ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta stavební
Thákurova 7, 166 29 Praha 6

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: STANČEKOVÁ Jméno: SIMONA Osobní číslo: 396306

Zadávající katedra: K 125

Studijní program: INTELIGENTNÍ BUDOVY

Studijní obor: INTELIGENTNÍ BUDOVY

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce: BEZPEČNOSŤ SYSTÉMOV V INTELIGENTNÝCH INŠTALÁCIÁCH

Název diplomové práce anglicky: SECURITY OF INTELLIGENT SYSTEMS

Pokyny pro vypracování:

- POPIS PRINCÍPOV INTELIGENTNÝCH SYSTÉMOV, ICH VZÁJOMNÉ POROVNANIE A UVEDENIE VÝHOD A NEVÝHOD
- POPIS RIZÍK A MOŽNÝCH NÁSLEDKOV
- ODPORÚČANIA A KONCEPTY RIEŠENÍ VHODNÉ PRE „SMART HOMES" A „SMART CITIES"
- EXPERIMENT NA DOKÁZANIE BEZPEČNOSTNÝCH RIZÍK V INTELIGENTNÝCH INŠTALÁCIÁCH A PRÍKLAD (INŠTA)APLIKÁCIE SPRÁVNEHO RIEŠENIA

Seznam doporučené literatury:

Jméno vedoucího diplomové práce: doc. Ing. Bohumír Garlík CSc.

Datum zadání diplomové práce: 1. 3. 2018 Termín odevzdání diplomové práce: 21. 5. 2018

Údaj uveďte v souladu s datem v časovém plánu příslušného ak. roku

Podpis vedoucího práce Podpis vedoucího katedry

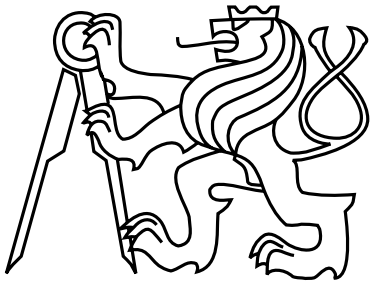
III. PŘEVZETÍ ZADÁNÍ

Beru na vědomí, že jsem povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je nutné uvést v diplomové práci a při citování postupovat v souladu s metodickou příručkou ČVUT „Jak psát vysokoškolské závěrečné práce" a metodickým pokynem ČVUT „O dodržování etických principů při přípravě vysokoškolských závěrečných prací".

1. 3. 2018

Datum převzetí zadání Podpis studenta(ky)

České vysoké učení technické v Praze
Fakulta stavební
Katedra technických zařízení budov



Diplomová práca

Bezpečnosť systémov v inteligentných inštaláciách

Bc. Simona Stančeková

Vedúci práce: doc. Ing. Bohumír Garlík, Csc.

Študijný program: Inteligentné budovy

2017/2018

Prehlásenie

Prehlasujem, že som predloženú prácu vypracovala samostatne a že som uviedla všetky použité informačné zdroje v súlade s metodickým pokynom o dodržiavaní etických princípov pri príprave vysokoškolských záverečných prác.

V Prahe dňa 28. 05. 2018 .....

Poďakovanie

Rada by som poďakovala vedúcemu mojej práce pánu doc. Ing. Bohumírovi Garlíkovi, Csc. za zaujímavé zadanie diplomovej práce a za jeho nadšenie technológiami inteligentných budov. Ďalšie poďakovanie patrí pánovi Vladimírovi Koreckému za hodiny konzultácií a prínosných diskusií na téma bezpečnosti systémov a za zapožičanie hardvérového vybavenia a tiež pánu Ing. Petrovi Bubákovi za vhľad do inštalácie systému z praxe. Na záver by som chcela poďakovať pánovi Simonovi Helbergovi za inšpiráciu a motiváciu k dokončeniu tejto práce.

Abstract

This thesis focuses on broad research of intelligent systems used in smart houses or smart cities, and describes their principles. Its goal is to provide general information about possible vulnerabilites of systems, to point out a topic which is not well-known in public and give recommendations how to improve security of such systems.

Abstrakt

Diplomová práca sa venuje širšej rešerši oblasti inteligentných systémov používaných v domácnostiach alebo v mestách a popisuje princípy fungovania týchto systémov. Jej cieľom je podať všeobecné informácie o možných spôsoboch zraniteľnosti, upriamiť pozornosť na problematiku, ktorá zatiaľ nie je širokej verejnosti známa a uviesť doporučené postupy pre zvýšenie bezpečnosti systémov.

Obsah

Zoznam obrázkov

Kapitola 1

Úvod

Inteligentné budovy vznikajú ako ďalší logický krok vďaka vývoju elektrotechnických a informačných technológií, ktoré sa do bežného života ľudí implementujú stále viac a poskytujú nám čoraz väčšie pohodlie a možnosti vylepšení v našich životoch.

Využitie týchto nových technológií je rôznorodé a nachádza uplatnenie v mestách, budovách, aj domácnostiach. Jedným z hlavných dôvodov vývoja inteligentných systémov je permanentné zvyšovanie spotreby energií. To sa stáva náročné ako z ekonomického hľadiska, tak aj z hľadiska ekologického. Inteligentné systémy, ktoré vedia sledovať spotrebu energií v aktuálnom čase, zbierať o tom dáta, analyzovať ich a automaticky podľa dát upraviť nastavenia zariadení pre ďalšie použitie, sa tak pomaly stávajú dôležitou súčasťou nie len priemyselných prevádzok, ale aj všetkých druhov budov a miest.

Pojmy Smart Home a Smart City (inteligentný dom a inteligentné mesto) sa skloňujú stále častejšie, a to nie len v akademickom výskume alebo médiách, ale prenikajú aj do každodenného života ľudí. Rozvoj technológií a hlavne ich dostupnosti v posledných rokoch má za následok aj masívny rozmach systémov, ktoré majú ľuďom uľahčovať život. Táto komplexná a ťažko definovateľná oblasť výrobkov, systémov a technológií tak dostala všeobecný prívlastok „Smart“ a stáva sa súčasťou každodenného života ľudí, ktorí si tento vplyv ani nemusia uvedomovať a tak si neuvedomia ani nebezpečenstvá, ktoré pri narušení týchto systémov hrozia.

Kapitola 2

Inteligentné systémy

Aby sme mohli vôbec začať rozoberať tému bezpečnosti systémov v inteligentnej budove, poťažmo v inteligentnom meste, musíme vedieť viac o inteligentných budovách všeobecne, pochopiť, o ako komplexnú tému sa jedná a definovať základné pojmy.

Prevádzka modernej budovy je ekonomicky a často aj ekologicky náročná a plne závislá od dodávky elektrickej energie (či už z verejnej elektrickej siete alebo z vlastných alternatívnych zdrojov). Použitím inteligentného riadiaceho systému je možné zautomatizovať, ovládať a kontrolovať prevádzku akéhokoľvek elektrotechnického prvku v budove (resp. len elektrotechnického prvku, ktorý je na to uspôsobený), čo má prispieť nielen k zvýšeniu pohodlia obyvateľov, ale aj k zníženiu prevádzkových nákladov, k optimalizovaniu využívania tepelnej a elektrickej energie a tiež k zvýšeniu bezpečnosti prevádzky.

V oboch prípadoch - budova či mesto - sa na inteligentné budovy dá pozerať z viacerých hľadísk a záleží na druhu a požadovaných funkciách. Moderné systémy sa využívajú ako v priemyselných a výrobných objektoch, tak aj v poľnohospodárstve, skladových objektoch, administratívnych, občianskych i obytných budovách.

Prvé hľadisko, na ktoré sa môžeme zamerať, je ekonomické. Je to optimalizovanie využívania energií a zníženie nákladov na prevádzku budov. Zahŕňa to napríklad vylepšenie ako sú systémy pre vykurovanie, vzduchotechnika, dodávka elektrickej energie, spotreba vody a podobne. Zdrojom energie nie je už len jej čerpanie priamo z verejnej siete, ale v mnohých prípadoch ide aj o využívanie už raz použitej energie, tzv. rekuperácia, využívanie alternatívnych zdrojov energie, prípadne využívanie energie z batérií. Zníženie nákladov na prevádzku je výhodné nielen z dlhodobého ekonomického hľadiska (je nutné vždy brať do úvahy dlhodobé hľadisko, pretože prvotná inštalácia inteligentných zariadení a systémov nie je lacnou záležitosťou), ale je aj šetrné k životnému prostrediu.

Druhým hľadiskom je, jednoducho povedané, pohodlie. Ovládanie a správa systémov a prípadné riešenie problémov systému v budove musí byť čo najjednoduchšie. Používanie moderných systémov a zariadení v domovoch západného sveta sa dnes už stalo štandardom. „Inteligentným“ alebo „Smart“ sa na trhu označuje nespočetné množstvo výrobkov, od Smartphonu až po, napríklad, inteligentnú chladničku[1]. Vďaka integrácií týchto inteligentných prvkov a systémov do obytných, administratívnych aj verejných budov sa trh a technológie rýchlo rozširujú, konkurenčné súťaže nútia výrobcov vylepšovať svoje výrobky a

[1] https://techbox.dennikn.sk/lg-smart-instaview-inteligentna-chladnicka-obrovskym-29-displejom/

tak sa s inteligentným domom stretneme čoraz častejšie. Toto sú však, zľahčene povedané, široko známe prvky, ktoré slúžia hlavne pre zábavu ľudí a nie sú kľúčové pre náš život. Ich poruchy a nefunkčnosť by nám ale mohli život rozhodne znepríjemniť.

Tretie hľadisko, na ktoré sa môžeme zamerať, je bezpečnosť budov a ľudí. Automatické bezpečnostné systémy, kamerové systémy a alarmy, ktoré chránia obyvateľov, nie sú ničím novým, ale aj v tejto oblasti sa systémy a prvky bezpečnosti vylepšujú. Vďaka tomu sú schopné pomáhať nie len priamo pri nebezpečenstve, ako napríklad požiari, vykradnutí a pod., ale týmto situáciám aj aktívne predchádzať[2].

2.1 Definície pojmov

2.1.1 Inteligentná budova

Napriek tomu, že je spojenie „inteligentná budova“ už zaužívané, nemá stanovenú presnú definíciu. Ako častá definícia sa uvádza, že: „inteligentná budova je budova, ktorá zaisťuje pre svojho obyvateľa pohodlné a optimálne prostredie pomocou viacerých prostriedkov: stavebnej konštrukcie, technologických zariadení, riadiacich systémov, služieb a manažmentu týchto služieb.“[1][3] V každej modernej ale aj staršej budove sa nachádzajú jednotlivé elektrotechnické zariadenia pre správu, automatizáciu alebo ovládanie iných prvkov. Prepojenie týchto systémov a naučenie ich reagovať na aktuálne zbierané dáta sa dá nazvať inteligenciou. Takýto systém potom reaguje rýchlo, presne, znižuje faktor ľudských chýb a vďaka svojej výpočtovej sile optimalizuje prevádzku budovy účinnejšie ako človek. Zároveň môže poskytnúť nepretržité sledovanie systémov a archiváciu údajov, čím je spätné vyhľadávanie a odhaľovanie chýb oveľa jednoduchšie. Skutočne inteligentné systémy cielia na to, aby ľudský zásah do prevádzky budovy nebol vôbec potrebný.

2.1.1.1 Čo môže znamenať inteligentná budova pre domácnosť

Aby sme si ďalej mohli predstaviť riziká spojené s bezpečnosťou takéhoto systému, predstavme si konkrétnejšie, ako môže inteligentná budova vyzerať v praxi. Predstavme si, čo všetko by sme mohli v našej domácnosti zautomatizovať. Ovládať na diaľkové ovládanie. Monitorovať. Optimalizovať. Prepojiť.

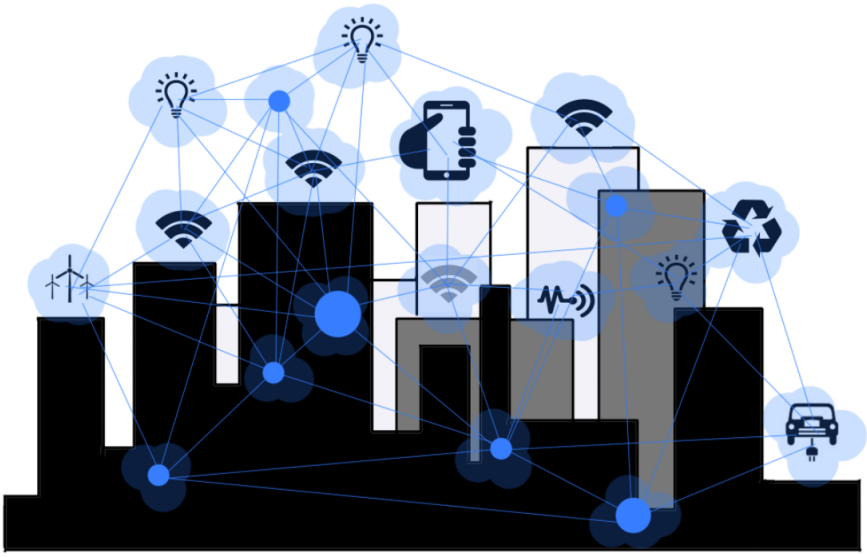
Na strechu si namontujeme fotovoltaický systém - solárne panely. Energiu z nich budeme ukladať do batérií. Spotrebu energie budeme podrobne monitorovať. Účinnosť solárnych panelov závisí od uhla dopadu slnečných lúčov, preto budeme môcť pomocou inteligentného systému natáčať solárne panely smerom k slnku, ako to robia kvety slnečnice.

V záhrade namontujeme zariadenie na automatické zavlažovanie, ktoré bude polievať záhradu len vtedy, keď je to podľa závlahových senzorov potrebné a vždy bude prietok vody plne kontrolovať. Využívať k tomu môže napr. zachytenú dažďovú vodu.

Namontujeme do domu bezpečnostný systém. Tých už dnes existujú stovky. Dajme tomu, že systém vie uzamknúť celý dom v prípade potreby, a obsahuje v sebe aj kamerový systém s dátovým úložiskom. Pri narušení bezpečnosti systém sám privolá pomoc.

[2]Možná ochrana proti vykradnutí domu pomocou inteligentného systému: inteligentný systém bude sám simulovať občasné zapínanie a vypínaine spotrebičov, aby to vyzeralo, že dom nie je prázdny

[3]Garlík, B.: Elektrotechnika a Inteligentní budovy, ČVUT Praha, 2010



Obr. 2.1: Inteligentné mesto

Vybavíme domácnosť inteligentnými doplnkami. Chladnička, ktorá sama vie, čo treba nakúpiť, a sama to cez intenrnet objedná. Chytré žiarovky a osvetlenie, chytrá televízia, automatická regulácia teploty, automaticky ovládané žalúzie v závislosti na poveternostných podmienkach, termostaty, práčka, chladnička, rýchlovarná kanvica, elektrické zásuvky, multimediálne zariadenia. To všetko môžeme napojiť do inteligentného systému a ovládať potom aj vzdialene, napríklad cez centrálny riadiaci systém. Môžeme na diaľku vypnúť a zapnúť elektrické zásuvky, spotrebiče, dopredu zapnúť kúrenie predtým, než prídeme z práce domov, a mnoho iného.

Dôležité ale je, aby toto všetko fungovalo automaticky, bez nášho zásahu, na základe naprogramovaných prvkov a dát zo senzorov. Systémy by mali komunikovať medzi sebou, zaťažovať človeka čo najmenej a vytvárať pre neho čo najpríjemnejšie prostredie. Tento ideálny stav je zatiaľ ešte stále budúcnosť.

Pri inštalácií inteligentného systému v domácnosti tak ide z veľkej časti o pohodlie a až v druhom rade o investíciu alebo šetrnosť k životnému prostrediu, pretože počiatočné náklady sú vysoké a návratnosť investície je dlhodobá.

2.1.1.2 Čo môže znamenať inteligentná budova vo verejnej stavbe

Ako druhý príklad si môžeme predstavovať administratívnu budovu, alebo napríklad hotel s vysokou kapacitou, ktorý bude používať inteligentný systém. To už dnes vo vyspelých mestách nie je nič výnimočné. Ale narozdiel od domácností, v budove s tak veľkou spotrebou energie ako je administratívna prevádzka pre tisíc ľudí bude najdôležitejším faktorom práve optimalizácia spotreby energií a prostredia v budove. Automatické ovládanie kúrenia a klimatizácie, čidlá, ktoré vypnú klimatizáciu, ak sa otvorí okno v danej miestnosti, monitorovanie spotreby vody a tepla a presné riadenie rozdelenia energie. Senzory monitorujúce stav

prostredia. Monitorovanie priestorov kamerami, kontrola prístupu do budovy a pohybu osôb po budove pomocou zamestnaneckých kariet, RFID[4] čipov či iných technológií. Ovládanie žalúzií, multimédií, osvetlenia.

Pri veľkých prevádzkach je optimalizácia a riadenie systémov dôležitejšie alebo rovnako dôležité ako pohodlie pre návštevníkov a obyvateľov budovy.

2.1.2 Inteligentné mesto

Definícia pojmu „inteligentné mesto“ taktiež nemá presný tvar. Zjednodušene by sa dalo povedať, že to je mesto, ktoré používa technológie na automatizáciu a zlepšenie služieb poskytovaných mestom, a ktoré zlepšuje a uľahčuje život svojim obyvateľom.

V mestách hrá obrovskú rolu práve zmenšenie spotreby energií a skvalitnenie životného prostredia. Rolu v inteligencii mesta nehrá len elektronika a informačné systémy, ale aj kvalitná a premyslená architektúra a plánovanie. Moderné mestá sa potýkajú s veľkou mierou znečistenia vzduchu, preľudnenia, a malou mierou flexibility. Systémy, ktoré už dnes v mestách fungujú, napr. riadenie dopravy a parkovania, zatiaľ nie sú schopné komunikovať medzi sebou a vymieňať si informácie. Inštalujú sa systémy, ktoré zbierajú obrovské množstvá dát, ale zatiaľ nie je úplne jasné, ako z týchto dát vyťažiť čo najviac. Budovy, aj keď samostatne môžu byť inteligentné, nekomunikujú medzi sebou, ani so svojím okolím. Inteligentné mestá sú ešte v zárodku, no o to dôležitejšie je zameriavať sa pri vývoji na ich bezpečnosť. Mestá budú disponovať obrovským množstvom dát a budú kontrolovať citlivé informačné systémy. Narušenie bezpečnosti vo veľkomeste môže narušiť alebo ohroziť život tisícom ľudí.

Spraviť z každej budovy v meste samostatnú inteligentnú budovu by nám nepomohlo k tomu, aby bolo mesto inteligentné ako celok. Čím sa mesto stane inteligentným?

- Inteligentné ovládanie dopravy - dopravná signalizácia je schopná prispôsobiť sa aktuálnemu stavu dopravy, predĺžiť alebo skrátiť intervaly na križovatkách, presmerovať dopravný tok áut v prípade nehody atď.
- Inteligentné parkovanie - obyvatelia dokážu nájsť aktuálne voľné parkovacie miesta v aplikácii a zaplatiť parkovné pomocou mobilného telefónu.
- Inteligentné pouličné osvetlenie - centrálne ovádané osvetlenie svetiel, ktoré sa dokáže adaptovať na aktuálne počasie, napríklad dokáže v sychravých dňoch zapnúť svetlá aj cez deň, alebo dokáže reagovať na pobyt a pohyb osôb a áut.
- Inteligentná hromadná doprava - obyvatelia by boli schopní nájsť aktuálne informácie o doprave v aplikácii na telefóne a súčasne aj na všetkých zastávkach a podľa toho prispôsobiť svoju plánovanú cestu alebo zvoliť spôsob dopravy.
- Inteligentný management elektrickej energie - smart grid - elektrická sieť, ktorá dopravuje energiu na základe aktuálnej potreby. Inteligentné merače spotreby dokážu naplánovať odber potrebnej elektriny zo siete smart grid a využívať tak napríklad lacnejší tarif. Inteligentné budovy zároveň majú schopnosť ukladať prebytočnú energiu a tú potom využiť neskôr alebo ju odovzdať naspäť do smart grid siete.

[4] bezkontaktná identifikácia čipov založená na rádio frekvencií, funguje na krátke vzdialenosti, https://cs.wikipedia.org/wiki/RFID

- Inteligentný management vody - senzory zmerajú aktuálnu kvalitu vody a jej množstvo. Je to užitočné hlavne v oblastiach, kde je vody nedostatok, a podľa najnovšícj údajov sa problém dostupnosti vody začína týkať aj Českej republiky. Obyvatelia sa potom môžu pomocou aplikácie dozvedieť o najbližších prístupných vodných zdrojoch a ich kvalite. Obdobne je možné využívať aj senzory pre plynové rozvody.
- Inteligentný zber odpadu - senzory upozornia technické služby na preplnené kontajnery, prípadne na zápach. Optimalizujú sa trasy pri zbere odpadu a znížia sa výdaje za zvoz.
- Bezpečnosť - dopravné a bezpečnostné kamery, detektory streľby a iné real-time ochranné prvky, ktoré pomáhajú s lokáciou ľudí a udalostí. Užitočné sú aj technológie počítajúce počet ľudí prítomných v daných oblastiach, ulici, parku alebo budove, a v prípade potreby schopné presmerovať veľký dav ľudí na inú ulicu a pod.

2.1.2.1 Technológie, ktoré toto všetko môžu umožniť

- City Management Systems (CMS) - technológie určené pre správu systémov v mestách
- Machine to machine (M2M) - ak chceme urobiť mesto naozaj inteligentným, musíme naučiť zariadenia (machine) rozprávať sa medzi sebou. Týmto spôsobom budú môcť aj zariadenia z rôznych oblastí reagovať a rozhodovať sa automaticky, podľa daných pravidiel, bez zásahu človeka.
- Senzory - primárne zdroje všetkých dát. Využívajú sa na všetko a bez prestávky plnia mestské systémy dátami. Často bývajú bezdrôtové a sú hlavným prvkom inteligentných inštalácií. Napríklad: senzory teploty, vlhkosti vzduchu, znečistenia vzduchu, senzory obsahu CO_2, zápachu, záplav, hlasitosť zvuku, prítomnosť dymu...
- Otvorené dáta - (angl. Open Data) dáta sú zdieľané s verejnosťou, takže vývojári môžu vytvárať vlastné prospešné aplikácie. Môže sa jednať o dáta dlhodobo zbierané, o rôzne databázy, napr. cestovné poriadky, alebo o ral-time dáta, napríkald o aktuálnom stave dopravy, teplôt, ovdzušia a i.
- Mobilné alebo počítačové aplikácie - slúžia ako interakcia medzi obyvateľmi a inteligentnými systémami mesta.

2.1.3 Ostatné pojmy

Už sme si definovali inteligentnú budovu a mesto, ale musíme vymedziť ešte niekoľko s tým súvisiacich pojmov. Trh je dnes presýtený výrobkami, ktoré sa za inteligentné vydávajú, ale v chápaní skutočne inteligentného systému do tejto skupiny nepatria.

