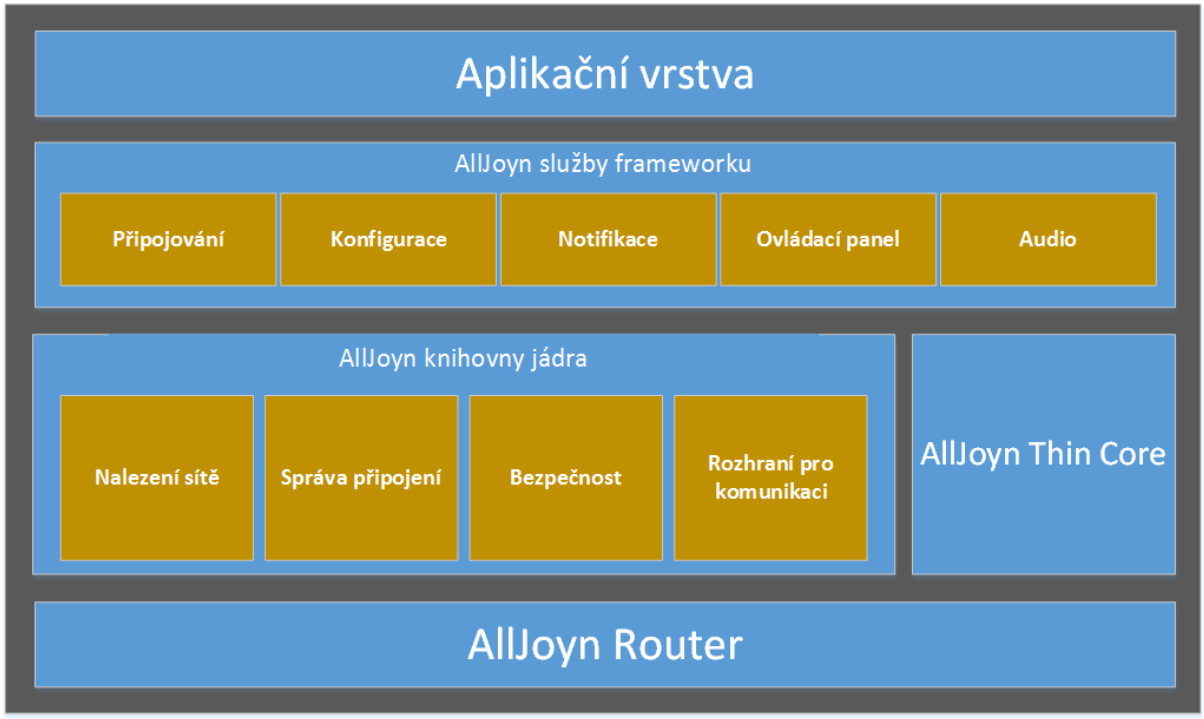
Obrázek 9: *Grafické znázornění modulů frameworku IoTivity*[19]

3.3.2 ALLJOYN

Jedná se o open source framework, který usnadňuje zařízením a aplikacím jejich vzájemné vyhledání a komunikaci. Vývojáři tak mohou vytvářet aplikace, které nebudou závislé na transportní vrstvě a výrobci. Je spustitelný na různých platformách, jako je Linux, Android (Linux), iOS, Windows a také na dalších jednoduchých systémech real-time. Za tímto frameworkem stojí AllSeen aliance. Framework je postaven na několika blocích (ALLSEEN ALLIANCE, 2016a):

- fyzická vrstva,
- základní framework,
- tenký klient,
- framework běžných služeb,
- aplikační vrstva.

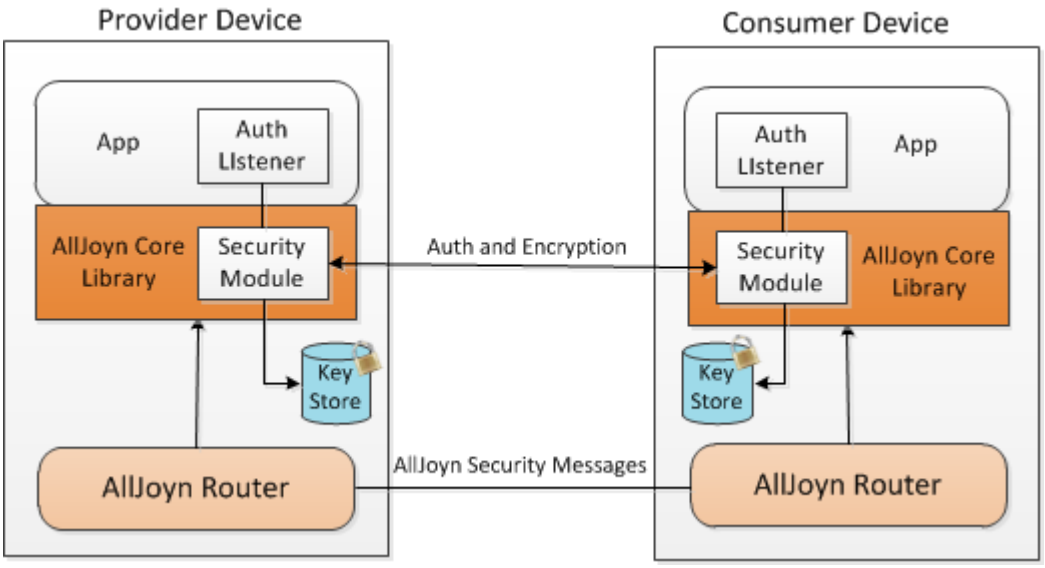
[19] Zdroj: IOTIVITY. Architecture Overview. 2016 [online]. [cit. 2016-04-28]. Dostupné z: https://www.iotivity.org/documentation/architecture-overview



Obrázek 10: *Prvky frameworku*[20]

Bezpečnost je řešena přímo pomocí implementace v samotném jádře frameworku a je velice dobře popsána v dokumentaci. Aplikace se mezi sebou autentizují a posílají zašifrovaná data. Autentizace a šifrování dat je prováděno přímo v aplikaci, jak je ilustrováno na v obrázku 11. Klíče pro autentizaci a šifrování jsou uloženy ve výchozím úložišti klíčů, které je spravováno pomocí modulu zabezpečení, případně může být v aplikaci implementováno vlastní úložiště. Pro autentizaci využívá framework Simple Authentication and Security Layer (ALLSEEN ALLIANCE, 2016b).

[20] Zdroj: vlastní



Obrázek 11: *Bezpečnostní architektura frameworku*[21]

Dále existuje bezpečnostní rozšíření, které je označeno jako „Security 2.0“. Cílem je povolit aplikaci ověření přístupu k zabezpečenému rozhraní nebo objektu na základě bezpečnostních politik nainstalovaných vlastníkem. Vlastník může tyto politiky nastavovat pomocí ACL (ALLSEEN ALLIANCE, 2016c).

3.4 DATOVÉ SKLADIŠTĚ A SLUŽBY TYPU CLOUD

Rychlé rozšiřování všemožných IoT řešení je jedna část evoluce. Další část, na kterou je nutné myslet, jsou data získaná z těchto systémů. Jaká data získávat? Za jakým účelem je získávat? Jak a kde je zpracovávat? Kde a jak dlouho je uchovávat? – Tyto a mnoho dalších otázek je nutné si položit.

Na začátek je nutné definovat, co se skrývá pod označením cloud. Definicí a druhů cloudu je několik. Cloud computing je síť propojených serverů, na kterých je možné spouštět výpočetní úkony (aplikace) nebo je využít jako úložiště dat. Toto byla jedna z možných definic cloudu. Na cloud se dá také nahlížet dvěma pohledy – pohledem vývojáře a pohledem uživatele. Pro vývojáře je typické jeho využití pro běh jeho aplikací mimo jeho vlastní počítač. Uživatel typicky využívá cloud pro ukládání dat a následný přístup k těmto datům odkudkoliv. Cloud computing je založen na jednoduché myšlence, pozadí je však velmi obsáhlé a tudíž složité na pochopení a není cílem této práce se jím dále zabývat (MALÝ, 2011).

