Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Zabezpečení komunikace mezi prostředky IoT

Vít Stránský

Bakalářská práce
2019

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2018/2019**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Vít Stránský**
Osobní číslo:	**E15079**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Zabezpečení komunikace mezi prostředky IoT.**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem práce je klasifikace vývoje trendů zabezpečení prostředků používaných ke komunikaci v rámci sítí IoT.

Osnova:
– Stanovení časového rámce sledovaného období vývoje.
– Prostudování vybraných komunikačních technologií včetně standardně používaných způsobů jejich zabezpečení ve zvoleném období.
– Přehledné zpracování získaných informací v maximálně názorné podobě využitelné např. jako výukový materiál.

Rozsah grafických prací:

Rozsah pracovní zprávy: **30 - 40 stran**

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

Seznam odborné literatury:

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

SATRAPA, Pavel. *IPv6: Internet Protokol, verze 6.* **Praha: Neocortex, c2002. ISBN 80-86330-10-9.**

HU, Fei, ed. *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations.* **Boca Raton: CRC Press, 2016. ISBN 978-1-4987-2319-0.**

WATTS, Silvia, ed. *The Internet of things (IoT): applications, technology, and privacy issues.* **New York,: Nova Publisher's, 2016. ISBN 978-163-4846-264.**

Vedoucí bakalářské práce: **RNDr. Ing. Oldřich Horák, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **3. září 2018**

Termín odevzdání bakalářské práce: **30. dubna 2019**

L.S.

doc. Ing. Romana Provazníková, Ph.D.
děkanka

doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 3. září 2018

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.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30.4.2019 Vít Stránský

PODĚKOVÁNÍ:

Tímto bych rád poděkoval svému vedoucímu práce RNDr. Ing. Oldřichu Horákovi, Ph.D., za jeho odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce.

ANOTACE

Tato bakalářská práce je zaměřena na zabezpečení komunikace mezi prostředky Internetu věcí. V první části je definováno, co pojem IoT znamená, poté jsou popsány bezdrátové komunikační technologie podle dosahu signálu. Druhá polovina práce se zabývá útoky a bezpečností komunikace prostředků Internetu věcí.

KLÍČOVÁ SLOVA

Internet věcí, bezpečnost, bezdrátová komunikace, výukový materiál

TITLE

Security of Communication between Objects of IoT

ANNOTATION

This bachelor's thesis is focused on securing communication between objects of Internet of Things. The first part defines what the term IoT means, then wireless communication technologies are described according to the signal range. The second half of the thesis is focused on attacks and security of Internet of Things.

KEYWORDS

Internet of Things, Security, Wireless Communication, Learning Materials

OBSAH

ÚVOD ... **10**

1 DEFINICE IOT ... **11**

1.1 CHARAKTERISTIKA IOT ... **11**
1.2 OBLASTI IOT ... **12**
1.2.1 Inteligentní elektronika ... 12
1.2.2 Inteligentní zdravotnictví ... 12
1.2.3 Inteligentní domy ... 12
1.2.4 Inteligentní automobily ... 13
1.2.5 Inteligentní města ... 13
1.2.6 Inteligentní zemědělství ... 13
1.2.7 Průmysl 4.0 ... 14
1.3 ARCHITEKTURA IOT ... **14**
1.3.1 Věci ... 15
1.3.2 Síť ... 16
1.3.3 Cloud a Fog computing ... 18

2 KOMUNIKAČNÍ TECHNOLOGIE IOT ... **20**

2.1 PROXIMITY ... **21**
2.1.1 RFID ... 21
2.1.2 NFC ... 21
2.2 WPAN ... **22**
2.2.1 Infraport ... 22
2.2.2 Bluetooth ... 22
2.3 WLAN ... **23**
2.3.1 WiMAX ... 23
2.4 WNAN ... **24**
2.4.1 6LoWPAN ... 24
2.5 WWAN ... **24**
2.5.1 Protokoly WWAN ... 25
2.5.2 LTE, LTE – Advanced a 5G ... 25
2.5.3 LoRa ... 26

3 HROZBY V SÍTÍCH IOT ... **28**

3.1 ÚTOKY ZALOŽENÉ NA FÁZÍCH IOT ... **30**
3.2 ÚTOKY NA ARCHITEKTURU SÍTĚ ... **31**
3.3 ÚTOKY NA KOMPONENTY SÍTĚ ... **34**

4 BEZPEČNOST V SÍTÍCH IOT ... **36**

4.1 OWASP INTERNET OF THINGS TOP 10 LIST ... **36**
4.2 PRINCIPY BEZPEČNOSTI IOT ... **36**
4.3 METODY ZABEZPEČENÍ BEZDRÁTOVÉ KOMUNIKACE ... **39**
4.3.1 SSL ... 40
4.3.2 TLS ... 40
4.3.3 AES ... 41
4.3.4 Model Body + Envelope ... 44

ZÁVĚR ... **47**

POUŽITÁ LITERATURA ... **48**

SEZNAM OBRÁZKŮ

Obrázek 1 – Aplikace IoT 14
Obrázek 2 – Ideální blokové schéma architektury technologie IoT 15
Obrázek 3 – Volba komunikačního systému podle potřebného přenosového dosahu 20
Obrázek 4 – Útok na zařízení IoT 29
Obrázek 5 – Fáze systému IoT 30
Obrázek 6 – Možné útoky založené na architektuře 32
Obrázek 7 – Možné útoky založené na komponentech 34
Obrázek 8 – Nezabezpečená komunikace internetu věcí 39
Obrázek 9 – Zabezpečená komunikace internetu věcí 40
Obrázek 10 – Záměna bajtů 42
Obrázek 11 – Prohození řádků 43
Obrázek 12 – Kombinování sloupců 43
Obrázek 13 – Přidání podklíče 44
Obrázek 14 – Šifrování pomocí SSL/TLS 45
Obrázek 15 – Šifrování TLS i AES v jedné zprávě 45

SEZNAM ZKRATEK

6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AP	Access Point
BLE	Bluetooth Low Energy
CAPTCHA	Completely Automated Public Turing Test to tell Computers and Humans apart
CSFB	Circuit Switched FallBack
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DLCI	Data-Link Connection Identifier
DLP	Data Leakage Prevention
DNS	Domain Name System
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISP	Internet Service Provider
IT	Informační technologie
LTE	Long Term Evolution
NAS	Network Attached Storage
NAT	Network Address Translation
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OSN	Organizace spojených národů
OWASP	Open Web Application Security Project

PC	Personal Computer
PIN	Personal Identification Number
RFID	Radio Frequency Identification
Sci-fi	Science Fiction
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UMTS	Universal Mobile Telecommunication System
VDSL	Very High Speed Digital Subscriber Line
VoIP	Voice over Internet Protocol
VoLTE	Voice over Long Term Evolution
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WNAN	Neighborhood Area Networks
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
XSS	Cross-site Scripting
LPWAN	Low-Power Wide Area Network

ÚVOD

V roce 1944 byl na univerzitě v Pensylvánii uveden do provozu první elektronkový počítač, který pracoval na podobném principu jako dnešní počítače. Kdybychom v té době jeho vynálezcům řekli, že v budoucnu bude výpočetní technika neodmyslitelnou součástí lidského života, nejspíše by to považovali za sci-fi.

Vývoj IT však šel kupředu mílovými kroky a proto dnes, na počátku 21. století, můžeme toto sci-fi skutečně prožívat. Z halových počítačů se stali stolní počítače, telefony se nám vejdou do kapsy a informační technologie se postupně implementují do všech odvětví lidské činnosti. Ať už se jedná o PC, notebook, tablet, telefon, auto nebo tzv. Wearables, všechny tyto vynálezy nám s pokračující digitální revolucí usnadňují životy čím dál více. V této práci se budu zabývat technologiemi

Jedním z nových trendů, které nám velice usnadní práci a zpříjemní volný čas je Internet věcí (zkratka „IoT“). Díky stále klesajícím cenám senzorů, jednotlivých prvků a internetu se budeme s implementací IoT setkávat stále častěji. A to jak ve firmách, tak u nás doma. Vzhledem k tomu, že se jedná o v posledních letech velmi používaný pojem, se budu touto problematikou zabývat v období od roku 2000 do současnosti.

Vše má však svou světlou i stinnou stránku, Internet věcí nevyjímaje. Často se můžeme setkat se studiemi, které zjistili, že široká veřejnost nepřikládá kybernetické bezpečnosti takovou váhu (například studie Fakulty sociálních věd Univerzity Karlovi v Praze z roku 2008), jako bezpečnosti fyzické. Dle mého názoru je to především tím, že je pro ně internet abstraktním pojmem a osvěta ohledně kybernetické bezpečnosti není dostačující na to, aby si lidé uvědomili, jaká nebezpečí jim hrozí a jak se před nimi bránit. Vzhledem k tomu, že Internet věcí je založený z velké části na sběru dat a sdílení těchto dat mezi prvky sítě, mohla by se tato data, úmyslně i neúmyslně, dostat do nepovolaných rukou.

Cílem práce je klasifikace vývoje trendů zabezpečení prostředků používaných ke komunikaci v rámci sítí IoT. Prostudování vybraných komunikačních technologií včetně standardně používaných způsobů jejich zabezpečení ve zvoleném období, přehledné zpracování získaných informací v maximálně názorné podobě využitelné např. jako výukový materiál.

1 DEFINICE IOT

Pro pojem IoT neexistuje jednoznačná definice, jedná se spíše o zastřešující sousloví.[21]

Zjednodušeně bychom mohli tento systém popsat jako propojení jednotlivých zařízení prostřednictvím internetu bez účasti člověka. Principem je sběr dat z různých senzorů a čidel a sdílení těchto dat prostřednictvím internetu za účelem dalšího zpracování a vyhodnocování. [19]

1.1 Charakteristika IoT

Internet věcí umožňuje zařízením, aby byla zjištěna, či vzdáleně kontrolována pomocí existující infrastruktury (počítačová síť, internet, mobilní síť, …), která umožňuje lepší integraci fyzických zařízení do počítačově řízených systémů. A to i přesto, že stále ještě nespolupracují pod jednou technologií a společným protokolem. [20][21]

Díky tomuto novému trendu dochází ke zvýšení účinnosti, přesnosti a ekonomické stránky věci ve spojení se sníženými nároky na uživatele. Pokud jsou v zařízení umístěna čidla či akční členy, technologie se stává částí více obecné kategorie kyber-fyzických systémů, která zahrnuje technologie jako jsou chytré sítě, virtuální elektrárny, chytré domácnosti a inteligentní přepravu či též chytrá města. [20]

Pojmem „věci“ v oblasti IoT může být definována široká škála zařízení, jako jsou například srdeční implantáty pro měření srdečního tepu, dálkově ovládané spotřebiče, biočipové senzory na farmách, kamery vysílající živé záběry divokých zvířat, automobily se zabudovanými senzory, přístroje na analýzu DNA nebo terénní zařízení, která pomáhají hasičům v pátracích a záchranných operacích. Nejčastějšího uplatnění se IoT dočká především tam, kde je potřeba sbírat data z velkého počtu lokalit, tato data vyhodnotit a na základě výsledku vyhodnocení provést v daných lokalitách nějaké případné korekce. [20][19]

Tato zařízení sbírají potřebná data s pomocí rozličných existujících technologií a poté samostatně rozesílají tato data mezi ostatními zařízeními. Rychlý vývoj a expanze Internetu věcí by také mělo znamenat produkci velkého množství dat z různých oblastí a následnou potřebu rychlého zařazení dat a zvýšení potřeby na indexování, ukládání a zpracovávání dat efektivněji. V posledních letech, spolu s masivních růstem globálních kybernetických hrozeb, se také objevuje výrazný růst zneužívání Internetu věcí pro páchání kybernetických zločinů. [20]

1.2 Oblasti IoT

Následující výčet oblastí a jejich popis je syntézou informací ze zdrojů [8], [22] a [30].

1.2.1 Inteligentní elektronika

Dříve byli spotřebitelé zvyklí na to, že jsou jejich smartphony vybaveny internetem, zatímco dnes již vyžadují připojení k internetu na každém zařízení, které používají. Televize, chladničky, reproduktory, termostaty, domácí bezpečnostní systémy, v podstatě na cokoliv si vzpomenete. Velkým trendem v této oblasti má v následujících letech být samotné oblečení, obohacené o prvky senzorů či vylepšení, jako je integrovaný solární panel pro nabíjení mobilních zařízení. Výrobci elektroniky chtějí na tomto zájmu pochopitelně něco vydělat, takže uvádějí do prodeje zařízení, která už dávno známe a používáme, ale nově jsou vybavena síťovým čipem a softwarem, který umožňuje jejich komunikaci přes internet. Věk internetu tak posouvá své hranice opět o kus výše.

1.2.2 Inteligentní zdravotnictví

V souvislosti s inteligentní elektronikou nelze opomenout vzestup Wearables pro zdravotní či fitness účely. Tato zařízení, která mívají podobu hodinek, náramků nebo čelenek, mohou sledovat životní funkce, jako je srdeční frekvence, cyklus spánku a spálené kalorie. Poté mohou tyto nasbírané údaje odeslat do aplikace pro vyhodnocení zdravotního stavu uživatele nebo i přímo jeho ošetřujícímu lékaři. Získané informace pomohou s rozhodnutím, kdy je čas si po náročném tréninku odpočinout nebo navštívit lékaře, pokud některé údaje budou výrazně vybočovat z normálu.