Inteligentné zariadenie - smart zariadenie

Takto sa označuje samostatné zariadenie, ktoré je možné naprogramovať na určité automaticky vykonávané činnosti (napríklad kávovar, ktorý obsahuje budík, a pri nastavení času budenia pripraví čerstvú kávu). Ľudský zásah pri nastavovaní je nutný a zariadenie primárne nezbiera ani neanalyzuje dáta. Zariadenia môžu fungovať samostatne alebo môžu fungovať cez pripojenie na gateway[5], ako napr. inteligentné osvetlenie, kde je viac žiaroviek napojených na jednu kontrolnú gateway. Domácnosť, v ktorej sa nachádza aj niekoľko takýchto prvkov sa ale nedá považovať za inteligentnú v pravom slova zmysle.[13]

Pripojené zariadenie - connected device

Zariadenie ovládané na diaľku, väčšinou pomocou aplikácie v mobilnom telefóne. Napríklad kávovar, ktorému vzdialene z mobilu prikážete, aby uvaril kávu a nastavíte mu teplotu, ktorú má udržiavať, alebo sauna, ktorú si užívateľ rozohreje už po ceste z práce skrz mobilný telefón. Pripojené je väčšinou cez Wi-Fi, ale aj Bluetooth, LTE[6], alebo drôtovo. Tieto zariadenia sa sami o sebe tiež nepovažujú za inteligentné a netvoria inteligentnú domácnosť, ale môžu jej napomáhať.[13]

Internet vecí - Internet of Things (IoT)

IoT je termín používaný v posledných rokoch hlavne médiami a výrobcami zariadení a definovať ho nie je tak jednoduché. Je to termín pre sieť zariadení, ktoré si vedia vzájomne vymieňať dáta. Nemusí sa nutne jednať o sieť Internet, napriek tomu, že toto slovo obsahuje priamo názov technológie. Prvky sú vybavené dostatočnou elektronikou, senzormi, uspôsobeným softvérom, často aj pohyblivým časťami a hlavne schopnosťou sieťovej konektivity, vďaka ktorej sa môžu zariadenia prepojiť vzájomne a vymieňať si dáta. Nepotrebujú veľký výpočtový výkon a spravidla majú aspoň nejakú základnú pamäť. Každé zariadenie je jasne identifikovateľné aj v lokálnej sieti, aj po pripojení do celosvetového Internetu. Vďaka schopnosti čiastočne spracovávať dáta, prijímať dáta zo senzorov a schopnosti naprogramovať softvér tak, aby na základe analyzovaných dát reagoval aktualizovaním nastavení systému, IoT zariadenia sa dajú považovať za prvky tvoriace inteligentné budovy. Pod IoT môžu spadať samostatné inteligentné zariadenia, a aj pripojené zariadenia. IoT systémy sú využiteľné v domácnostiach, v občianskych budovách, administratíve, poľnohospodárstve, energetike, v mestách. Ich potenciál je obrovský. Vo väčšine prípadov sa jedná o bezdrôtové zariadenia, čo umožňuje jednoduché inštalácie. Slabina IoT zariadení ale spočíva v ich bezpečnosti, ktorej sa budeme venovať v ďalších kapitolách.[13]

[5] brána, zariadenie, ktoré prepája dve rôzne siete, https://cs.wikipedia.org/wiki/Gateway

[6] Long Term Evolution, technológia poskytujúca vysokorýchlostný internet, nástupca technológie GSM, https://cs.wikipedia.org/wiki/Long_Term_Evolution

If This Then That (IFTTT)

IFTTT je nástroj fungujúci ako webová služba alebo mobilná aplikácia, ktorý umožňuje zautomatizovať fungovanie iných služieb dostupných cez web. Funguje na princípe nastavenia reťazca jednoduchých podmienok, ktorý sa nazýva applet[7]. Bežne sa využíva na automatizovanie používania sociálnych sietí, ale v súčasnosti existujú aj zariadenia, vďaka ktorým je pomocou IFTTT možné ovládať inteligentné žiarovky alebo zásuvky.[14]

Z vyššie vymenovaných možností a definícií sme už určite získali predstavu toho, čo nám inteligentné mesto alebo budova môže ponúknuť. Rozšírenie implementácie jednotlivých smart súčastí je na svete veľmi rôzne, ale už aj malé mestá využívajú aspoň kamerové systémy. Systémy, ktoré sa využívajú v inteligentných budovách, sú dosť často rôzne, a sami o sebe nevytvoria inteligentné mesto. Až keď sa tieto systémy spoja dohromady a naučia sa reagovať sami na seba, hovoríme o skutočne inteligentných systémoch.

2.1.4 Delenie systémov pre zber a prenos dát v inteligentných budovách

Druhy jednotlivých systémov podľa aplikačnej oblasti:

1. **Systémy pre optimalizáciu spotreby energií** - Jednotným názvom sa tieto systémy môžu nazývať Building Automation Systems (BAS), ale používajú sa aj názvy Emergency Management System (EMS), Emergency Management and Control Systems (EMCS), Facility Management Systems (FMS) a iné. Slúžia k meraniu a zbieraniu dát spotreby energií, automatizovanému rozhodovaniu a optimalizovaniu vnútorného prostredia budov.

2. **Systémy riadiace prístup** - napríklad kartové systémy, systémy založené na rozpoznávani tváre, biometrické autentifikačné systémy, elektronické zabezpečovacie systémy alebo signalizácie (EZS)

3. **Systémy poskytujúce služby**

   Sledovacie a kamerové systémy - uzavreté kamerové systémy/televízia (CCTV)

   Bezpečnostné ohlasovacie systémy - protipožiarne systémy (EPS), detekčné systémy, hasiace systémy

   Pohotovostné systémy - riadenie a monitorovanie dopravných systémov, napr. výťahy a eskalátory, systémy detekujúce poruchy, záložné zdroje energie a iné

4. **Telekomunikačné systémy, IT** - systémy zabezpečujúce telefónne a počítačové spojenie

5. **Systémy správy a automatizácie** - napríklad systémy riadenia budovy integrujúce všetky rôznorodé subsystémy do jedného, umožňujúceho centrálny dohľad. Nazývajú sa Building Management Systems (BMS) alebo Intelligent Building Management Systems (iBMS).

[7] https://en.wikipedia.org/wiki/IFTTT

Druhy systémov podľa geografickej rozľahlosti:

1. Lokálne (miesnosť, budova) - napríklad riadenie osvetlenia, HVAC[8]
2. Rozľahlé (firma, mesto) - napríklad prístupové a kamerové systémy
3. Globálne (štát) - hromadné zbieranie dát

Druhy systémov podľa technológie prenosovej cesty

1. Metalické (drôtové)
2. Optické
3. Bezdrôtové

Podľa spôsobu prepojenia a spolupráce prvkov:

1. **Centralizované** - systém riadený z jedného centrálneho bodu, ktorý prijíma všetky riadiace signály, vyhodnocuje ich a komunikuje s každým koncovým zariadením. Koncové prvky nemusia o sebe navzájom vedieť a riadenie je plne zverené centrálnej stanici. Táto stanica môže byť kvôli vzdialenej správe pripojená k Internetu.
2. **Decentralizované, distribuované** - systém, v ktorom sú jednotlivé komponenty prepojené a komunikujú aj sami medzi sebou. Výhodou je, že pri poruche nebude vyradený celý systém, súčasne je ale náročnejšia diagnostika porúch a nastavovanie hierarchie systému a zabezpečenia.
3. **Zmiešané** - používajú prvky z oboch systémov

Podľa stupňa podpory práce v reálnom čase:

1. Real-time systémy - spracúvajú dáta a na základe analýz vykonávajú akcie okamžite, v reálnom čase
2. Non real-time systémy - zhromažďujú dáta do databáz, ktoré sa spracujú neskôr

Ďalej sa systémy dajú rozdeliť na budovy, kde sa s inteligentným systémom počíta už od začiatku, a na rekonštrukcie a systémy realizované až po dokončení stavby budovy. Tieto vylepšenia sa často nazývajú retrofit. Prvá skupina má už v projekte vypracovanú potrebnú kabeláž a infraštruktúru, pri zariaďovaní sa priamo počíta s inteligentnými zariadeniami. Druhá skupina sú budovy staršieho dáta alebo budovy, kde sa inteligentný systém dodáva dodatočne, a väčšinou je nepraktické a najmä príliš nákladné dodať celkovú novú kabeláž a všetky potrebné úpravy. V takýchto prípadoch sa hľadá alternatíva ku káblovým montážiam a na trhu už existuje dostatok bezdrôtových technológií, ktoré tento dopyt pokrývajú.

[8] heating, ventilation and air conditioning, v preklade vykurovanie, vetranie a klimatizácia, https://en.wikipedia.org/wiki/HVAC

Kapitola 3

Informačné a počítačové siete

Najdôležitejšou súčasťou inteligentných systémov je komunikácia prvkov, ktorá je možná vďaka rozvoju informačných a počítačových sietí.

3.1 História sietí

Počítačové siete sa začali rozširovať v 50. rokoch 20. storočia, keď postupne dochádzalo k rozvoju počítačovej techniky a bolo nutné, aby jednotlivé prístroje začali medzi sebou komunikovať. Dôležitým míľnikom bolo vytvorenie univerzitnej siete pod názvom ARPANET v roku 1969, vďaka grantovej agentúre ministerstva obrany USA. Sieť obsahovala 4 uzly umiestnené na amerických univerzitách a mala decentralizovaný charakter, teda bola relatívne odolná. Ak by bol vyradený niektorý z uzlov, sieť fungovala naďalej. ARPANET sa rozširoval na svoju dobu relatívne rýchlo. V roku 1971 mal už 15 pripojených uzlov (počítačov) a v roku 1972 dokonca až 37. V roku 1973 sa k tejto sieti pripojili zahraničné uzly vo Veľkej Británií a v Nórsku a počiatky celosvetovej siete boli na svete.[12] Dnes je celý svet pripojený hlavne k medzinárodnej sieti Internet. Všeobecným účelom sietí je komunikácia a výmena dát, zdieľanie prostriedkov a zvýšenie spoľahlivosti systémov.

3.2 Delenie sietí

Na informačné siete sa dá nazerať z niekoľkých hľadísk a od toho závisí aj ich rozdelenie. Pre ľahšiu orientáciu v problematike uvediem niektoré delenia sietí:

Z hľadiska vzájomného postavenia uzlov v sieti ich môžeme deliť na siete:

- **peer-to-peer (P2P)** - v preklade „rovný s rovným“ znamená, že všetky počítače v sieti (všetky uzly) sú si rovné, a všetky uzly komunikujú navzájom spolu. Na rovnakom princípe fungujú siete Machine to Machine (M2M), kde explicitne komunikuje stroj so strojom. Tento princíp je základ decentralizovaných systémov.
- **client-server** - v preklade „klient - server“ je architektúra, kde jeden alebo viac počítačov hrajú hlavnú úlohu a sú nadradené ostatným uzlom v sieti. Tento hlavný uzol

sa nazýva server a nemusí to byť vždy len jeden fyzický počítač. Niekedy môže jeden fyzický stroj obsahovať niekoľko virtuálnych serverov, a niekedy môže byť jeden stroj len jednoúčelový, napr. tlačový server. Záleží to od veľkosti a návrhu siete.

Podľa rozhľahlosti siete používame označenia:

- **Personal Area Network (PAN)** - prekladané ako osobná sieť, je sieť malého rozsahu používaná na prepojenie rôznych elektronických zariadení ako napr. mobilný telefón, notebook, tablet, a rôzne chytré výdobytky domácností. Pokrýva teda jednu domácnosť, dom, byt, alebo izbu. Zväčša sa týka bezdrôtových technológií ako je Bluetooth, ZigBee alebo IrDA[9].
- **Local Area Network (LAN)** - je termín pre lokálnu počítačovú sieť, takže sieť malého rozsahu. Spojuje uzly (počítače a iný hardvér schopný pripojenia) v rámci miestnosti, budovy, niekoľkých blízkych budov, alebo časti budov. Pokrýva teda desiatky a stovky metrov. Najpoužívanejším typom je Ethernet alebo Wi-Fi. LAN býva spravidla súkromne spravovaná sieť.
- **Metropolitan Area Network (MAN)** - označuje metropolitnú sieť. Je to sieť väčšieho rozsahu než LAN. Táto sieť spája lokálne siete, napr. v rámci mesta, a pokrýva jednotky až stovky kilometrov. Býva privátna, ale aj verejná.
- **Wide Area Network (WAN)** - označuje rozľahlú sieť. Tento druh siete prepojuje menšie LAN a MAN siete a má najväčšie pokrytie (napr. celoštátne siete). Najznámejším príkladom siete WAN je Internet.
- **Low Powered Wide Area Network (LPWAN)** - je menej známym typom siete, ktorý sa ale v posledných rokoch rozvíja práve kvôli inteligentným technológiám. Je to sieť navrhnutá na komunikáciu vo veľkých vzdialenostiach, ktorá pre prevádzku nebude vyžadovať príliš veľa energie. Príkladom je napríklad LoRaWan alebo SigFox.

3.3 Topológia sietí

Topológia sietí určuje akýsi virtuálny tvar siete, určuje, akým spôsobom sú jednotlivé prvky usporiadané. Tvar topológie nemusí vôbec vystihovať fyzické rozmiestnenie strojov, ale určuje, ako spolu prvky komunikujú. Najznámejšími topológiami sú:

- **zbernicová topológia** - angl. *bus topology* - spojenie uzlov (prvkov) so sieťou zabezpečuje zbernica, ku ktorej sú pomocou kábla pripojené všetky uzly v sieti. Je to jedno z najpoužívanejších pripojení, vhodné hlavne pre menšie siete, výhodou je jednoduchosť realizácie a menej potrebnej kabeláže, než napr. pri topológií typu hviezdy. Nevýhodami je obmedzená najväčšia možná dĺžka kábla a obmedzenie počtu staníc, poruchovosť (pri poruche vodiča vedúceho do zbernice sa stane nefunkčná celá časť siete) a potreba implementácie protokolu pre vyhýbanie sa kolíziám, napr. CSMA/CA[10].

[9] bezdrôtová komunikácia skrz infraport, https://cs.wikipedia.org/wiki/IrDA

[10] Carrier sense Multiple Access/Collision Avoidance, protokol pre vyhýbanie sa kolíziám dát v sieti, https://cs.wikipedia.org/wiki/CSMA/CA

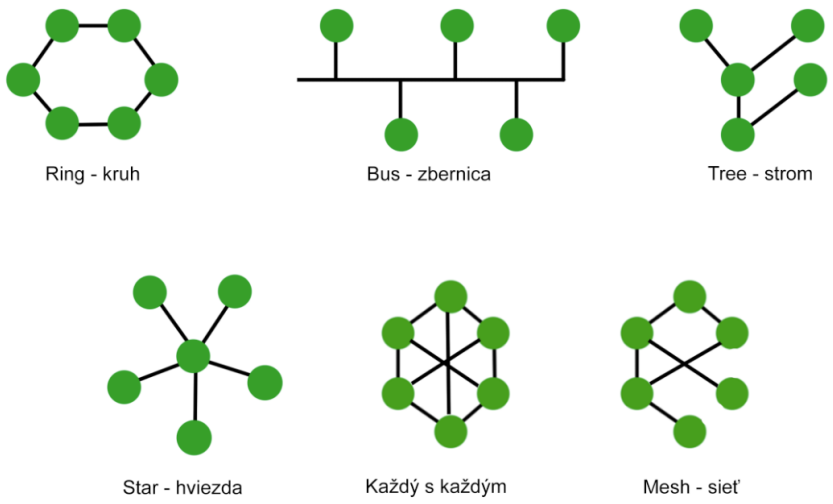
- **hviezdicová topológia** - angl. *star* - prepojuje uzly (počítače) k centrálnemu aktívnemu prvku, napr. k switchu (prepínači). Je to najpoužívanejší spôsob pripojenia. Výhodou je, že pri poruche jedného kábla nie je ovplyvnená funkčnosť ostatných uzlov a závady sú ľahko lokalizovateľné. Nevýhodou je nutnosť špeciálneho hardvéru (hub, switch), ktorého porucha môže vyradiť celú sieť, resp. zneprístupniť všetky prvky, ktoré sú priamo k nemu pripojené.

- **kruhová topológia** - angl. *ring* - uzly sú pripojené jeden k druhému tak, že spolu vytvárajú uzavretý okruh. Aby nedochádzalo ku kolíziám pri vysielaní uzlov, používa sa tzv. token, ktorý si stanice navzájom posúvajú a ktorý určuje, ktorý uzol môže vysielať. Prenos dát je rýchly a jednoduchý a pridanie ďalšieho uzlu nie je problém. Nevýhodou je, že prerušením kruhu poruchou jednej stanice prestane fungovať celá sieť, preto sa implementujú aj tzv. záložné kruhy (ring).

- **stromová topológia** - angl. *tree* - vzniká prepojením aktívnych prvkov, ktoré figurujú v hviezdicovej topológii. Používa sa predovšetkým v rozsiahlych sietiach.

- **zmiešaná topológia** - angl. *mesh* - niektoré uzly sú prepojené s viac než jedným ďalším uzlom v sieti a tým vzniká redundancia pripojenia. Preto sa táto topológia používa v sietiach, kde nie je možné realizovať pripojenie každý s každým, ale je nutné zabezpečiť, aby pri výpadku jedného uzlu nedošlo k výpadku siete. Kvôli pripojeniu uzlu k viacerím uzlom je potom nutné správne smerovať prenos dát a adresáciu. Hovorí sa jej aj „ibecn7 graf“ alebo „sieťová topológia“. Je to často využívaná topológia pri IoT sieťach a inteligentných distribuovaných systémoch.

- **topológia každý s každým** - platí v podstate to isté, čo pri mesh topológii



Obr. 3.1: Topológie sietí

3.4 Referenčný model ISO/OSI

Aby bolo možné rôzne systémy navzájom prepojovať a aby mohli spolu komunikovať, vytvoril sa v roku 1984 model ISO/OSI[11]. Nejaká modifikácia tohoto modelu funguje v každom modernom systéme alebo sieti.[15]

Používa sa ako názorný príklad vrstvového modelu riešenia komunikácie v telekomunikačných a počítačových sieťach. Bezpečná implementácia funkčnej siete je komplikovaná a navyše existuje príliš veľké množstvo zariadení a softvérov, ktoré nevedia komunikovať medzi sebou. Riešením tohoto problému sa stalo rozloženie celku na menšie časti, jednotlivé vrstvy modelu Open Systems Interconnection (OSI). Vrstvy v modeli sú vzájomne hierarchicky usporiadané, vrstva čislo N poskytuje služby vrstve čísle N+1. V modeli je stanovených 7 vrstiev (v súčasnosti je toto číslo považované za zbytočne vysoké a funkcie niektorých vrstiev sa komprimujú do seba):

1. Fyzická
2. Linková
3. Sieťová
4. Transportná
5. Relačná
6. Prezentačná
7. Aplikačná

3.4.1 Fyzická vrstva - Physical layer

Komunikácia medzi systémami môže prebiehať mechanickou, optickou alebo bezdrôtovou cestou. Táto vrstva sa zaoberá výhradne prenosom signálu srz médium vo forme tzv. bitov[12]. Nijak neinterpretuje to, čo prenáša. Zaoberá sa otázkami typu kódovania signálu, moduláciou signálu, časovaním, synchronizáciou, elektrickými parametrami signálu, konektormi, riadiacimi signálmi rozhrania a i.

Mechanické vedenie - uzly (počítač, server, senzor, spotrebič...) sú prepojené fyzickým medeným káblom. Najtypickejšie v súčasnosti je tzv. krútená dvojlinka (twisted pair), alebo koaxiálny kábel (drahší, menej flexibilný). Prenosová rýchlosť je rôzna v závislosti na druhu kábla, ale možná až do 10Gbit/s bez obmedzenia vzdialenosti. Komunikácia niektorých služieb je možná aj po silovej eletrickej sieti (PLC - Powerline communication), tu je však možné veľké rušenie signálu a zároveň je sieť ohrozená elektrickými výbojmi. Komunikácia na mechanickom vedení sa dá odpočúvať, prípadne sa k nechránenému vedeniu dá pripojiť, alebo ho násilne prerušiť. Mechanická kabeláž patrí medzi pasívne prvky siete (aktívne prvky sú napr. router, switch, hub, repeater). Štruktúrovanú kabeláž sieťe môže tvoriť:

[11] https://en.wikipedia.org/wiki/OSI_model

[12] bit z angl. „binary digit“ je základná najmenšia jednotka dát, nadobúda vždy jednu z dvoch hodnôt 0 alebo 1, značí sa b alebo bit, 8 bitov tvorí 1 byte (bajt), https://cs.wikipedia.org/wiki/Bit

- **koaxiálny kábel** - asymetrický kábel s jedným válcovitým vonkajším vodičom a jedným trubkovým alebo drôtovým vodičom vnútri. Vonkajší a vnútorný vodič sú oddelené nevodivou vrstvou. Používa sa v telekomunikáciách, v telefónií, pre káblové televízie, počítačové siete...
- **krútená dvojlinka** - angl. *twisted pair*, TP, je kábel tvorený z párov vodičov, ktoré sú pravidelným spôsobom zakrútené, a výsledné páry sú zakrútené tiež. Dôvodom je zlepšenie elektromagnetických vlasností kábla. Je to najpoužívanejší kábel pre Ethernet, ale používa sa aj v telekomunikáciách. Z fyzického hľadiska na ňom nie je možné robiť odbočky, preto sa používajú prvky ako rozbočovač, alebo sa odbočky riešia elektronicky. Pre použitie počítačových sietí býva kábel ukončený koncovkou RJ-45, ktorá popisuje rozmery a usporiadanie kontaktov v konektore. Existuje niekoľko kategórií (štandardov) pre krútenú dvojlinku, ktorej sa v bežnej reči hovorí zjendodušene „ethernet“ kábel. V súčasnosti sú najpoužívanejšie štandardy tohoto kábla CAT5, ktorý zvláda rýchlosť prenosu dát do 100Mbps, CAT5e do rýchlosti 1Gbps alebo CAT6 a CAT7 pre rýchlosti až do 10Gbps.

Optické vedenie - vedenie signálu optickým vláknom, v ktorom sa prenáša svetelný signál. Kábel môže byť jednovidový alebo mnohovidový. Odpočúvať optickú komunikáciu nie je jednoduché, ale toto vedenie je veľmi citlivé na deformáciu a na narušenie vedenia. Prenosové rýchlosti sú veľmi vysoké (1-100 Gbit/s), ale cena tohto vedenia je väčšia než u medených spojov. Používa sa hlavne na veľké vzdialenosti.

Bezdrôtové spojenie - bezdrôtových spojení existuje množstvo druhov, od rádiového spojenia, cez štandard Bluetooth, až po Wi-Fi. Niektoré vyžadujú malú vzdialenosť zariadení, niektoré zas vyžadujú priamu viditeľnosť, ale vo všeobenosti sú veľmi flexibilné. Bezdrôtové spojenie je najzraniteľnejšie na odpočúvanie komunikácie a zraniteľné na rušenie frekvenčného pásma.

Príklady štandardov používaných v tejto vrtstve: RS-232, RS485, IEEE802.3 (Ethernet), IEEE802.11 (Wi-Fi), GSM (GPRS)

3.4.2 Linková (spojová, datová) - Data link layer

Táto vrstva prenáša bloky dát. Zaisťuje prenos v dosahu priameho spojenia staníc, „bez prestupov“. Je jej jedno, či komunikácia prebieha bezdrôtovo, alebo po metalickom spojení. Táto vrstva väčšnou zabezpečuje synchronizáciu prenosu dát a stará sa, aby sa navzájom nezahltil odosieľateľ a príjemca. V tejto vrstve sa rieši adresácia zariadení a prístup zariadení k sieti: podvrstva MAC (Media Access Control) a LLC (Logical Link Control). MAC vrstva zaobstaráva metódy prístupu k médiu. Najznámejšie z aplikovaných protokolov bývajú:

- **CSMA/CD** - Carrier Sense Multiple Access/Collision Detection - stanica, ktorá sa chystá vyslať dáta, počúva na sieti, či neprebieha iné vysielanie. Ak je sieť voľná, začne vysielať. Ak sa súčasne rozhodne vysielať aj iná stanica, dôjde ku kolízii. Stanice obdržia informáciu, že došlo ku kolízii, a vysielanie rámca sa po náhodnej dobe opakuje
- **CSMA/CA** - Carrier Sense Multiple Aceess/Collision Avoidance - je pomalší protokol. Ak chce stanica vysielať, chvíľu na sieti počúva. Ak je sieť voľná, začne vysielanie. Ak voľná nie je, stanica počká, kým sa iné vysielanie skončí, a až potom začne vysielať

3.4.3 Sieťová vrstva - Network layer

Prenáša bloky dát označované ako pakety[13] a datagramy[14] od adresátov k príjemcovi. Je to posledná vrtsva, ktorú musí mať každá prenosová infraštruktúra. Najrozšírenejším protokolom tejto siete je IP - Internetový Protokol, ktorý je implementovaný napr. v routroch (smerovačoch).