[21] Zdroj: ALLSEEN ALLIANCE. *AllJoyn Security*. 2016 [online]. [cit. 2016-04-28]. Dostupné z: https://allseenalliance.org/framework/documentation/learn/core/system-description/alljoyn-security

Analytici odhadují, že do roku 2020 bude každý člověk generovat 5 200 GB dat. To je dost velký obsah, který je potřeba někde uchovat (EMC, 2012). Pro osobní počítače dnes existují různé služby cloud, které mnoho lidí používá a nemusí se jednat pouze o prosté úložiště dat. Skoro každý velký hráč na trhu IT nabízí nějaká svá řešení. Dropbox, Microsoft OneDrive, Google Drive nebo dokonce i Mega, u jehož zrodu stála kontroverzní postava Kim Dotcom, je pouze výčet některých z nich (CASSERLY, 2016).

Firmy poskytující IoT vědí, že jejich zařízení budou generovat velké množství dat a je nutné si s tím nějakým způsobem poradit. K tomu využívají právě cloud computing. Někteří vkládají prostředky do vývoje svých proprietárních řešení. Ti ostatní, kteří nemají takové možnosti, preferují využití služeb třetích stran. Zde však hraje velkou roli otázka ohledně bezpečnosti dat. Pokud jsou data uložena u poskytovatele, teoreticky k ním může mít přístup kdokoliv jiný než vlastník (MICRIUM, 2015a).

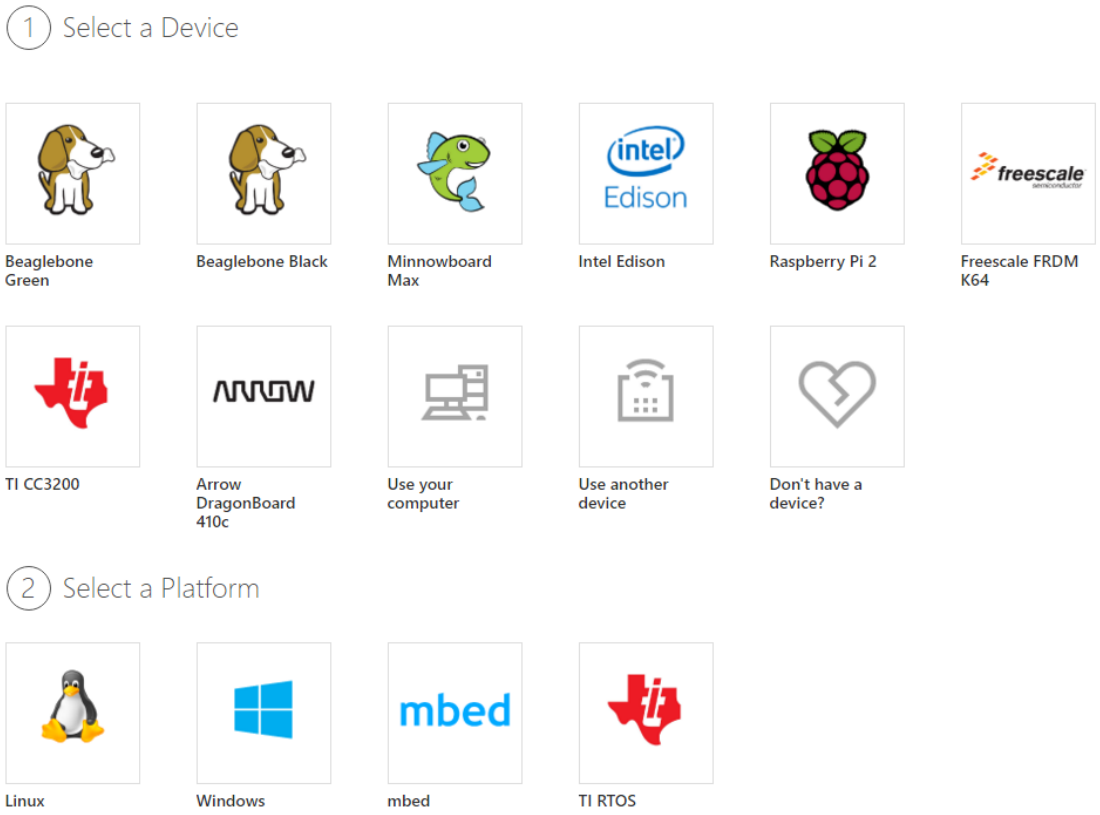
3.4.1 PŘEHLED KOMERČNÍCH SLUŽEB CLOUD COMPUTINGU PRO IOT

Amazon Web Service IoT

AWS IoT je jedna z mnoha služeb, která cílí na propojení zařízení s cloudem, za kterou stojí společnost Amazon. Služba dokáže propojit miliardy zařízení a zpracovat miliardy zpráv, které tato zařízení vyprodukují. Nesporná výhoda je ta, že AWS IoT může využívat dalších služeb cloud computingu, které Amazon nabízí. Sběr dat, jejich zpracování a analýza, prezentace i následné skladování, tak probíhá výhradně v cloudu a není potřeba vlastnit nákladnou infrastrukturu. Takzvaná AWS IoT Device Gateway se stará o zabezpečenou komunikaci mezi zařízeními a AWS IoT. Podporované protokoly jsou MQTT, WebSockets a HTTP 1.1, ale není potřeba se omezovat pouze na ně. Je totiž možné velice jednoduše implementovat jiné proprietární nebo starší protokoly. Veškerá komunikace je šifrována pomocí TLS a probíhá až po vzájemné autentizaci mezi zařízením a AWS IoT. Autorizace probíhá na základě zadaných politik, ty se zadávají ve formátu JSON. Data přímo v cloudu jsou chráněna pomocí bezpečnostních mechanik AWS. Cenová politika je založena na počtu přenesených zpráv od zařízení k AWS IoT a naopak. Základní balíček zahrnuje přenos 250 000 zpráv zdarma a například přenos milionu zpráv stojí $5. Jedna zpráva je definována jako blok dat o velikosti 512 bajtů. Amazon nabízí velice detailní dokumentaci ke svému SDK, ve které popisuje nejen možnosti zabezpečení (AMAZON WEB SERVICES, 2016).

Azure IoT Hub

Ani Microsoft nezahálel a nabízí tak své řešení pojmenované jako Azure Internet of Things Hub. Myšlenka je opět podobná jako u předchozího – propojit miliardy zařízení. Samotný Azure IoT Hub se stará spíše o správu zařízení. Zpracování zpráv řeší další poskytované služby jako je Azure IoT Suite nebo Stream Analytics. Podporované komunikační standardy jsou AMQP, MQTT a HTTP/1, zabezpečení transportní vrstvy je řešeno pomocí TLS. Služba podporuje různá zařízení a také různé platformy, jak je vidět na obrázku 12. Služba v základu nabízí balíček pro připojení 500 zařízení a přenosu 8 000 zpráv za den zdarma. Základní placený balíček je omezen pouze přenosem 400 000 zpráv za den a stojí $50 měsíčně (MICROSOFT AZURE, 2015).



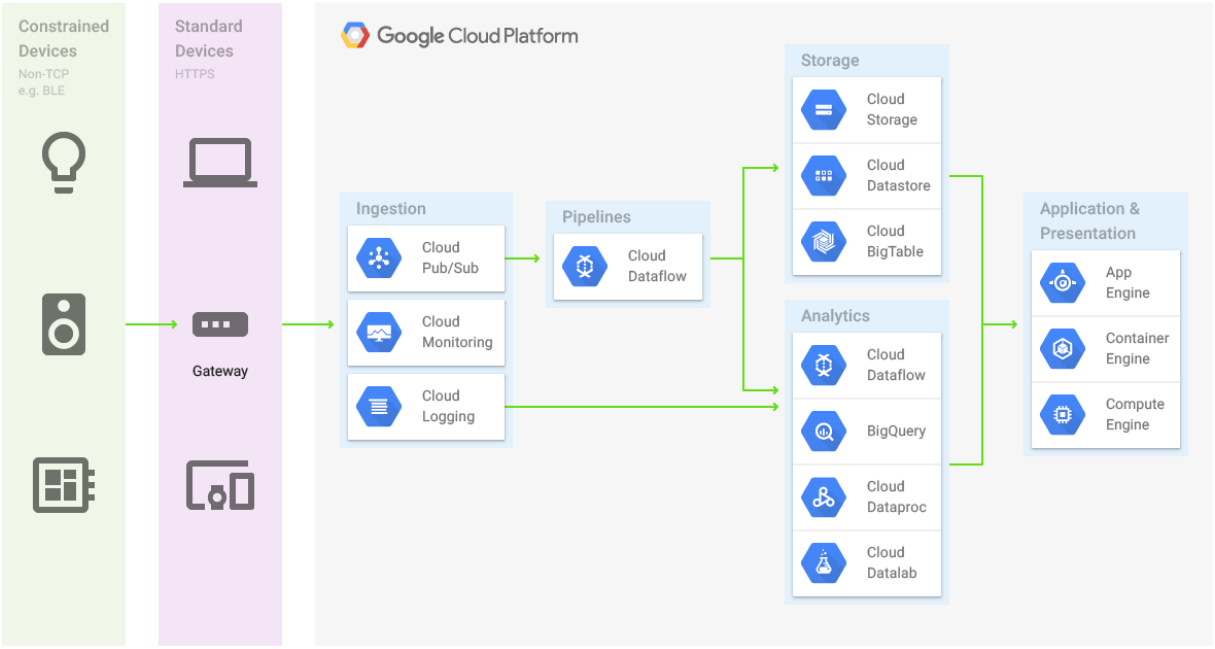
Obrázek 12: *Přehled podporovaných zařízení a platforem službou Azure IoT Hub*[22]