1.2.3 Inteligentní domy

IoT se v žádném případě neomezuje pouze na jednotlivá zařízení, která jsou inteligentní a připojená. Stejná koncepce se rozšiřuje i na celé domovy. Inteligentní domov shromažďuje užitečná data, je vybaven mnoha inteligentními spotřebiči téměř v každé místnosti, počínaje kuchyní, přes obývák a dětský pokoj až po koupelnu. Domácí vybavení je přístupné online a je ovládatelné prostřednictvím aplikací v mobilním telefonu, tabletu či přes internetový prohlížeč. Stačí jen zadat své přihlašovací údaje a rovnou můžete třeba zkontrolovat, zda jste při odchodu nezapomněli vypnout klimatizaci nebo zamknout garáž. Už to samo o sobě představuje velkou úsporu času oproti nutnosti se vrátit a vše zkontrolovat osobně. Téměř samozřejmostí je si navolit požadovanou teplotu, barvu světel, nebo možnost říct konvici, aby

v 8 hodin ráno uvařila vodu o teplotě 80°. Fantazii se meze nekladou a vývojem zařízení pro chytré domy se zabývá nejedna velká společnost či startup.

1.2.4 Inteligentní automobily

Mnoho prototypů automaticky řízených vozidel již bylo vyrobeno a úspěšně otestováno. Výrobci, jako jsou Tesla a Volvo, se dokonce zavázali zpřístupnit takové automobily i běžnému spotřebiteli. Největším problémem v dopravě však v tuto chvíli je, že spolu jednotlivé automobily nekomunikují. Budoucí komplexní síť, ve které budou vozidla, řidiči a různé části dopravní infrastruktury navzájem komunikovat, slibuje přinést nejen příjemnější zážitek z jízdy, ale také by měl pomoci určit směr rozvoje této infrastruktury, například v otázce řízení provozu a správy parkovacích ploch. Přestože ještě nedávno byly samořízené automobily nedaleko od reality, dnes už můžeme s jistotou hovořit o tom, že jsou součástí dnešní reality. Byť na plošné rozšíření, dobrou cenovou dostupnost i dořešenou otázku bezpečnosti si jistě ještě počkáme, v budoucnu bychom se mohli dočkat světa bez kolon a nehod.

1.2.5 Inteligentní města

Myslet ve velkém je možné prakticky v čemkoli, a tak se zrodil nápad neomezovat se na pouhou elektroniku, automobily či domy, ale udělat chytřejším rovnou celé město. Počínaje řízením veřejných služeb, jako je voda, odpad, elektřina a plyn, až po veřejnou správu, jako je veřejná bezpečnost a doprava. Dlužno dodat, že vlády i magistráty měst se k podobným nápadům rozhodně nestavějí zády, ba naopak, takže mnohé z nich již oficiálně deklarovaly své dlouhodobé závazky na cestě k budování inteligentních měst. Chytrá revoluce města své obyvatele zasáhne nejspíš pomalu a téměř nepozorovaně, protože její primární cíl spočívá v efektivnějším využívání energie, materiálu a lidských zdrojů. Pokud se technologie správně využijí, dojde k nárustu životní úrovně obyvatel. Za příklad chytrého města je dáván Amsterodam, kde je využíváno mj. chytrého systému upozorňujícího na možnosti parkování po městě.

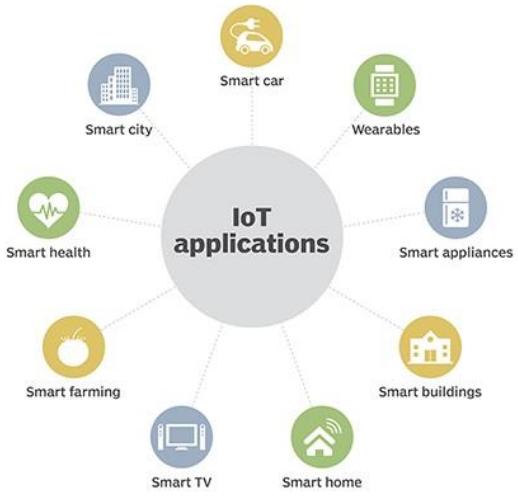
1.2.6 Inteligentní zemědělství

Chytré zemědělství je jedním z nejdůležitějších témat IoT, neboť zvýšení výroby potravin je výzvou dnešní doby. OSN konstatuje, že aby se rostoucí populace bez problémů uživila v roce 2050, musí se výroba potravin zvýšit o 60 %. Toho lze dosáhnout integrací konceptu chytrých technologií do zemědělství. Zde by jeho primární rolí bylo pomáhat stanovit správná

rozhodnutí podporovaná daty, jako jsou údaje o plodinách a počasí, ale také sledovat stav plodin v reálném čase a navrhovat optimalizace pěstitelských postupů za účelem dosažení vyšší produktivity. Výhodou je, že IoT čidla (např. pro síť LoRA) jsou připravena na provoz i v místech, kde musí na jednu baterii vydržet třeba 10 let.

1.2.7 Průmysl 4.0

Koncept Průmysl 4.0 dostal svůj název podle čtvrté průmyslové revoluce, která právě probíhá a popisuje budoucí výrobu v éře internetu věcí. Jeho podstatou je digitalizace, rozšiřování vysokorychlostního internetu, rozvoj chytrých technologií a komunikace. Je to cesta, jak učinit výrobní a dodavatelský řetězec inteligentní, agilní, efektivní a udržitelný. V tomto paradigmatu budou výrobní zdroje, jako jsou stroje a člověk, inteligentně komunikovat a na základě datových vstupů budou schopni přijímat proaktivní výrobní rozhodnutí. Jedním z příkladů je prediktivní údržba strojů, což je velká příležitost ke snížení nákladů a posílení efektivity provozu.

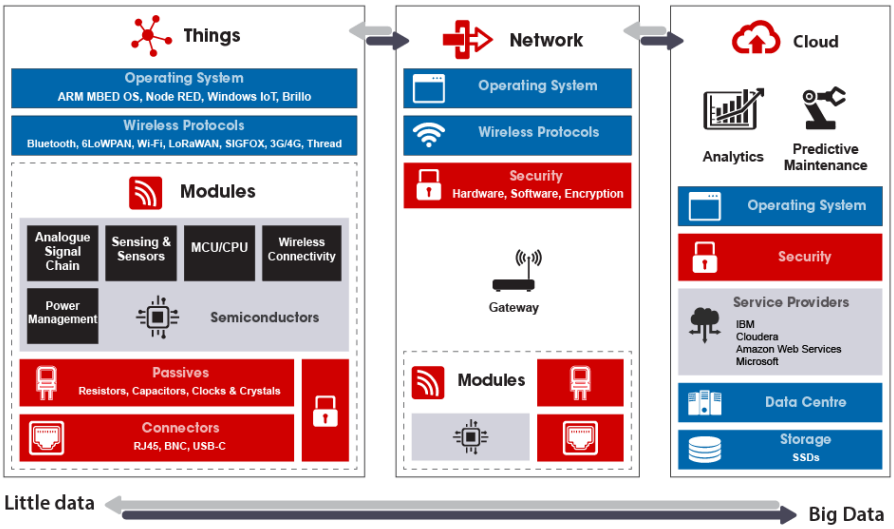


Obrázek 1 – Aplikace IoT

Zdroj: [18]

1.3 Architektura IoT

Internet věcí se již v dnešní době skládá z miliard zařízení. V roce 2017 bylo takto propojeno 8,4 miliard zařízení a experti odhadují, že to v roce 2020 bude 30 miliard zařízení. [28] Vzhledem k tomu, že součástí internetu věcí může být prakticky jakákoliv věc s možností připojení do sítě, je nemožné je zde všechny vyjmenovat. Lze však definovat tři základní stavební kameny IoT – věci, síť a cloud.



Obrázek 2 – Ideální blokové schéma architektury technologie IoT

Zdroj: [44]

1.3.1 Věci

V současnosti se na obalech stále většího množství výrobků objevuje nálepka „IoT Ready“ apod. Jednak je to tím, že se výrobci snaží jít s moderním trendem, kdy spotřebitelé vyžadují vlastnit chytrá zařízení připojená k internetu.

Na druhou stranu však mnoho výrobců prostě jen takto označí již svoje dlouhodobě prodávaná zařízení a jednotky, které například umožňují dnes již běžný Ethernet, Bluetooth nebo WiFi. V zásadě však mají pravdu, protože i tyto již dlouho využívané technologie v zásadě slouží k vzájemnému propojí a elektronické komunikaci zařízení nebo připojení na internet. Nicméně hlavní hybnou silou pro všeobecné masivní rozšíření IoT systémů se mají stát až nejnovější bezdrátové LPWAN technologie pro dálkovou bezdrátovou nízkopříkonovou komunikaci. Ty mají umožnit prakticky realizovat onu ideu absolutní automatické elektronické komunikace každého elektronického zařízení s každým, a tak pomoci maximálně automatizovat domy, domácnosti, výrobní procesy, dopravu, služby a podobně. [44]

Aby se možnosti praktického použití a nasazení co nejvíce urychlily, již mnoho výrobců nabízí nejen specializované integrované obvody i kombinované mikročipy s podporou různých IoT komunikačních protokolů, ale také různé testovací nebo vestavné karty a soupravy ve formě modemů nebo routerů pro různou bezdrátovou IoT komunikaci. Ty pak umožňují snadnou zástavbu nejen do malosériových zařízení, kde se vývoj na úrovni součástek nevyplatí, ale také vestavbu do již stávajících zařízení. [44]

1.3.2 Síť

Síťovým prvkem se rozumí jakékoliv zařízení, které se podílí na tvorbě nejen internetového připojení. Každý má v síti své místo a funkci, avšak ne všechny jsou pro její fungování nezbytné. Níže si podle zdroje [34] vysvětlíme, k čemu který prvek slouží.

WiFi routery a AP

- WiFi router – jako WiFi router označujeme ucelená řešení starající se o chod domácí sítě. Obvykle v domácím WiFi routeru najdeme kromě routovací funkce také DHCP server, Firewall, NAT a také switch. Kromě bezdrátového výstupu obsahuje také konektory RJ-45.
- AP – neboli Access Point je síťové zařízení, jehož úkolem je transformovat drátovou síťovou komunikaci v bezdrátovou. Zjednodušeně to znamená, že pokud připojíme místo počítače na konec síťového kabelu AP, vytvoří WiFi síť.

3G/LTE modemy

- 3G/LTE modemy připojují bezdrátovou lokální síť pomocí mobilních dat. Vložíme do nich SIM kartu, stejně jako do telefonu, datové připojení však bude dostupné pro všechna zařízení v dosahu. LTE modem je vlastně velmi sofistikovaný mobilní hotspot, který zároveň obsahuje funkce domácího WiFi routeru.

ADSL a VDSL

- S okolním světem ADSL a VDSL modemy propojují lokální síť pomocí telefonního vedení. To je v České republice již silně zavedené, a proto je skrze DSL připojena velká část domácností. ADSL a VDSL modemy jsou často zároveň taktéž domácími WiFi routery.
- ADSL je připojení nesymetrické, rychlost stahování je vyšší než rychlost nahrávání.
- VDSL naopak umožňuje symetrické připojení se stejnou rychlostí stahování i nahrávání a je schopno vyšších přenosových rychlosti než ADSL.

NAS – chytrá síťová úložiště

- Jako NAS (Network Attached Storage) označujeme síťová úložiště připojitelná do místní sítě. Mají tedy funkci jakéhosi serveru, který se nemusí omezovat na úschovu dat, nýbrž může fungovat také například jako server webový.

Antény

- WiFi antény mají funkci, která se nijak výrazně neliší od funkce jiných antén. Jejím úkolem je šířit WiFi signál. Nejtypičtější antény se připojují pomocí konektoru SMA, existuje ale také řada dalších řešení, například pro příjem signálu od poskytovatele. Do kategorie antén částečně spadají také přístupové body AP.

IP kamery

- IP kamery jsou především zabezpečovacím síťovým prvkem. Umožňují sledování v reálném čase i odesílání záznamu na vzdálené úložiště. Jedná se o spolehlivé řešení při monitorování osobních či firemních prostor a majetku. IP kamery mohou obsahovat také přídavné senzory.

Monitorovací systémy

- Kategorie monitorovací systémy obsahuje různá zařízení, především ale ucelené kamerové systémy se síťovými rekordéry.

Síťové karty

- Síťové karty reprezentují koncová zařízení v lokální síti. Do této kategorie nespadají jen interní karty, nýbrž také externí WiFi adaptéry, díky kterým můžeme zpracovávat WiFi signál zařízeními, která tomu nemají dedikovány interní komponenty, například desktopovými počítači.