3.4.3.1 Internetový protokol

Základný protokol na sieťovej vrstve je Internetový protokol (IP). Zjednodušene slúži na prenos datagramov zo zdrojového počítača do cieľového. Sám protokol však nie je zodpovedný za správne doručovanie paketov, o to sa starajú protokoly vyšších vrstiev OSI modelu. IP protokol zabezpečuje len tzv. „najlepšie úsilie“, snaží sa datagram alebo paket poslať čo najbližšie k cieľu podľa adries. IP je dôležitý protokol, pretože zabezpečuje adresovanie a smerovanie v sieti. Prideľuje adresy uzlom v sieti a zoskupuje uzly do podsietí.

Adresa IP

Adresa Internetového protokolu je jednoznačný číselný identifikátor zariadení v sieti. Každé zariadenie, ktoré má prístup do siete, musí mať jedinečnú adresu IP.

- **IPv4** - v súčasnosti najpoužívanejší je protokol verzie 4, ktorý používa 32bitové adresy v dekadickom zápise a každých osem bitov oddeľuje bodkou, napríklad:

  ```
  192.168.0.1
  ```

  V binárnom zápise tak má podobu:

  ```
  11000000.10101000.00000000.00000001
  ```

  Poskytuje obmedzený adresný priestor, teroeticky 2^{32}, to je 4 miliardy adries, ktorý už bol oficiálne rozdelený a vyčerpaný. O pridelovanie adries sa stará organizácia Internet Assigned Numbers Authority (IANA)[15].

  Nedostatok adries IPv4 sa rieši používaním technológií NATu, a rozdeľovaním adries na verejné a privátne.

  Network Address Translation (NAT) - doslova preklad sieťových adries. Upravuje prenos v sieti prepisovaním zdrojovej alebo cieľovej IP adresy. Využíva sa, ak je nutný prístup viacerých počítačov z lokálnej siete do Internetu a k dispozícii je len jedna verejná IP adresa.

  Súkromná IP adresa - Adresný priestor IPv4 bol rozdelený na verejný a súkromný. Boli vymedzené adresné okruhy, ktoré sa používajú len v rámci siete lokálne, ale nikdy nie v rámci Internetu. Sú to adresy spadajúce do rozsahov:

[13] formátované bloky dát, ktoré sa skladajú z riadiacich údajov ako sú napr. cieľová a zdrojová adresa, tzv. metadát, a užívateľských dát

[14] blok dát podobne ako paket (obsahuje hlavičku s riadiacimi údajmi a prenášané údaje), ale nezaručuje sa správnosť doručenia dát, zachovania poradia a ani eliminácia duplicít

[15] http://www.iana.org/

```
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255
```

Verejná IP adresa - je unikátna adresa, identifikátor v rámci celej siete. Žiadne dve zariadenia na Internete nemôžu mať rovnakú verejnú IP adresu.

- **IPv6** - nastupujúci protokol verzie 6, vzniká ako nutná náhrada za protokol Ipv4. Poskytuje oveľa väčší adresný priestor, jedna adresa má až 128 bitov. To znamená, že može poskytnúť 3,4 x 10^{38} unikátnych adries pre zariadenia. Zapisuje sa pomocou hexadecimálnych čísel oddelených dvojbodkov. V prípade, že úsek obsahuje samé nuly, používa sa skrátenie a 0 sa nahradia dvojbodkou. Príklad celého a skáteného zápisu IPv6 adresy:

```
2001:0db8:0000:0000:0000:0000:1428:57ab
2001:0db8::1428:57ab
```

3.4.4 Transportná vrstva - Transport layer

Existuje preto, že často nie je možné zmeniť vlastnosti prechádzajúcich troch sietí (napr. Ak infraštruktúra v bytovom dome patrí niekomu inému). Vyššie vrstvy majú iné požiadavky na charakter komunikácie, ako nižšia, už existujúca vrstva ponúka. Úlohou tejto vrstvy je zabezpečiť potrebné prispôsobenie sa. Protokoly tejto vrstvy sú implementované v koncových zariadeniach. Typických protokolom tejto vrstvy je TCP/IP a UDP.

- **TCP** - Transmission Control Protocol je protokol, ktorý zabezpečuje spoľahlivosť doručenia paketov a dát. TCP využíva protokol IP, preto sa často označuje TCP/IP. Funguje na princípe naviazania spojenia podľa cieľovej adresy, prenosu dát a ukončenia spojenia. Na naviazanie spojenia sa využíva tzv. *handshake*, kedy si počítače musia virtuálne dohodnúť spojenie „podaním ruky“, potvrdiť si, že zdroj a cieľ sú správne, a až potom môžu prenášať dáta.
- **UDP** - User Datagram Protocol takisto prenáša datagramy, ale nezaručuje ich doručenie a ani správnosť poradia doručenia. Nevyužíva technológiu handshake. Je ale omnoho rýchlejší a preto sa v praxi na niektoré služby často používa. Neobsahuje žiadne šifrovanie prenášaných dát, preto je jednoduché komunikáciu odpočúvať, odchytiť alebo sfalšovať.

3.4.5 Relačná vstva - Session layer

Zaisťuje zostavenie, riadenia a zrušenie relácie. Na tejto vrstve funguje napríklad protokol SSL (Secure Socket Layer), ktorý poskytuje šifrovanie komunikácie a autentizáciu komunikujúcich strán, najviac medzi transportnou vrstvou s protokolom TCP/IP a apikačnou vrstvou s protokolom napr. HTTP. Nad týmto potom stojí protokol TLS (Transport Layer Security). Zabezpečenie cez SSL prebieha pomocou tzv. asymetrického šifrovania, kde každá z komunikujúcich strán má 2 kľúče - súkromný a verejný. V tomto protokole sú používané rôzne kryptografické algoritmy, napríklad: AES, DES, RC2 pre symetrickú šifru, RSA a DSA pre výmenu kľúčov, alebo jednocestné hashovacie funkcie ako MD5.

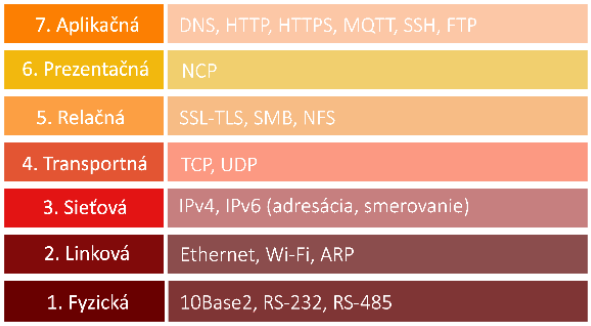
3.4.6 Prezentečná vrstva - Presentation layer

Má na starosti rôzne konverzie dát - kódovanie prenášaných znakov, poradie bitov, atď do podoby, akú sú schopné spracovať aplikácie. Zaoberá sa štruktúrou prenášaných dát, nie ich významom. Príklad používaného protokolu môže byť XML (eXtensible Markup Language) - rozšíriteľný značkovací jazyk používaný pre serializáciu dát, JSON či YAML.

3.4.7 Aplikačná vrstva - Application layer

Neobsahuje priamo aplikácie dát, ale obsahuje jadro aplikácií, ktoré je možné štandardizovať. Sú to napríklad protokoly pre prístup k objektom v sieti (SMTP, FTP, SSH, DHCP, DNS, NTP, HTTP ale aj Telnet alebo naprílkad ModBus, ktorý sa používa aj pre komunikáciu PLC zariadení).

Nasledujúci obrázok priraďuje jednotlivým vrstvám modelu ISO/OSI príklady protokolov, ktoré na nich pracujú.



Obr. 3.2: Vrstvy ISO/OSI modelu a príklady protokolov, ktoré na nich operujú

Kapitola 4

Štandardy, protokoly

Protokol je v informatike označenie pre dohodnutý spôsob komunikácie medzi koncovým a ovládacím zariadením (prípadne medzi zariadeniami navzájom). Je závislý na prenosovom médiu, to znamená že platí iný protokol pri prenose dát káblom a iný pri prenose dát vzduchom. Používaných prenosových protokolov existuje veľké množstvo, ale len niektoré z nich sú schopné komunikovať medzi sebou. Kedysi neexistovali žiadne medzinárodné štandardy a komunikácia medzi jednotlivými vyrábanými prístrojmi bola obtiažna, výrobcovia nezdieľali svoje protokoly a kompatibilita systémov bola mizivá, preto sa začalo so štandardizovaním a vytváraním protokolov pre počítače a sieťové prvky. Rozvoj IoT a inteligentných systémov ale priniesol ďalšiu vlnu nových protokolov, ktoré nie sú medzi sebou kompatibilné, a navyše ani nemusia byť - obchodníci si tak chránia svoju značku a zabezpečujú, že si užívatelia kúpia ich nové výrobky. Bohužiaľ, toto správanie je menej výhodné pre používateľov.

Za autoritu pri určovaní protokolov sa považuje spoločnosť **Institute of Electrical and Electronics Engineers (IEEE)**[16].

[16] https://www.ieee.org/

4.1 Bezdrôtové pripojenia

Mechanické protokoly (resp. niektoré z nich) boli popísané už v predchádzajúcej sekcii, preto ďalej popíšem hlavne bezdrôtové pripojenia).

4.1.1 WPAN - Wireless Personal Area Network:

Bluetooth - štandard IEEE 802.15.1 z roku 1994. Slúži k prenosu informácií na krátku vzdialenosť. Dosah je približne 10 metrov a závisí aj na viditeľnosti. Rýchlosť prenosu 1,4 Mbit/s. Spotreba energie je menšia ako pri prevádzke Wi-Fi, ale stále dosť vysoká. Z hľadiska zabezpečenia je technológia Bluetooth relatívne bezpečná, pretože pred započatím komunikácie sa obe zariadenia musia spolu spárovať.

ZigBee - 802.15.4 - štandard siete určenej pre komunikáciu priemyslových zariadení, má veľmi nízku spotrebum, dosah cca 75 metrov a nízky prenosovú rýchlosť. Tento štandard je v súčasnej dobe relatívne rozšírený v oblasti automatizácie v budovách.

4.1.2 WLAN - Wireless Local Area Network:

Wi-Fi - IEEE 802.11xx, kde „xx“ môže byť nahradené rôznymi písmenami (a, b, g, n, ac, ad) a ich kombináciou. Má výrazne vyšší dosah než WPAN siete (závisí od prekážok a prostredia). Využíva sa pre vysokorýchlostný prenos dát, zároveň spája navzájom viacero zariadení v lokálnom význame. Spravidla slúži pre pripojenie viacerých zariadení k Internetu a vyžaduje relatívne veľké množstvo energie. Zabezpečenie Wi-Fi štandardu závisí od nastavení jednotlivých sietí (názov siete SSID, šifrovanie: WEP, WPA, WPA2-PSK, a ďalšie nastavenia), prístupových bodov (AP - access point), a používaných aplikácií. Odpočúvať a narušiť komunikáciu na tomto štandarde môže byť veľmi jednoduché aj pre málo skúseného útočníka, zvlášť ak sa nepoužíva žiadne šifrovanie siete a ak šifrovanie nepoužívajú ani vyššie vrstvy ISO/OSI.

Technológia Wi-Fi funguje v bezlicenčnom pásme 2,4 GHz, alebo novšia verzia 802.11a v pásme 5GHz. Tieto hodnoty sú používané len ako všeobecná informácia, v skutočnosti totiž 802.11 pracuje v pásme od 2,4 do 2,4835 GHz a používa kanál o šírke 22 MHz. To značí, že prenosové kanály, ktoré spolu nebudú interferovať, sú v tomto najpoužívanejšom licenčnom pásme len tri a odstup medzi jednotlivými kanálmi je len 5 MHz.[3]

4.1.3 LPWAN - Low Power Wireless Area Network:

Z-Wave - Protokol Z-Wave je relatívne nový protokol používaný primárne pre automatizáciu domácností. Bol vyvinutý spoločnosťou Zen-sys v roku 2001, k masívnemu rozšíreniu došlo až v roku 2005. Pracuje na bezdrôtovom frekvenčnom pásme medzi 800-900 MHz (v závislosti na krajine, v ktorej sa zariadenie nachádza). Má lepší dosah a menšiu spotrebu energie než Bluetooh, zariadenia sú schopné bežať v úspornom režime. Veľkou výhodou protokolu je používanie šifrovania komunikácie nevýhodou je zas nekompatibilita s inými zariadenia, v niektorých prípadoch dokonca nekompatibilita aj medzi stršími a novšími verziami zariadení.[2]

Sigfox - Sigfox je názov spoločnosti, ktorá začala stavať bezdrôtové siete pre prepojenie nízkoenergetických zariadení, ktoré musia byť neustále zapnuté, ale nepotrebujú prenášať rozsiahle objemy dát (napríklad rôzne druhy senzorov). Technológia využíva bežnú frekvenciu pásma 868 MHz (Európa) a 902 MHz (USA). Sigfox patrí medzi LPWAN siete. Sieť má hviezdicovú topológiu. Všetky dáta sú prenášané na server firmy Sigfox, odkiaľ má užívateľ k nim prístup cez webové rozhranie.

Využívanie komunikačných pásiem má svoje pravidlá. V ČR ich určuje Český telekomunikačný úrad pomocou dokumentov Všobecných Oprávnení. Pri používaní výrobkov dovezených z iných krajov tak môže nastávať problém rušenia v pásme, pretože každá krajina môže mať vlastné pravidlá licencované pásma pre typy komunikácií. U nás sa pre prenos dát najviac používajú pásma 433 MHz a pásmo 868 MHz.[4]

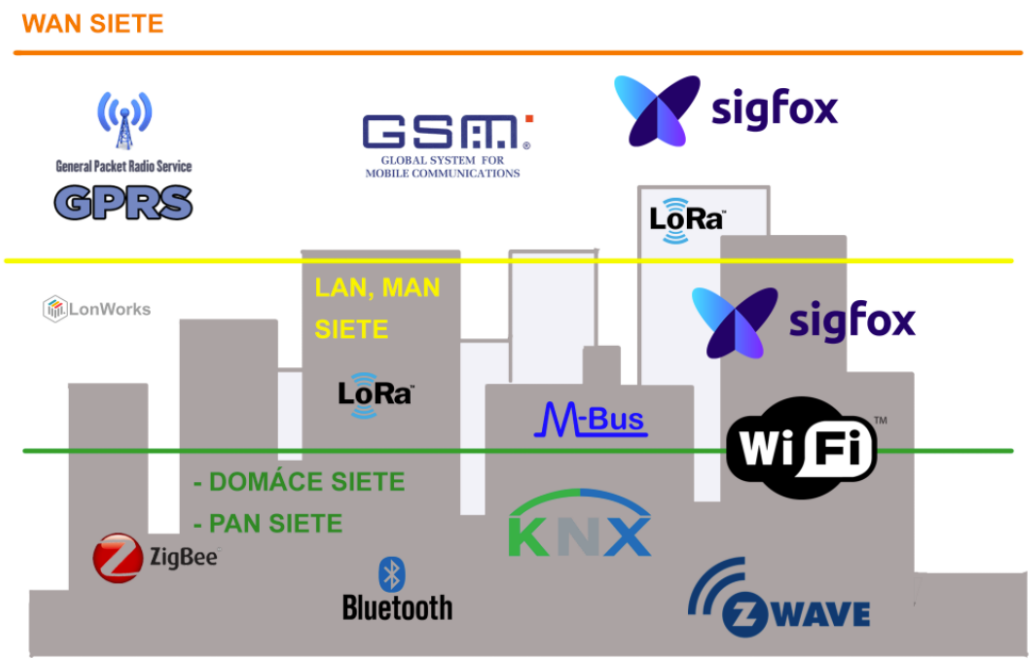
LoRa Technology - LoRa je technológia využívaná pre IoT systémy, ale aj pre zariadenia Long Range Signaling and Control, LRSC (riadenie a signalizáciu) určené pre inštaláciu na veľkej rozlohe. Očakáva sa malé množstvo prenášaných dát a malá spotreba energie, podobne ako pri SigFoxe. LoRa zahŕňa pod sebou dva dôležité pojmy, moduláciu Lora a protokol LoRaWan. LoRa (Long Range) je modulácia patentovaná firmou Semtech, ktorá využíva hlavne kódovanie 4/5, doprednú korekciu chýb a moduláciu Chirp. Protokol LoRaWAN zase zaisťuje transparentný a bezpečný prenos dát medzi koncovými zariadeniami (IoT, senzory) a aplikáciou bežiacou na serveri a späť. O štandardizáciu a rozvoj protokolu LoRaWAN se stará nezisková organizácia LoRa Alliance, ktorej členmi sú desiatky firiem a ktorej komunita sa rozrastá aj v ČR.

Sigfox aj LoRa patria v posledných rokoch medzi často skloňované technológie. Dôležité pri výbere použitia sú ich základné vlastnosti. Sigfox je úzkopásmova technológia, ktorá ma dosah desiatky kilometrov. Výhodou je lepšia kvalita signálu v budovách, než LoRa. Ďalšou výhodou je, že sa jedná o komerčne dostupnú a overenú sieť s pokrytím v mnohých zemiach, ktorá navyše nevyžaduje žiadne roamingové poplatky. Nevýhoda môže byť v tom, že payload jednej správy je max. 12 byte (LoRaWan až desiatky bytov), obmedzený downlink (teda prenos dát medzi serverom a zariadením), obedzené potvrdzovanie doručenia správ a v neposlednej rade to, že napriek tomu, že je to overený poskytovateľ siete, je na ňom závislá celá infraštruktúra a teda aj pokrytie. LoraWan má oproti tomu silné stránky tam, kde je nutné pokrytie relatívne malého územia kvalitným signálom. Základňové bunky LoRaWan sú dostupné a nie je problém zapojiť ich do infraštruktúry alebo vytvoriť si vlastnú sieť. LoRaWan je open-source a je otvorená vlastným implementáciam. Ponúka možnosť potvrdzovania správ alebo peer-to-peer komunikáciu (s duálnymi transceivermi), nevýhodou je horšia kvalita spojenia v budovách a obecne kratší dosah než SigFox.

4.2 KNX/EIB

V súčasnosti asi najrozšírenejší systém pre automatizáciu vo všetkých typoch budov. Založený a kompatibilný so starším protokolom skupiny EIBA[17] (z toho sa používa názov EIB/KNX[18]). Vužíva technológiu zbernice Konnex bus, z toho pochádza skratka KNX. Tento

[17] https://cs.wikipedia.org/wiki/EIBA
[18] https://en.wikipedia.org/wiki/Instabus



Obr. 4.1: Protokoly a štandardy sietí a IoT a oblasť ich použitia

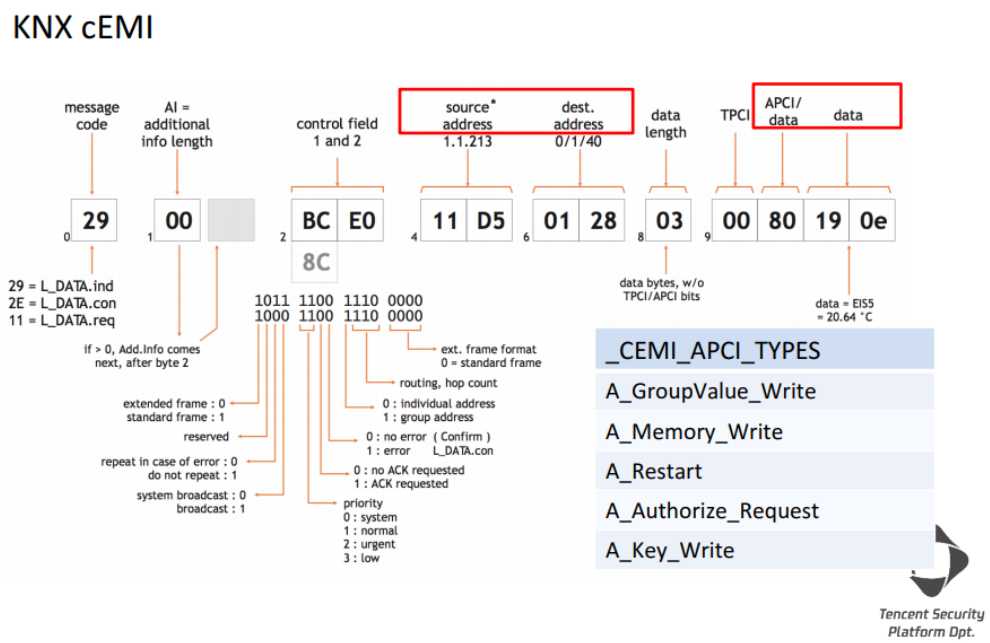
systém tiež rešpektuje OSI systém siete. Môže využívať krútenú dvojlinku, silovú kabeláž, rádio spojenie, infra spojenie alebo ethernet. Systém môže byť rôznej topológie (bus, strom, hviezda) a môže ich navzájom kombinovať. Systém je väčšinou centralizovaný, s jednou ovládacou stanicou pripojenou do internetu (umožnujúcou vzdialené ovládanie). Patrí medzi BAS (Building Automation System).[5]

Asociácia KNX[19] vyžaduje pre certifikáciu vysokú kvalitu vyrábaných prvkov, ktoré musia byť certifikované nielen touto asociáciou ale musia zároveň vyhovieť európskym a medzinárodným normám. Systém KNX je decentralizovaný zbernicový systém nezávislý na hardwarových platformách, takže akýkoľvek prvok s certifikáciou a logom KNX (prípadne KNX/EIB) je kompatibilný a môže byť pridaný do systému. Všetky zariadenia sú rovnocenné zbernicové prístroje, ktoré komunikujú medzi sebou. Účastníkmi systému sú senzory (snímače) - teplotné senzory, senzory pohybu, stlačenia vypínača a pod., akčné členy (aktuátory), systémové prístroje - napájacie zdroje, datové zbernice, sériové rozhrania ako RS-232, USB, atd., a riadiace prvky. KNX je prevážne drôtový zbernicový systém, avšak rozvoj konkurenčných technológii a dopyt trhu prinútil KNX vyvinúť aj bezdrôtovú technológiu. Pre bezdrôtovú komunikáciu existuje KNX-RF protokol, ktorý využíva pásmo 868 MHz, po ktorom odosiela KNX telegramy.[5]

KNX telegram má presne dané zloženie, ktoré nájdeme na nasledujúcom obrázku.

Komunikácia v protokole nie je nijak šifrovaná.

[19] https://www.knx.org/knx-en/index.php



Obr. 4.2: Podrobné zloženie telegramu KNX, obrázok prevzatý od Tencent Security Dpt., 2018

4.2.1 Zraniteľnosť KNX systému

Napriek tomu, ako dlho je tento protokol a systém na trhu, nemôžeme povedať, že je bezpečný. Jeho najväčšia zraniteľnosť spočíva v tom, že keď sa pripojí priamo k sieti (ako napr. na obrázku 1), stane sa ľahko dostupným z Internetu. Je tu niekoľko spôsobov, akými sa dá tento systém napadnúť.

Tím ľudí z Milána napísal v roku 2014 prácu[**?**] o presnom postupe, ktorý je aplikovateľný na široké spektrum sietí pracujúcich na protokole KNX ale aj iných (ZigBee, BacNet, LonTalk) [3]. Hlavným problémom ktorý využili, je ten, že komunikácia v rámci KNX je nešifrovaná, to znamená, že keď má niekto prístup do siete, komunikácia je ľahko odpočúvateľná, ľahko analyzovateľná, a ľahko sfalšovateľná. Je pravda, že prístup do systému pre naprogramovanie jednotky môže byť ochránený heslom, a útočník sa k danému zariadeniu siete nemusí dostať. Výskumníci ale zistili, že stačí zariadenie napadnúť posielaním náhodných udalostí, napríklad pre zapínanie a vypínanie svetla, a donútiť ho tak, aby si myslelo, že dochádza k nefunkčnosti a chybe systému (pomocou malware). Systém potom bude vyžadovať zadanie hesla. A keďže komunikácia v rámci systému nie je šifrovaná a heslo je posielané ako čistý text, útočník ho veľmi jednoducho získa. Potom sa do systému prihlási a heslo zmení, aby zamedzil pôvodným používateľom zmeniť ho znova.