Google Cloud Platform

Google nabízí v rámci své platformy různé nástroje, díky kterým lze jednoduše propojit zařízení, ze kterých se pak přenášejí data. Tyto nástroje jsou rozšířeny o další, které dokáží získaná data analyzovat. Pro lepší představu je vše znázorněno na obrázku 13. Google si pak za

[22] Zdroj: MICROSOFT AZURE. *Connect your device to Azure IoT Hub*. 2016 [online]. [cit. 2016-04-28]. Dostupné z: https://azure.microsoft.com/en-us/develop/iot/get-started/

přenos 5 000 000 zpráv za měsíc naúčtuje $2. K této ceně je nutné připočíst náklady za zpracování a uložení dat (GOOGLE CLOUD PLATFORM, 2016).



Obrázek 13: *Zpracování IoT dat ve službě Google Cloud Platform*[23]

3.5 REÁLNÉ BEZPEČNOSTNÍ HROZBY

Od základu, kdy byly jednoduché prvky, přes jejich připojení do sítě a využití frameworků, až po přenos dat do cloudu a jejich zpracování, všude je nějakým způsobem řešeno zabezpečení. Na první pohled se tak může zdát, že IoT je bezpečné. Vzhledem k tomu, že využívá různé prvky, které jsou zde již řadu let a je u nich tak vyvinuta bezpečnost na dobré úrovni, je to reálný pohled. Ovšem IoT je naprosto nový koncept, ve kterém musíme čelit novým bezpečnostním výzvám a hrozbám. Je třeba myslet také na soukromí uživatelů. Útoky proti IoT je možné rozdělit na různé části. Zpravidla se však jedná o 3 hlavní kategorie podle cíle útoku (GEMALTO, 2015):

- proti IoT zařízení,
- na komunikaci,
- proti správcovskému (hlavnímu) zařízení.

Jedním z problémů je, že většina těchto koncových zařízení má pouze tolik výpočetních prostředků a paměti, kolik potřebují pro vykonání úlohy, na kterou jsou určeny. Není tedy reálné na zařízení používat různé druhy black listů nebo white listů, protože zabírají mnoho

[23] Zdroj: GOOGLE CLOUD PLATFORM. *Overview of Internet of Things*. 2016 [online]. [cit. 2016-04-28]. Dostupné z: https://cloud.google.com/solutions/iot-overview

místa. Další z problému je samotné fyzické zabezpečení miliardy těchto nových zařízení od vnějších vlivů. Šíření aktualizací a jejich instalace je také jedna z nových bezpečnostních výzev a bude nutné vyřešit otázku, jak zajistit jejich distribuci do těchto jednoúčelových zařízení bez výrazného dopadu na jejich funkčnost a také na spotřebu energie. Nakonec i ochrana a soukromí dat je velice důležitá. Jiné bezpečnostní politiky budou nastaveny u dat, které prezentují teplotu na zahradě a jiné u dat, které reprezentují aktuální odběr proudu (WIND RIVER SYSTEMS, 2015).

Společnost HP vydala v roce 2015 zprávu o svém výzkumu o 10 nejvíce používaných zařízeních v IoT, ve kterém se zaměřila na zabezpečení. Čísla jsou opravdu alarmující (HEWLETT PACKARD ENTERPRISE, 2015):

- 70 % zařízení nepoužívá šifrovaný přenos,
- 80 % zařízení (spolu s aplikací a cloudem) má nízké požadavky na heslo,
- 90 % zařízení uchovává minimálně jednu osobní informaci (zahrnuje i aplikaci a cloud),
- 6 z 10 zařízení má různé chyby ve webovém rozhraní.

Mezi nejvíce zranitelná místa IoT podle OWASP patří (2014):

1. nezabezpečené webové rozhraní,
2. nedostatečná autentizace/autorizace,
3. nezabezpečené síťové služby,
4. nedostatek šifrování a ověřování integrity dat na transportní vrstvě,
5. soukromí,
6. nezabezpečené rozhraní cloudu,
7. nezabezpečené mobilní rozhraní,
8. nedostatečné možnosti nastavení zabezpečení,
9. nezabezpečený software nebo firmware,
10. slabé fyzické zabezpečení.

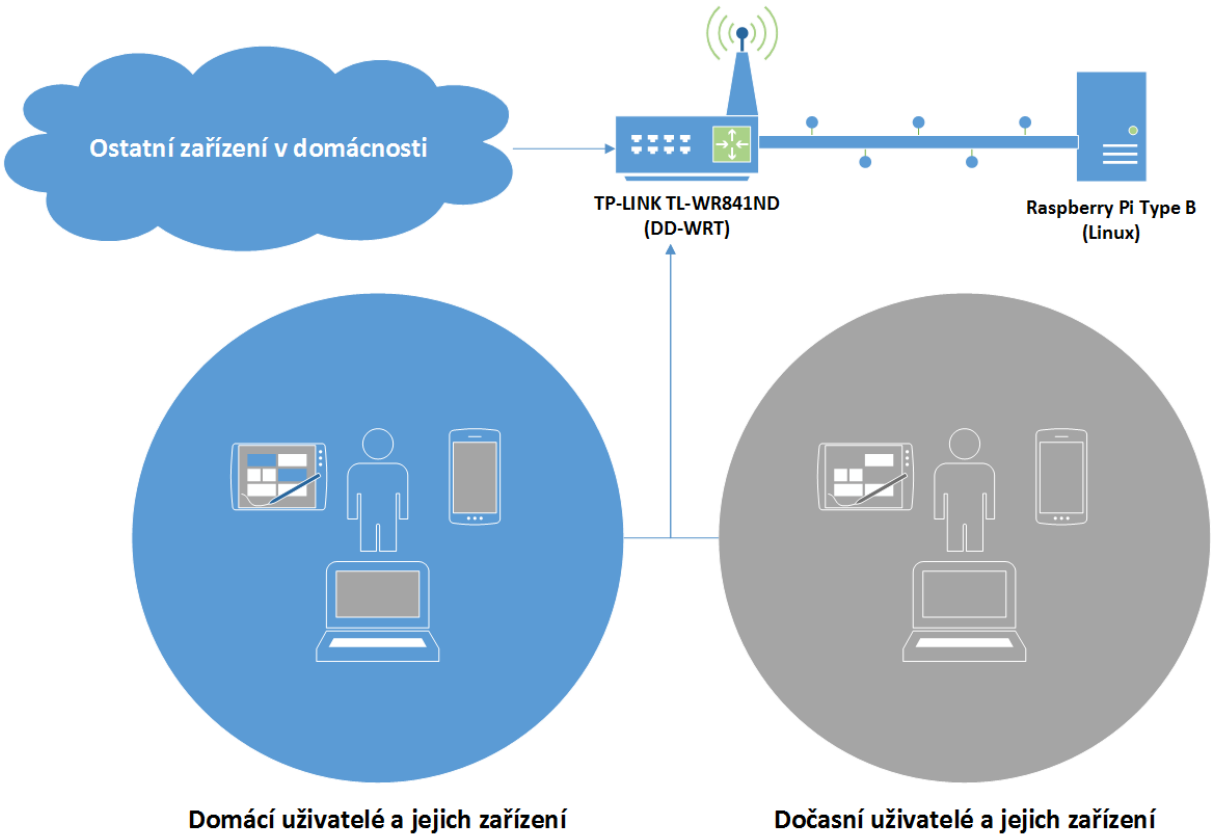
Tato zranitelná místa nahrávají útočníkům. Následuje příklad zneužití některé z chyb v kritickém odvětví – automobilismu. V roce 2014 se povedlo bezpečnostním expertům (Charlie Miller a Chris Valasek) vzdáleně ovládnout vůz značky Jeep a mohli tak ovládat veškerou jeho elektroniku. Nejdříve se jim podařilo pomocí prolomení hesla k Wi-Fi sítí vozu kompletně ovládnout multimediální systém. Ten je však oddělen od sběrnice CAN, která je využívaná pro interní komunikaci senzorů a ovládacích jednotek vozu. Po dalším výzkumu přišli na to, že multimediální systém dokáže komunikovat s modulem, který je připojen na tuto

sběrnici a po úpravě softwaru se jim tak podařilo ovládnout kompletní elektroniku vozu (DROZHZHIN, 2015).