Switche, routery a firewally

- V kategorii switche, routery a firewally najdeme především velmi úzce specializované síťové prvky, které mají místo především ve složitějších síťových strukturách.
- Switch je prvek, který má za úkol spojovat počítače a další koncová zařízení v lokální síti.
- Router dohromady spojuje více lokálních sítí a zajišťuje mezi nimi komunikaci.
- Firewall definuje pravidla komunikace mezi sítěmi, čímž ji nízkoúrovňově zabezpečuje.

VoIP

- VoIP (Voice over Internet Protocol) neboli technologie IP telefonů umožňuje telefonní přenos skrze internetovou síť.

Printservery

- Použití printserveru je jednoduchý způsob, jak k počítačové síti připojit tiskárnu, která sama síťovou funkcí nedisponuje.

Rozvaděče

- Rozvaděče jsou skříně na síťové prvky. Obvykle ctí standardizovaný systém rack a umožňují usazení několika switchů, routerů nebo firewallů, které rozměrově odpovídají.

1.3.3 Cloud a Fog computing

Definice cloudu nemusí být úplně jasná, ale v zásadě je to termín, který se používá pro popis globální sítě serverů, z nichž každý má svoji funkci. Cloud není fyzický objekt, ale rozsáhlá síť vzájemně propojených vzdálených serverů po celém světě, které fungují jako jeden ekosystém. Tyto servery jsou navržené buď k ukládání a správě dat, spouštění aplikací, nebo doručování obsahu a služeb, jako je streamování videí, webová pošta, kancelářský software nebo sociální média. Místo přistupování k souborům a aplikacím z místního nebo osobního počítače k nim přistupujeme online z jakéhokoli zařízení s podporou internetu – informace tak budou dostupné kdekoli a kdykoli je budeme potřebovat. Nikdo přesně neví, jak jsou všechny cloudy velké, nicméně jeden cloud může pojmout až 1 exabajt dat, což odpovídá 1 milionu terabajtů. [4][7]

Cloud otevřel před světem informačních technologií nové možnosti. Rostoucí počet zařízení připojených do cloudu ovšem znamená i vyšší nároky na síťovou infrastrukturu, protože je nutné přenést rychle rostoucí objem dat. Přitom některá data není nutné přenášet až na místo do datových center, stačí rozhodovací logiku přesunout blíže zdroji. Právě tato potřeba zrodila koncept Fog Computingu. [12]

Fog Computing poskytuje právě takovou virtualizovanou vrstvu umístěnou na samé hranici sítě, která poskytne výpočetní výkon, úložiště a síťové služby na rozhraní mezi koncovými zařízeními a cloudem. Zjednodušeně řečeno, rozhodovací logika se přesune z cloudu blíže jednotlivým připojeným zařízením, ať již jsou to přepínače, směrovače, kamery a další. Díky tomu nemusí v některých případech procházet po linkách do datového centra a zpět. To znamená nejen menší zátěž na infrastrukturu, ale také například snížení latence, což je důležité zejména u aplikací vyžadujících rozhodování v reálném čase či zvýšení spolehlivosti a vyšší odolnost v případech, kdy dojde k výpadku komunikace s centrálním cloudem. To je

důležité třeba u zařízení z kategorie eHealth, různá zdravotní monitorovací zařízení, které vysílají informace o zdravotním stavu nositele. [12]

K tomu, aby se využití Fog Computing více rozšiřovalo bude nejprve potřeba vyřešit nově vzniklé výzvy jako jsou programovatelnost, odpovědnost, standardizace, správa, zjišťování/synchronizace, výpočetní/ukládací omezení a bezpečnost. [42]

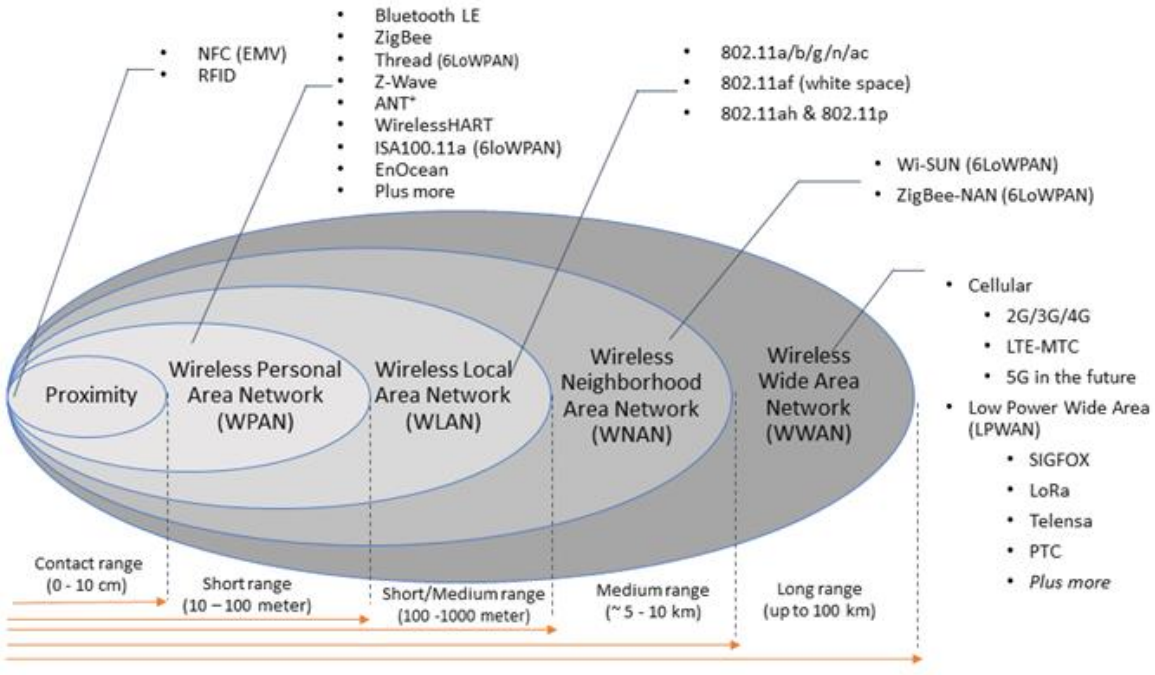
2 KOMUNIKAČNÍ TECHNOLOGIE IOT

S vývojem bezdrátových technologií se začalo slovo Internet věcí objevovat stále častěji. Vedle již klasických technologií jako například Bluetooth nebo Wi-Fi se začali objevovat i nové, pro Internet věcí specializované způsoby bezdrátové komunikace. Snahou u nových, či vyšších verzí současných technologií je dosáhnout co možno největšího dosahu při co nejmenší spotřebě energie.

Každý ze systémů je vhodný pro jiné použití. To záleží na několika klíčových faktorech. Mezi tyto faktory můžeme zařadit:

- Přenosovou rychlost
- Spotřebu energie
- Dosah
- Frekvence

Podle těchto kritérií bychom mohli technologie internetu věcí roztřídit do jednotlivých skupin. Nejlépe se dají rozdělit podle přenosového dosahu, jak je vidět na obrázku 3.



Obrázek 3 – Volba komunikačního systému podle potřebného přenosového dosahu

Zdroj: [44]

Dosah jednotlivých skupin bezdrátových technologií pro Internet věcí může velice lišit. Můžeme využívat systémy s dosahem v řádech centimetrů, nebo také ve stech kilometrů. Velice důležité je si při založení nové sítě Internetu věcí určit, jaký dosah je pro ni ideální. Na jedné straně je důležité mít dostatečný dosah, na straně druhé je třeba myslet na spotřebu energie a zároveň i na větší bezpečnostní hrozby, které budou tento velký dosah doprovázet. Proto by mělo jít o kompromis těchto veličin.

2.1 Proximity

Jedná se o skupinu technologií s dosahem maximálně 10 centimetrů. Nejzásadnějším rozdílem u těchto zařízení je, že k přenosu dat informací využívá elektromagnetickou indukci, z čeho plyne největší výhoda těchto technologií, protože tento způsob může být použit k indukci elektrických proudů v pasivních součástkách a následné komunikaci s nimi.

2.1.1 RFID

Technologie RFID (Radio Frequency Identification) používá bezkontaktní, rádiovou komunikaci s paměťovými čipy. Existují jak aktivní, tak pasivní verze čipů, vzhledem k vysoké ceně aktivních čipů, které obsahují i zdroj napájení a umí proto samy vysílat svou identifikaci, jsou mnohem rozšířenější levnější pasivní čipy. Snímač čipů, který do svého okolí vysílá periodické pulsy, nabije kondenzátor pasivního čipu, který se objeví v jeho okolí. Tím mu dodá energii k odeslání odpovědi. Tu tvoří údaje uložené na tomto čipu. Pasivní RFID čipy se používají především v biometrických pasech, nebo na identifikačních kartách pro monitorování vstupu osob do objektů, ale také k identifikaci zboží, kde nahrazují čárové kódy. [9]

2.1.2 NFC

NFC (Near Field Communication) je technologie radiové bezdrátové komunikace mezi elektronickými zařízeními na velmi krátkou vzdálenost (do 4 cm). Tuto vzdálenost je však možno za použití většího výkonu a antény značně prodloužit. Technologií NFC jsou dnes již běžně vybaveny bezkontaktní platební karty. NFC je de facto rozšířením RFID, oproti tomuto standardu mohou ovšem spolu prostřednictvím NFC technologie komunikovat i dva aktivní přístroje. [9]

2.2 WPAN

Wireless Personal Area Network je skupina technologií s dosahem maximálně mezi 10 až 100 metry. Jedná se o zařízení, která jsou pro svého uživatele snadno dosažitelná. Vzhledem k malé vzdálenosti mezi uzli sítě se používají technologie s nízkou energetickou náročností. Do této skupiny patří velké množství různých řešení komunikace, ze které jsem vybral 2 nejznámější.

2.2.1 Infraport

Neboli infračervený port představuje rozhraní, které pro přenos dat využívá infračerveného záření. Tato technologie byla před časem velice oblíbená a rozšířená a používala se zejména u mobilních telefonů, ale také u notebooků a dalších zařízení. Nevýhodou však byl malý dosah a také nutnost, aby na sebe zařízení přímo mířila. Infračervený přenos byl postupně nahrazen přenosem rádiovými vlnami. [17]

2.2.2 Bluetooth

Technologie Bluetooth měla primárně sloužit jako náhrada kabelů na krátkou vzdálenost mezi počítači a periferními zařízeními, pro sdílení a přenos souborů, tisk a elektronickou komunikaci v rámci kanceláře. Kromě komunikačních a výpočetních systémů jsou dnes možnosti využití technologie Bluetooth velice široké a setkat se s ní můžeme všude kolem nás. Zdaleka se neomezují pouze na propojení dvou mobilních telefonů nebo na připojení mobilního telefonu k dalšímu příslušenství jako jsou například bezdrátové klávesnice nebo headsety. Hojně se používá v počítačových periferiích, jako jsou bezdrátové myši či klávesnice, ale objevují se i například v digitálních fotoaparátech nebo fitness zařízeních. V automobilismu si Bluetooth našlo cestu například do senzorů tlaku v pneumatikách, dálkovém otevírání dveří, ale setkáme se s ním v podobě nejrůznějších ovladačů, senzorů a spínačů i ve svých domácnostech. Ve zdravotnictví se pak používá pro různé senzory např. měřič krevního tlaku nebo programovatelné vydávače léků. V podnikovém prostředí se Bluetooth ujal pro výměnu vizitek či synchronizaci souborů, e-mailů či kalendářů mezi PDA a laptopy. [38] [31]

Bluetooth Low Energy (BLE) se stává novým standardem pro bezdrátový přenos dat. Jedná se sice o Bluetooth, ale zároveň je to něco úplně jiného, než čím byl tento standard doposud. Původní Bluetooth samozřejmě zůstává zpětně kompatibilní a oba typy budou nadále existovat vedle sebe. Zásadní rozdíl je, že má oproti předešlé verzi nízkou spotřebu. Tak nízkou, že zařízení vybavené BLE by mělo být schopné na baterii fungovat až několik let.

Jaké jsou cesty k dosažení tak významné úspory energie? Nejlepší možnost je zkrátit na minimum dobu, ve které se modul probudí, naváže spojení, vyřídí potřebnou komunikaci a opět přejde do úsporného režimu. Tento takzvaný „enumeration time“ je v případě BLE přibližně 20× nižší než u klasického Bluetooth. Není však vhodný na přenášení velkého množství dat. [10] [6]

2.3 WLAN

Wireless Local Area Network je bezdrátová síť používaná v rámci jednoho domu, bytu, kanceláře apod. Její dosah je 100–1000 metrů a k jejich fungování se používá norem IEEE 802.11.xyz, které nesou komerční označení Wi-Fi.