Akonáhle má útočník heslo a môže preprogamovávať jednotky v systéme, má vyhrané. Výskumníci vytvorili knižnicu požiadavkov v závislosti na prvkoch použitých v sieti (ktoré zistili pomocou reverzného inžinierstva) a mohli plne ovládať a preprogramovať systém podľa svojich predstáv.

Problémom KNX protokolu je teda to, že nevyžadoval autentifikáciu požiadavkov a nepoužíval šifrovanie na úrovni sieťového protokolu.

Tento útok by sa dal ľahko zautomatizovať a na trhu sú k dispozícií rôzne zariadenia, ktoré napadnutiu systému pomôžu. Napríklad ak má útočník fyzický prístup, je možné napojiť predprogramované zariadenie (napríklad KNX konvertor) k zbernici KNX termostatu, ktorý je najčastejším a najdostupnejším zariadením v miestnosti. [4] Po pripojení a odpočúvaní komunikácie útočník získa potrebné dáta o zložení siete a o posielaných správach a zariadeniach v sieti. Tieto informácie naprogramuje do zariadenia, ktoré má v sebe GSM modul a bude ho môcť vzdialene ovládať, a ukryje ho znova pod krytom termostatu. Takýto útok už vyžaduje mierne pokročilé znalosti a prvotný fyzický prístup k sieti, ale na druhú stranu môže byť veľmi účinný a ťažko zistiteľný.

4.3 Protokoly vzdialenej správy

4.3.1 SSH

Jeden z najčastejších protokolov vzdialeného pripojenia v dnešnej dobe je založený na systémoch GNU/Linux a BSD. Pracuje na TCP porte 22 a všetku prebiehajúcu komunikáciu medzi koncovými účastníkmi šifruje. Využíva na to tzv. SSH kľúče, ktoré si účastníci medzi sebou vymenia a tým sa autorizujú. Používateľ môže na ovládanie používať príkazový riadok (CLI - Command Line Interface) alebo textové rozhranie TUI (Text User Interface), ak je pre danú aplikáciu dostupné. Protokol je popísaný v RFC 4251[6].

4.3.2 Telnet

Protokol Telnet je pôvodom starší než SSH. Pracuje na TCP porte 23. Hlavným rozdielom oproti SSH je, že nevyužíva šifrovanie, preto je v dnešnej dobe už na okraji používania, ale niektorí výrobcovia ho stále implementujú, najmä kvôli špecifikám niektorých aplikácii. Takisto ako SSH využíva na ovládanie príkazový riadok alebo textové rozhranie. Tento protokol je definovaný v RFC 854[7].

4.3.3 Webové rozhranie

Webové rozhranie, alebo aj používateľské rozhranie (UI - user interface) je veľmi častá, hlavne vďaka jej prívetivosti pre používateľov, ktorí nerozumejú používaniu príkazového riadku CLI. Využíva protokol aplikačnej vrstvy HTTP[8] (Hypertext Transfer Protocol) alebo HTTPS[9] (Hypertext Transfer Protocol Secure). Verzia HTTP beží na porte 80 a nepoužíva šifrovanie a tak sa v dnešnej dobe dostáva pomaly do pozadia a vyzdvihuje sa radšej šifrovaná verzia HTTPS, ktorá počúva na porte 443.

Webové UI závisí vždy od konkrétneho výrobcu, v každom prípade je veľmi odlišné. Vstup do webového rozhrania je väčšinou podmienený prihlasovacími údajmi administrátora, ktoré nesmú byť jednoduché. V rozhraniach pre ovládanie niektorých zariadení, ako napr. routere, bývajú administrátorké údaje prednastavené, napríklad

```
username: admin
password: 1234
```

A ak sa tieto administrátorké údaje nezmenia pri konfigurácii zariadenia, v sieti dochádza k zníženiu bezpečnosti aplikácie a systému.

4.3.4 API

API z angl. Application Programming Interface znamená, že výrobca umožní ovládanie zariadenia skrz špeciálny súbor procedúr, funkcií a príkazov, ktoré môže využiť programátor ako vstup pre vlastný ovládací program alebo pre ďalšie spracovanie dát. Je to akýsi súbor knižníc programovacieho jazyka, ktorý pracuje priamo s jadrom určitého systému a nemusí využívať grafické rozhranie.

Každý výrobca poskytuje vlastné API (teda, ak ho poskytuje) a tak je kompatibilita systémov náročná, zvlášť, ak chceme použiť pre systém centrálny riadiaci prvok, ktorý má ovládať aj iné technológie.

API nepopisuje žiadny štandard, závisý vždy len od výrobcu.

4.4 Centralizovaný vs. decentralizovaný systém

Cieľom všetkých intelignetných systémov a zariadení IoT je prepojenie zariadení, systémov a služieb tak, aby mohli poskytnúť čo najviac dát, ktoré sa dajú využiť pre ďalšie spracovanie a aplikácie. Rozdiely ale nastávajú v motivácii zberu dát, ich spracovaní a v spôsobe využitia dát medzi užívateľským (consumer) a priemyselným (industrial) prostredím. Pri tvorbe inteligentných systémov je treba zodpovedať nasledujúce otázky a podľa toho postupovať:

- **Zbieranie dát** - akým spôsobom budem dáta dostávať? Potrebujem senzory, alebo len ovládací prvok?
- **Ukladanie dát** - Potrebujem tieto dáta ukladať, prípadne zálohovať?
- **Analýza dát** - Potrebujem dáta analyzovať, alebo chcem systém, ktorý len reaguje na aktuálne pokyny?
- **Zdieľanie výsledkov** - Potrebujem výsledky analýzy prezentovať alebo posielať ďalej, zakladať na nich nastavenia systému?

A v neposlednom rade musí architektúra systémov spĺňať prísne požiadavky na bezpečnosť. Z pohľadu bežného používateľa je tiež dôležité, aby sa zvolené riešenie dalo ľahko implementovať, aby bolo možné integrovať ho s ostatnými aplikáciami a aby bolo možné prehľadne organizovať a spravovať dáta, informácie alebo znalosti.

Ďalšími dôležitými faktormi pri voľbe systému sú tieto vlastnosti:

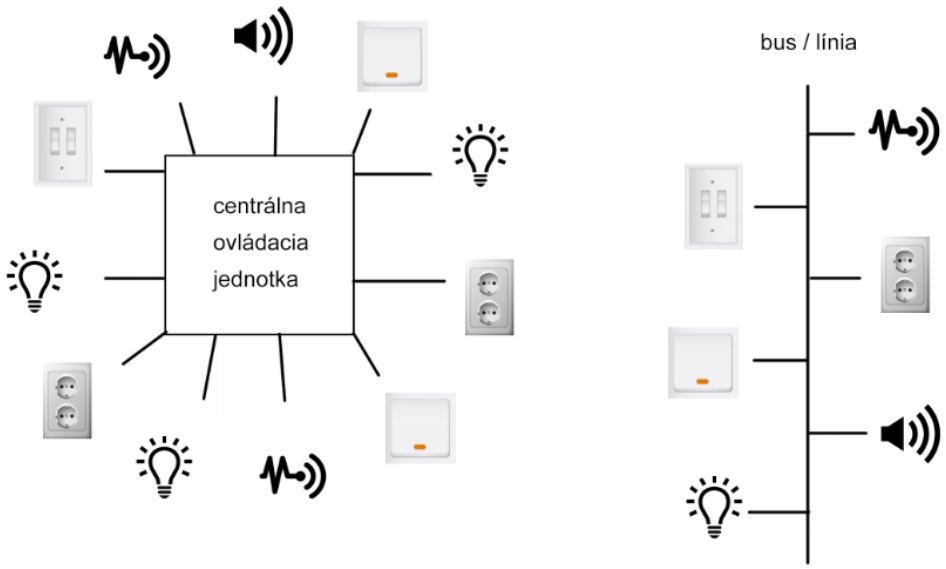
- **Prenosová rýchlosť** - Koľko dát/infomácií potrebujem posielať a za aký čas?

- **Spotreba energie** - možné napájanie z batérií alebo zo siete
- **Dosah** - Stačí dosah niekoľko metrov, alebo je treba kilometre?
- **Frekvencie** - Aké frekvencie sú k dispozícii v tejto oblasti?

Z týchto požiadavkov (a ďalších ktoré tu nie sú menované) je možné vyberať druh systému, ktorý bude používateľovi vyhovovať. Možností, ako môžu byť prvky prepojené, je niekoľko, ale základné rozdelenie systémov by sa dalo rozdeliť na dva druhy: **centralizované** a **decentralizované** systémy.

4.4.1 Centralizovaný systém

Centralizovaný systém je postavený na tom, že každý prvok/uzol/zariadenie v sieti je schopné komunikovať len s hlavným ovládacím prvkom siete. To môže byť riadiaca jednotka, samostatný server, ovládací panel... Môžeme mu hovoriť master, hlavný panel, hlavný uzol a iné. Celá sieť je závislá od daného riadiaceho prvku a ak bude nefunkčný, bude nefunkčná aj sieť. Dáta z uzlov a senzorov sa posielajú na riadiacu jednotku a tam sa buď spracovávajú alebo zdieľajú ďalej (napr. do lokálneho úložiska alebo cloudu). Odozva systému môže byť pomalšia a kabeláž má násobne väčšie náklady (ak musí byť každý prvok pripojený k centrálnej jednotke zvlášť) a nie je možné používať bezdrôtové prvky.



Obr. 4.3: Centralizovaný vs. decentralizovaný systém

Centralizované riešenia sa používajú napríklad v spotrebiteľskom svete, kde nie je potrebná veľká rýchlosť odozvy a prípadný výpadok nemá závažné dopady, narozdiel od výpadku výrobných staníc alebo nemocníc. Spravidla poskytnú ľahkú a rýchlu inštaláciu a riadiaci prvok prepoja s jednoduchým používateľským rozhraním, ktoré umožní ľahko ovládať domácnosť. Pri rozsiahlých inštaláciách, ktoré sa týkajú celej budovy alebo komplexu

budov, je výhodou centrálneho prvku ovládania ľahšia kontrola systému. Riadiaci prvok alebo server môže byť umiestnený v jednej, špeciálne zabezpečenej miestnosti s obmedzeným prístupom len pre vybrané osoby obsluhy. Pri správnom nakonfigurovaní je ľahké určiť, kde v sieti nastal problém a ktoré zariadenie má poruchu. Ak však vypadne riadiaci prvok, prestane fungovať celá sieť a to je hlavná nevýhoda tohoto systému. Ďalšou nevýhodou takéhoto systému je jeho robustnosť pri veľkých inštaláciách, vo veľkých budovách alebo firmách, čo môže systém predražiť.

4.4.2 Decentralizované systémy

Decentralizované systémy môžeme popísať ako systémy, ktoré delegujú časť svojich funkcií na jednotlivé uzly v ich sieti. Uzly sú schopné komunikovať medzi sebou a tým navzájom na seba reagovať, lokálne ukladať dáta alebo ich zdieľať, napríklad pomocou zbernice. Typickým decentralizovaným systémom je systém KNX, ale existuje rada ďalších ako napr. EATON, LON (Local Operated Network), XComfort, BACnet a ďalšie.

Decentralizovaný, alebo tiež **distribuovaný** systém je oproti centralizovanému riešeniu odolnejší voči výpadku jeho prvkov. Je flexibilnejší z hľadiska inštalácie, ale komplikovanejší na správu celého systému. Problém môže nastávať pri hľadaní chyby v sieti.

4.4.3 Zmiešané systémy

Pre niektoré inštalácie je najvýhodnejšie skombinovať obidva druhy systémov. Napríklad rozdeliť funkcionality v budove na tie, pre ktoré je centralizácia výhodná, ako napríklad vykurovanie pomocou PLC[20] systémov, a funkcie osvetlenia, klimatizácie a ovládania žalúzií pomocou decentralizovaného systému. Taktiež je možné rozdeliť systém na jednotlivé podsystémy, napríklad podľa poschodí, podľa bytových jednotiek, podľa firiem, ktoré sídlia v budove atď. Obvyklým riešením býva použitie Individual room control (IRC) - individuálnej kontroly miestností spolu s centrálnym ovládaním celej budovy, napríklad kontrolou vstupu a fyzického zabezpečenia budovy.

[20] z angl. Programmable Logic Controller - programovateľný logický automat, je systém používaný pre kontrolu systémov a automatizáciu v reálnom čase. Využívaný je často v priemyslových inštaláciách.

Kapitola 5

Riziká

Aké sú riziká nezabezpečených inteligentných systémov? Ako sa líšia riziká v domácnostiach, vo firemných prevádzkach a mestách? Čo hrozí, ak niekto získa prístup do siete a môže odpočúvať, meniť alebo mazať komunikáciu a dáta v systémoch? Povedomie o bezpečnosti informatických systémov sa dlhodobo zlepšuje a potrebu zabezpečovať počítačové údaje a siete si uvedomujú už nie len firmy, ale aj bežní používatelia a prispôsobuje sa tomu aj legislatíva. Ale čo inteligentné systémy?

5.1 Dôvody

5.1.1 Napadnutie domácnosti

Pýtate sa: „Prečo by to niekto robil? Prečo by niekto napadal moju domácnosť?“ Nemáte osobných nepriateľov a neznámy človek by na vás predsa neútočil len preto, aby vám pomocou Internetu vypol svetlo v spálni. Nemáte veľký majetok, nie ste významná alebo verejne známa osoba. Aké dôvody by potom viedli k napadnutiu akéhokoľvek inteligentného systému alebo IoT zariadenia, ktoré používate?

Odpovedí môže byť niekoľko. Za prvé, ak by niekto napadol domácnosť, pravdepodobne by nešlo o útok osobného charakteru. Útočníkovi by naozaj nešlo o to, aby mohol cudzím ľuďom vzdialene zapnúť a vypnúť svetlo. Mohol by ale využiť prítomné inteligentné zariadenia a pripojiť ich k veľkému Distributed Denial of Service (DDoS)[21] útoku na inú službu. DDoS útoky sú v dnešnej dobe veľmi často používané a verejnosť sa dozvedá len o malom percente z nich. A prečo sú tieto útoky na webové služby tak obľúbené? Vo vyhrotených prípadoch totiž stačí na pár minút znefunkčniť server konkurenčnej firmy, napríklad portál pre predaj leteniek, lístkov na koncerty a pod. a zákazníci budú dobrovoľne prinútení prejsť ku konkurencii. DDoS útoky sa dajú objednať na tzv. darknete[22] a v roku 2017 boli dostupné už za 7500$ na hodinový útok.

Druhým dôvodom na napadnutie domácnosti môže byť snaha o krádež. Keď sa útočník dostane do vašej vnútornej siete vďaka slabému zabezpečeniu a je schopný odchytávať a

[21] útok na webovú službu alebo server, ktorého cieľom je znefunkčniť alebo zneprístupniť túto službu používateľom

[22] čierny trh Internetu. Stránky, ktoré nie sú bežne prístupné verejnosti

ukladať dáta z vašich zariadení, vie si rýchlo urobiť obrázok napríklad o tom, kedy ste doma, prípadne aké všetky zariadenia doma máte a ukradnúť aj niektoré osobné údaje. Tieto informácie potom môže využiť buď sám alebo ich niekomu predať.

5.1.2 Napadnutie firmy

Väčšina útokov má finančné dôvody. Útočník môže cieliť priamo na peniaze alebo dáta prístupné vo firme, alebo sa snažiť niekoho poškodiť nepriamo. Útok na hotel, z ktorého sa na nejakú dobu stane nepríjemné alebo neobývateľné miesto (napríklad ak útočník bude náhodne prenastavovať a ovládať svetlá, termostat, žalúzie, klimatizáciu a podobne) znamená okamžitý odliv zákazníkov. Útok na administratívnu budovu znamená veľké finančné náklady danej firmy, ktorá musí pozastaviť na pár hodín svoju činnosť. Útok na továreň pozastaví samotnú výrobu. A útok na budovu a systémy napríklad banky, to snáď ani nemusím vysvetľovať.

Okrem útokov na firmy, ktoré v inteligentných budovách sídlia a systémy používajú, sa môžu diať aj útoky, ktoré majú poškodiť priamo firmu, ktorá inteligentné a automatizačné systémy poskytuje. Ak systém firmy nebude dôveryhodný a bude mať časté výpadky, zákazník sa radšej obráti na konkurenciu.

Zatiaľ sa v médiách hlavných prúdov nešíria vo veľkom správy o útokoch, ktoré boli vymenované, a tak toto celé môže znieť len ako paranoja. Faktom ale je, že čím viac budov s inteligentnými systémami bude existovať, tým väčšie riziko útokov bude nastávať, a to obzvlášť vtedy, ak sa nebude nijak zlepšovať zabezpečenie zo strany výrobcov alebo prevádzkovateľov.

5.1.3 Napadnutie mesta

Útoky na mesto ohrozujú najväčší počet ľudí. Nemusí ísť nutne o ohrozenie života, ale o narušenie bežnej činnosti, narušenie činnosti firiem alebo znepríjemnenie pobytu. V niektorých prípadoch ale môžu byť priamo alebo nepriamo ohrozené aj životy obyvateľov.

Podľa predpokladov bude v roku 2018 v inteligentných mestách celosvetovo použitých 2.3 miliardy zariadení (to je 42% nárast oproti roku 2016)[17]. Nárast všetkých týchto technológií rapídne zvýši riziko útokov. Nárast kybernetických útokov bol z počtu 200 v roku 2012 až 300 v roku 2015 (a to sú len známe útoky)[18]. Môžeme predpokladať, že toto číslo bude stúpať. Mestá sa stanú zraniteľné, pretože takmer každé zariadenie v nich bude mať v sebe nejaký druh firmware alebo software, a bude pripojené k nejakej sieti.

Ako príklad môžeme uviesť viacmenej neškodný nedávny útok na sieť v Dallase[18]. Útočník zduplikoval rádiový signál, ktorý spúšťa sirénu (varovanie pred tornádom) a spustil 156 mestských sirén až 15 krát po sebe uprostred noci. Toto spôsobilo veľké zvýšenie počtu hovorov na tiesňovú linku, ktorá bola preťažená a mohlo sa stať, že ak sa v tom čase stala vážna nehoda, linka by nespracovala hovor včas. Mesto muselo celý systém vypnúť a trvalo im celý víkend, kým dali systém znova dohromady a pridali vrstvu zabezpečenia (dočasne) a šifrovania k vysielačom signálu, vďaka čomu ich napadnutie už nebude tak ľahké. Na prvý pohľad je teda tento útok neškodný, pretože „len spustil sirénu“, ale tu môžeme vidieť, že mesto ako živý organizmus je ohrozené viacerými spôsobmi, nie len priamym útokom.

Ďalším príkladom, ktorý mohol byť nebezpečnejší, ale skončil bez vážnych následkov, je prípad z roku 2008, kedy sa 14 ročný chlapec zmocnil ovládania električkovej siete v Poľskom meste Lodz a spôsobil tak chaos a vykoľajenie 4 električiek[19]. Polícií uviedol, že zmenil nastavenia systému len ako žart. Desivá časť tohoto príbehu nie je to, čo sa stalo, ale to, že bolo možné, aby sa to stalo tak ľahko. Ale toto bol prípad teenagerského samostatného „útočníka“, ktorému o žiadne reálne poškodenie nešlo.

Oveľa nebezpečnejšie sú prípady z rokov 2015 a 2016 týkajúce sa masívnych výpadkov elektrickej energie na Ukrajine[20][23]. Prípady boli podrobne vyšetrované a zistené už boli mnohé technické detaily, ale konkrétny útočník, ani spôsob napadnutia zatiaľ nebol určený. Niektoré stopy vedú k ruským hackerským skupinám. Bol analyzovaný použitý malware, ktorý spôsobil odstavenie power gridu v Kyjeve na niekoľko hodín. V roku 2015 bol použitý malware pomenovaný BlackEnergy trójan, ktorý napadol niekoľko ukrajinských spoločností naraz. Podľa správ mal slúžiť len k špionáži, ale ukázalo sa, že toho vie viac. Neskôr sa potvrdila spojitosť s použitím malware KillDisk. V Decembri roku 2016 bol ale použitý úplne iný druh malware nazvaný Industroyer, ktorý mieril priamo na power grid. Je to modulovateľný druh malware, ktorý umožňuje útočníkom meniť ho „za pochodu“ a vyhýbať sa tak odhaleniu. Tento útok bol navyše navrhnutý priamo na eletrické siete s veľmi jasným cieľom, je však veľmi ľahko prispôsobiteľný k napadnutiu iných industriálnych systémov. Časť malware, ktorá je zodpovedná za vymazávanie dát a systémov, bola podľa analýzy priamo určená pre produkty ABB. Komponenta DoS zas cieli priamo na Siemens SIPROTECT.

Nebezpečenstvo Industroyera je vo fakte, že využil existujúce protokoly pre systémy Supervisory Control and Data Acquisition (SCADA) presne tak, ako boli navrhnuté. Problém týchto protokolov je, že boli navrhnuté pred desiatkami rokov, a v tom čase boli industriálne systémy izolované od sveta. Pri návrhu týchto protokolov sa nemyslelo na všeobecné zabezpečenie. Útočníci v tomto prípade nemuseli hľadať diery a zraniteľnosti daných systémov, stačilo im, aby sa malware správal presne podľa daného protokolu.

5.2 Riziká v inteligentných mestách

- Neotestované programy a systémy - bohužiaľ, často sa stáva, že mestá implementujú málo alebo vôbec neotestované riešenia. Napríklad výskum v USA odhalil, že viaceré mestá (napr. Chicago, New York a i. používajú zraniteľný systém na ovládanie signalizačných dopravných svetiel[22]).

- Chabá alebo neexistujúca ochrana (zabezpečenie) - predajcovia často tvrdia, že ich zariadenia majú špičkové zabezpečenie, ale v skutočnosti to tak byť nemusí. Je to časté najmä pre zariadenia IoT (Internet of Things), a prekvapivo aj pre priemyselné zariadenia. Táto prax sa môže dostať aj do mestského vybavenia.

- Nešifrovaná komunikácia a dáta - väčšina nových zariadení funguje pomocou bezdrôtovej komunikácie, ktorá je ľahšie napadnuteľná, ako káblové pripojenie. Niektoré systémy neponúkajú možnosť šifrovania, ale tie, ktoré áno, je nutné správne nakonfigurovať.

- Nedostatok tímov Computer emergency response team (CERT) - tímy ľudí, ktoré sa majú starať o IT bezpečnosť. Problémom je, ak takýto tím neexistuje, alebo ak nefun-

guje zdieľanie dôležitých informácií a dát medzi tímto oficiálnym tímom a vojenskými alebo inými vládnymi jednotkami.

- Veľký priestor pre útoky - inteligentné mestá sú v podstate neprebádaná oblasť. Ponúkajú zdanlivo nekonečný priestor pre útočníkov a druhy útokov. Ovplyvňujú veľké množstvo ľudí a zariadení a môžu tak mať nečakané dopady.
- Neaktualizované systémy - niektoré staršie systémy už nejde aktualizovať, niektoré je drahé aktualizovať, a niektoré zostávajú neaktuálne len kvôli lenivosti správcov. Avšak zraniteľnosti a útoky založené na dierach v starých verziách software/firmware sú jednými z najčastejších.
- Chyba v systéme - Aj malá chyba v rozsiahlom systéme môže spôsobiť veľké problémy.
- Riziko DoS útoku (Denial of Service) - v súčasnosti veľmi častý druh útoku, kedy sa cieľový server alebo služba zahltí sieťovými požiadavkami, na ktorých spracovanie nemá kapacitu, a služba sa tak stane na určitú dobu nefunkčnou. Špecifikom DoS alebo DDoS (Distributed Denial of Service) sú útoky z tzv. botnetov, čo sú siete obsahujúce tisíce uzlov, od počítačov až po smart televízie. Majitelia zariadení často nemusia tušiť, že sú časťou takéhoto botnetu, ale môžu tak nechcene pomáhať útočníkom.
- Nedostatok plánov pre postup pri útoku a výnimočnej situácii.
- Obchodné značky alebo výrobcovia, ktorí bránia bezpečnostnému výskumu kvôli strachu z konkurencie.
- Napadnutie služby Software as a service (SaaS), ktorú využíva mesto - riziko, ak mesto využíva služby tretích strán. Dnes je to v praxi viac než bežné, že aj kľúčové časti infraštruktúry riešenia sa outsourcujú do spoločností, ktoré za danú službu odborne zodpovedajú.
- Nevzdelaný personál - nebezpečný ľudský faktor, ktorý môže dať dôležité prístupové informácie nesprávnym osobám, používať slabé heslo k prístupu do kľúčovej služby, alebo sám nechtiac nainštalovať na nejaký PC malware, ako napr. aktuálne populárny ransomware.