4 ZABEZPEČENÍ CHYTRÉ DOMÁCNOSTI

Jedno z odvětví, kde IoT zažívá doslova „boom“, jsou domácnosti. Jak bylo uvedeno v předchozích kapitolách, na trhu je dostupných mnoho řešení. Uživatelé si mohou vše sestavit samostatně, zaplatit firmě za řešení na míru, nebo koupit již hotové produkty. Je pouze na nich, co si zvolí. Velice reálná je jejich kombinace, protože například chytrou televizi si člověk koupí již jako hotovou věc. Všechny zmíněné řešení mají však jedno společné – jsou součástí domácí sítě. Ta se v této době řeší většinou jedním centrálním prvkem (v domácnostech), který zastupuje pozici směrovače, přepínače a přístupového bodu. Rozvody už nejsou omezeny jen na kabelové, ale hojně se využívá přístupu pomocí sítě Wi-Fi. Obyvatelé se k těmto sítím připojují pomocí osobních počítačů nebo mobilních zařízení. Další provoz tvoří například návštěvy, které do objektu přicházejí a běžně je jim od vlastníků domu (provozovatele sítě) umožněn přístup do sítě. To je nejčastěji poskytnutí jednotného klíče, který slouží pro autentizaci. Ten je pak v zařízení uložen a osoba, která tento klíč zná, ho může poskytnout dalším osobám. S tím přicházejí bezpečnostní rizika, které není možné přehlížet. Pokud je do těchto sítí dále začleněno IoT řešení, je potřeba přehodnotit, jak je síť postavena a jaké jsou zde modely zabezpečení. Z hlediska soukromí není žádoucí, aby bylo možné odposlouchávat komunikaci cizími osobami. Je tedy nutné, aby síť byla dostatečně zabezpečena a monitorována. A tím se bude zabývat tato kapitola. Tématem nebude přímo zabezpečení IoT zařízení, to je úloha jeho výrobce, ale hlavně zabezpečení sítě, ve které se tyto zařízení nasazují. V této kapitole bude představen návrh jednoduché sítě pro domácnost, ve které je kladen důraz na zabezpečení a monitorování aktivit uživatelů. Hlavním činitelem bude SOHO zařízení, které kombinuje směrovač, přepínač, přístupový bod a zároveň je kompatibilní s open source firmwarem DD-WRT. Oporu pro využití architektury AAA bude tvořit Raspberry Pi Type B s příslušným softwarem.

4.1 PŘEDSTAVENÍ DOMÁCNOSTI, SÍŤOVÝCH PRVKŮ A JEJICH SOFTWARU



Obrázek 14: *Modelová domácnost*

Modelová domácnost je na obrázku 14 a skládá se z několika částí:

- síťové prvky a server,
- domácí uživatelé a jejich zařízení,
- dočasní uživatelé a jejich zařízení,
- a ostatní zařízení v domácnosti (chytré TV, tiskárny, výchozí brána IoT).

V této sítí bude úkolem provést základní nastavení zabezpečení síťových prvků, nasazení AAA protokolu a oddělení Wi-Fi sítě pro domácí uživatele od sítě pro dočasné uživatele. Pro místní síť se předpokládá číslování 192.168.1.0/24. Síť pro dočasné uživatele bude 192.168.2.0/24, přičemž bude zakázáno těmto uživatelům komunikovat s uživateli v jiné síti. První adresa v síti odpovídá směrovači a klientům DHCP je vyhrazen prostor od 100 adresy výše.

Směrovač

Pro praktickou ukázku byl zvolen TP-LINK TL-WR841N. Jedná se o zařízení, které v sobě kombinuje funkce směrovače, přepínače a přístupového bodu. V tomto zařízení je nahraný alternativní firmware DD-WRT, který otevírá další možnosti, jak zařízení využít. Zařízení

slouží jako hlavní směrovač, přiděluje adresy pomocí serveru DHCP a také je v režimu AP, kdy dovoluje bezdrátové připojení uživatelů přes Wi-Fi. Ta je rozdělena na dvě sítě. Jedna pro domácí uživatele a druhá pro dočasné uživatele, jak je vidět na obrázku 14. Zabezpečení této sítě tvoří WPA2 Enterprise, kdy se klienti ověřují pomocí protokolu RADIUS.

Server

Jako server je použit Raspberry Pi Type B s nainstalovaným operačním systémem MINIBIAN. Pro protokol RADIUS je využito jeho implementace do open source produktu, jímž je FreeRADIUS. Pro evidenci klientů a uživatelů je využita databáze MySQL. Pro pohodlnou správu FreeRADIUS, přístupových serverů, uživatelů a přehled účtování je využito daloRADIUS. Díky tomu musí být na serveru nainstalovaný Apache. Adresa serveru je 192.168.1.10. Tato práce se zabývá pouze instalací a konfigurací FreeRADIUS a nástavby daloRADIUS.

4.2 KONFIGURACE CENTRÁLNÍHO PRVKU

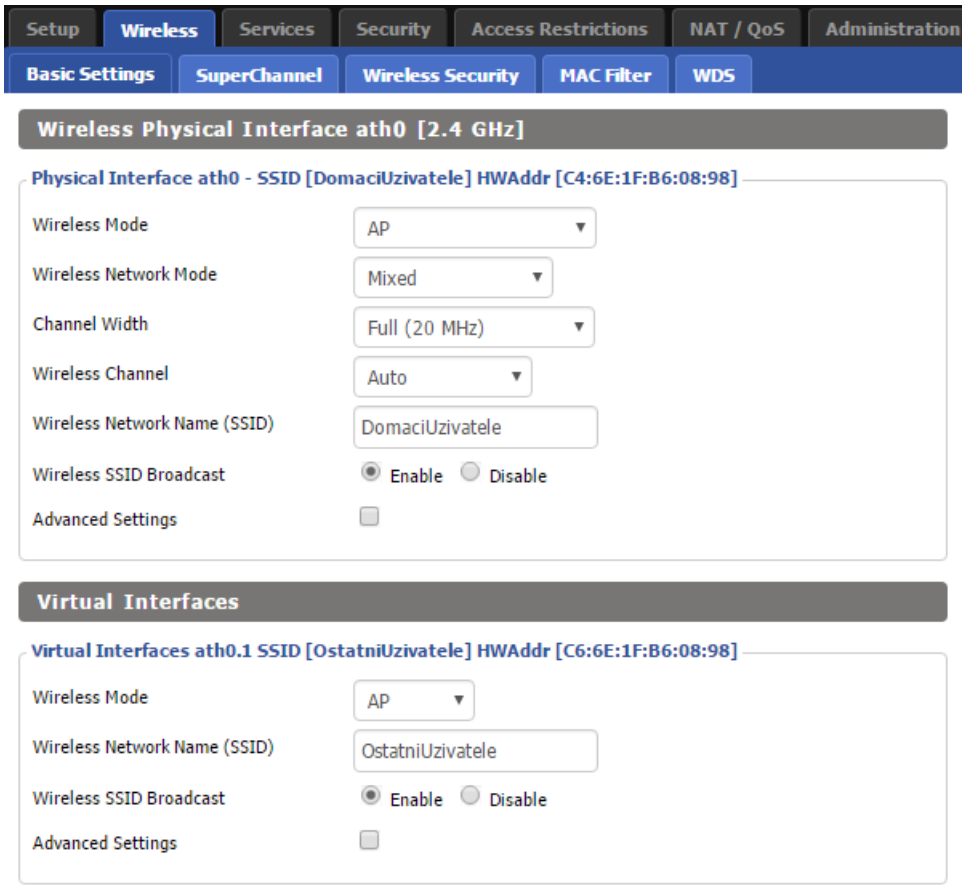
Zařízení je po prvním spuštění ve výchozím stavu, proto je nutné vše nastavit. To bude provedeno pomocí webového rozhraní. První krok je propojení centrálního prvku s počítačem pomocí síťového kabelu.