Úspěch Wi-Fi přineslo využívání bezlicenčního pásma 2,4 GHz, což má negativní důsledky ve formě silného zarušení příslušného frekvenčního spektra a dále častých bezpečnostních incidentů. Další bezdrátovou technologií je WiMAX, která se zaměřuje na zlepšení přenosu signálu na větší vzdálenosti. [43]

2.3.1 WiMAX

Rádiová širokopásmová technologie WiMAX (Worldwide Interoperability for Microwave Access) je určena pro mnohabodovou komunikaci na velkou vzdálenost, nejen datovou, ale i hlasovou, obrazovou, či multimediální díky zabudované podpoře pro interaktivní provoz citlivý na zpoždění. Často bývá s technologií Wi-Fi házeny do jednoho pomyslného pytle, a WiMax bývá dokonce prezentován jako novější verze Wi-Fi, či jako jakési „Wi-Fi na maximum“. Není to ale pravda, neboť jde o dvě různé technologie, směřující do úplně jiných segmentů. Zatímco Wi-Fi je určeno do rukou samotných koncových uživatelů, pro nasazení uvnitř budov a překlenutí tzv. posledního metru, technologie WiMax je určena spíše do rukou poskytovatelů služeb a pro překlenutí tzv. poslední míle, na podstatně větší vzdálenosti a spíše vně budov. Nově pak WiMax aspiruje i na to, aby se stal konkurencí mobilním technologiím 3. generace (UMTS, resp. 3G) a umožnil nabízet skutečně mobilní služby. [26][32]

I přes všechny vzájemné odlišnosti ale mají WiMax a Wi-Fi také mnoho společného. Kromě toho, že se jedná o bezdrátové technologie, jde například o neustálé oddalování nástupu jejich novějších verzí. Rychlejší verze Wi-Fi, označované podle svého standardu 802.11n, již sice v určité podobě existují na trhu, ale samotný standard ještě nebyl dokončen. A možná ještě dlouho nebude. Podobně mobilní WiMax je slibován již poměrně dlouho, ale jeho reálný nástup je neustále oddalován. V České republice má navíc specifické problémy

i tzv. pevný WiMax, a kvůli nim se u nás nerozvíjí tak intenzivně jako v zahraničí. Naopak v oblasti Wi-Fi se Česká republika řadí mezi nejvyspělejší státy. [26]

2.4 WNAN

Sousedské sítě (Neighborhood Area Networks) se principiálně označují odlišně od sítí lokálních, přestože jejich dosah také není příliš velký, ale pokrytí a účel jsou trochu jiné. NAN využívají moderní bezdrátové technologie k umožnění bezplatného přístupu k internetu prostřednictvím připojení jednoho souseda. Důvodem je především celková cena připojení (hardware, software, placený přístup), která může být nedostupná pro řadu lidí, ale také technická náročnost samotného přístupu (zejména konfigurace), která je pro mnohé překážkou využívání internetu. [36]

NAN je založena na přístupovém bodě bezdrátové lokální sítě, který umožňuje připojení v dosahu maximálně kolem 0,5–1 kilometr (za použití všesměrové antény). Zájemci v nejbližším sousedství se pak mohou připojovat k bezdrátové síti pomocí své antény nasměrované na přístupový bod. NAN se ve skutečnosti neomezují pouze na poskytování sdíleného přístupu k internetu, ale nabízejí sdílení síťových služeb a zařízení v rámci dané WLAN. Poskytovatelé placeného připojení k internetu mohou v rámci svých zákaznických smluv zakazovat zprostředkování svých služeb dál, pak samozřejmě NAN možné nejsou. Ale řada ISP to (zatím) nedělá. [36]

2.4.1 6LoWPAN

6LoWPAN (z anglického IPv6 over Low-Power Wireless Personal Area Networks) je nový protokol vystavěn na standardu IEEE802.15.4. Díky němu je možné rozšířit široce používaný IP protokol i do oblasti bezdrátového spojení s nízkou spotřebou. Právě nízká spotřeba a pořizovací cena z něj dělají lepší volbu pro bezdrátové sítě Internetu věcí oproti Wi-Fi.

2.5 WWAN

Pod třípísmenným označením WAN se skrývá počítačová síť, která může plnit hned několik užitečných funkcí. Nejčastěji jde o propojení dvou vzdálených míst. Firmy obvykle s pomocí WAN propojují lokální sítě (LAN). Umožní tak například pracovníkům přistupovat k interním dokumentům společnosti z rozdílných míst. Prakticky nejznámější příklad typický pro WAN představuje internet. Mnoho organizací, které se pro nasazení vlastní Wide Area Network rozhodnou, však budují síť pouze pro své soukromé potřeby. [41][11]

Cisco v tomto případě doporučuje rozdělit topologii na tři skupiny zařízení [11]:

- Enterprise Campus – servery uvnitř firmy apod.
- Enterprise Edge – rozhraní sloužící pro propojení s ISP
- ISP Edge – zajišťuje samotné spojení s druhou (vzdálenou) stranou

Většina přenosu dat se v případě WAN realizuje pouze na prvních dvou vrstvách ISO/OSI modelu. To znamená, že není zajištěna detekce chyb. [41]

V současnosti existuje několik rozdílných metod komunikace ve WAN prostředí:

- Point-to-Point (Cisco HDLC, PPP) – jde o spojení dvou bodů, které je trvalé (vyhrazené).
- Packet Switched (X.25, Frame Relay, ATM) – data se přenáší po paketech, které putují rozdílnými cestami. Stává se proto, že dorazí v jiném pořadí, než byly odeslány.
- Circuit Switched (ISDN) – nejlepší příklad symbolizuje klasický telefon. Dochází zde k vytvoření dočasného spojení, které se však během přenosu nemění. [41]

2.5.1 Protokoly WWAN

Jedním z protokolů je protokol X.25, který však rozhodně nepatří mezi moderní technologie. Díky své velmi omezené přenosové kapacitě se s ním například dnes setkáme u platebních terminálů či bankomatů. Mnohem širším využitím již disponuje Frame relay. S vyšší rychlostí se logicky proměňuje v zástupce zastaralého protokolu X.25. Během komunikace si vytváří virtuální permanentní okruh (tzv. PVC), k jehož identifikaci používá DLCI (Data-Link Connection Identifier). ATM se někdy přiřazuje do skupiny fungující na principu přepojování buněk. Data totiž posílá v tzv. cells a dosahuje rychlosti přes 600Mb/s. Nasazuje se proto i pro přenos VoIP či videa. [41]

2.5.2 LTE, LTE – Advanced a 5G

LTE a LTE-A jsou nejnovější komerčně dostupné generace standardů pro mobilní telefony a další bezdrátová zařízení. Oproti starším 3G a 2G sítím přináší rychlejší stahování a nahrávání dat. V některých zdrojích bývá LTE uváděn jako 4G. V jiných pouze jako 3.5G, protože rychlosti, které definují standard 4G, jsou v běžných podmínkách stále jen obtížně dosažitelné.

LTE – Advanced je rychlejší verzí LTE. S teoretickou rychlostí stahování 300 Mb/s a nahrávání 150 Mb/s bývá nejčastěji označována jako 4G+ nebo 4.5G

Vedle zvýšených rychlostí bylo jedním z hlavních cílů LTE zjednodušit architekturu sítě. Ta se posunula od techniky přepínání okruhů CSD používané v sítích 2G a 3G kombinovaných sítí využívajících přepínání obvodů a paketů na systém ploché architektury založený na IP. Tato jednodušší architektura umožňuje nižší provozní náklady pro mobilní operátory. [37]

LTE byl původně podle návrh standardu 3GPP koncipován pouze pro přenos dat. Když bylo zřejmé, že přenos hlasu je rovněž potřebný GSM asociace vyvinula a standardizovala funkci označenou Voice over Long Term Evolution (VoLTE), která umožňuje přenos hovorů jako datových toků v síti LTE. Jestliže mobilní operátor zavedl síť 4G ale zatím nebyla implementována služba VoLTE, mohou účastníci využívat své 4G telefony k přenosům dat. Hlasové hovory jsou přepojovány prostřednictvím sítě 2G nebo 3G operátora. Tato technika se nazývá záložní přepnutí okruhů (CSFB), hlasové hovory se uskuteční přes síť 2G / 3G a datové přenosy jsou přepojeny do 4G sítě. [37]

5G síť neboli síť páté generace označuje novou technologii telekomunikačního standardu – rychlé bezdrátové připojení s nízkou latencí. Má vyšší kapacitu než stávající 4G síť a je až 100krát rychlejší. Zásadní je ale především její blesková odezva, která se pohybuje kolem jedné milisekundy. Díky tomu propojí síť páté generace bez problémů jak mobilní telefony, tak i nejrůznější chytrá zařízení z oblasti Internetu věcí. Předpokládá se, že 5G síť zrychlí vývoj virtuální reality, masivně rozšíří strojovou komunikaci, usnadní autonomní řízení automobilů a rozvine projekty chytrých měst. [35]

Mobilní síť 4G je nyní nasazena v 188 zemích. Ve většině zemí však stále není hlavní technologií mobilních sítí, tou jsou stále s více než 37% podílem sítě 3G a v některých zemích stále ještě převládají sítě 2G. Aktuálně tedy vzniká poněkud paradoxní situace. Zatímco výrobci už pracují na specifikacích pro pátou generacích mobilních sítí, některé země ještě ani nezačaly rozšiřovat sítě 4G. [37]

2.5.3 LoRa

LoRa je globální síť pro Internet věcí, která umožňuje svým zařízením obousměrnou komunikaci s omezeným počtem zpětných zpráv ve frekvenčním pásmu 868 MHz s dosahem 10 kilometrů za ideálních podmínek a relativně příznivou průchodností signálu do staveb. Vzhledem k výkonu řádu jednotek až desítek miliwattů a občasnému vysílání jen několikrát

denně může být životnost baterií mnoho let. Tato technologie umožňuje zařízením komunikovat levně, bezpečně a na velké vzdálenosti při zcela minimální spotřebě energie. [24][23]

Specifikace LoRaWAN je veřejně dostupná a definuje protokol přístupové vrstvy pro řízení komunikace mezi bránami LPWAN a koncovým zařízením. Verzi 1.0 vydalo sdružení LoRa Alliance v roce 2015. Zařízení v síti jsou asynchronní a vysílají data, jakmile jsou k dispozici nebo uplyne-li stanovený interval. Data vyslaná koncovým zařízením mohou být přijímána jednou nebo vícero branami, které je přeposílají centrálnímu serveru. Ten kromě řízení sítě odfiltruje duplicitní pakety, kontroluje zabezpečení a předává data aplikačním serverům. [23]

3 HROZBY V SÍTÍCH IOT

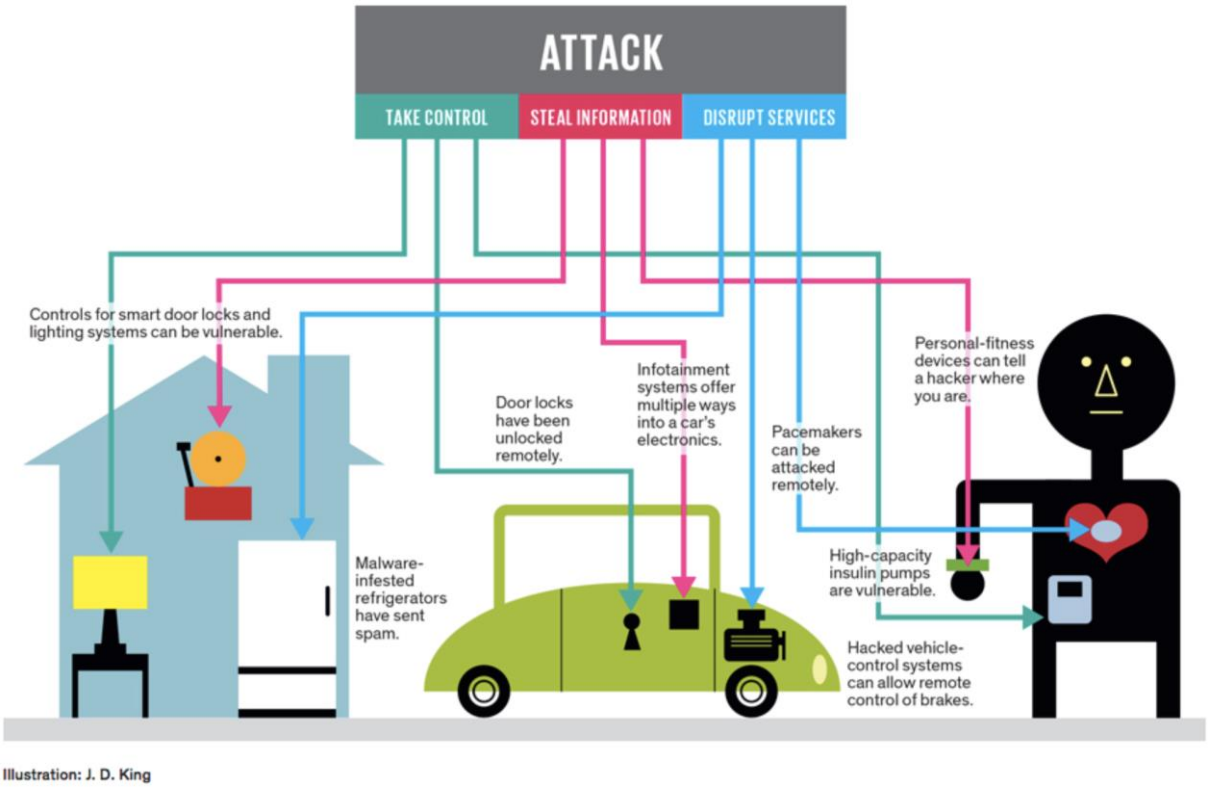
S novými možnostmi bezdrátových sítí vznikají i nové hrozby pro jejich provoz a uživatele. Strach z těchto hrozeb může zpomalit rozšíření nových technologií do praxe. Dosud nevyzkoušené technologie mohou mít několik úskalí. Těmi mohou být chyby, které by ohrozili životaschopnost sítě, nebo bezpečností nedostatky, kterých mohou útočníci využít k útoku na ni. Internet věcí nás začíná obklopovat ze všech stran a v nedaleké budoucnosti se bez něj zcela jistě neobejdeme. A proto je i jeho zabezpečení na pořadu dne. Mnoho výrobců však upřednostňuje, aby bylo propojení zařízení mezi sebou pro uživatele co nejjednodušší, a to i na úkor zabezpečení. Zaběhlejší bezdrátové komunikační technologie, které jsou využívány celosvětově však na bezpečnost komunikace velice dbají. V této kapitole se zaměřím nejprve na hrozby, které v oblasti internetu věcí hrozí a poté na zabezpečení komunikace. Vzhledem k tomu, že technologií a hardwaru je na trhu nespočet a jejich zabezpečení se v mnohém shoduje, bych se rád zaměřil pouze na bezpečnost těch nejpoužívanějších z nich. Nejprve je však důležité si stanovit hrozby, před kterými je potřeba se chránit.