Len počas písania tejto práce sa objavilo v médiách niekoľko nových zraniteľností a útokov na inteligentné systémy alebo zariadenia IoT po celom svete.

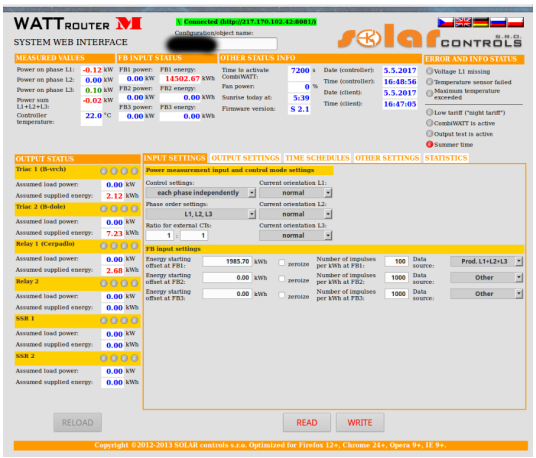
5.3 Riziká v ČR

Medzi veľké riziká patria už spomenuté SCADA systémy, ktoré sú často zastaralé a neaktualizované. Dobrou správou je, že už aj u nás vzniká snaha firiem zabezpečiť svoje vlastné systémy, a niektoré firmy sa priamo na penetračné testovanie a následné zabezpečenie špecializujú. Útokov alebo pokusov o útok v ČR je podľa zdroja na serveri lupa.cz až niekoľko tisíc ročne. „Lidé, kteří se SCADA technologiemi pracují, byli dlouho přesvědčení, že se jich bezpečnostní hrozby příliš netýkají, protože jde o takzvané ostrovní instalace," navazuje Uher. To zjednodušeně řečeno znamená, že SCADA většinou běží jako izolovaná síť a systém

bez vnějšího přístupu. I zde se ovšem objevují do očí bijící rizika. K systémům je obvykle možné připojení i přes vzdálený přístup. Dodavatelé a partneři jej často mezi sebou sdílejí, protože je to rychlejší. Poměr může být i deset ku jedné."[11]

To ale nie sú jediné útoky. Podľa aktuálnych dát čelila nejakému druhu kybernetického útoku každá tretia firma v ČR, najviac hlásení podali firmy z oblastí energetiky, financí a výroby[24]. Tieto útoky zatiaľ neboli zamerané na inteligentné systémy.

Pre konkrétnejšiu predstavu o nebezpečenstve nezabezpečených systémov uvediem ako ďalší príklad nezabezpečené systémy pre ovládanie solárnych systémov v rodiných domoch a iných súkromných inštaláciách. Server shodan.io[23] sa zaoberá zhromažďovaním a upozorňovaním na nezabezpečené a verejne prístupné systémy po celom svete, od webových kamier až po industriálne systémy. Na tomto serveri bolo k 31.5.2017 až 13 nezabezpečených webových systémov na ovládanie solárnych panelov a ich funkcií. Znamená to, že ktokoľvek z celého sveta je schopný tieto nastavenia, možno aj omylom, zmeniť. Kontréne stránka na obrázku bola verejne prístupná z internetu a úpravy povoľovala pod prednastaveným menom "admin" a heslom "1234".



Obr. 5.1: Webový portál na ovládanie solárnych panelov

5.4 Druhy útokov

Útoky na inteligentné systémy sa nelíšia od známych druhov útokov na počítače a siete. Dajú sa rozdeliť na pasívne a aktívne:

- **aktívne** - DoS, MITM, spoofing, hijacking
- **pasívne** - odpočúvanie, skenovanie portov, sniffing

[23] https://www.shodan.io/

5.4.1 Man in the middle (MITM)

V doslovnom preklade **muž v strede** je druh útoku, kde útočník potajme prenikne do komunikácie medzi dvomi subjektmi. Subjekty veria, že komunikujú priamo spolu, ale útočník môže sledovať, odpočúvať alebo meniť prebiehajúcu komunikáciu.

Môže sa jednať o útok fyzický, kde sa útočník sústreďuje na prenosové médium: káble, bezdrôtovú komunikáciu alebo na aktívny sieťový prvok (ako je napríklad hub, switch, router a iné). Útočník sa tak fyzicky pripojí do siete a môže odpočúvať komunikáciu, môže sa snažiť prelomiť šifrovanú komunikáciu pomocou podvrhnutia certifikátu SSL, alebo môže sieťové prvky donútiť, aby všetku komunikáciu presmerovali na neho, tzv. ARP poisoning.

Ďalšou formou môže byť útok pomocou malware nainštalovanom na zariadení, ktoré používa subjekt, ktorý o ňom nevie, a tento malware potom môže manipulovať s dátami a komunikáciou už na zariadení.

5.4.2 DNS spoofing

Domain Name Server (DNS) spoofing sa prekladá ako **podvrhnutie DNS** a znamená podstrčenie falošnej adresy IP nejakého doménového mena. Doménové mená sú ľudsky čitateľné názvy pre adresy IP, a tieto názvy spravujú rôzne servery. Ľudia si nebudú pamatať, že 8.8.8.8 je IP adresa pre google.com, ale zapamätajú si práve názov google.com. Toto spárovanie medzi číselnou adresou a určitým menom zabezpečuje DNS server. Ak útočník podvrhne užívateľovi svoj vlastný DNS server, užívateľ tak môže byť presmerovaný na falošné webové stránky, napríklad stránky, ktoré vyzerajú ako presná kópia Facebooku alebo prihlásenia do internetového bankovníctva. Tým môže útočník nie len vylákať heslo a prístupové údaje, ale môže takto podsunúť do počítača používateľa malware tým, že ho presmeruje na falošnú stránku, z ktorej si používateľ stiahne sám program, ktorý bude infikovaný malwareom.

5.4.3 Denial of Service (DoS)

DoS v preklade **odopretie služby** je útok na webovú službu alebo server, ktorého cieľom je znefunkčniť alebo zneprístupniť túto službu používateľom. Útočník môže využiť chybu systému alebo zahltiť systém nadmerným množstvom požiadaviek. Prejaviť sa to môže spomalením služieb a systému alebo úplným odoprením služieb pre používatelov a enormným množstvom spamu a chybových hlásení pre administrátorov systému.

5.4.4 Distributed Denial of Service (DDoS)

DDoS je **distribuovaný DoS** útok. To znamená, že útočník využije nie jeden, ale niekoľko počítačov, v niektorých prípadoch aj tisícky počítačov a rôznych zariadení s prístupom na Internet, aby útočili. Majitelia daných strojov nemusia vedieť o tom, že tvoria súčasť takejto siete a že sú ich prístroje zneužívané. Tie môžu byť buď infikované nejakým malwareom, ktorý obsahuje inštrukcie k útoku, typicky IP adresu cieľa a dátum a čas spustenia, alebo môžu byť pripojené k tzv. botnetu. Botnet[24] je v tomto kontexte sieť počítačov alebo zariadení, ktoré sú infikované špeciálnym softvérom, pomocou ktorého sú ovládané a po príkaze

[24] označenie pre sieť internetových robotov, ktoré fungujú automaticky, https://cs.wikipedia.org/wiki/Botnet

k zahájeniu útoku na daný cieľ generujú obrovské množstvo požiadaviek, ktoré cieľový server nie je schopný spracovať. DDoS útok je zložitejší na odhalenie a obrana voči nemu je náročnejšia. Útočník, ktorý ovláda tisíce počítačov, môže silu útoku škálovať, a tak po prvých minútach, kedy cieľový server zaregistruje útok a zvýši prenosovú kapacitu siete, môže kapacitu útoku zvýšiť aj útočník.

Špeciálnym druhom DDoS je **Reflected/Spoofed Dos**, v preklade **Odrazený/Podvrhnutý DoS**, skratkou DRDoS. Útočník rozpošle podvrhnuté požiadavky na veľké množstvo počítačov. Bežné správanie počítačov je na požiadavku odpovedať podľa zdrojovej adresy požiadavku, ale táto adresa je v prípade útoku podvrhnutá a nahradená adresou cieľa. Cieľ je tak zasiahnutý tisíckami odpovedí na tieto požiadavky.

5.4.5 Eavesdropping

V preklade **odpočúvanie** je útok, pri ktorom sa jedná o tajné odpočúvanie cudzej komunikácie pomocou technických prostriedkov, bez vedomia jej účastníkov.

5.4.6 Phishing, Pharming

Obidva tieto útoky sa zameriavajú na získanie prihlasovacích údajov, čísel platobných kariet a iných citlivých údajov podvodnými metódami. **Phishing** sa snaží vylákať tieto údaje z používateľa prostrednístvom falošných emailov nabádajúcich k zmene hesla alebo zadaniu hesla alebo pomocou webových stránok, ktoré žiadajú o zadanie nejakého citlivého údaju. Po zadaní údaju stránka môže presmerovať používateľa na skutočnú stránku, takže si ani nemusí všimnúť, že práve odhalil svoje dáta útočníkovi.

Pharming sa snaží ukradnúť dôverné informácie používateľov skrz ovládnuté webové stránky. Rozdiel oproti phishingu je ten, že útočník nevytvára falošné stránky ani falošné požiadavky na zadanie citlivých údajov, ale presmerováva obsah skutočných webových stránok.

5.4.7 Ransomware

Ransomware, v preklade **vydieračský program** je špeciálny druh škodlivého programu, ktorý zablokuje počítačový systém alebo zašifruje uložené dáta a na obnovenie dát požaduje od svojej obete výkupné. Tým sa dá považovať za špecifický druh útoku na systém. V posledných rokoch sú útoky pomocou rôznych ransomware rozšírené a nenapadajú už len počítače samotné, ale môžu napadnúť aj inteligentné televízie a iné pripojené zariadenia. Čiastky, ktoré útočník požaduje zaplatiť, nemusia byť vysoké, pretože cieli na obrovské množstvo ľudí, preto majú niektoré obete ransomware tendenciu zaplatiť. Avšak to nemusí garantovať, že svoje dáta dostanú späť.

„Napadá ransomware i mou platformu? Ano. A pokud ne dnes, poptejte se zítra.“ [25]

Ransomware sa do systému môže dostať rôznymi spôsobmi, ako každý malware - prílohou v emaili, otvoreným portom v sieti, neaktualizovaným operačným systémom, infikovaným

[25] https://www.lupa.cz/clanky/ransomware-hrozba-na-vzestupu-nebylo-lepsi-kdyz-nam-viry-nedavaly-na-vyber/

dokumentom... kreativite útočníkov sa medze nekladú, o to ťažšia je obrana proti takémuto útoku. Jeho hrozba spočíva hlavne v tom, že sa môže po sieti rozšíriť na dôležité systémy a zablokovať napríklad ovládanie nemocničného systému alebo systému riadenia dopravy, ak sú tieto pripojené k Internetu. O to dôležitejšia je správna konfigurácia takto dôležitých sietí a zamedzenie fyzických prístupov k týmto počítačom neautorizovaným osobám.

Kapitola 6

Experiment

Hlavné nebezpečenstvo dnešných a starších inteligentných inštalácií spočíva v tom, že protokoly, na ktorých fungujú, nepredpokladajú pripojenie do Internetu a nepredpokladajú ani to, že by mal niekto motiváciu na ne útočiť. Používanie nešifrovaného prenosu komunikácie, žiadne zabezpečenie heslom, priame prepojenie systému s Internetom, fyzicky nezabezpečené prenosové médiá a ovládacie prvky alebo iné nedostatky umožňujú určitý druh napadnutia systému vykonať aj človeku bez hlbších technických znalostí. Preniknúť do počítačového systému alebo elektroinštalácie a manipulovať s dátami je podľa Trestného zákoníka ČR trestné a pri odhalení útočníka je možné ho potrestať odňatím slobody až na 3 roky, zákazom činnosti alebo prepadnutím veci.[16] Útočník ale vôbec nemusí byť vystopovateľný a dostihnutý.

Preto je experiment pre túto prácu testovaný na vlastnej malej inštalácií vytvorenej len pre tento účel. Použité sú prvky pracujúce na protokole KNX/EIB, ktorý sa radí medzi najpoužívanejšie otovrené protokoly na svete. Inštalácia obsahuje 4 prvky a jedno koncové zariadenie, ktoré slúži pre lepšiu predstavu, ako sa útok na systém môže priamo prejaviť.

Experiment je zameraný na dokázanie toho, že sa do siete môže ľahko dostať aj lajk a stačí mu na to prístup k vyhľadávaniu na Internete.

6.1 Testovacia inštalácia

Testovacia sústava pozostáva zo 4 prvkov HDL KNX/EIB, a to:

1. Modul zdroja napájania 960 mA HDL-M/P960.1[26]
2. Modul výkonového relé HDL-M/R4.10.1 [27]
3. Modul brány Ethernet KNX IP Router M/IPRT.1 [28]
4. Ovládací panel DLP, EU, s LCD, HDL-M/DLP04.1-48[29]

[26] https://b2b.hdl-automation.cz/cz/produkty/knx/napajeci-zdroje/hdl-m-p960-1
[27] https://b2b.hdl-automation.cz/cz/produkty/knx/spinace/hdl-m-r4-10-1
[28] https://b2b.hdl-automation.cz/cz/ke-stazeni/katalogove-listy/knx/komunikacni-brany/m-iprt-1-cz
[29] https://b2b.hdl-automation.cz/cz/produkty/knx/uzivatelska-rozhrani/dlp-panely/hdl-m-dlp04-1-48

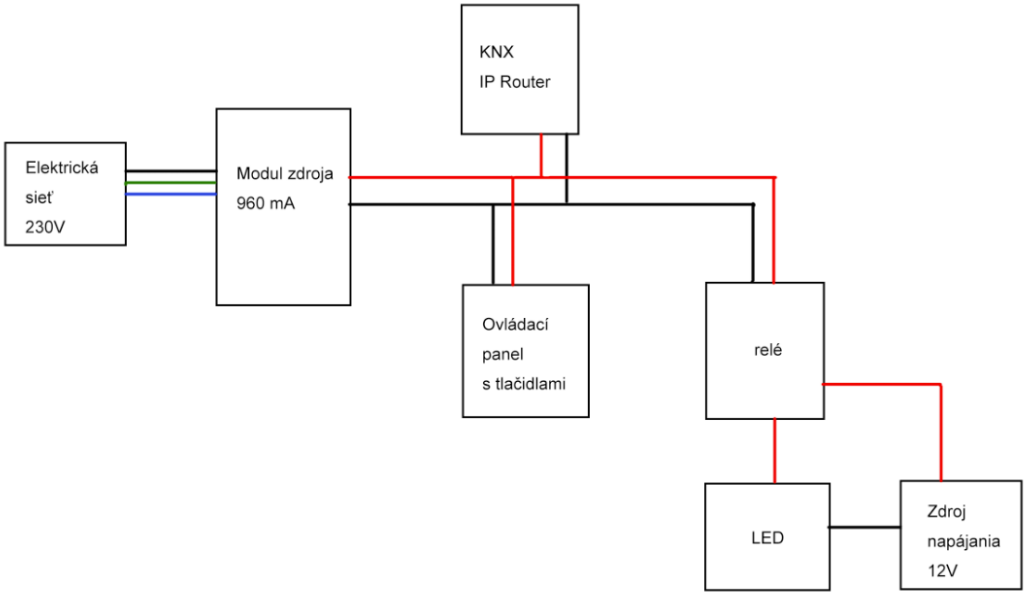
Obr. 6.1: Prvky použité v testovacej inštalácii

Schému zapojenia môžeme vidieť na obrázku. Na relé je pripojené LED osvetlenie so samostatným napájaním 12V, ktorá je príkladom koncového ovládaného prvku spotrebiča z reálneho života.

Aby systémom prúdili dátové telegramy, bolo nutné previesť nastavenie systému pomocou oficiálneho programu ETS od KNX, ktorý je v obmedzenej verzii po registrácií na stránkach[30] organizácie knx prístupný zdarma. Rozhranie programu ETS je prehľadné, ale pre správne nastavenie bol potrebný podrobnejší manuál.

Aby bolo možné programovať prvky v ETS, je nutné mať konfiguračné katalógové súbory ku každému zariadeniu. Tieto súbory dodáva vždy konkrétny výrobca (v tomto prípade firma HDL[31]) a tie je nutné naimportovať do programu ETS. Potom sa určí fyzické umiestnenie zariadení v budove a ich topológia,čím zariadenia dostanú pridelené svoje fyzické adresy. Následne sa nastavia požadované parametre správania každého zariadenia a ich interakcie medzi sebou. Príklad: tlačidlo na krátke stlačenie svetlo zapne, a na dlhé stlačenie svetlo vy-

[30] https://my.knx.org/
[31] https://www.hdl-automation.cz/



Obr. 6.2: Schéma zapojenia testovacej inštalácie

pne. Ak sa začnú sťahovať vonkajšie žalúzie, svetlo sa zapne. Ak sa otvorí okno, klimatizácia sa vypne.

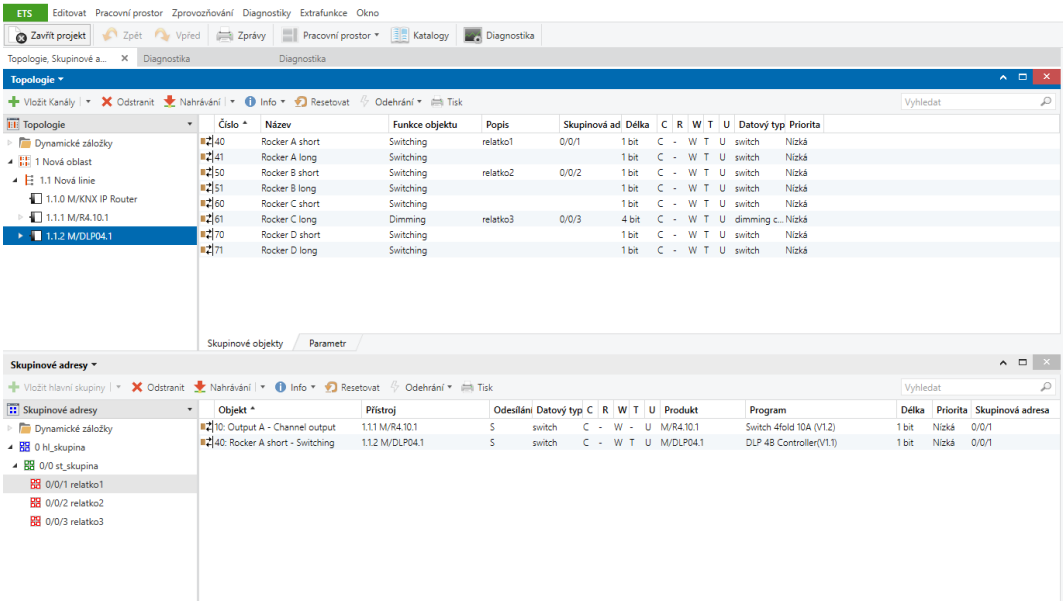
Naprogramovali sme ovládací panel s LCD displejom tak, aby na stlačenie prvého ľavého tlačidla spojil kontakty relé na kanáli A, na ktorý je pripojené LED osvetlenie. Druhé tlačítko spínalo kanál C, takisto stisknutím ľavého tlačidla, a pravé tlačidlo ho rozpojilo. Prvé tlačidlo ovládacieho panela a kanál A v relé interagovali spolu, obidva prvky mali rovnakú skupinovú adresu 0/0/1. Kanál C a druhé tlačidlo dohromady mali skupinovú adresu 0/0/2. Naproti tomu fyzická adresa relé bola 1.1.1 a ovládacieho panela s tlačidlami 1.1.2. KNX IP Router umožnil pripojiť sa do siete skrz Ethernet a nahrať konfiguráciu do zariadení. Mal fyzickú adresu 1.1.0, ale v tomto prípade nemal pridelenú žiadnu skupinovú adresu, pretože sa na interakcii medzi relé a tlačidlom sám nepodieľal. Adresáciu zariadení môžeme vidieť na obrázku č.6.3.

Týmto bola minimalistická testovacia inštalácia funkčná a pripravená.

6.2 Príprava na útok

Príprava spočívala v prehľadávaní internetu a hľadaní návodov a inšpirácií na to, ako sa pripojiť ku KNX sieti a ako ju začať ovládať, sa našlo niekoľko. Nakoniec som zvolila dva rôzne prístupy, ktoré ponúkali najjednoduchší postup pripojenia, jeden aplikovaný pomocou operačného systému Windows a druhý pomocou systému Raspbian, distribúcie GNU/Linux určenej pre malé počítače Raspberry Pi[32].

[32]https://www.raspberrypi.org/



Obr. 6.3: Konfigurácia zariadení KNX v programe ETS verzie 5

Bolo nutné stiahnuť si voľne dostupné programy Wireshark[33], Net'n Node[34] pre Windows, a programy eibd[35] a knxmap[36] pre operačný systém linux.

Okrem toho bolo je výhodné vedieť aspoň základy fungovania systému KNX, napríklad, že zariadenia sú adresované pomocou trojčíselnej fyzickej alebo skupinovej adresy, fyzická adresa je oddelená bodkami (1.1.1) a skupinová je delená lomítkom (0/0/1), že si posielajú dáta vo forme telegramov a ako približne telegram vyzerá.

6.3 Prienik do systému

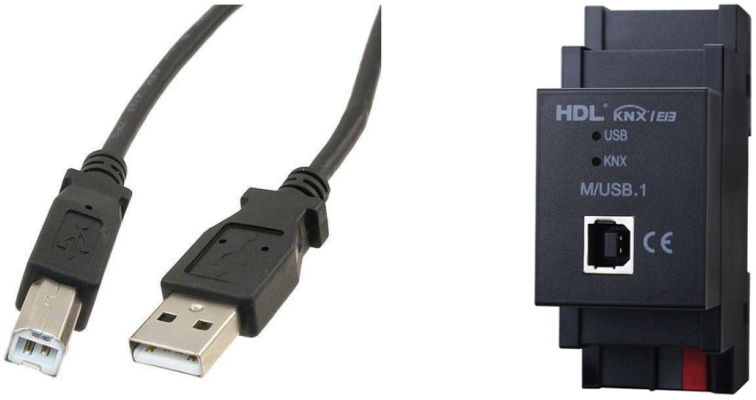
6.3.1 Windows

Prienik do testovacieho systému pomocou operačného systému Windows už ani nemôže byť jednoduchší.

Na začiatok je potrebný fyzický prístup ku kabeláži KNX. Ideálnym vstupným bodom je KNX IP Router, pod ktorým by mali byť pripojené zariadenia v miestnosti. Obvyklá topológia systému je zobrazená v kapitole 3 v podrobnostiach systému KNX.