V této chvíli je na počítači nutné otevřít internetový prohlížeč a zadat do adresního řádku IP adresu 192.168.1.1 (výchozí IP adresa zařízení s nainstalovaným DD-WRT). Při prvním přístupu je uživatel vyzván ke změně výchozího jména a hesla pro přihlašování do webové administrace zařízení. Pro příklad bude využito jméno „spravce“ a heslo „Spravc3Domu“.

Ve výchozím stavu je povoleno zobrazení informační stránky o využití zařízení a o připojených klientech. To je nežádoucí, a proto bude tato stránka nastavena jako nedostupná pro nepřihlášené uživatele. To se provede v nastavení dostupném pod Administration → Management a zde zvolením „Disabled“ u řádku Enable Info Site.

Vytvoření a zabezpečení sítí Wi-Fi

Na začátku je nutné vytvořit dvě sítě Wi-Fi. Nastavení se provede v záložce Wireless a poté Basic Settings. Zde se musí kliknutím na tlačítko „Add“ přidat další síť. Kompletní nastavení je na obrázku 15. Nastavení se aplikuje kliknutím na tlačítko „Apply Settings“.

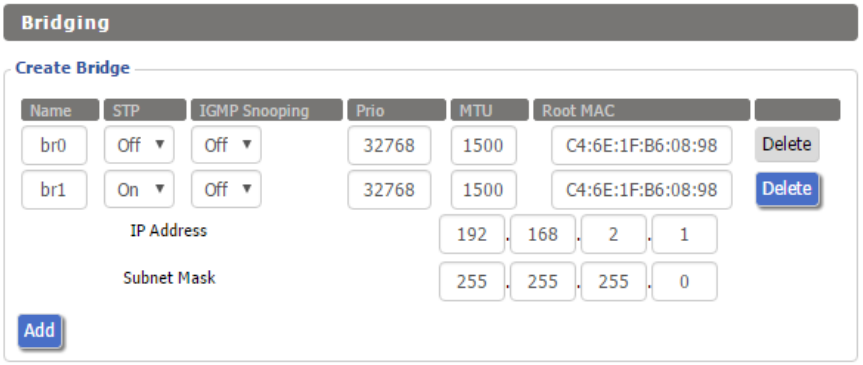


Obrázek 15: *Vytvoření bezdrátových sítí*

Dalším krokem je sítě zabezpečit. To se provádí také v záložce Wireless a poté Wireless Security. Následující instrukce jsou pro obě sítě stejné. Jak bylo řečeno dříve, ověřování uživatelů bude řešeno pomocí serveru RADIUS, proto je nutné jako Security Mode zvolit „WPA2 Enterprise“. Radius Auth Server Address je 192.168.1.10. Radius Auth Shared Secret je heslo, které bude pro klienta zvoleno při konfiguraci FreeRADIUSu (v kapitole 4.3), v tomto případě je heslo „Super1H3s!o“. Radius Accounting musí být zvoleno jako „Enable“. Adresa a sdílené heslo pro Accounting je stejné jako pro předchozí nastavení Auth. V této chvíli se nastavení aktivuje kliknutím na tlačítko „Apply Setings“.

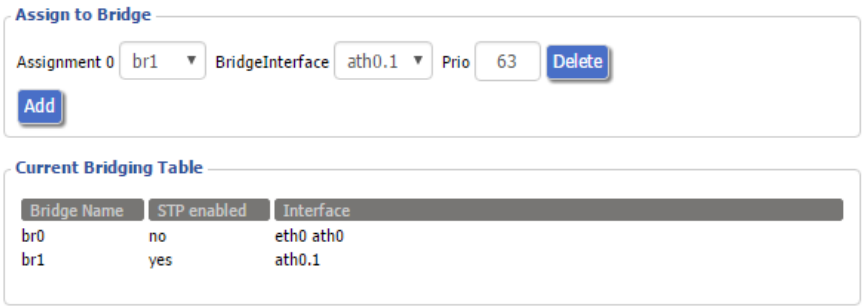
Oddělení komunikace mezi sítěmi

V tomto kroku je potřeba oddělit komunikaci mezi soukromou sítí a sítí pro dočasné uživatele. První nastavení se provádí pod záložkou Setup a poté Networking. V části Create Bridge je nutné kliknout na tlačítko „Add“, nově vytvořený záznam pojmenovat „br1“ a aplikovat nastavení kliknutím na tlačítko „Apply Setings“. Po obnovení stránky je třeba nastavit novému mostu adresu, která je v jiné podsíti, než je soukromá síť. V tomto případě bude nastavena IP adresa 192.168.2.1 a síťová maska bude 255.255.255.0, nastavení je uvedeno na obrázku 16.



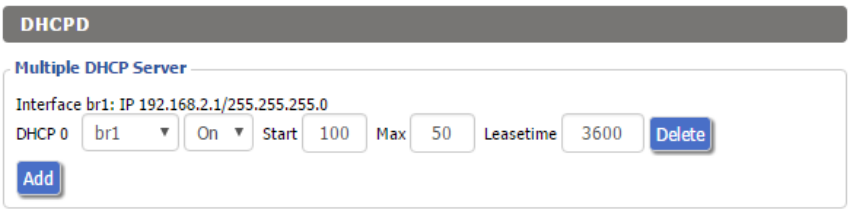
Obrázek 16: *Vytvoření nového síťového mostu*

V části Assign to Bridge se musí kliknout na tlačítko „Add“, vybrat „br1“ z rozevíracího seznamu a jako BridgeInterface vybrat označení rozhraní sítě pro dočasné uživatele, v tomto případě „ath0.1“. Nakonec je třeba aplikovat nastavení kliknutím na tlačítko „Apply Settings“. Nastavení je uvedeno na obrázku 17.



Obrázek 17: *Přiřazení síťového mostu bezdrátovému rozhraní*

V dalším kroku se musí nastavit DHCP server pro tuto oddělenou síť. To se nastavuje v části Multiple DHCP Server na stejné stránce jako u předchozího. Kliknutím na tlačítko „Add“ se zobrazí nový záznam, u kterého je nutné vybrat v prvním seznamu „br1“ a poté kliknout na tlačítko „Apply Settings“. Nastavení je uvedeno na obrázku 18.



Obrázek 18: *Konfigurace DHCP serveru pro nový síťový most*

Jako poslední krok je nastavení izolace dočasných klientů od přístupu do soukromé sítě. To se nastavuje v části Network Configuration br1, kde je nutné u položky Net Isolation nastavit hodnotu „Enable“. Následuje aplikování nastavení a je doporučen restart zařízení. V této chvíli se musí nainstalovat a nastavit server RADIUS.

4.3 INSTALACE A KONFIGURACE SW NA RASPBERRY PI

Jak bylo výše zmíněno, jako server, na kterém je spuštěn FreeRADIUS, byl zvolen miniaturní počítač Raspberry Pi Type B.

Instalace FreeRADIUS

Při zadávání příkazů se předpokládá, že má uživatel dostatečná práva, případně že je vše zadáváno pod správcem systému. Pro instalaci FreeRADIUS stačí zadat příkaz *apt-get install freeradius freeradius-mysql*. V této chvíli je server nainstalovaný, je však nutné provést dodatečnou konfiguraci, aby bylo možné využívat databázi a nástavbu daloRADIUS.

Následuje přístup do konzole databáze pomocí příkazu *mysql –u root –p*. Vytvoření databáze je provedeno příkazem *create database radius*, přidání uživatele a nastavení práv pomocí *grant all on radius.* to radius@localhost identified by "password"*. V této chvíli je nutné opustit konzoli MySQL. Příkazem *mysql -u root -p radius < /etc/freeradius/sql/mysql/schema.sql* a dále *mysql -u root -p radius < /etc/freeradius/sql/mysql/nas.sql* je naimportováno databázové schéma.

Nyní je třeba nastavit samotný FreeRADIUS pro komunikaci s databází. To se provede úpravou několika konfiguračních souborů. První z nich je *sql.conf*, umístěný typicky v adresáři /etc/freeradius/. Ten musí mimo-jiné obsahovat následující řádky:

- database = mysql,
- login = radius,
- password = password,
- readclients = yes.