Ač si to neuvědomuje, naše zařízení mohou být snadno ovládnuty někým jiným, což často může ohrozit životy. Pěknými příklady jsou pokusy agentury DARPA z roku 2015, kdy pouze s notebookem a vysílačem dokázali téměř ihned proniknout a zcela převzít kontrolu nad cizím dronem. Závažnější hrozbu však ukázali během druhého pokusu, kdy se jim s tím samým vybavením podařilo zneužít chyby v systému inteligentního automobilu a převzít nad nim kontrolu do takové míry, že řidič mohl pouze otáčet volantem. Všechny ostatní systémy, včetně brzdy a plynu ovládal hacker.

V roce 2014 firma Hewlett-Packard provedla studii zaměřenou na zabezpečení 10 nejpoužívanějších zařízení na trhu. I tato studie zjistila vážné nedostatky, a to nejen u zařízení, ale i u řešení cloudu a mobilních aplikací. Nedostatky, které jsou čerpány ze zdroje [15], byly:

- Soukromí – u 8 z 10 testovaných zařízení vyvstaly otázky ohledně shromažďování údajů o spotřebitelích. Mezi tyto údaje patří jméno, e-mailová adresa, adresa bydliště, datum narození, údaje o platebních kartách a zdravotním stavu.
- Nedostatečná autorizace – 8 z 10 řešení nevyžadovalo dostatečně složité a dlouhé heslo. Většina povolila uživateli si zvolit velice slabé heslo „1234“. S těmito slabě zabezpečenými účty se poté uživatel přihlašoval i do mobilních a webových aplikací.

- Nedostatečné šifrování při přenosu dat – 7 z 10 zařízení nešifrovala komunikaci do lokální a internetové sítě a polovina mobilních aplikací nepoužívala šifrování ani při komunikaci s cloudem.
- Nezajištěné webové rozhraní – 6 z 10 webových rozhraní vyvolalo obavy o bezpečnost uživatelského rozhraní. Jednalo se o trvalé XSS, špatnou správu relací, slabá výchozí pověření a pověření přenášení v čistém textu. 70% zařízení by potenciálnímu útočníkovi umožnilo určit platné uživatelské účty díky výčtu účtů nebo funkci resetování hesla.
- Nedostatečná ochrana software – 6 z 10 zařízení nepoužilo šifrování při stahování aktualizací software, což je alarmující číslo, vzhledem k tomu, že software zajišťuje správný chod zařízení. Některá stahování mohla být dokonce zachycena, extrahována a připojena jako souborový systém v operačním systému Linux, kde by mohlo dojít k jejich prohlížení či úpravám.



Obrázek 4 – Útok na zařízení IoT

Zdroj: [39]

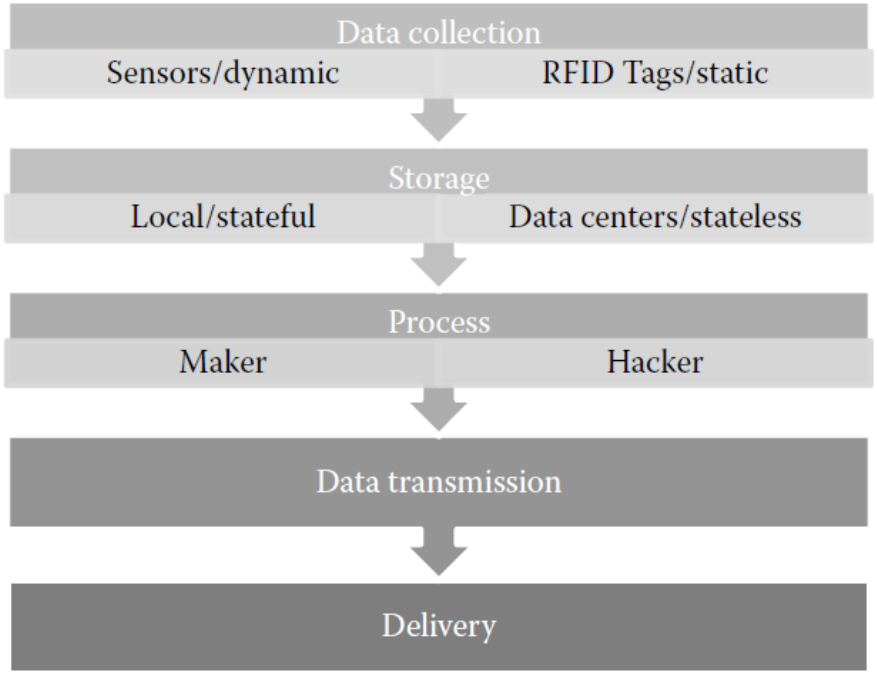
Pokud se útočníkovi podaří prolomit naši ochranu sítě, může:

- Ukrást citlivé informace
- Přerušit dostupnost služeb
- Převzít kontrolu nad zařízeními

K těmto cílům může použít různorodého množství nástrojů, které mohou být zaměřené proti fázím IoT, architektuře sítě a komponentům sítě. Nyní si postupně projdeme všechny tři cílové oblasti útoků, které jsou detailně popsané ve zdroji [16].

3.1 Útoky založené na fázích IoT

Komunikační řetězec IoT se skládá z 5 fází. Od sběru dat po jejich doručení koncovému uživateli. Všechny fáze můžeme vidět na obrázku 5.



Obrázek 5 – Fáze systému IoT

Zdroj: [16]

- Data leakage or breach

Únik dat může být vnitřní nebo vnější, úmyslný nebo neúmyslný, autorizovaný i zlomyslný, zahrnující hardware i software. Častou příčinou úniku jsou nečestní či nespokojení zaměstnanci organizací. Velké riziko úniku dat hrozí i při jejich přesunu po cloudu. Omezit se dá za použití DLP (Data Leakage Prevention)

- Data sovereignty

Internet věcí zahrnuje všechny věci napříč světem, přesto však jsou informace uložené v digitální podobě předmětem zákonů určitého státu.

- Data loss

Ke ztrátě dat dochází neúmyslně, náhodou. Může se tak stát v důsledku chyby hardwaru nebo softwaru či při přírodních pohromách.

- Data authentication

Autentizace dat má zajisti integritu a správnost přijatých dat. Toho lze docílit tak, že jsou data přijímána pouze od zamýšlených či důvěryhodných uživatelů. Zároveň má zajistit, že nebyla data upravena během přenosu.

- Attack on availability

Zajištění dostupnosti služeb pro uživatele má nejvyšší prioritu. K odmítnutí služby dochází v případě, kdy je služba přetížena z důvodu nadměrného počtu požadavků. Může se jednat o cílený útok, kdy útočníci posílají do datových center škodlivé či neúplné pakety dat. K nedostupnosti služeb však může dojít i z důvodu velkého množství či častého opakování požadavků oprávněných uživatelů.

- Modification of sensitive data

Během přenosu mohou být data zachycena, upravena a v této formě poslána dále. Může dojít ke změně obsahu, pořadí či času ve kterém zprávu obdržíme. To může učinit zprávu bezvýznamnou, či dokonce škodlivou.

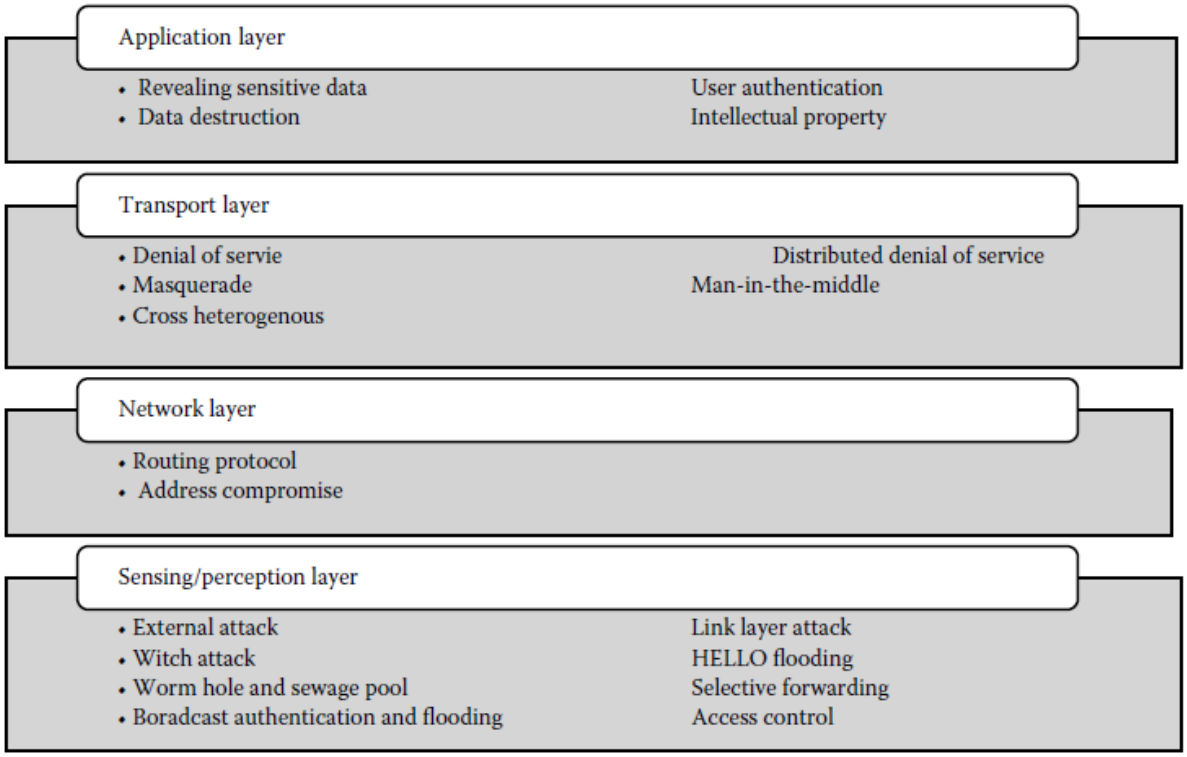
3.2 Útoky na architekturu sítě

Pro internet věcí dosud nebyla dohodnuta žádná jednotná architektura. Obecně se však předpokládá, že má každá síť internetu věcí 4 vrstvy: snímací, síťovou, přenosovou a aplikační. Na obrázku 6 můžeme vidět jednotlivé vrstvy a možné útoky pro každou z nich, které si dále popíšeme.

- External attack

Internet věcí by se neobešel bez cloudových služeb na něž ukládáme data včetně těch citlivých, a proto je na snadě se zamyslet nad důvěryhodností poskytovalete těchto služeb. V případě nahrání dat do cloudu neznáme lokaci, kde budou data skladována případně

zpracovávána. Nad daty ztrácíme kontrolu a poskytoval cloudu by je mohl sdílet s ostatními, či je dokonce použít pro své vlastní účeli.



Obrázek 6 – Možné útoky založené na architektuře

Zdroj: [16]

- Wormhole attack

Útok červí dírou je velice populární v ad hoc bezdrátových sítích. Princip útoku spočívá v tom, že útočník vytvoří v síti dva či více uzlů. Tím vznikne tunel, kdy je možné na jednom konci zachytávat data a posílat je tunelem na druhý. Tento druh útoku je možný i když nebyl kompromitován žádný původní uzel a je velice těžké ho objevit, neboť veškerá komunikace vykazuje autentičnost a důvěrnost. [16]

- Selective forwarding attack

Škodlivé uzly sítě filtrují pakety, z nichž některé zachytí a zbytek nechají pokračovat dále. Takto může dojít ke ztrátě důležitých dat pro další pokračování procesů.