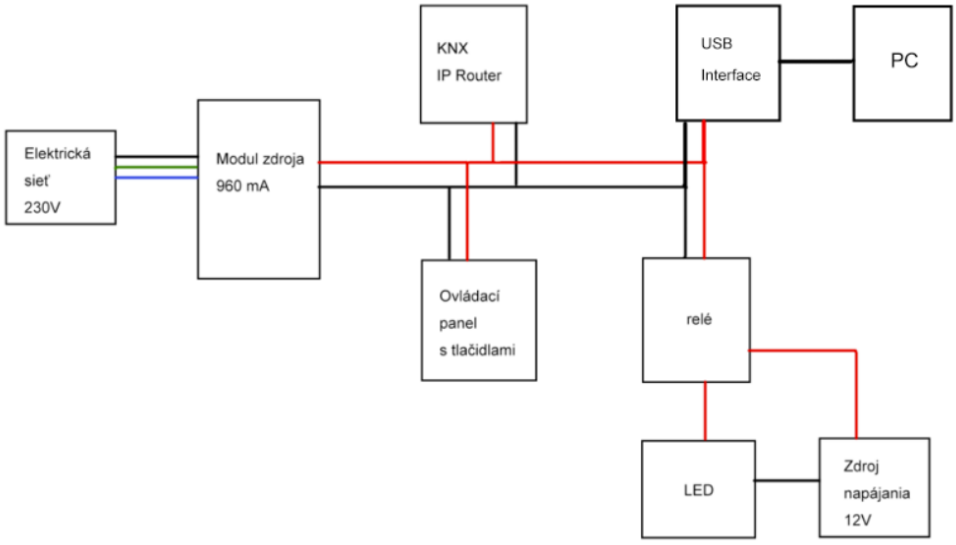
V prípade, že KNX IP router nie je k dispozícií, je možné pripojiť sa napojením páru vodičov krútenej dvojlinky priamo na krútenú dvojlinku vedúcu od koncového zariadenia v miestnosti a použiť vlastné zariadenie, napríklad KNX USB Interface, ktoré prepojíme s vlastným počítačom pomocou kábla typu USB/B.

[33] https://www.wireshark.org/
[34] https://www.weinzierl.de/index.php/en/all-knx/software-tools-en/net-n-node-en
[35] https://sourceforge.net/projects/bcusdk/
[36] https://github.com/takeshixx/knxmap/



Obr. 6.4: Kábel typu USB/B a zariadenie KNX USB Interface

V tomto prípade bola použitá krútená dvojlinka pripojená do kabeláže a ako prepojenie medzi inštaláciou KNX a počítačom je použité zariadenie KNX USB Interface[37]. Toto zariadenie je pripojené k počítaču pomocou kábla USB/B.



Obr. 6.5: Prepojenie inštalácie s PC s použitím prvku USB Interface

Nasledujúce kroky sú jednoduché a nevyžadujú žiadne extra znalosti systému:

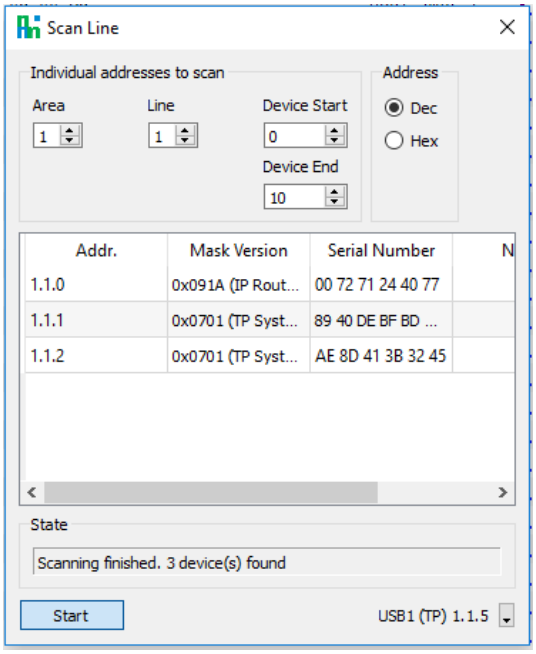
1. Otvoriť program **Net'n Node**
2. Vybrať rozhranie, cez ktoré sa chcem pripojiť, v tomto prípade je to KNX USB Interface. Program je schopný detekovať ho sám
3. Kliknúť na tlačidlo **Open**, ktoré otvorí prepojenie medzi počítačom a KNX

[37] http://www.hdlautomation.ca/product/knx-usb-interface/

4. Nájsť nástroj, ktorý dokáže urobiť sken sieťe. V hlavnej ovládacej lište programu je k dispozícii pod **Tools -> Scan Line**

5. Pustiť sken siete. V možnostiach skenu je treba nastaviť trojčíselné fyzické adresy, ktoré by sa mohli v sieti nachádzať a ktoré sa majú prehľadávať. Keďže je zvykom číslovať zariadenia od 0, zvolíme 0 ako začiatok a 10 ako konečné skenované číslo.

6. Kliknúť na tlačidlo **Start** a spustiť sken



Obr. 6.6: Zariadenia nájdené v sieti

Na obrázku vidíme, aké výsledky nám ukázal náš sken. Hneď pod fyzickou adresou 1.1.0 je pripojený KNX IP Router. Pod adresou 1.1.1 a 1.1.2 vidíme ďalšie 2 zariadenia, ktoré majú uvedenú fyzickú adresu, ale nevieme, o aké zariadenia sa jedná a aké sú ich skupinové adresy.

7. Vyvoláme akciu v sieti, napríklad stlačením tlačidla, ktoré zapne svetlo

8. Sledujeme telegramy, ktoré prechádzajú sieťou. Teraz je jasne vidieť, ktoré zariadenie posiela príkaz (stĺpec **Src-Addr**) a aká skupinová adresa príkaz prijíma (stĺpec **Dest-Addr**)

9. Vyskúšame vyvolať čo najviac akcií v sieti. Vidíme, že druhé tlačidlo je spojené s inou skupinovou adresou, než prvé. (Pomocou tohto postupu môžeme odhadnúť aj ďalšie skupinové adresy zariadení v inej línii, pretože väčšie systémy sa adresujú čo najprehľadnejšie. Zariadenia sú adresované trojčíslím X/Y/Z, kde prvé dve čísla označujú líniu, na ktorej sa zariadenie nachádza, napr. miestnosť alebo chodbu a posledné číslo je väčšinou identifikátor konkrétneho zariadenia. Vedľašia miestnosť môže používať adresy 0/1/1 atď.)

Num	Telegram	Interface	Timestamp	Service	Src-Addr	Dest-Addr	Control	Prio	H-Cnt	TPC
0001	29 00 BC E0 11 02 00 01 01 00 81	USB1 (TP) 1....	2018-05-27 02:02:22...	L-Data.ind	1.1.2	0/0/1	S	lo	6	U-D
0002	29 00 BC E0 11 02 00 01 01 00 80	USB1 (TP) 1....	2018-05-27 02:02:23...	L-Data.ind	1.1.2	0/0/1	S	lo	6	U-D
0003	29 00 BC E0 11 02 00 02 01 00 81	USB1 (TP) 1....	2018-05-27 02:02:24...	L-Data.ind	1.1.2	0/0/2	S	lo	6	U-D
0004	29 00 BC E0 11 02 00 02 01 00 80	USB1 (TP) 1....	2018-05-27 02:02:24...	L-Data.ind	1.1.2	0/0/2	S	lo	6	U-D
0005	29 00 BC E0 11 02 00 02 01 00 81	USB1 (TP) 1....	2018-05-27 02:02:32...	L-Data.ind	1.1.2	0/0/2	S	lo	6	U-D
0006	29 00 BC E0 11 02 00 02 01 00 80	USB1 (TP) 1....	2018-05-27 02:02:33...	L-Data.ind	1.1.2	0/0/2	S	lo	6	U-D
0007	29 00 BC E0 11 02 00 01 01 00 81	USB1 (TP) 1....	2018-05-27 02:02:33...	L-Data.ind	1.1.2	0/0/1	S	lo	6	U-D
0008	29 00 BC E0 11 02 00 01 01 00 80	USB1 (TP) 1....	2018-05-27 02:02:34...	L-Data.ind	1.1.2	0/0/1	S	lo	6	U-D

Obr. 6.7: Telegramy prúdiace KNX sieťou pri vyvolaní akcie stlačením tlačidla

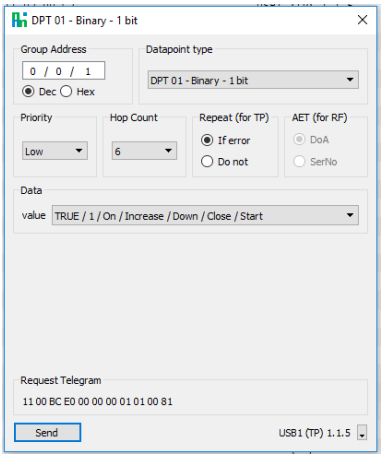
10. Musíme vyhľadať v ponuke nástrojov funkciu, ktorá bude obsahovať kľúčové slovo Send alebo Write. V našom prípade je to **Send KNX** -> **Group Value Write**

11. Vyskúšame hneď prvú možnosť, DPT 01 Binary 1 Bit, a to preto, že vidíme, že pri posielaní signálu zapnutia a vypnutia z tlačidla sa mení len jeden koncový bit telegramu, zbytok telegramu je vždy rovnaký

12. Nastavíme potrebnú skupinovú adresu, v tomto prípade 0/0/1

13. V riadku **value** vyberieme možnosť, ktorá obsahuje slovo „ON“ alebo „start“, pretože aktuálne je svetlo vypnuté a my ho chceme zapnúť

14. Skontrolujeme pripravený telegram, vidím, že posledná časť sa priamo zhoduje s telegramami, ktoré sme predtým odchytávali, a v tele telegramu sa líši časť označujúca adresy a druh telegramu. Klikneme na „Send“



Obr. 6.8: Dialóg pre poslanie vlastného telegramu prvku v KNX sieti

15. Svetlo sa zaplo. Sledujeme telegramy posielané v sieti, a vidíme, že komunikácia neprebehla medzi zariadením 1.1.2 a skupinovou adresou 0/0/1 ako predtým, ale telegram pochádza z nášho počítača na USB rozhranie[38] a smeruje na skupinovú adresu 0/0/1.

[38] USB rozhranie má nastavenú fyzickú adresu 1.1.5, ktorú sme mu ešte predtým nahrali pomocou voľne dostupného programu ETS. Snažili sme sa zvoliť adresu, o ktorej tušíme, že v sieti zatiaľ nie je použitá, to je v našom prípade malého množstva prvkov adresa s koncovkou 5

0081	KNX	29 00 BC E0 11 02 00 01 01 00 80	USB1 (TP) 1...	↑	2018-05-27 01:59:15...	L-Data.ind	1.1.2	0/0/1	S	lo	6	1
0082	KNX	29 00 BC E0 11 02 00 01 01 00 81	USB1 (TP) 1...	↑	2018-05-27 01:59:23...	L-Data.ind	1.1.2	0/0/1	S	lo	6	1
0083	KNX	29 00 BC E0 11 02 00 01 01 00 80	USB1 (TP) 1...	↑	2018-05-27 01:59:24...	L-Data.ind	1.1.2	0/0/1	S	lo	6	1
0084	KNX	11 00 BC E0 00 00 00 01 01 00 81	USB1 (TP) 1...	↓	2018-05-27 02:00:17...	L-Data.req	PC	0/0/1	S	lo	6	1
0085	KNX	2E 00 BC E0 11 05 00 01 01 00 81	USB1 (TP) 1...	↑	2018-05-27 02:00:17...	L-Data.con	1.1.5	0/0/1	S	lo	6	1
0086	KNX	11 00 BC E0 00 00 00 01 01 00 80	USB1 (TP) 1...	↓	2018-05-27 02:00:22...	L-Data.req	PC	0/0/1	S	lo	6	1
0087	KNX	2E 00 BC E0 11 05 00 01 01 00 80	USB1 (TP) 1...	↑	2018-05-27 02:00:22...	L-Data.con	1.1.5	0/0/1	S	lo	6	1

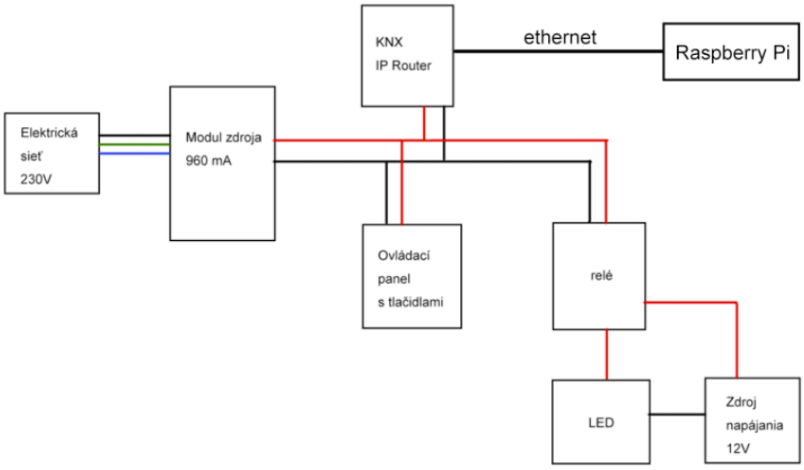
Obr. 6.9: Telegramy posielané z PC do siete KNX

16. Test bol úspešný, takto môžeme ovládať akýkoľvek prvok, ktorý v sieti detekujeme a sme schopní určiť jeho presnú skupinovú adresu.

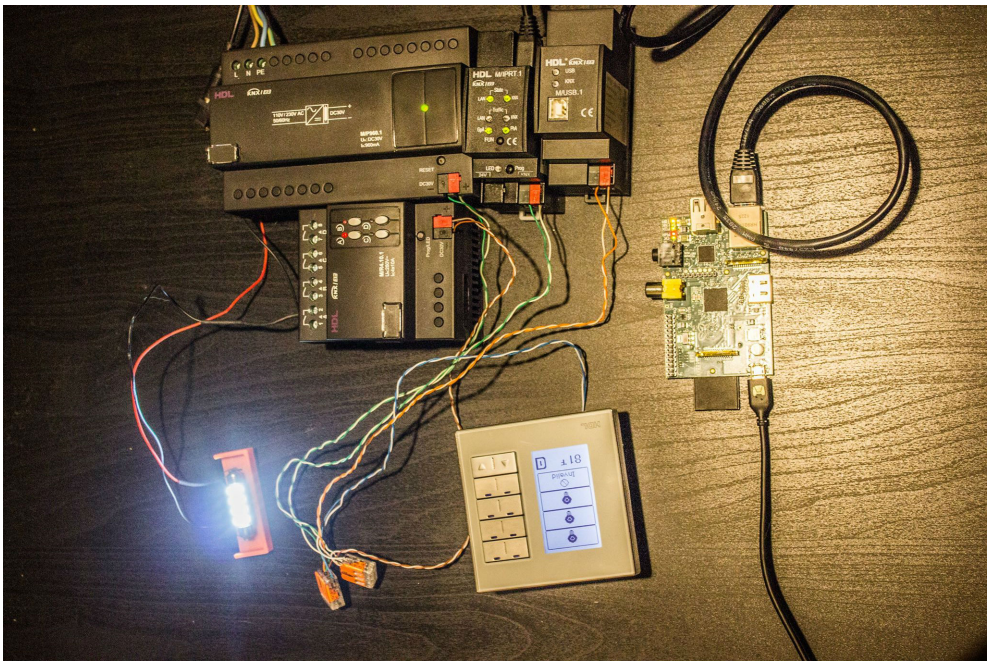
Podarilo sa nám dostať sa do systému a to iba s pomocou vlastného zariadenia s rozhraním a programu, ktorý je voľne dostupný na Internete. Celé prevedenie trvalo len niekolko minút, najviac času zaberie zorientovať sa v programe Net'n'node a ETS. Je možné, že reálny systém bude mať nastavenú autentifikáciu prvkov a používať autorizačný kľúč. V tom prípade môžeme vyskúšať zadať prednastavenú hodnotu 0xFFFFFFFF, alebo sa snažiť kľúč uhádnuť a prelomiť útokom. Takisto je možné zahltiť prístroj posielaním určitých dát, preprogamovaním prístroja (ak máme prístup k ETS, k programovaciemu tlačidlu na KNX prístroji, a nastavovanie prítrojov nie je nijak chránené heslom), posielaním dát application protocol control information (APCI), ale to všetko už vyžaduje viac času a snahy.

6.3.2 GNU/Linux na Raspberry Pi

Pre druhý pokus s inštaláciou sme vybrali malý počítač Raspberry Pi verzia z roku 2011, na ktorom je nahratý operačný systém Raspbian, konkrétne jeho staršia verzia Wheezy. K Rasperry sme pre ľahšie ovládanie pripojili externý monitor, ale je možné použiť Raspberry Pi (napríklad s integrovanou Wi-Fi kartou) a ovládať tento malý počítač vzdialene pomocou SSH bez nutnosti priameho pripojenia zobrazovacieho zariadenia.



Obr. 6.10: Schéma prepojenia inštalácie s Raspberry Pi



Obr. 6.11: Schéma prepojenia inštalácie s Raspberry Pi

Druhý pokus zabral o niečo viac času a vyžaduje základnú znalosť práce s príkazovým riadkom v systéme GNU/Linux.

Pred útokom bolo nutné stiahnuť a nainštalovať voľne dostupné programy, ktoré sú schopné pracovať s protokolom KNX, sú to napríklad program **eibd** alebo **knxd**, ktoré slúžia priamo na ovládanie siete KNX, ďalej program **Wireshark** s pluginom pre KNX, ktorý dokáže odpočúvať všetku komunikáciu v pripojenej sieti a dokáže rozpoznať KNXnetIP protokol, program **knxmap**, ktorý dokáže zmapovať pripojenú sieť KNX.

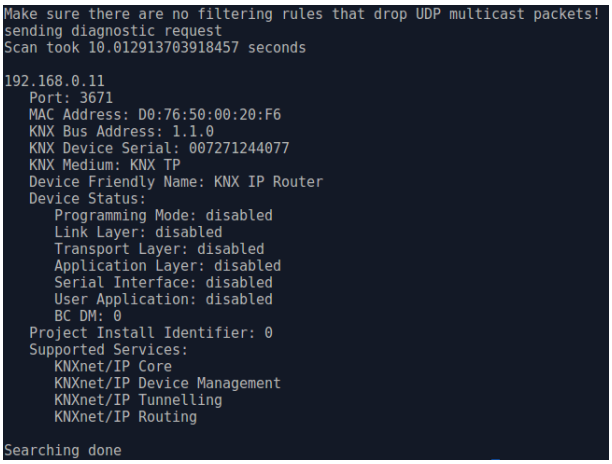
Zvolili sme inštaláciu programu eibd, ktorý bolo nutné stiahnuť a vyžadoval doinštalovanie niekoľkých knižníc a balíčkov navyše. Po stiahnutí všetkých potrebných komponent sa program skompiloval priamo na Raspberry Pi pomocou príkazov:

```
./configure
make
make install
```

Po úspešnej inštalácii stačí už len niekoľko krokov:

1. Pripojiť Raspberry pomocou sieťového káblu k Raspberry Pi
2. V príkazovom riadku spustiť program, ktorý detekuje prvky pripojené na rozhranie, napríklad **knxmap**, ktorému ako parameter nastavíme rozhranie ethernetu:

   ```
   knxmap -i eth0 search
   ```



Obr. 6.12: Výstup programu knxmap, ktorý našiel v sieti KNX IP Router

3. Program našiel jedno zariadenie, a to KNX IP Router

4. Z výstupu vyčítame IP adresu zariadenia KNX Routeru a túto adresu dopíšeme do konfiguračného súboru pre eibd

```
script
DAEMON_OPTS="-d -D -T -R -i -u --no-tunnel-client-queuing --eibaddr=0.0.1
ipt:192.168.0.11"
exec start-stop-daemon --start -c *eibd* --exec $DAEMON -- $DAEMON_OPTS
end script
```

5. Je nutné spustiť eibd. Ten sa pripojí na zadanú IP adresu KNX IP Routeru a na localhoste [39] vytvorí rozhranie na odpočúvanie dát z adresy 192.168.0.11.

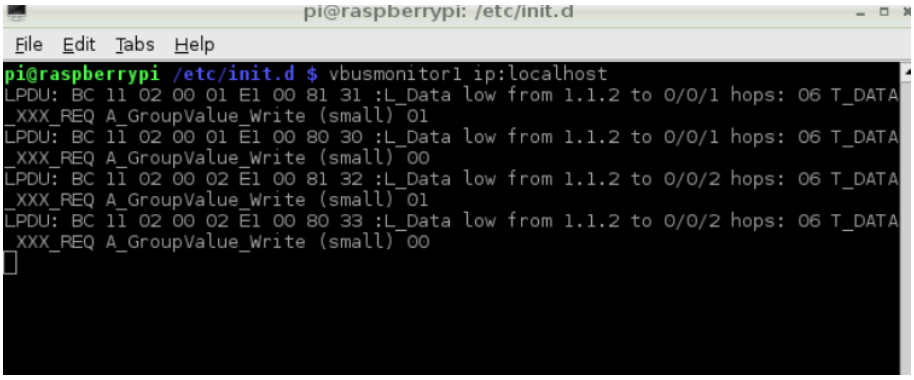
```
$ sudo initctl reload-configuration
$ sudo initctl start eibd
```

6. Ak všetko funguje správne, pokúsime sa zobraziť komunikáciu z KNX siete na zbernici pomocou príkazu:

```
vbusmointor ip:localhost
```

7. Vyvoláme akciu v sieti, napríklad rozsvietením a zhasnutím svetla. Pozorujeme telegramy, ktoré v sieti prúdia. Na obrázku 6.12 vidíme, že zariadenie s fyzickou adresou 1.1.2 posiela telegram do skupinovej adresy 0/0/1 a vidíme ako presne telegram vyzerá.

[39] localhost znamená práve používaný počítač, bežne má IP adresu 127.0.0.1



Obr. 6.13: Telegramy prebiehajúce v KNX sieti

Pripojenie ku KNX sieti a čítanie dát bolo úspešné. Ako by sme to mohli využiť? Program eibd ponúka niekoľko možností, napríklad funkciu **groupswrite**, ktorá po zadaní parametra skupinovej adresy pošle telegram na dané zariadenie (obdobne ako to urobil program Net'n'node pri prieniku z Windows).

Ale ak máme základné znalosti skriptovania, môžeme využiť jednoduchosť použitia programu eibd v príkazovej riadke a vytvoriť skript, ktorý bude telegramy posielať sám. Pre tento test sme zvolili jazyk Python, ktorý je jednoduchý aj pre začiatočníkov, a vytvorili sme krátky skript s názvom **knxhack.py**, ktorý dokáže zapnúť a vypnúť svetlo (Obr. 6.14).

Spustili sme skript pomocou príkazu

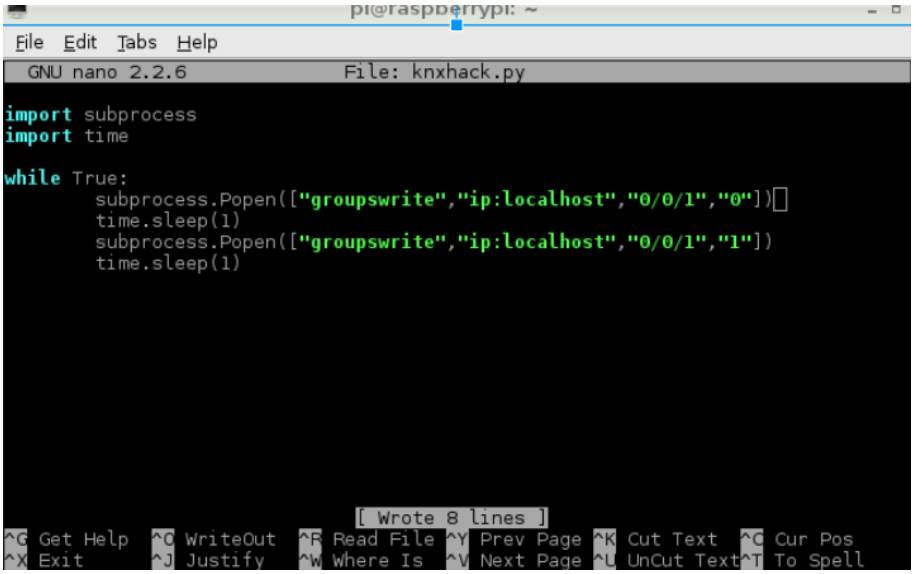
```
python knxhack.py
```

a svetlo sa začalo samé zapínať a vypínať vždy po 1 sekunde. Keďže v skripte nebola nastavená žiadna ukončujúca sekvencia týchto príkazov (čo značí otvorený blok kódu **while True**), po sputený skriptu sa bude svetlo zapínať a vypínať až kým nedojde k manuálnemu ukončeniu skriptu alebo prerušenia kabeláže medzi Raspberry Pi a KNX.