Další upravovaný soubor je *default*, ten je umístěn typicky v adresáři /etc/freeradius/sites-enabled/. Zde je v blocích *authorize*, *accounting*, *session*, *post-auth* a *post-auth-type* potřeba odstranit znak # před slovem *sql*, tedy provést odkomentování. Dále je nutné v souboru *radiusd.conf*, který se nachází v adresáři /etc/freeradius/, odstranit znak # před *$INCLUDE sql.conf*. Spuštění se provede příkazem *service freeradius start,* případně v režimu ladění pomocí *freeradius -X*.

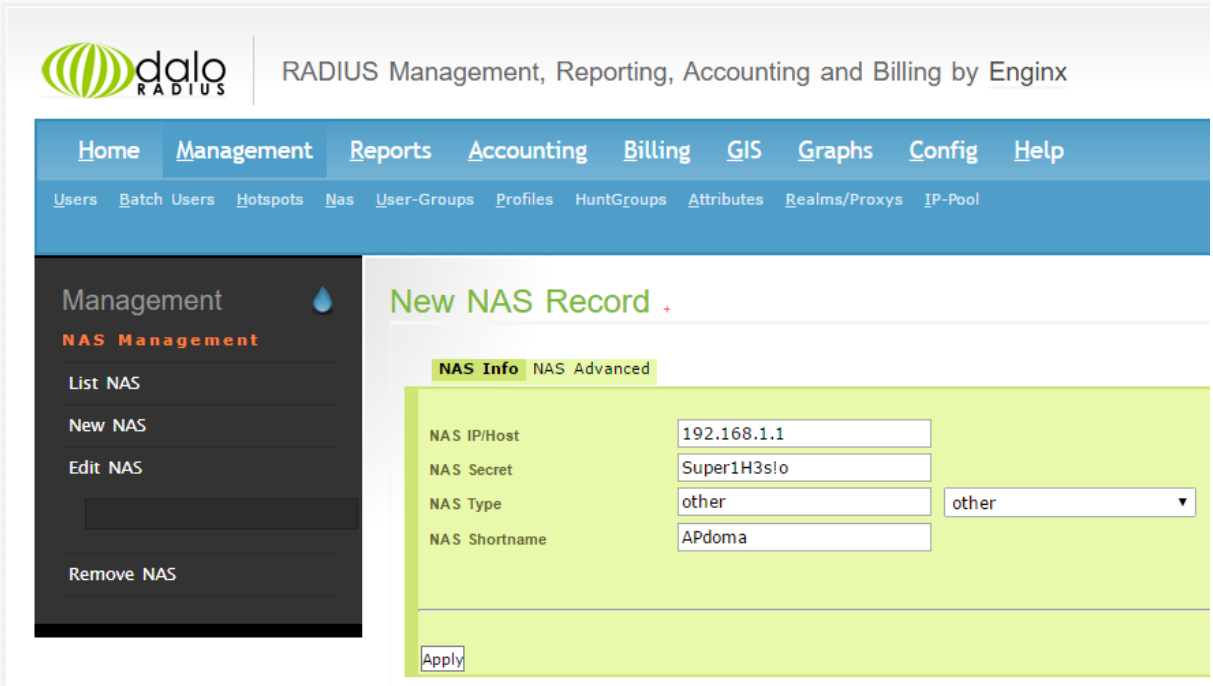
Instalace daloRADIUS

Archív se soubory je nutné stáhnout z oficiálních stránek. V této práci je použita verze 0.9-9. Zadáním příkazu *tar xvfz daloradius-0.9-9.tar.gz* v adresáři, kde je archív stažen, se provede

rozbalení. Tyto soubory se musí přesunout do adresáře pro data web serveru. Nejdříve se příkazem *mv daloradius-0.9-9 daloradius* přejmenuje výsledný adresář. Příkazem *mv daloradius /var/www* se pak přesune celý adresář se soubory do adresáře web serveru. Ještě se musí přenastavit práva pomocí příkazu *chown www-data:www-data /var/www/daloradius –R* a dále *chmod 644 /var/www/daloradius/library/daloradius.conf.php*. Nahrání schéma tabulek daloRADIUS do databáze se provede příkazem *mysql -u root -p radius < /var/www/daloradius/contrib/db/mysql-daloradius.sql*. Dále se v souboru *daloradius.conf.php*, který se nachází v adresáři /var/www/daloradius/library/, upraví údaje pro přístup k databázi. Mezi poslední úkony při instalaci patří přidání konfiguračního souboru pro webový server. Příkazem *nano /etc/apache2/sites-available/daloradius.conf* se vytvoří a otevře nový konfigurační soubor. Do něj je nutné vložit řádky, které se nachází v příloze A této práce. Stránka se povolí příkazem *a2ensite daloradius.conf* a webový server jí začne používat po zadání příkazu *service apache2 restart*. V této chvíli je webové rozhraní daloRADIUS dostupné po zadání adresy 192.168.1.10/daloradius. Výchozí přihlašovací jméno je „administrator“ a heslo „radius“. Tyto údaje je doporučeno po přihlášení změnit.

Konfigurace klienta a přidání nového uživatele pomocí daloRADIUS

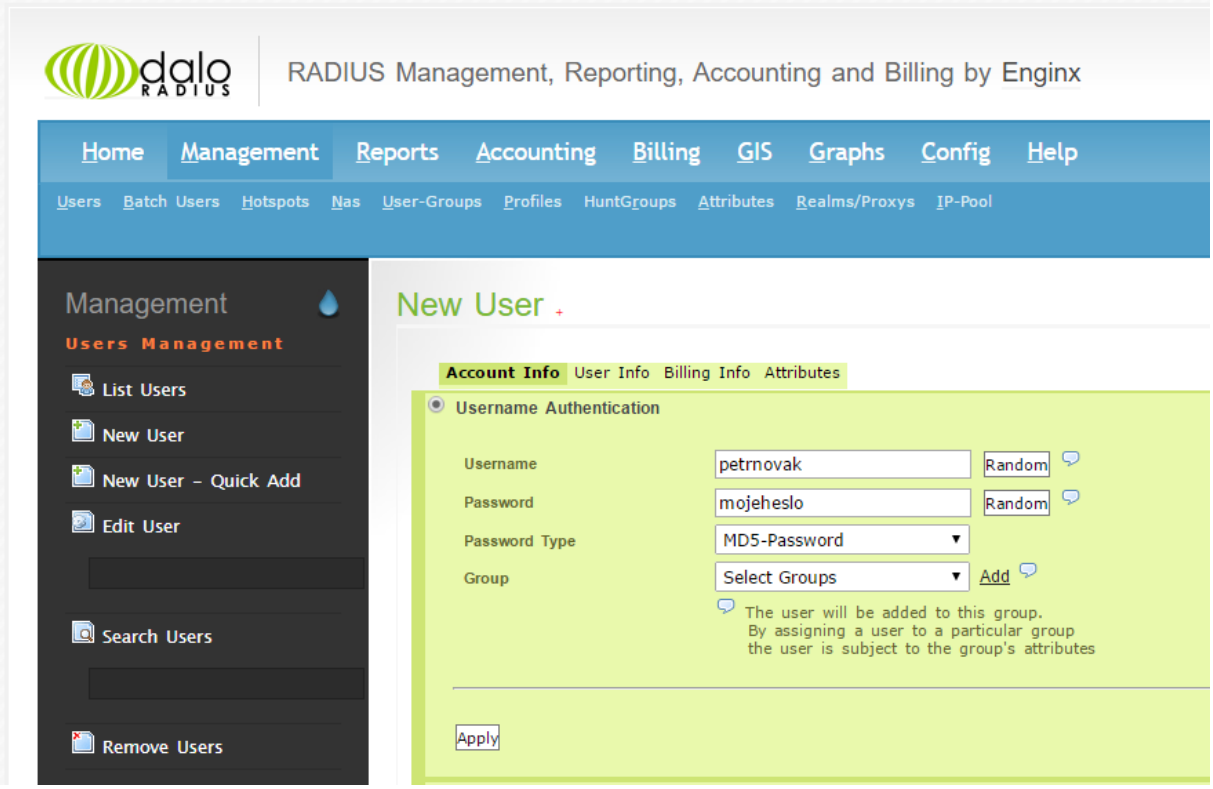
Pomocí webového rozhraní je možné spravovat celý FreeRADIUS. Také je možné sledovat různé záznamy, účtovací údaje a další. Tato práce se zabývá přidáním jednoho klienta a uživatele do databáze.