- Witch attack

Škodlivý uzel v síti vyčkává, až dojde u některého důvěrného uzlu k chybě. Poté převezme její místo v síti včetně veškeré komunikace což může vyústit ve ztrátu dat.

- HELLO flood attacks

V první fázi se všechny uzli sítě představí všem svým sousedům na stejně frekvenci zprávou HELLO. Škodlivý uzel pokryje velký rozsah frekvencí a stává se tak sousedem všech uzlů v síti. V druhé fázi také vyšle sousedům zprávu HELLO, díky které získá oprávněný přístup do sítě, ve které poté posílá velké množství nesmyslných požadavků na služby a ta se stává pro uživatele nedostupnou.

- Distributed denial of service (DDoS)

DDoS, je koordinovaný útok stovek až tisíců útočníků, kteří posílají nežádoucí objemné pakety s cílem vyčerpat paměťové kapacity oběti, čímž zároveň zastaví vyřizování požadavků oprávněných uživatelů.

- IP spoof attack

Spoofing je druh útoku, při kterém se útočník vydává za někoho jiného a tím získá přístup k pro něj jinak nedostupným zdrojům informací. IP address spoofing se nazývá metoda tvorby IP paketů do kterých byly vloženy různé IP adresy. Ty jsou poté často použity při DDoS útoku, neboť jsou obtížněji filtrovatelné z důvodu zdánlivě různého původu a zároveň skryjí skutečný zdroj útoku.

- Botnet

Botem nazýváme zařízení, jehož bezpečnost byla prolomena a kontrolu převzal útočník. Je-li těchto zařízení více a jsou propojeny přes internet, poté mluvíme o botnetu. Všechny zařízení této kompromitované sítě mohou být použity například pro útok DDoS.

- Eavesdropping

Eavesdropping spočívá v zachycení síťové komunikace k získání neautorizovaného přístupu. Může vyústit v selhání důvěrnosti komunikace. Příkladem eavesdroppingu je útok man in the middle. Při něm je komunikace mezi účastníky, ač to tak nevypadá, posílána přes útočníka, který může konverzaci ovlivňovat.

- Replay attack

Útočník zachytí a uloží staré zprávy, které může později odeslat jako jeden z účastníků komunikace a tím získat přístup do sítě.

- Back door

Za použití zadních vrátek může útočník obejít kontrolní mechanismy sítě a tím do ní získat přístup.

- Byzantine failure

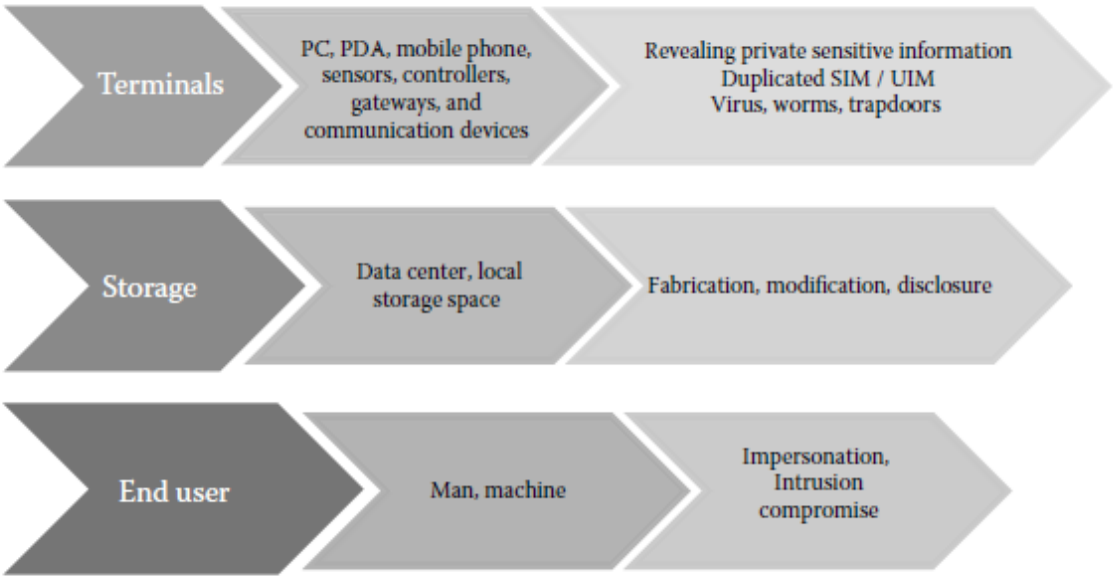
Byzantine failure je škodlivá aktivita ovlivňující výkon serveru či skupinu serverů, a tak dojde k radikálnímu snížení výpočetního výkonu cloudu.

- Data protection

Zákazník cloudových služeb by si měl ověřovat, zda je s jeho uloženými daty zacházeno pouze legální cestou. Toto je však v praxi velice náročné.

3.3 Útoky na komponenty sítě

Internet věcí spojuje „všechno“ skrze internet. Tyto věci jsou heterogenní povahy posílající citlivá data na velké vzdálenosti. Kromě útlumu, krádeže, ztráty, prolomení či ztráty dat z důvodu přírodní katastrofy mohou být vytvořeny či upraveny kompromitovanými senzory. Na obrázku 7 jsou vidět různé možné útoky na komponenty internetu věcí.



Obrázek 7 – Možné útoky založené na komponentech

Zdroj: [16]

Ověření koncového uživatele na vstupní úrovni je pro bezpečnost povinné. Rozlišení mezi skutečným člověkem a strojem je nesmírně důležité a jsou k tomu používány zcela

automatické veřejné Turingovy testy, které známe pod anglickou zkratkou CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans apart). Principem Turingova testu je kladení otázek v přirozeném jazyce a náhodném pořadí. Respondenty jsou člověk a testovaný subjekt (např. počítač nebo umělá inteligence). Pokud tazatel nedokáže rozlišit mezi odpověďmi jednotlivých dotazovaných, můžeme testovaný subjekt považovat za skutečně inteligentní.

Z této teze vychází software CAPTCHA, který dokáže kladením otázek (jednoduchých pro člověka, ale téměř nevyřešitelných pro počítač) určit identitu návštěvníka a podle ní povolit či zakázat přístup. Novější verze programu již nevyžaduje opisovat text nebo vybírat z nabízených obrázků, ale snaží se lidského uživatele identifikovat podle parametrů internetového připojení a jeho chování ve virtuálním prostředí.

4 BEZPEČNOST V SÍTÍCH IOT

4.1 OWASP Internet of Things Top 10 list

Roku 2014 se uskutečnil hackerský útok ve velkém měřítku. Za několik týdnů bylo rozesláno přes 750.000 škodlivých e-mailů z více než 100.000 zařízení běžné potřeby, ledničky nevyjímaje. Po tomto incidentu se začali o bezpečnost Internetu věcí zabývat experti na bezpečnost z Open Web Application Security Project (OWASP), a ještě toho roku vytvořili desatero, které má pomoci výrobcům, vývojářům a spotřebitelům lépe porozumět problémům spojeným s Internetem věcí a tím dosáhnout větší bezpečnosti. Roku 2018 byla vydána aktualizovaná verze desatera, do které patří: [14] [27]

1 Slabá, uhodnutelná nebo pevně zakódovaná hesla

2 Nezabezpečené síťové služby

3 Nezabezpečené rozhraní

4 Chybějící zabezpečení při procesu aktualizace

5 Použití slabě zabezpečených nebo zastaralých systémů

6 Nedostatečná ochrana soukromí

7 Nezabezpečený přenos a skladování dat

8 Špatná správa zařízení

9 Základní nastavení z výroby

10 Slabá fyzická ochrana zařízení

4.2 Principy bezpečnosti IoT

The Internet of Things Project, za jehož vytvořením také stojí OWASP se zabývá bezpečností internetu věcí velice podrobně. Kromě desatera z minulé kapitoly bych ještě rád zmínil principy bezpečnosti, které v rámci toho projektu vypracovali. Následující výčet principů je převážně čerpán ze zdroje [29]

- Předpokládat nepřátelský okraj

Okrajová zařízení mohou s největší pravděpodobností padnou do nepřátelských rukou. Předpokládáme, že útočníci budou mít fyzický přístup k okrajovým komponentům a budou

s nimi manipulovat, přesunou je do nepřátelských sítí a ovládnou jejich zdroje, jako například DNS, DHCP nebo směrování na internet.

- Testovat pro měřítko

Při návrhu bezpečnostního řešení musíme brát v potaz velikost internetu věcí. Pokud nebude brána v potaz, může i jednoduché řešení fungující v sítích WLAN způsobit v měřítku internetu věcí samovolné odmítnutí služby.

- Internet lží

Automatizované systémy jsou extrémně schopné prezentovat dezinformace v přesvědčivých formách. Systémy IoT by měly vždy ověřovat data od okraje, aby se předešlo autonomní dezinformaci z poškození systému.

- Využívat autonomie

Automatizované systémy jsou schopny složitých, monotónních a pro lidského uživatele nudných operací. Bezpečnost systémů internetu věcí by měla těchto výhod využívat.

- Očekávat izolaci

Výhoda autonomie by se měla rozšířit i na situace, kdy je komponenta izolována. Protiopatření v oblasti bezpečnosti nesmí v případě přerušení připojení se sítí degradovat.

- Chránit rovnoměrně

Šifrování data chrání pouze na šifrovaných spojeních. V bodech, které šifrované nejsou, mohou být data v ohrožení. Například před šifrováním, po dešifrování a na všech cestách, které šifrování nevyžadují. Je třeba pečlivě zvážit celý životní cyklus dat, aby se zajistila rovnoměrná, jednotná a vhodná aplikace šifrování. I metadata o šifrovaných datech však mohou útočníkům poskytnout cenné informace.

- Šifrování je složité

Aplikace šifrování není jednoduchá a je velice snadné při ní provést chyby. Mezi běžné úskalí patří například použití šifrování bez provedení ověření certifikátů, neověření přechodných certifikátů, zašifrování komunikace slabým klíčem, zveřejnění soukromého klíče. Základem je provést důkladnou kontrolu všech možností šifrování, aby se těmto chybám předešlo.

- Opevnit systém

Musíme zajistit, že komponenty IoT jsou omezeny pouze nezbytnou sadu funkcí potřebnou pro jejich životaschopnost, čímž zmenšíme možnou plochu útoku. Nepoužité porty a protokoly by měly být zakázány a nepotřebné prvky software by měly být odinstalovány nebo vypnuty. Důležité také je sledovat komponenty třetích stran a zajistit jejich aktualizace.

- Omezit přístup na minimum

V maximální možné míře omezit přístup k internetu na základě přijatelných kritérií použití. V tom, že vystavíme, bez dobrého důvodu, rozhraní senzoru celému internetu není žádná výhoda. Důležité proto je si vytvořit správný seznam přístupových pravidel.

- Podpora životního cyklu

IoT systémy by měly být schopny rychle přijmout nové komponenty, ale zároveň by měly být schopny znovupověření stávajících komponent a jejich udržení po celou dobu jejich životního cyklu. Tato schopnost by měla zahrnovat všechny složky systému, od zařízení po uživatele.

- Výsledky agregace dat jsou nepředvídatelné

Systémy internetu věcí jsou schopny nasbírat obrovské množství dat, která se mohou zdát neškodná. Po komplexní analýze však mohou být odhaleny velmi citlivé vzory nebo informace v datech skryté. Systém IoT musí být připraven na ochranu a správu dat s neočekávaně citlivou informací, která se projeví až po jeho nasazení.

- Připravit se na nejhorší

Systém IoT by měl mít schopnost reagovat na kompromisy, nepřátelské účastníky, malware nebo jiné nepříznivé události. Měl by mít zavedené funkce pro opětovné vydání pověření, vyloučení účastníků, distribuci bezpečnostní záplat a aktualizací.

- Bezpečnost zařízení po celý jejich životní cyklus

Návrháři systému internetu věcí si musí uvědomit, že prodloužená životnost zařízení bude vyžadovat dopředně kompatibilní bezpečnostní funkce. Systém, i přes své stárnutí, musí být stále schopen reagovat na vývoj v oblasti bezpečnosti. Nové šifrování, pokroky v protokolech, nové metody a techniky útoků a změna topologie vyžadují, aby systémy IoT byly schopny řešit vznikající problémy s bezpečností po celou dobu jejich životního cyklu.

- Útočník vyhledává slabiny

Útočníci identifikují nejslabší článek a pokusí se ho využít. Proto by mělo být zabezpečené rovnoměrné. Mobilní rozhraní, skrytá rozhraní API nebo prostředí s omezenými prostředky musí být zabezpečeno stejným způsobem jako robustnější rozhraní nebo rozhraní s bohatými funkcemi. Například vícefaktorová autentizace pro webové rozhraní je k ničemu, pokud k přístupu přes mobilní aplikaci stačí zadat čtyřmístný PIN.

- Přechodné vlastnictví

Komponenty IoT se často prodávají nebo převádějí během jejich životního cyklu. Je proto nutné zajistit možnosti ochrany a izolace dat, které zabezpečí data tak, že by byla v bezpečí i při prodeji konkurentům nebo útočníkům.