Útok na testovaciu inštaláciu bol úspešený. Len s malými úpravami by bolo možné rozšíriť skript aj na ďalšie prvky v sieti, ktoré by sme tiež mohli zapnúť na nekončenú slučku zapínania a vypínania, prípadne im úpravou parametra **sleep** nastaviť náhodné časy, kedy sa majú zapnúť alebo vypnúť. Výhodou útoku cez Raspberry Pi je to, že tento počítač je veľmi malý a dal by sa ľahko ukryť do inštalácie systému KNX. Ak by sme zabezpečili, že Raspberry Pi bude mať pripojenie k Internetu, mohli by sme ho nainštalovať na miesto a neskôr sa k nemu pripojiť vzdialene a spustiť útok na sieť z akéhokoľvek miesta na Zemi.

6.4 Zhodnotenie experimentu

Prienik do systému sa podaril z platformy Windows aj z platformy GNU/Linux. Testovacia inštalácia nemala nainštalované žiadne ochranné poistky. Programovanie prístrojov nebolo ochránené žiadnym heslom ani žiadnou formou autorizácie. Mala voľný alebo ľahko dostupný prístup ku KNX IP Routeru a ku kabeláži krútenej dvojlinky. Tieto dve chyby



Obr. 6.14: Skript ovládajúci zapnutie a vypnutie svetla

zabezpečenia môžu byť v reálnom prostredí veľmi časté, pretože sa nepredpokladá, že niekto bude na systém chcieť útočiť.

Testovaná inštalácia tiež neobsahovala žiadne grafické používateľské rozhranie, ktorým by užívateľ mohol ovládať viaceré prvky KNX z jedného miesta. V skutočnosti, ak by tu toto používateľské rozhranie bolo, pravdepodobne by bolo bezdrôtovo prepojené s KNX IP Routerom pomocou iného routera, ktorý by presmerovával informácie z KNX siete do grafického rozhrania, napríklad tabletu. Tým pádom by bolo možné odchytiť presnú komunikáciu, ktorá sa posiela zo zariadenia KNX do ovládacieho tabletu. Zároveň by tento tretí router mohol mať priamy prístup k Internetu a slabé zabezpečenie a to by otvorilo možnosti útoku z akéhokoľvek miesta na svete s prístupom k Internetu.

Potenciál takéhoto útoku je ale obrovský. Páchateľ môže po vstupe do systému nielen posielať falošné telegramy, ale môže sa mu podariť aj preprogamovať nechránené zariadenia v sieti, určiť im nové parametre, a zabezpečiť ich vlastným heslom. Tým sťaží vyhľadanie chyby a jej následné nápravy a preprogamovanie na pôvodné nastavenia, pretože obsluha systému bude musieť buď celý systém obnoviť, alebo prelomiť heslo nastavené útočníkom. To môže trvať niekoľko hodín.

Alebo môže páchateľ jednoducho sledovať aktuálne dianie v sieti. Ak sa sa sieti nebudú dlhšiu dobu posielať žiadne nové telegramy, je jasné, že v danej miestnosti alebo budove sa nikto nenachádza.

Kapitola 7

Dotazníkový prieskum

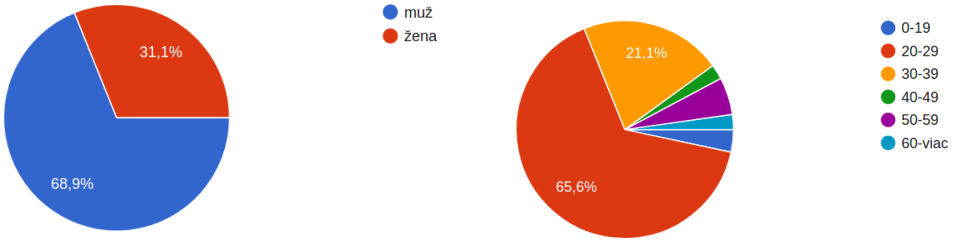
Jedným z cieľov práce bolo vytvoriť všeobecný súhrn o inteligentných systémoch a ich nebezpečiach tak, aby táto téma bola zrozumiteľná bežným používateľom a širokej verejnosti. Dotazníkový prieskum mal určiť úroveň povedomia o tejto téme. Všeobecným predpokladom je, že ľudia zo širokej verejnosti sa problematike inteligentných systémov a automatizácie v budovách nevenujú, neprichádzajú s nimi do styku alebo si to neuvedomujú, napriek tomu, že sú výrazy ako „Chytré bývanie“ a „Inteligentná domácnosť“ prítomné v každom novom developerskom projekte a reklamy sú plné inteligentných zariadení na vylepšovanie života, telefónov, kávovarov, chladničiek a iných zariadení.

Vzorke 90 respondentov bol predložený internetový dotazník s 24 otázkami, z toho 18 otázok bolo uzavretých s možnosťou voľby odpovede a 6 otvorených, vyžadujúcich vlastnú stručnú odpoveď. Časť dotazníka bola zameraná na počítačovú bezpečnosť všeobecne a časť priamo na znalosť inteligentných systémov, až potom na ich bezpečnosť. Jednak preto, že sa obe témy (téma počítačovej bezpečnosti a bezpečnosti inteligentných systémov) čiastočne prelínajú a jednak preto, že bolo nutné zistiť, aká je úroveň vedomostí bežných používateľov počítačov o inteligentých systémoch. Otázky boli formulované priamo na koncového používateľa a spotrebiteľa v bežnej domácnosti, nezaoberali sa bezpečnosťou systémov vo firmách alebo mestách. Kompletný zoznam otázok je uvedený v prílohe. Vyhodnotenie odpovedí s komentárom je uvedené v tejto kapitole.

Dotazník bol propagovaný cez sociálne siete a bol anonymný.

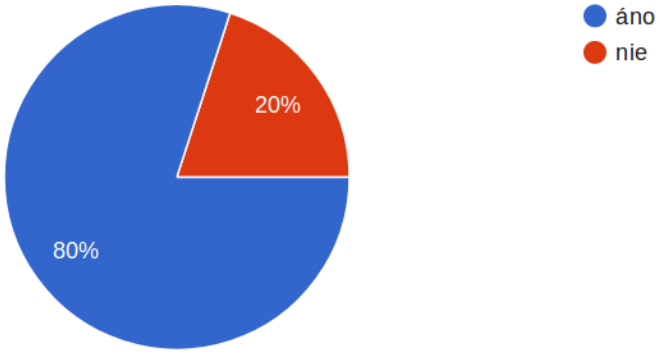
7.1 Vyhodnotenie prieskumu

7.1.1 Všeobecné informácie



Obr. 7.1: Pohlavie a vek respondetov

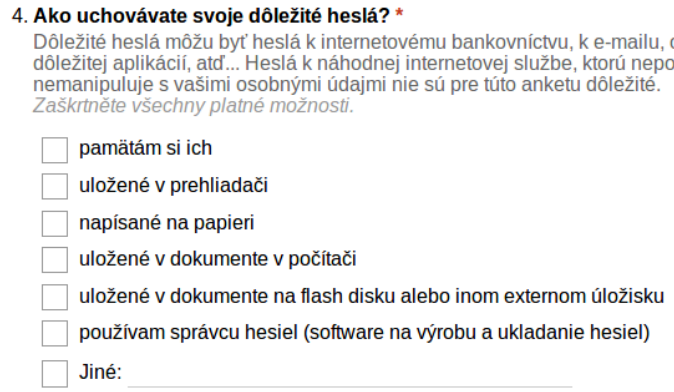
Na otázky odpovedali respondenti rôznych vekových kategórií a pohlaví. Najviac respondentov je vo veku 20-29 rokov, teda prevažne mladí ľudia. Hneď na začiatku vybrali z možností áno/nie, či sa zaujímajú o akékoľvek technologické témy. 73 ľudí odpovedalo áno, 17 ľudí odpovedalo nie.



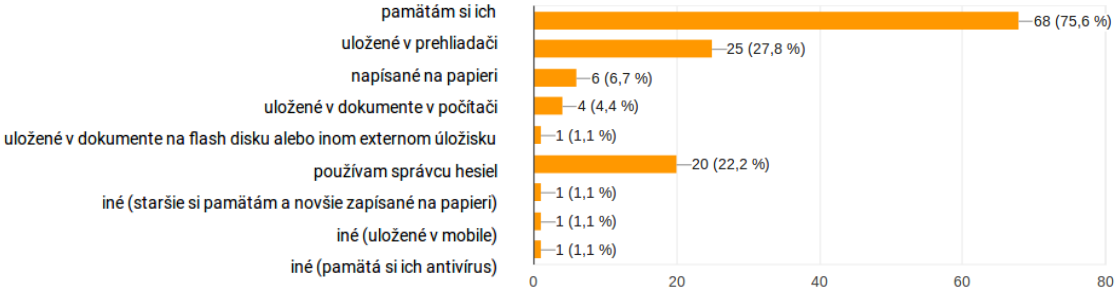
Obr. 7.2: Zaujímate sa o akékoľvek témy súvisiace s informatikou a novými technológiami?

7.1.2 Počítačová bezpečnosť

V nasledujúcej sekcií nasledovalo 9 otázok z počítačovej bezpečnosti, ktoré ukázali, ako jednotliví respondenti nakladajú so svojimi heslami, akú majú k heslám dôveru a aký majú prehľad aspoň o svojej domácej sieti.



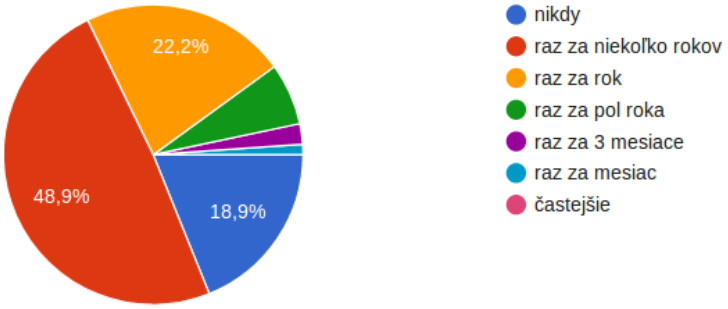
Obr. 7.3: Ako uchovávate svoje dôležité heslá? Otázka s možnosťou viacerých odpovedí



Obr. 7.4: Ako používatelia uchovávajú svoje heslá

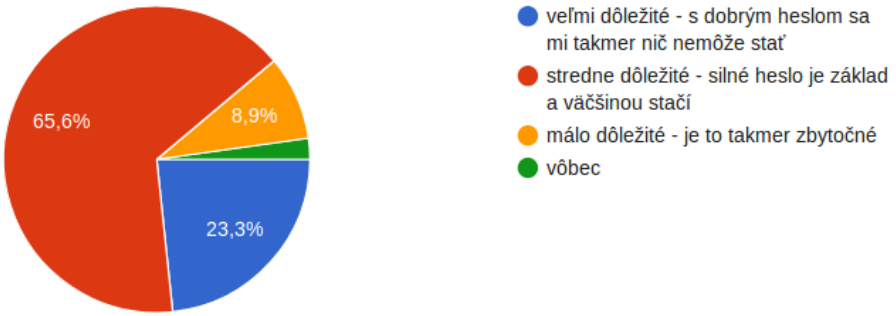
Drvivá väčšina respondetov (68) uchováva svoje heslá vo vlastnej pamäti a kombinuje to s inou možnosťou, napríklad uložené v prehliadači (25). Za predpokladu, že používateľ je schopný pamätať si dlhé a originálne heslá k službám je toto uchovávanie hesiel najbezpečnejšie. Riešenie ukladania hesiel priamo v prehliadači nie je bezpečené. Uľahčuje to prístup k heslám útočníkovi, ktorý sa dostane fyzicky k počítaču používateľa, ale zároveň je možné heslá ukradnúť aj na diaľku, ak ich prehliadač neukladá bezpečne. Moderné prehliadače sa snažia zabezpečovať ukladanie hesiel alebo implementovať a podporovať používanie správcov hesiel, špeciálnych programov, ktoré sa starajú o generovanie silných hesiel a zároveň zašifrované ukladanie hesiel na počítači. Používateľ si potom musí zapamätať len jedno heslo, to, ktorým odšifruje svoje heslá v správcovi hesiel. Správcu hesiel používa podľa ankety až 20 respondetov. 7 respondentov si zapisuje heslá na papier. Ak sa tento papier nachádza v blízkosti daného počítača, jedná sa o bezpečnostné riziko. Heslá uložené v dokumente v počítači, mobile alebo na flashdisku sú dnes väčšinou výnimočné, ale túto techniku používa 6 respondetov. Nebezpečenstvo môže nastať, ak útočník získa fyzický prístup do zariadenia, alebo ak sa do zariadenia dostane vzdialene a vie, čo presne hľadá, napríklad malý textový súbor s náhodnými reťazcami znakov, to samo o sebe napovedá, že sa jedná o heslá. A ešte ľahšie to útočník bude mať, ak bude súbor nazvaný „heslá“.

Ďalšie dve otázky sa sústredili na frekvenciu zmeny hesla používateľov a na ich dôveru v



Obr. 7.5: Ako často si meníte svoje dôležité heslá?

dôležitosť dobrého hesla. Z uvedených odpovedí vyplýva, že polovica odpovedajúcich mení svoje heslá raz za niekoľko rokov, čo nemusí byť alarmujúce v prípade, že nedošlo k úniku žiadnych databáz, ktorých sa heslá týkajú. Dve osoby označili možnosť zmeny hesla raz za 3 mesiace a jedna osoba dokonca raz za mesiac. V dnešnej dobe sa príliš častá zmena hesla nedoporučuje a môže byť skôr na škodu, obzvlášť ak sa heslo mení na cudzom zariadení (kde hrozí nebezpečenstvo prítomnosti keyloggera[40]), na nezabezpečenej sieti alebo kvôli podnetu z podvodného phishingového emailu. V poslednom prípade používateľ zadá nové heslo do falošnej stránky, ktorá ho ihneď odošle útočníkovi, a používateľ si nemusí nič všimnúť.



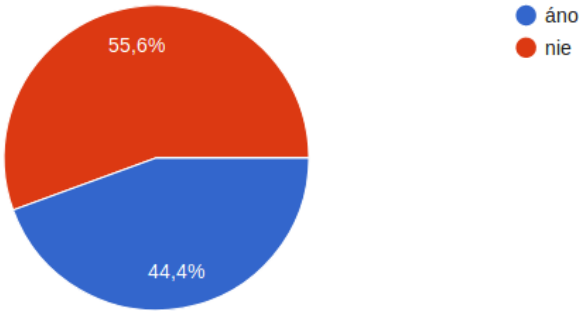
Obr. 7.6: Ako veľmi veríte, že je silné heslo dôležité?

Za dôležité pokladá heslo trištvrtina odpovedajúcich, z toho 24% ho pokladá za veľmi dôležité. Je dobré, ak ľudia pristupujú k heslám zodpovedne, teda ak veria tomu, že ich silné

[40] program, ktorý zachytáva stlačenia kláves a ukladá alebo ich odosiela na určené úložisko

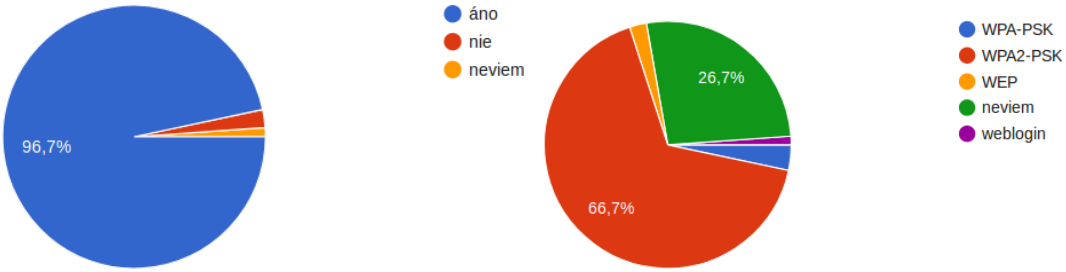
heslo ochráni, ale bohužiaľ je v tomto prípade najdôležitejší práve spôsob práce s heslami na strane programu a služieb. Aj keď má užívateľ nastavené silné, dlhé heslo z 40 znakov a číslic, ak služba ukladá používateľské mená so slabým alebo žiadnym šifrovaním, riziko prelomenia hesla je vysoké.

V naväzujúcej otázke je zaujímavé, že až 45% odpovedajúcich používa pre rôzne služby rovnaké heslá, čo sa v dnešnej dobe hodnotí ako jedno z najväčších nebezpečenstiev, zvlášť pri častých verejných únikoch databáz hesiel. Používateľ môže si môže ľahko overiť, či nedošlo k úniku databáze služby, ktorú používa, napríklad pomocou stránky https://haveibeenpwned.com/.



Obr. 7.7: Používate pre rôzne dôležité služby rovnaké heslá?

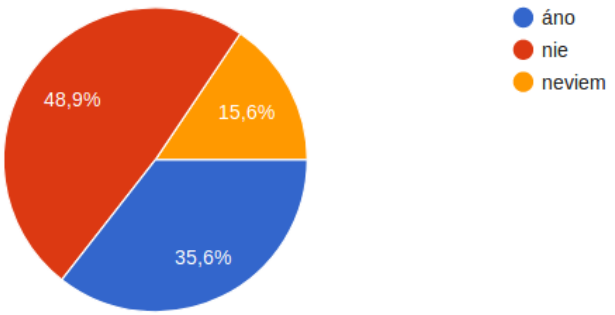
Nasledujúca otázka sa zamerala na používanie domácej bezdrôtovej siete a jej zabezpečenia. Nie je prekvapivé, že takmer všetci respondenti volili možnosť „áno“, používam doma bezdrôtovú šifrovanú sieť. Komplikovanejšie to už bolo pri voľbe, aké šifrovanie ich domáca sieť ponúka. Až 60 ľudí (67%) uviedlo, že ich sieť je zabezpečená protokolom WPA2-PSK, ktorý sa dnes považuje za najbezpečnejší pre domácu sieť a kombinuje sa aj s ďalšími formami zabezpečenia. Otázka nezachádzala do detailov o tom, či majú používatelia nastavené aj overovanie prihlásenia do siete pomocou MAC adries, alebo nejak inak, ale je potešujúce, že väčšina odpovedajúcich (66 ľudí) vie, ako je ich domáca sieť zabezpečená.



Obr. 7.8: Požívate doma bezdrôtovú šifrovanú sieť (Wi-Fi)? Aké má šifrovanie?

Horšie výsledky ukazuje otázka na používanie prednastaveného SSID siete, teda továr-

neho názvu domácej Wi-Fi. Až 16 používateľov označilo možnosť, že si ponechávajú SSID prednastavené z výroby. Napríklad len v minulom roku sa objavila zraniteľnosť routerov UPC[25], ktoré vytvárajú prednastavené heslá pomocou tohto prednastaveného mena siete. Ak používateľ použije prednastavené SSID, ktoré je verejne viditeľné, je tu určitá pravdepodobnosť, že nezmení ani prednastavené heslo a na to, aby sa útočník dostal do siete mu potom stačí vyhľadať verejne prístupný program[41], ktorý továrne heslá vytvára pomocou SSID a tieto heslá postupne vyskúšať.



Obr. 7.9: Aktualizujete pravidelne firmware svojho domáceho routeru?

Pri otázke na pravidelné aktualizácie firmware domácich smerovačov vidíme, že polovica odpovedajúcich odpovedala „nie“, prípadne „neviem“. To je spôsobené čiastočne tým, že sa bežní používatelia nezaujímajú a nevyznajú v firmware a nevedia, ako ho aktualizovať, pretože nespravujú svoju domácu sieť sami. Zároveň to ale môže byť spôsobené tým, že niektoré lacnejšie alebo staršie zariadenia nedostávajú pravidelné aktualizácie firmware. Používať zastaralý firmware, prípadne priamo router, ktorý prekázateľne obsahuje už objavenú zraniteľnosť, je veľké riziko.

[41] napríklad na stránke https://upc.michalspacek.cz/

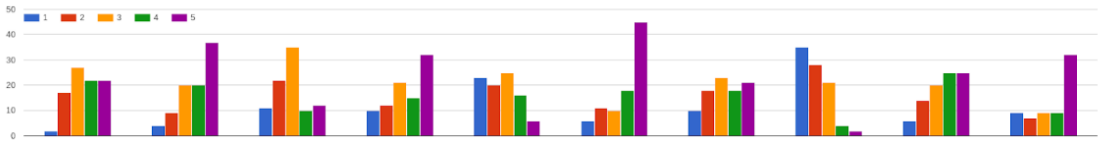
Najzaujímavejší prehľad povedomia ľudí o počítačovej bezpečnosti ponúkla otázka, kde mali ohodnotiť každý z daných pojmov hodnotou 1 (najmenej dôležité), alebo 5 (veľmi dôležité). Tu môžeme vidieť nesúrodosť názorov rôznych ľudí na rôzne druhy zabezpečenia.

19. Ohodnoťte stupeň dôležitosti každého z nasledujúcich pojmov (1 - najmenej dôležité, 5 - veľmi dôležité) *

Označte jen jednu elipsu na každém řádku.

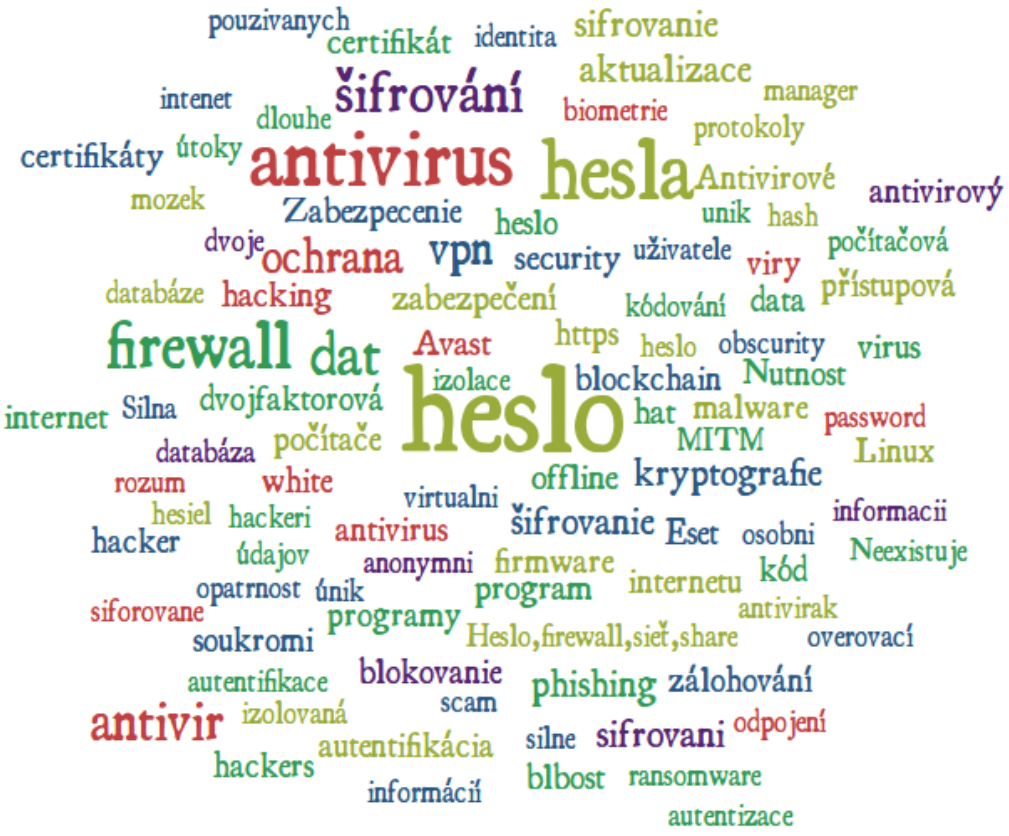
	1	2	3	4	5
dlhé heslo					
heslo ktoré obsahuje veľké a malé písmená, čísla, špeciálne znaky					
šifrovanie dát na úložisku doma					
šifrovanie komunikácie					
používanie software správcu hesiel					
zmena prednastaveného hesla v routeri (heslo k wifi)					
zmena prednastaveného názvu siete (SSID) v routeri					
zmena hesla každý mesiac					
pravidelné aktualizácie software, firmware					
zmena prednastaveného hesla do administrácie routeru					

Obr. 7.10: Otázka na číselné hodnotenie dôležitosti pojmov počítačovej bezpečnosti



Obr. 7.11: Odpovede na číselné hodnotenie dôležitosti pojmov počítačovej bezpečnosti, 1-najmenej dôležité, 5-veľmi dôležité

V téme počítačovej bezpečnosti bola ešte jedna otvorená otázka: „Napíšte kľúčové slová, ktoré vám napadnú pri spojení „počítačová bezpečnosť"“. Z vizuálne spracovaných výsledkov môžeme vidieť, že najčastejšími pojmami v počítačovej bezpečnosti sú pre ľudí heslo, antivírus, šifrovanie, firewall, VPN, certifikáty, mozog a premýšľanie, ochrana súkromia a iné, a to hodnotím ako kladný výsledok tejto otázky.