Obrázek 19: *Konfigurace klienta ve webovém rozhraní*

Pro přidání klienta je nutné v menu zvolit Management a poté Nas. V levém menu je potřeba zvolit New NAS a dále vyplnit požadované údaje. V této práci je využito údajů uvedených na obrázku 19. Adresa odpovídá přístupovému bodu, následuje sdílené heslo, typ klienta a volitelné označení klienta.

Uživatelé se přidávají obdobně. V menu je třeba zvolit Management a poté Users. V levém menu je nutné zvolit New User a dále vyplnit požadované údaje. V této práci je využito údajů uvedených na obrázku 20. Je vhodné zvolit šifrování hesla. Uživatel může mít mnoho dalších nastavení, ale těmi se tato práce nezabývá. Také je možné zvolit jiný typ ověřování.



Obrázek 20: *Přidání uživatele pomocí webového rozhraní*

V této chvíli je spuštěný FreeRADIUS, který naslouchá na portech 1812 a 1813 pro příchozí komunikaci. Do systému je zavedený jeden klient a jeden uživatel.

ZÁVĚR

Cílem práce bylo představit modely a přístupy k IoT a provést analýzu možných bezpečnostních rizik, které s rozvojem tohoto odvětví souvisí.

Teoretická část nejprve uvádí čtenáře do tématu Internet of Things. Na modelových příkladech je představeno, do jakých odvětví IoT přináší nové možnosti a jaké to jsou. Dále je představeno, o jak rozsáhlé řešení se jedná a jsou uvedeny některé přínosy i negativa, která s rozvojem souvisí.

Po základním představení IoT následuje kapitola, ve které je IoT rozděleno na menší stavební části. Tyto části jsou zde popsány, a u některých je provedena analýza toho, jaké bezpečnostní mechanizmy nabízejí. Tato kapitola také obsahuje popis toho, proč je pro další rozvoj IoT důležitý přechod z IPv4 na IPv6. V poslední části této kapitoly jsou uvedeny reálné bezpečnostní hrozby, kterým musí IoT čelit. Jednu z uvedených hrozeb představují nezabezpečené síťové služby a právě jejich zabezpečením se zabývá praktická část.

V praktické části je popsáno, jak zabezpečit síť v chytré domácnosti pomocí architektury AAA. V úvodu je představen model této domácnosti a prvky, které budou k zabezpečení použity – TP-LINK TL-WR841N a Raspberry Pi. Následuje popis konfigurace směrovače, na kterém jsou vytvořeny dvě oddělené bezdrátové sítě (v různých podsítích), pro které je nastaven mód ověřování WPA2 Enterprise. Dále je popsána instalace a nastavení FreeRADIUS spolu s daloRADIUS, což je webová nástavba pro pohodlné ovládání prvního zmíněného, na miniaturní počítač Raspberry Pi.

Autor práce se domnívá, že za bezpečnostními hrozbami stojí hlavně absence jednotného standardu, který by jasně definoval to, jak při vývoji IoT postupovat. Samotné používané prvky, jako jsou komunikační protokoly a frameworky, totiž nabízejí pokročilé mechanizmy zabezpečení. Autor dále předpokládá, že v budoucnu bude růst poptávka po specialistech se zaměřením na bezpečnost IoT.

Práce by měla odpovědět na otázky bezpečnosti IoT. Možné rozšíření této práce by mohlo být o pohled na to, jak je to se soukromím a bezpečností samotných uživatelů IoT.

POUŽITÁ LITERATURA

1. ABI RESEARCH. *Over 5 Billion Wireless Connectivity Chips Will Ship in 2013, Broadcom and Qualcomm are the Leading Suppliers.* 2012 [online]. [cit. 2016-03-09] Dostupné z: https://www.abiresearch.com/press/over-5-billion-wireless-connectivity-chips-will-sh/
2. ACCENTURE. *Driving Unconventional Growth through the Industrial Internet of Things*. s. 20. 2015 [online]. [cit. 2016-04-28]. Dostupné z: https://www.accenture.com/us-en/_acnmedia/Accenture/next-gen/reassembling-industry/pdf/Accenture-Driving-Unconventional-Growth-through-IIoT.pdf
3. AKYILDIZ, I. a VURAN, M. *Wireless sensor networks*. Hoboken, NJ: Wiley, 2010. 516 s. ISBN 978-0-470-03601-3.
4. ALLSEEN ALLIANCE. *AllJoyn Framework*. 2016 [online]. [cit. 2016-04-28]. Dostupné z: https://allseenalliance.org/framework
5. ALLSEEN ALLIANCE. *AllJoyn Security*. 2016 [online]. [cit. 2016-04-28]. Dostupné z: https://allseenalliance.org/framework/documentation/learn/core/system-description/alljoyn-security
6. ALLSEEN ALLIANCE. *Security 2.0*. 2016 [online]. [cit. 2016-04-28]. Dostupné z: https://allseenalliance.org/framework/documentation/learn/core/security2_0
7. AMAZON WEB SERVICES. *AWS IoT*. 2016 [online]. [cit. 2016-04-28]. Dostupné z: https://aws.amazon.com/iot/
8. BUSINESS WIRE. *Strategy Analytics: A Quarter of Households Worldwide Now Have Wireless Home Networks*. 2012 [online]. [cit. 2016-04-28]. Dostupné z: http://www.businesswire.com/news/home/20120404006331/en/Strategy-Analytics-Quarter-Households-Worldwide-Wireless-Home
9. CASSERLY, M. *Best cloud storage services 2016 UK: Best alternatives to Copy*. PC Advisor. 2016 [online]. [cit. 2016-04-28]. Dostupné z: http://www.pcadvisor.co.uk/test-centre/internet/14-best-cloud-storage-services-2016-uk-copy-3614269/
10. CISCO. *Internet Of Everything*. [online]. [cit. 2016-04-28]. Dostupné z: http://ioeassessment.cisco.com/

11. DEERING, S. a HINDEN, R. *Internet Protocol, Version 6 (IPv6) Specification, RFC 1883*. 1995 [online]. [cit. 2016-04-28]. Dostupné z: http://dx.doi.org/10.17487/rfc1883

12. DONG, J. A KOL. *Efficient Handovers Help Wireless Sensor Networks*. Microwaves & RF. 2014 [online]. [cit. 2016-04-28]. Dostupné z: http://mwrf.com/systems/efficient-handovers-help-wireless-sensor-networks

13. DROZHZHIN, A. *Black Hat USA 2015: The full story of how that Jeep was hacked*. Kaspersky Lab. – Blog. 2015 [online]. [cit. 2016-04-28]. Dostupné z: https://blog.kaspersky.com/blackhat-jeep-cherokee-hack-explained/9493/

14. EMC. *Executive Summary: A Universe of Opportunities and Challenges*. 2012 [online]. [cit. 2016-04-28]. Dostupné z: http://www.emc.com/leadership/digital-universe/2012iview/executive-summary-a-universe-of.htm

15. EPRIN. *Základní přehled standardů IEEE 802.11*. Technologie. 2015 [online]. [cit. 2016-04-28]. Dostupné z: http://www.eprin.cz/zakladni-prehled.html

16. EVANS, D. The Internet of Things, *How the Next Evolution of the Internet Is Changing Everything*. 2011 [online]. [cit. 2016-03-08] Dostupné z: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

17. FOX RUBIN, B. *Intel, Samsung create Internet of Things group*. CNET - Tech Industry. 2014 [online]. [cit. 2016-04-28]. Dostupné z: http://www.cnet.com/news/intel-samsung-create-internet-of-things-group/

18. FRIEDEMANN, M. a FLOERKEMEIER, CH. *From the Internet of Computers to the Internet of Things*. Distributed systems group. 2010 [online]. [cit. 2016-04-28]. Dostupné z: http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf

19. GARTNER. *Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020*. 2013 [online]. [cit. 2016-03-09]. Dostupné z: http://www.gartner.com/newsroom/id/2636073

20. GEMALTO. *Securing the Internet of Things (IoT).* 2015 [online]. [cit. 2016-04-28]. Dostupné z: http://www.safenet-inc.com/data-protection/securing-internet-of-things-iot/

21. GOOGLE CLOUD PLATFORM. *Overview of Internet of Things*. 2016 [online]. [cit. 2016-04-28]. Dostupné z: https://cloud.google.com/solutions/iot-overview