- N: N autentifikace

Sítě internetu věcí nefungují na tradičním modelu 1:1 uživatelů aplikací. Každá komponenta může mít více než jednoho uživatele a uživatel může komunikovat s více komponentami. Někteří uživatelé mohou mít přístup k různým datům nebo možnostem na jednom zařízení a jeden uživatel může mít různá práva na více zařízeních. Více zařízení může potřebovat zprostředkovat oprávnění jménem jednoho uživatelského účtu a tak dále. IoT systém musí být na takovéto komplexní otázky důvěryhodnosti a ověřování připraven.

4.3 Metody zabezpečení bezdrátové komunikace

Internet věcí je založen převážně na obousměrné bezdrátové komunikaci, které je velice snadné odposlouchávat. Na obrázku 8 můžeme vidět nezabezpečenou komunikaci IoT.

Obrázek 8 – Nezabezpečená komunikace internetu věcí

Zdroj: [25]

Cílem bezpečnosti internetu věcí je aplikovat takový model, který bude fungovat se všemi koncepty komunikace mezi zařízeními. Důležitou složkou této strategie je přesun bezpečnosti do sítě. Poté bude mít síť schéma jako na obrázku 9.

Obrázek 9 – Zabezpečená komunikace internetu věcí

Zdroj: [25]

4.3.1 SSL

Secure Sockets Layer, (SSL, doslova vrstva bezpečných socketů) je protokol, resp. vrstva vložená mezi vrstvu transportní (např. TCP/IP) a aplikační (např. HTTP), která poskytuje zabezpečení komunikace šifrováním a autentizaci komunikujících stran. [33]

Historie SSL sahá již do začátků veřejného využívání internetu v 90. letech. Společnost Netscape tento protokol vytvořila v roce 1994, jelikož si uvědomovala nutnost zabezpečení internetu. Cílem Netscapu bylo vytvořit šifrování mezi klientem a serverem, které by bylo nezávislé na operačním systému. [13]

V březnu 1995 byla uvedena SSL verze 2 v Netscape Navigatoru 1.1, což byl v té době populární webový prohlížeč. Poslední verze SSL je verze 3.0. Od roku 1999 je SSL protokol nahrazován TLS protokolem, který již vydává a standardizuje IETF (Internet Engineering Task Force). SSL protokol byl z důvodu nedostatečného zabezpečení prohlášen zastaralým v červnu 2015. [13]

4.3.2 TLS

Transport Layer Security, (TLS, zabezpečení transportní vrstvy) je protokol umožňující aplikacím komunikovat po síti způsobem, který zabraňuje odposlouchávání či falšování zpráv. Pomocí kryptografie poskytuje TLS svým koncovým bodům autentizaci a soukromí při

komunikaci internetem. Typicky je autentizován pouze server (tedy jeho totožnost je zaručena), zatímco klient zůstává neautentizován. To znamená, že koncový uživatel (ať člověk či aplikace, jako třeba webový prohlížeč) si může být jist, s kým komunikuje. Další úroveň zabezpečení – při níž oba konce „konverzace“ mají jistotu, s kým komunikují – je označována jako vzájemná autentizace. Vzájemná autentizace vyžaduje nasazení infrastruktury veřejných klíčů (PKI) pro klienty. [40]

TLS zahrnuje tři základní fáze:

1. Dohodu účastníků na podporovaných algoritmech
2. Výměnu klíčů založenou na šifrování s veřejným klíčem a autentizaci vycházející z certifikátů
3. Šifrování provozu symetrickou šifrou

Během inicializačního protokolu (Handshake Protocol) se klient a server dohodnou na používaných kryptografických algoritmech a šifrovacích a dešifrovacích klíčích, které jsou používány po celou dobu spojení. Současné implementace podporují následující algoritmy:

- Pro kryptografii s veřejným klíčem: RSA, Diffie-Hellman, DSA
- Pro symetrické šifrování: RC2, RC4, IDEA, DES, Triple DES, AES, Camellia
- Pro jednosměrné hashování: Message-Digest algorithm (MD2, MD4, MD5), Secure Hash Algorithm (SHA-1, SHA-2, SHA-3)

Pokud dojde při libovolném kroku inicializačního protokolu k chybě, nedojde k vytvoření spojení.

4.3.3 AES

Advanced Encryption Standard (AES, standard pokročilého šifrování) je standardizovaný algoritmus používaný k šifrování dat v informatice. Jedná se o symetrickou blokovou šifru šifrující i dešifrující stejným klíčem data rozdělená do bloků pevně dané délky. Norma nahradila dříve užívanou šifru DES. Je používána například pro bezdrátové Wi-Fi sítě v rámci zabezpečení WPA2 dle standardu IEEE 802.11i. [2]

Původní název šifry AES je Rijndael. Její název vznikl přesmyčkou jmen jejích dvou autorů Joana Daemena a Vincenta Rijmena z belgické Lovaně, kteří tuto šifru přihlásili do veřejné soutěže NIST o federální šifrovací algoritmus AES vyhlášené 2. ledna 1997. Americký úřad pro standardizaci (NIST) vybral po pěti letech schvalovací procedury šifru

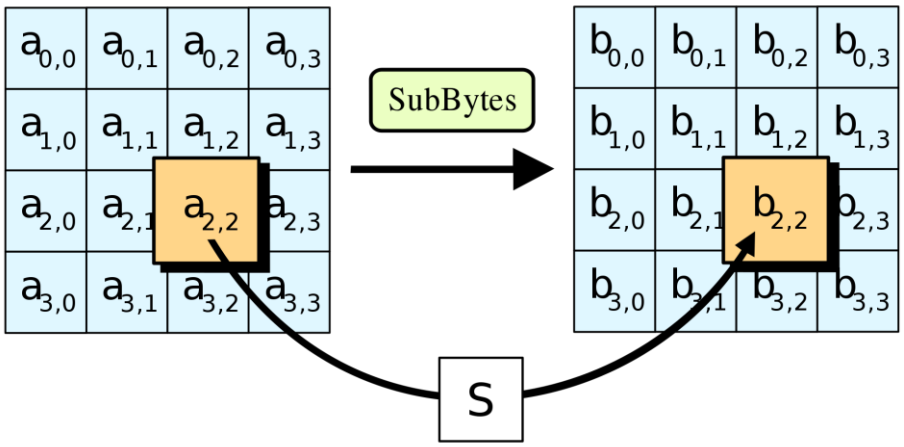
AES jako nejvhodnější návrh z patnácti předložených. AES je první šifra dostupná široké veřejnosti, která byla zároveň uznaná Národní bezpečností agenturou NSA ke šifrovaní nejtajnějších dokumentů. Dne 26. května 2002 začala být ke svému účelu používána jako federální standard USA. [3][2]

AES má pevně danou velikost bloku na 128 bitů a velikost klíče na 128, 192 nebo 256 bitů. V současné době není možný útok hrubou silou ani na 128bitový klíč. Jediná možná reálná hrozba útoku hrubou silou je ze strany kvantových počítačů a počítačů založených na bázi DNA. Ty se však v dohledné době mezi obyčejné uživatele nerozšíří. Bohužel ani AES není nerozluštitelná a dříve nebo později se podaří šifru prolomit. Dle odhadů by k tomu však ještě minimálně 10 let nemělo dojít. [3][2]

Šifrování probíhá ve čtyřech krocích:

1. **Záměna bajtů**

Při záměně bajtů je každý bajt v matici nahrazen pomocí 8bitového zaměňovacího boxu, Rijndeal S-boxu (nelineární substituční funkce měnící jednotlivé bity). Tato operace zajišťuje nelinearitu v šifře. Aby S-box minimalizoval pravděpodobnost možných útoků založených na jednoduchých algebraických vlastnostech, je konstruován tak, aby v něm nevznikaly pevné body a žádné jejich protějšky. [1]



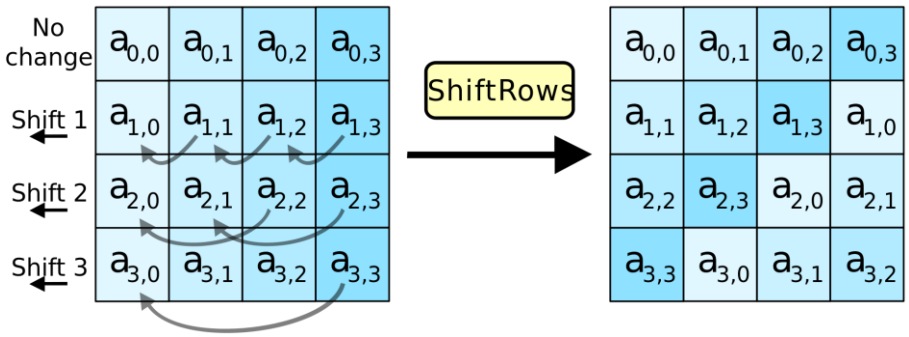
Obrázek 10 – Záměna bajtů

Zdroj: [2]

2. **Prohození řádků**

Tato operace probíhá na úrovních řádků, kde jednotlivě prohazuje bajty v každém řádku o určitý přesah. V případě AES je první řádek ponechán beze změn. Každý bajt druhého řádku je posunut o jeden doleva. Stejným způsobem je třetí a čtvrtý řádek posunut o dvě,

respektive tři pozice. Pro bloky o velikostech 128 bitů a 192 bitů je postup prohození řádků stejný. V těchto případech je každý sloupec výstupu složen z bajtů z každého sloupce na vstupu. [1]

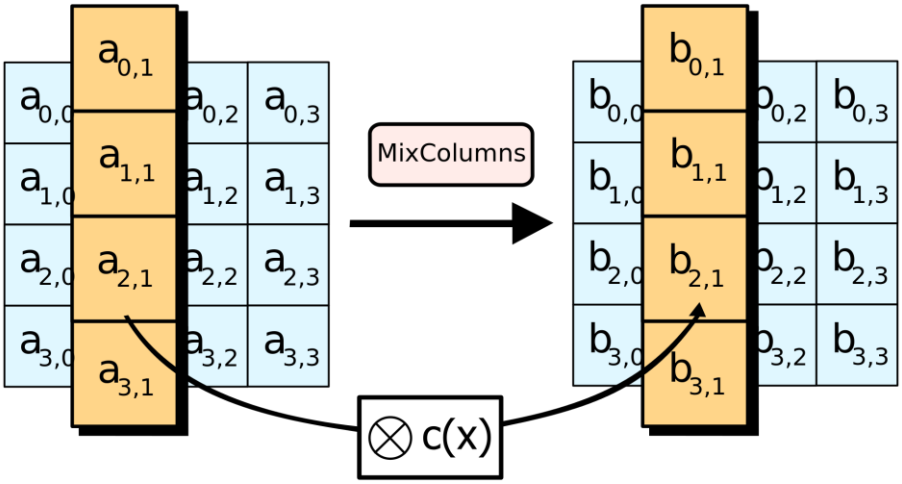


Obrázek 11 – Prohození řádků

Zdroj: [2]

3. Kombinování sloupců

V tomto kroku kombinujeme 4 bajty v každém sloupci. Tato funkce vezme čtyři bajty jako vstup a vrátí čtyřbajtový výstup, kde každý vstupní bajt ovlivní všechny výstupní bajty. Společně s předchozími kroky zajistí dostatečnou náhodnost v šifře. [1]

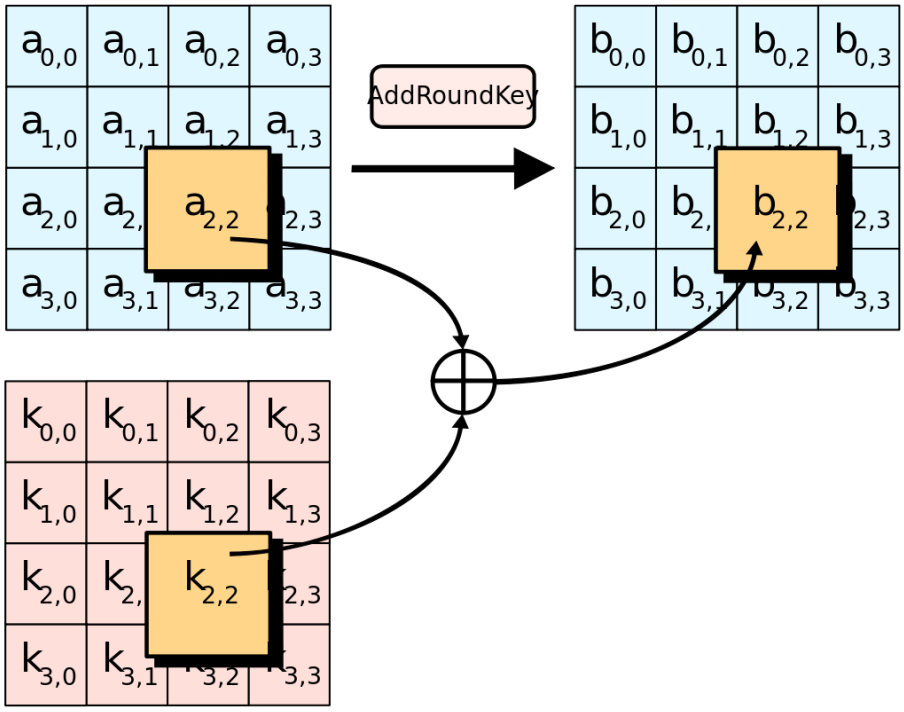


Obrázek 12 – Kombinování sloupců

Zdroj: [2]

4. Přidání podklíče

Při přidání podklíče je každý bajt zkombinován s podklíčem. Pro každou iteraci je podklíč odvozen z hlavního klíče. Každý podklíč má stejnou velikost a je přidán za pomoci kombinace každého bajtu stavu s odpovídajícím bajtem podklíče užitím operace XOR nad všemi bity. [1]



Obrázek 13 – Přidání podklíče

Zdroj: [2]

U systémů s 32bitovými a většími délkami slov je možné urychlit provádění této šifry pomocí zkombinování operací záměna bajtů a prohození řádků s operací kombinování sloupců, přičemž se transformují do sekvencí vyhledávacích tabulek. Pro provedení této operace jsou nezbytné čtyři 32bitové tabulky o 256 vstupech. Iterace může být nyní provedena s šestnácti vyhledávacími tabulkami a dvanácti 32bitovými XOR operacemi, následovanými čtyřmi 32bitovými XOR operacemi v kroku přidání podklíče. [2]

Kryptologové považují za částečné prolomení šifry jakýkoliv přístup, který vede k rozluštění rychleji než vyzkoušení všech možných klíčů (metoda útoku hrubou silou). Útok hrubou silou proti AES s 256bitovým klíčem by vyžadoval 2^{256} operací. Celkový výpočet by tedy trval mnohem déle, než je stáří celého vesmíru. [1]

4.3.4 Model Body + Envelope

Výše jsme si popsali nejrozšířenější šifrovací metody. Jaké však použijeme k zabezpečení komunikace v sítích IoT? SSL/TLS slouží k zašifrování dat od jednoho bodu k druhému, viz. obrázek 14. My však potřebujeme zabezpečit data od jednoho konce sítě k druhému tzn. přes větší množství bodů. [39][25]

Obrázek 14 – Šifrování pomocí SSL/TLS

Zdroj: [39]

Pro tento účel je lepší AES, protože dokáže zašifrovat data skrze celý řetězec bodů až do cíle. Vzhledem k tomu, že ale v IoT potřebujeme data číst a zpracovávat při přenosu i v jiných bodech než pouze cílovém, bylo by velice náročné data v průběhu přenosu dešifrovat a poté zase zašifrovat metodou AES. [39][25]

Ideálním řešením je model Body and Envelope, česky tělo a obálka. Tento model využívá výhod TLS i AES. Princip spočívá v tom, že celé tělo zprávy je šifrováno v TLS a všichni s právy TLS mají přístup k datům mimo obálku. Zbytek dat v obálce je šifrován za pomoci AES. [25]

Obrázek 15 – Šifrování TLS i AES v jedné zprávě

Zdroj: [39]

Takto jsou citlivá data v obálce chráněna i případě, kdy by byl jeden uzel v síti napaden. Útočník by pouze získal data, která byla odšifrována z TLS.

ZÁVĚR

Ačkoli je Internet věcí stále relativně mladý pojem a na plné využití jeho potenciálu si ještě nějakou dobu počkáme, tak již dnes zcela běžně narážíme na bezpečnostní problémy s ním spojené. Data, alfa i omega celého Internetu věcí, jsou věc nehmotná, a proto si možná tolik neuvědomujeme, že mohou být odcizena a zneužita stejně jako např. telefon, automobil či platební karta.

Výrobci zařízení se snaží držet krok s rychlým vývojem IoT, a to i na úkor jejich bezpečnosti. Proto se může stát, že se do rukou uživatele dostane produkt s nejmodernějšími funkcemi, avšak bez či jen s částečným zabezpečením. Možnou hrozbou pro takováto zařízení je i nedostatečný čas na vývoj či testování, které může vyústit v chyby, kterých poté útočník využije k průniku do sítě a k citlivým informacím uvnitř.

Vzhledem k tomu, že rozměry a funkce Internetu věcí zatím nemají v historii informačních technologií obdoby, je většina dosavadních bezpečnostních opatření pro využití v IoT nedostačujících. Pro takové množství dat může být např. šifrování nedostatečně silné, nebo požadavky na výkon jeho implementace tak velké, že by síť zpomalovaly. Proto začali vznikat společnosti, jako je firma PubNub (založena roku 2010), které se zabývají vývojem optimálních softwarů pro realizace IoT řešení včetně dostatečného zabezpečení.

Naštěstí existují organizace, jako je OWASP, které se soustřeďují na bezpečnost IoT zařízení a vydávají, či alespoň aktualizují doporučení pro výrobce i uživatele těchto zařízení. Uživatelům v České republice bych doporučil sledovat informační servis Národního centra kybernetické bezpečnosti, kde jsou zveřejněny kybernetické hrozby.

POUŽITÁ LITERATURA

[1] Advanced Encryption Standard. *Guard-dynamics.cz* [online]. [cit. 2019-04-25]. Dostupné z: http://www.guard-dynamics.cz/aes-advanced-encryption-standard

[2] Advanced Encryption Standard. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-04-15]. Dostupné z: https://cs.wikipedia.org/wiki/Advanced_Encryption_Standard

[3] AES. *Kryptografie.wz.cz* [online]. [cit. 2019-04-15]. Dostupné z: http://www.kryptografie.wz.cz/data/aes.html

[4] Co je cloud. *Azure.microsoft.com* [online]. [cit. 2019-03-18]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-the-cloud/

[5] Co je LTE? A jaké nabízí výhody oproti 3G a 2G sítím? *Alza.cz* [online]. [cit. 2019-04-28]. Dostupné z: https://www.alza.cz/co-je-lte

[6] Co je to Bluetooth LE, BLE, Bluetooth Low Energy, Bluetooth Smart, Bluetooth 5? *365tipu.cz* [online]. [cit. 2019-03-21]. Dostupné z: https://365tipu.cz/2017/09/06/tip883-co-je-to-bluetooth-le-ble-bluetooth-low-energy-bluetooth-smart-bluetooth-5/

[7] Co je to Cloud? Patří mu budoucnost dat? *Lenovo.blog.cz* [online]. [cit. 2019-03-18]. Dostupné z: http://www.lenovoblog.cz/2014/05/co-je-to-cloud-patri-mu-budoucnost-dat.html

[8] Co je to Internet věcí (IoT) a jak vám může zlepšit život. *Kvalitni-internet.cz* [online]. [cit. 2019-03-03]. Dostupné z: https://www.kvalitni-internet.cz/co-je-internet-veci-iot-jak-vam-muze-zlepsit-zivot

[9] Co znamená RFID/NFC. *Obalnakartu.cz* [online]. [cit. 2019-03-21]. Dostupné z: https://obalnakartu.cz/technologie/uvod-do-rfid-nfc/

[10] Bluetooth Low Energy. *Dps-az.cz* [online]. [cit. 2019-03-21]. Dostupné z: https://www.dps-az.cz/soucastky/id:9912/bluetooth-low-energy

[11] Enterprise Internet Edge Design Guide. *Cisco.com* [online]. [cit. 2019-04-28]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/IE_DG.html

[12] Fog Computing aneb Rozhodování blíže zdroji. *Systemonline.cz* [online]. [cit. 2019-03-18]. Dostupné z: https://m.systemonline.cz/clanky/fog-computing-aneb-rozhodovani-blize-zdroji.htm

[13] Historie SSL/TLS certifikátů. *Sslmentor.cz* [online]. [cit. 2019-04-15]. Dostupné z: https://blog.sslmentor.cz/clanky/historie-ssl-tls-certifikatu/

[14] How to Test the Security of IoT Smart Devices. *Resources.infosecinstitute.com* [online]. [cit. 2019-03-31]. Dostupné z: https://resources.infosecinstitute.com/test-security-iot-smart-devices/

[15] HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. *Hp.com* [online]. [cit. 2019-03-31]. Dostupné z: https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676

[16] HU, Fei, ed. *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations.* Boca Raton: CRC Press, 2016. ISBN 978-1-4987-2319-0.

[17] Infraport. *It-slovník.cz* [online]. [cit. 2019-03-21]. Dostupné z: https://it-slovnik.cz/pojem/infraport

[18] Internet of things. (IoT). *Internetofthingsagenda.techtarget.com* [online]. [cit. 2019-03-03]. Dostupné z: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

[19] Internet věcí (Internet of Things) - propojení různých zařízení díky internetu. *Kodys.cz* [online]. [cit. 2019-03-02]. Dostupné z: https://www.kodys.cz/technologie/internet-veci-internet-things.

[20] Internet věcí. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-03-02]. Dostupné z: https://cs.wikipedia.org/wiki/Internet_v%C4%9Bc%C3%AD.

[21] IoT portál. *Iot-portal.cz* [online]. [cit. 2019-03-03]. Dostupné z: https://www.iot-portal.cz

[22] Kde najde IoT největší využití? 10 oblastí, které pravděpodobně ovlivní nejvíce. *Cdr.cz* [online]. [cit. 2019-04-15]. Dostupné z: https://cdr.cz/clanek/kde-najde-iot-nejvetsi-vyuziti-10-oblasti-ktere-pravdepodobne-ovlivni-nejvice

[23] LoRa In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-04-20]. Dostupné z: https://cs.wikipedia.org/wiki/LoRa

[24] LORA. *Elkoep.cz* [online]. [cit. 2019-04-20]. Dostupné z: https://www.elkoep.cz/lora

[25] *Micro Solutions* [online]. 2015 [cit. 2019-04-15]. Dostupné z: http://ww1.microchip.com/downloads/en/Market_Communication/Jan_Feb_2015_MicroSolutions.pdf

[26] Není WiMax jako Wi-Fi. *Earchiv.cz* [online]. [cit. 2019-03-22]. Dostupné z: http://www.earchiv.cz/b07/b1100001.php3

[27] OWASP Internet of Things Project. *Owasp.org* [online]. [cit. 2019-03-31]. Dostupné z: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[28] Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. *Spectrum.ieee.org* [online]. [cit. 2019-03-08]. Dostupné z: https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

[29] Principles of IoT Security. *Owasp.org* [online]. [cit. 2019-03-31]. Dostupné z: https://www.owasp.org/index.php/Principles_of_IoT_Security

[30] Průmysl 4.0. *Siemens.cz* [online]. [cit. 2019-04-28]. Dostupné z: https://www.siemens.cz/prumysl40/

[31] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace: jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G.* Brno: CP Books, 2005. ISBN 80-251-0791-4.

[32] Reálné kroky směrem k WiMAX. *Dsl.cz* [online]. [cit. 2019-04-28]. Dostupné z: http://www.dsl.cz/clanky/46-realne-kroky-smerem-k-wimax

[33] Secure Sockets Layer. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-04-15]. Dostupné z: https://cs.wikipedia.org/wiki/Secure_Sockets_Layer

[34] Síťové prvky. *Alza.cz* [online]. [cit. 2019-04-28]. Dostupné z: https://www.alza.cz/sitove-prvky/18842916.htm#f&cst=0&cud=1&pg=1&prod=&sc=191

[35] Slovník pojmů. *Vodafone.cz* [online]. [cit. 2019-04-28]. Dostupné z: https://www.vodafone.cz/uzitecne-odkazy/slovnik-pojmu/5g-sit/

[36] Sousedská výpomoc: přístup k Internetu? *Lupa.cz* [online]. [cit. 2019-03-22]. Dostupné z: https://www.lupa.cz/clanky/sousedska-vypomoc-pristup-k-internetu/

[37] Stručný průvodce technologií 4G LTE. *Hyt.cz* [online]. [cit. 2019-03-25]. Dostupné z: https://www.hyt.cz/strucny-pruvodce-technologii-4g-lte/

[38] Techbox: Bluetooth sjednotilo bezdrátovou komunikaci. *Mobilenet.cz* [online]. [cit. 2019-03-21]. Dostupné z: https://mobilenet.cz/clanky/techbox-bluetooth-sjednotilo-bezdratovou-komunikaci-12085

[39] The 10 Challenges of Securing IoT Communications. *Pubnub.com* [online]. [cit. 2019-03-31]. Dostupné z: https://www.pubnub.com/blog/10-challenges-securing-iot-communications-iot-security/

[40] Transport Layer Security. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-04-15]. Dostupné z: https://cs.wikipedia.org/wiki/Transport_Layer_Security

[41] WAN – Wide Area Network. *Sjz.cz* [online]. [cit. 2019-03-25]. Dostupné z: http://szj.cz/wan-wide-area-network/

[42] WATTS, Silvia, ed. *The Internet of things (IoT): applications, technology, and privacy issues.* New York,: Nova Publisher's, 2016. ISBN 978-163-4846-264.

[43] Wi-Fi. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2019-03-22]. Dostupné z: https://cs.wikipedia.org/wiki/Wi-Fi

[44] Základní úvod do oblasti internetu věcí (IoT). *Automatizace.hw.cz* [online]. [cit. 2019-03-07]. Dostupné z: https://automatizace.hw.cz/zakladni-uvod-do-oblasti-internetu-veci-iot.html