22. HAJDARBEGOVIC, N. *Are We Creating An Insecure Internet of Things (IoT)? Security Challenges and Concerns*. 2015 [online]. [cit. 2015-12-09] Dostupné z: http://www.toptal.com/it/are-we-creating-an-insecure-internet-of-things
23. HALLER, S., a kol. The Internet of Things in an Enterprise Context. *Future Internet – FIS 2008*. 2009. [cit. 2016-03-08]. DOI: 10.1007/978-3-642-00985-3_2. ISBN 978-3-642-00984-6. Dostupné z: http://papers.duckdns.org/files/2008_FIS2008.pdf
24. HALUZA, M., MACHÁČEK, J. *Spotřeba elektrické energie domácností, predikce a potenciální úspory pomocí BACS* [online]. 2012 [cit. 2016-04-19]. ISSN 1801-4399. Dostupné z: http://elektro.tzb-info.cz/8570-spotreba-elektricke-energie-domacnosti-predikce-a-potencialni-uspory-pomoci-bacs
25. KOPETZ, H. *Real-Time Systems Design Principles for Distributed Embedded Applications*. 2nd ed. Boston, MA: Springer US, 2011. ISBN 9781441982377.
26. HEWLETT PACKARD ENTERPRISE. *Internet of things research study*. 2015 [online]. [cit. 2016-04-28]. Dostupné z: http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en
27. IEEE. *IEEE 802.15 WPAN™ Task Group 4 (TG4)*. 2016 [online]. [cit. 2016-04-28]. Dostupné z: http://www.ieee802.org/15/pub/TG4.html
28. IOT6. *IPv6 advantages for IoT*. IPv6 for IoT. 2014 [online]. [cit. 2016-04-28]. Dostupné z: http://iot6.eu/ipv6_advantages_for_iot
29. IOTIVITY. *IoTivity 1.1.0 Features*. 2016 [online]. [cit. 2016-04-28]. Dostupné z: https://www.iotivity.org/documentation/features
30. IOTIVITY. *IoTivity Security Architecture Overview*. 2016 [online]. [cit. 2016-04-28]. Dostupné z: https://wiki.iotivity.org/iotivity_security_architecture_overview
31. JENNINGS, C. *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP, RFC 4787.* 2007 [online]. [cit. 2016-04-28]. Dostupné z: http://dx.doi.org/10.17487/rfc1883
32. LESWING, K. *How to find the best beacon hardware for everything from stores to cities*. 2014 [online]. [cit. 2016-03-09] Dostupné z: https://gigaom.com/2014/11/04/how-to-find-the-best-beacon-hardware-for-everything-from-stores-to-cities/
33. LINUX FOUNDATION. *IoTivity Open Source Project Announces Preview Release.* 2015 [online]. [cit. 2016-04-28]. Dostupné z: http://www.linuxfoundation.org/news-media/announcements/2015/01/iotivity-open-source-project-announces-preview-release

34. LINUX FOUNDATION. *Technology Leaders Establish the AllSeen Alliance to Advance the 'Internet of Everything'*. 2013 [online]. [cit. 2016-04-28]. Dostupné z: http://www.linuxfoundation.org/news-media/announcements/2013/12/technology-leaders-establish-allseen-alliance-advance-%E2%80%98internet
35. MAJDA, D. *Knihovny vs. Frameworky.* 2009 [online]. [cit. 2016-04-30]. Dostupné z: http://majda.cz/blog/265
36. MALÝ, M. *Co je a co není cloud*. Lupa.cz - server o českém Internetu. ISSN: 1213-0702. 2011 [online]. [cit. 2016-04-28]. Dostupné z: http://www.lupa.cz/clanky/co-je-a-co-neni-cloud/
37. MARR, B. *The 5 Biggest Risks of Big Data*. Data Informed. 2015 [online]. [cit. 2016-04-28]. Dostupné z: http://data-informed.com/the-5-biggest-risks-of-big-data/
38. MICRIUM. *Designing the Internet of Things - IoT and the Cloud*. 2016 [online]. [cit. 2016-04-28]. Dostupné z: https://www.micrium.com/iot/cloud/
39. MICRIUM. *Designing the Internet of Things - IoT Devices and Local Networks*. 2015 [online]. [cit. 2016-04-28]. Dostupné z: https://www.micrium.com/iot/devices/
40. MICRIUM. *Designing the Internet of Things - Protocol Stack Options*. 2015 [online]. [cit. 2015-12-09] Dostupné z: http://micrium.com/iot/internet-protocols/
41. MICROSOFT AZURE. *Azure IoT Hub - Connect, monitor, and control millions of IoT assets*. 2015 [online]. [cit. 2016-04-28]. Dostupné z: https://azure.microsoft.com/en-us/services/iot-hub/
42. MITCHELL, S., a kol. *The Internet of Everything for Cities*. CISCO. 2013 [online]. [cit. 2015-12-09] Dostupné z: http://www.cisco.com/web/strategy/docs/gov/everything-for-cities.pdf
43. OLSSON, J. *6LoWPAN demystified*. Texas Instruments. 2014 [online]. [cit. 2016-04-28]. Dostupné z: http://www.ti.com/lit/wp/swry013/swry013.pdf
44. OPEN CONNECTIVITY FOUNDATION. *IoTivity.* 2016 [online]. [cit. 2016-04-28]. Dostupné z: http://openconnectivity.org/resources/iotivity
45. OPEN CONNECTIVITY FOUNDATION. *Specifications*. 2016 [online]. [cit. 2016-04-28]. Dostupné z: http://openconnectivity.org/resources/specifications

46. OWASP. *OWASP Internet of Things Project - Top 10 IoT Vulnerabilities (2014) Project*. 2014 [online]. [cit. 2016-04-28]. Dostupné z: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Top_10_IoT_Vulnerabilities__282014_29

47. PERKINS, C., a kol. *Mobility Support in IPv6, RFC 6275*. 2011 [online]. [cit. 2016-04-28]. Dostupné z: http://dx.doi.org/10.17487/rfc6275

48. PUŽMANOVÁ, R. *Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G*. Vyd. 1. Brno: CP Books, 2005. ISBN 80-251-0791-4.

49. SATRAPA, Pavel. *IPv6: internetový protokol verze 6*. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC, 2011. CZ.NIC. ISBN 978-80-904248-4-5.

50. TECHTARGET. Essential Guide. *A guide to healthcare IoT possibilities and obstacles*. 2015 [online]. [cit. 2016-04-28]. Dostupné z: http://searchhealthit.techtarget.com/essentialguide/A-guide-to-healthcare-IoT-possibilities-and-obstacles

51. THE GOVERNMENT OF THE HONG KONG SPECIAL ADMINISTRATIVE REGION. *Ipv6 Security*. 2011 [online]. [cit. 2016-04-28]. Dostupné z: http://www.infosec.gov.hk/english/technical/files/ipv6s.pdf

52. T-MOBILE. *Budoucnost patří internetu věcí*. 2015 [online]. [cit. 2015-12-09] Dostupné z: http://t-press.cz/cs/tiskove-materialy/tiskove-zpravy-t-mobile/t-mobile-pokryje-ceskou-republiku-siti-sigfox-pro-internet-veci.html

53. UNIVERZITA PARDUBICE. *IPv4 (Internet Protocol version 4)*. 2014 [online]. [cit. 2016-04-28]. Dostupné z: https://wiki.upce.cz/fei/studijni-materialy/ipv4_internet_protocol_version_4

54. UNIVERZITA PARDUBICE. *IPv6 (Internet Protocol version 6)*. 2014 [online]. [cit. 2016-04-28]. Dostupné z: https://wiki.upce.cz/fei/studijni-materialy/ipv6_internet_protocol_version_6

55. WEARABLE DEVICES. *Wearable Technology and Wearable Devices Everything You Need to Know*. 2014 [online]. [cit. 2016-04-28]. Dostupné z: http://www.wearabledevices.com/what-is-a-wearable-device/

56. WIND RIVER SYSTEMS. *Security In The Internet Of Things - Lessons from the Past for the Connected Future.* 2015 [online]. [cit. 2016-04-28]. Dostupné z:

http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

57. YAKOVLEV, G. *Chytrá města: Inovace všude kolem nás*. 2015 [online]. [cit. 2016-03-08] Dostupné z: http://iq.intel.cz/chytra-mesta-inovace-vsude-kolem-nas/

SEZNAM PŘÍLOH

Příloha A – *Konfigurační soubor pro webovou stránku daloRADIUS*

```
Alias /daloradius /var/www/daloradius/

<Directory /var/www/daloradius/>

        Options None

        Order allow,deny

        allow from all

</Directory>
```