Obr. 7.12: Mrak kľúčových slov o počítačovej bezpečnosti. Vytvorené pomocou webovej služby https://worditout.com/word-cloud/create

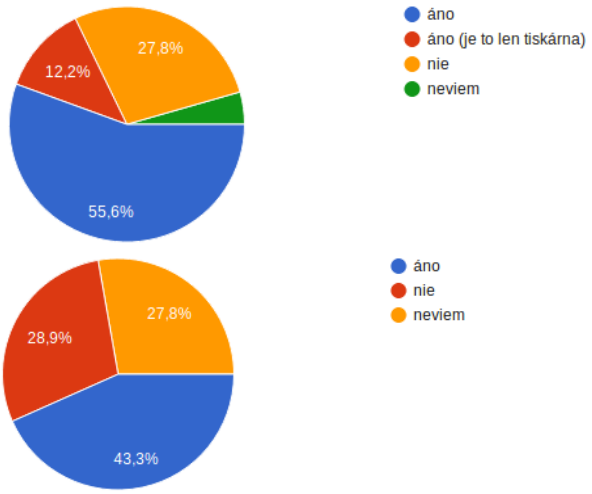
7.1.3 Inteligentné budovy a IoT

Druhá časť ankety sa zaoberala otázkami súvisiacimi s inteligentnými systémami a IoT, pretože tieto pojmy sa z pohľadu koncových spotrebiteľov prelínajú. Anketa ale ukázala, že veľká časť ľudí nemá prehľad o tom, čo jednotlivé pojmy znamenajú.

Táto časť obsahovala niekoľko otvorených otázok, kde bolo nutné uviesť odpoveď vlastnými slovami. Odpovede boli spracované podľa toho, ako veľmi sa daná odpoveď blížila oficiálnym definíciám uvedených v 1. kapitole tejto práce.

V otázke: **„Čo si predstavíte pod pojmom Inteligentná budova / domácnosť?“** uviedlo správnu definíciu, ktorá sa týka automatizácie, ovládania alebo prepojenia systémov, až 44 % odpovedajúcich. 24 % uviedlo charakteristiku, ktorá sa blíži skôr charakteristike IoT, častou odpoveďou bolo „zariadenia a spotrebiče prepojené internetom“. 6 % ľudí kládlo v odpovedi dôraz na ekológiu a sebestačnosť budovy, nie len jej automatizáciu, a len 11 % zvolilo odpoveď „neviem, nie som si istý“.

Naproti tomu v otázke: **„Čo si predstavíte pod pojmom IoT (Internet of Things)?“** uviedlo „neviem“ až 46,6 % ľudí. Na druhú stranu sa do správnej charakteristiky trafilo 41 % odpovedajúcich, a 3 % ľudí napísali definíciu, ktorá nebola ani len blízka IoT.



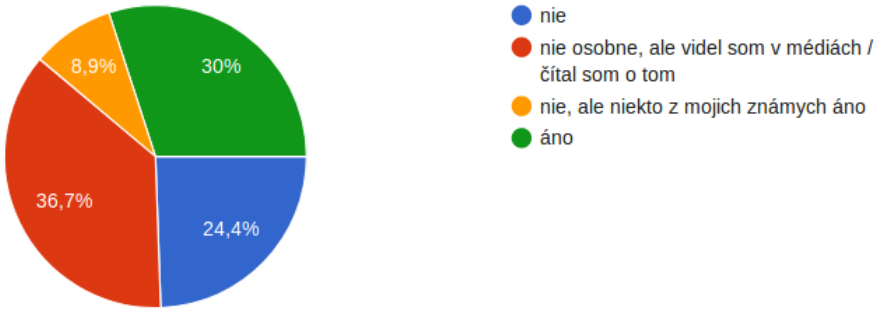
Obr. 7.13: Máte na váš domáci router pripojené aj iné zariadenie, než je počítač/notebook? Máte doma zariadenie, ktoré je IoT / Smart?

43 % odpovedajúcich uviedla, že má doma zariadenie, ktoré je IoT alebo Smart, ale najčastejšie sa jedná o Smart televízie, smartfóny a podobné veci bežného využitia.

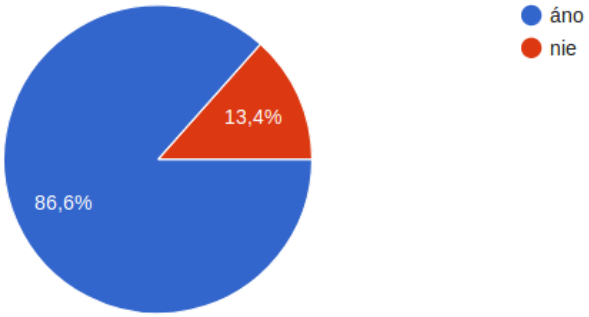
Z výsledkov je jasne vidieť, že minimálne polovica odpovedajúcich má predstavu o tom, čo je to inteligentná budova a čo je to IoT a má predstavu o počítačovej bezpečnosti, ale tá časť respondentov, ktorá neuviedla definíciu IoT a uviedla nesprávnu definíciu pre inteligentnú budovu, má aj menšie znalosti o počítačovej bezpečnosti.

7.1.4 Dôležitosť bezpečnosti a osobné skúsenosti

Posledná sekcia dotazníku sa zamerala na to, či má odpovedajúca osoba priamu skúsenosť s nejakým druhom napadnutia počítača a čo si myslí o bezpečnosti a dodržiavaní jej zásad.



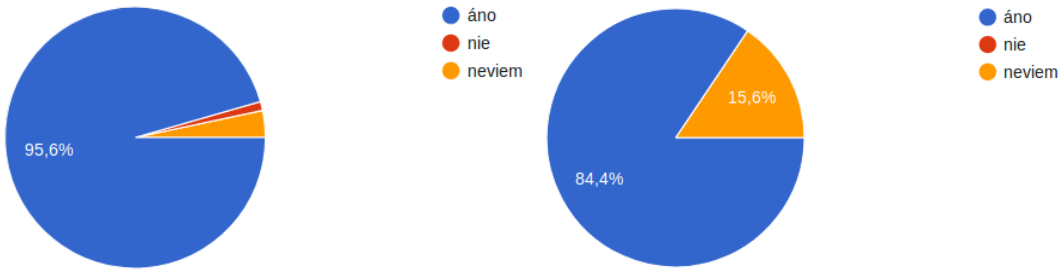
Obr. 7.14: Stretli ste sa osobne s nejakými následkami po počítačovom útoku alebo s narušením počítačovej bezpečnosti?



Obr. 7.15: Myslíte, že sa s nejakým útokom alebo narušením PC bezpečnosti reálne stretnete v budúcnosti?

V otvorenej otázke, ktorá naväzovala na otázku „Stretli ste sa osobne s nejakými následkami po počítačovom útoku alebo s narušením počítačovej bezpečnosti?“, uviedlo voliteľnú odpoveď 36 ľudí. 4 z nich nevedeli presne definovať, o aký útok sa jedná. S preniknutím do nejakého systému, či už osobného počítača alebo spravovaného webu sa stretlo 6 ľudí (16,6 %). S krádežou dát ako sú prihlasovacie údaje do platobného systému alebo účtu na sociálnej sieti sa stretlo 7 ľudí (19,4 %), a s nejakým typom vírusu (trojan, ransomware alebo nešpecifikovaný malware) sa stretlo až 19 ľudí (52,7 %).

Je zaujímavé, že napriek tomu, že sa 62 respondentov nestretlo osobne so žiadnym útokom, až 71 odpovedajúcich verí, že sa s nejakým druhom napadnutia stretne v budúcnosti. S tým určite súvisí, že pri otázke, či je potrebné dodržiavať zásady počítačovej bezpečnosti až 96% ľudí uviedlo, že áno. Ľudia si uvedomujú, že počítače, ktorými sú obklopení, sú zraniteľné, často obsahujú ich osobné citlivé údaje, ich tvorbu, fotografie a spomienky alebo tvoria spôsob živobytia, a že môže dojsť k ich napadnutiu a preto by ich mali chrániť. Až na jedného respondenta, ktorý nepovažuje dodržiavanie bezpečnostných zásad za dôležité. Otázka neponúkala možnosť zdôvodnenia vlastnými slovami, a tak môžeme len hádať, či respondent myslel na to, že zásady bezpečnosti nie sú dôležité, pretože vôbec nepomáhajú, alebo na to, že aj keď zásady pomáhajú v určitých situáciach, tak silne odhodlaný útočník môže prekonať všetky prekážky.



Obr. 7.16: Myslíte si, že je dôležité dodržiavať zásady bezpečnosti na počítači? A v IoT a Inteligentných domácnostiach?

Naproti tomu na otázku, či je dôležité dodržiavať zásady bezpečnosti v inteligentných systémoch a IoT zariadeniach odpovedalo kladne len 85% ľudí, zbytok vybral možnosť „neviem“. Nikto neoznačil možnosť „nie“. Toto by sa dalo prisúdiť tomu, že mnoho odpovedajúcich nevedela definovať, čo to inteligentný systém je a čo všetko predstavuje.

7.2 Zhrnutie

Zo získaných odpovedí je jasne vidieť, že verejnosť sa v téme inteligentných systémov zatiaľ neorientuje tak dobre, ako v téme počítačov a ich bezpečnosti. Počítače v našich domácnostiach figurujú už tretiu dekádu a v dnešnej dobe má počítač alebo výkonný telefón veľká časť populácie a používa ich dennodenne, kdežto inteligentné systémy a zariadenia IoT zažívajú svoj globálny nástup až v posledných rokoch. Samozrejme, prístroje a protokoly pre automatizáciu ovládania zariadení sa rozvíjali súčasne s počítačmi a ich technikou, ale uplatnenie nachádzali najskôr len v priemysle a výrobe[42], tam, kde mali zmysel veľké investície a kde automatizácia bola prínosom. Prvky, ktoré sa dnes používajú v budovách a tvoria inteligentné systémy, sú trendom posledných rokov. Obrovský dopyt po tom modernom pocite, úsporách energií alebo po pohodlí zrýchľuje ich vývoj a postupne sa dostávajú do životov stále viac a viac ľudí, ale ešte potrvá, kým budú súčasťou takmer každého života tak, ako sú dnes počítače. Počítače pri svojom nástupe vo veľkom zanedbávali zabezpečenie,

[42] systémy merania a regulácie (MaR)

až kým sa nápor počítačových vírusov nestal tak veľký, že každý videl, že je bezpečnosť a obozretnosť potrebná. Podobný príbeh čaká aj inteligentné systémy. Preto je potrebné, aby sa okrem jednoduchej implementácie nových systémov vývojári a ľudia už dnes sústredili aj na ich zabezpečenie.

Kapitola 8

Odporúčania

8.1 Zoznam odporúčaní

Nasledujúca kapitola uvádza odporúčania, ktorými by sa mal riadiť každý používateľ počítačových sietí a ešte väčšiu pozornosť by im mal venovať každý, kto bude konfigurovať nejaký systém. Pri dodržiavaní bezpečnostných zásad sa riziko útoku znižuje, ale nemusí byť nulové.

8.1.1 Domácnosť a siete malého rozsahu

Používateľ inteligentného systému v domácnosti a v menších inštaláciách by mal mať na pamäti tieto zásady:

- **Silné heslo** - Je dobré mať nastavené heslo všade, kde je to možné. Heslo musí byť originálne a dostatočne dlhé. Malo by obsahovať rôzne znaky: veľké a malé písmená, čísla, špeciálne znaky. Uvádza sa, že by heslo malo mať aspoň 8 znakov, ale čím viac znakov bude mať, tým náročnejšie bude prelomiť ho nejakým bruteforce[43] útokom. V niektorých prípadoch sa odporúča používať zabezpečené programy pre správu hesiel, ktoré automaticky generujú dlhé reťazce náhodných znakov, ktoré sú uložené zašifrované v programe v počítači. Nebezpečenstvom v tomto prípade je, ak nie je program správcu hesiel dostatočne bezpečný, má slabé šifrovanie alebo dôjde k úniku informácií.

- **Obmena hesla** - Používajte rôzne heslá k rôznym službám. Nepoužívajte jedno rovnaké heslo k viacerím službám, obzvlášť nie súčasne k banálnym službám, kam používateľ nezadáva žiadne osobné údaje, a k dôležitej službe ako je napr. internetové bankovníctvo. Zároveň je dobré občas heslo zmeniť, hlavne ak niektorá zo služieb, ktorú používate, čelí úniku dát. Naopak, meniť heslo príliš často bez dôvodu sa neodporúča.

- **Vždy zmeniť prednastavené prihlasovacie údaje** - Nikdy nenechávajte prednastavené údaje zakúpeného zariadenia. Videli sme príklad ovládania solárnych panelov

[43] útok „hrubou silou“, napríklad slovníkový útok, kedy počítač prechádza slovník s miliónmi možných kombinácií písmen a snaží sa nájsť zhodu so šifrovaným zápisom hesla

s prednastavenými údajmi, ale často sa tento problém týka hlavne domácich smerovačov (routerov). Zoznamy prednastavených hesiel („default“ hesiel) sa totiž čas od času nájdu na Internete, alebo sa zistí, že sú tieto administrátorské prihlasovacie údaje odvoditeľné podľa sériového čísla zariadenia a jeho MAC adresy alebo podľa prednastaveného SSID, ako to bolo už v spomenutom prípade UPC[25].

- **Používať systém rôznych prístupových práv** - Nepoužívajte rovnaký účet v operačnom systéme pre viacero osôb. Nedávajte bežným používateľom administrátorské práva. Ak púšťate k svojmu počítaču cudziu osobu, dajte jej k dispozícií len účet hosťa s obmedzenými právami.

- **Aktualizujte** - Starajte sa o to, aby bol používaný software alebo firmware vždy aktuálny a sťahujte všetky bezpečnostné záplaty (patche), ktoré sú vydané.

- **Používať bezpečné technológie** - Nesťahujte programy z nedôveryhodných zdrojov. Nepripájajte zariadenia, ktoré to nepotrebujú, priamo k Internetu. Samotný Internet je nebezpečné miesto, preto sa vždy presvedčujte, že je webová služba chránená tak, ako má, napríklad že používa bezpečnostné certifikáty, protokol HTTPS a podobne.

- **Používať VPN** - Pri používaní nezabezpečených sietí alebo nešifrovaných komunikačných zariadení je použitie Virtual Private Network (VPN) vhodné a bezpečné. VPN vytvára šifrované prepojenie, akýsi tunel medzi našim zariadením a cieľom (napríklad webovou stránkou).

- **Zabezpečiť fyzické prístupové body systému** - Nenechávajte voľne prístupné porty, ktoré nie sú potrebné. Veľmi nebezpečný môže byť obyčajný USB port, ktorý je bežne naprogramovaný na to, aby automaticky spustil program nájdený na pripojiteľnom zariadení, napr. Flashdisku.

- **Prevádzkujte minimálne množstvo portov v sieti** - V sieti na ovládanie inteligentného systému pravdepodobne nebudete potrebovať port využívaný pre prenos súborov alebo pošty, ktorý sa používa v bežných sieťach. Je rozumné tieto porty uzavrieť, ak sú nevyužívané.

- **Nikdy neklikať na podozrivé súbory** - Nespúšťajte neznáme programy, obzvlášť, ak máte v tej iste sieti pripojenú kritickú infraštruktúru akou je aj inteligentný systém.

- **Použiť firewall** - Nastavte v sieti firewall, prípadne použite server, ktorý poslúži ako brána medzi internetovou sieťou a KNX sieťou. Vďaka tomu nebude možné dostať sa priamo do inteligentného systému, ktorý ovláda domácnosť, z ktoréhokoľvek miesta na svete.

- **Používať DMZ (demilitarizovanú zónu)** - DMZ je bežne zaužívaný termín pri konfigurácii siete, kde sú prvky rozčlenené tak, aby časť z nich mohla byť prístupná z Internetu (DMZ zóna), ale druhá časť z nich bola oddelená (napr. firewallom) a neprístupná z verejnej siete. Takáto konfigurácia je vhodná pri používaní rôznych IoT zariadení a inteligentných systémov.

8.1.2 Firmy, verejné budovy a siete väčšieho rozsahu

V inteligentných inštaláciách vo firmách, verejných budovách a iných väčších projektoch platia rovnaké zásady, ale naviac tomu sa doporučuje:

- Vytvoriť tzv. **checklist**, jednoduchý prehľad všeobecnej kyberbezpečnosti systému, podľa ktorého sa dá postupovať pri kontrolovaní stavu bezpečnosti. Skontrolovať šifrovanie, overovanie/autentifikáciu a autorizáciu používateľov, ktorí majú prístup k systému a schopnosť jednoduchých aktualizácií systémov.

- Vyžadovať od predajcov a poskytovateľov systémov všetku dostupnú dokumentáciu k systému, hlavne tú, ktorá sa týka zabezpečenia a údržby. Ubezpečiť sa, že zmluvy o službách zahŕňajú opravy zraniteľností v reálnom čase a 24 hodinovú podporu v prípade incidentov.

- Opravovať bezpečnostné chyby hneď, ako sú objavené.

- Vytvoriť špeciálny CERT tím, ktorý vie, ako postupovať pri kyberbezpečnostných incidentoch, a bude o nich okamžite informovať, reportovať, zdieľať informácie a opravovať chyby. Každá inštituácia by mala mať vlastný CERT tým špecializovaný na ich vlastné siete, ale rôzne CERT tímy by mai spolupracovať medzi sebou a zdieľať informácie navzájom.

- Definovať oficiálne protokoly a komunikačné kanály v prípade útoku a preškoliť svojich zamestnancov. Zamestnanci musia vedieť, ako rozpoznať útok, a kam a komu ho nahlásiť.

- Implementovať do systémov a infraštruktúry poistky, ktoré v prípade útoku alebo havárie umožnie ručné ovládanie každého systému.

- Pravidelne skúšať penetračné testy systémoch a sieťach kritickej infraštruktúry.

- Oddeľovať od seba siete jednodlitvých systémov a nepripájať k Internetu systémy, ktoré to nepotrebujú.

- Vytvárať zálohy dát a konfigurácie systému.

- Pripraviť sa na najhoršie a vytvoriť modelové scenáre pre rôzne hrozby a situácie.

8.2 Bezpečné technológie

V zozname odporúčaní stojí, že je nutné používať bezpečné a aktuálne technológie. Obzvlášť obozretný musí byť každý, kto používa staršie systémy a systémy, ktoré neponúkajú žiadnu formu šifrovania a zabezpečenia. V experimente sme si ukázali, že dostať sa do systému KNX, ktorý nemá zabezpečenie, je jednoduché. Ako sa proti tomu dá brániť?

8.2.1 KNX Secure

V dôsledku stúpajúceho počtu digitálnych hrozieb sa organizácia KNX prispôsbila a vydala vylepšený protokol KNX Secure, ktorý získal potvrdenie medzinárodnou štandardizáciou podľa EN 50090-4-3.

Protokol KNX Secure funguje na princípe šifrovacieho algoritmu AES 128 CCM. Má dva spôsoby implementácie:

- **KNX IP Secure** - rozširuje IP protokol a šifruje všetku komunikáciu vzdialeného prenosu dát protokolu KNX
- **KNX Data Secure** - šifruje všetky dáta v rámci komunikácie KNX siete

Výrobky pracujúce na tomto novom protokole sú značené ako KNX Secure. Dobrou správou je, že sú plne kompatibilné so starými nezabezpečenými výrobkami, a tak na ochránenie nainštalovanej siete nie je nutné meniť každé jedno zariadenie, ale len niekoľko kľúčových výrobkov.

Zabezpečenie ďalej prináša aj program ETS a jeho verzia ETS Inside, ktorý na akúkoľvek manipuláciu s projektom vyžaduje zadanie prístupového hesla. Tento program je možné používať aj v starších inštaláciach KNX, nie len v protokole KNX Secure.

Ak nie je možné použiť KNX Secure, je možné zvýšiť bezpečnosť KNX inštalácie aj úpravami konfigurácie systému pomocou ETS. Napríklad je možné nastaviť filtrovanie líniových spojek podľa adresácie a tým zabrániť posielaniu telegramov zo zariadení, ktoré nie sú v sieti nakonfigurované. Je tiež možné nastaviť zariadeniam zákaz prijímania nových programovacích telegramov a tým ich uchrániť pred preprogramovaním.[10]

8.3 Fyzické zabezpečenie

Nutnosť fyzického zabezpečenia sa týka každého prvku v sieti. Riadiace servery a ovládacie prvky by mali byť umiestnené v chránenej a dobre zabezpečenej miestnosti so zvýšenou odolnosťou voči vode (a miestnosťou by nemali prechádzať potrubia a rozvody vody) a ohňu. Prístroje by nemali byť ukladané priamo na podlahe, ale na vyvýšené miesta. Zároveň by malo byť zabezpečené účinné vetranie. Ovládacia miestnosť musí mať funkciu manuálneho otvárania ako poistku pri výpadku systému, aby sa nestalo, že systém, ktorý ovláda prístupové dvere pri svojom výpadku zablokuje aj dvere do ovládacej miestnosti.

Kabeláž býva chránená inštaláciou v stenách alebo lištách, pod podlahou alebo v podhľadoch stropu. Zvlášť dôležitá je ochrana kabeláže prístupná vonku budovy, ktorá väčšinou zaisťuje hlavné pripojenie celej budovy. Vnútri budovy je dôležitý hlavný chrbticový spoj systému, pri jeho fyzickom zničení dôjde k nefunkčnosti celej siete.

Obr. 8.1: Príklad zlého stavu kabeláže bez zabezpečenia vo voľne prístupných bytových domoch. Autor fotografie: Jan Žejdl, Ostrava 2017

8.4 Príklad správneho nastavenia systému

Ako konkrétny príklad správneho nastavenia systému nám môže poslúžiť budova Enterprise, ktorá sa nachádza v Prahe 4 na Pikrtovej ulici. Je to 11 poschodová administratívna budova, ktorá ponúka kancelárske priestory o rozlohe 29 069 m2 a ďalších 2 622 m2 obchodných plôch v prízemí. V podzemí má 4 podlažia a dohromady 401 parkovacích miest. Budova ponúka automatické ovládanie vonkajších žalúzií, centrálne ovládanie klimatizácie a vzduchotechniky všetkých priestorov budovy, reguláciu vlhkosti, kontrolu vstupu cez magnetické karty, detektory dymu a elektrickú požiarnu signalizáciu, kamerový systém kontrolujúci budovu a jej okolie a inteligentný systém riadenia budov.

Obr. 8.2: Budova Enterprise, http://www.enterprise-prague.cz/

Ovládanie rozdielnych funkcionalít je rozdelené do samostatných sietí. Zároveň je budova je rozdelená do jednotlivých zón tak, aby zamestnanci jednej firmy neboli ovplyvňovaní zmenami v inej firme sídliacej na inom poschodí.

Osvetlenie v budove je riadené protokolom Digital addressable Lighting Interface (DALI). Podrobnosti pre kamerový systém a systém riadiaci prístup osôb mi nie sú známe. Automatizácia zariadení MaR (Meranie a regulácie) funguje na princípe protokolu BACnet[44].

BACnet je protokol vyvíjaný od roku 1987, zaštítený organizáciou ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers) a tiež organizáciami ANSI

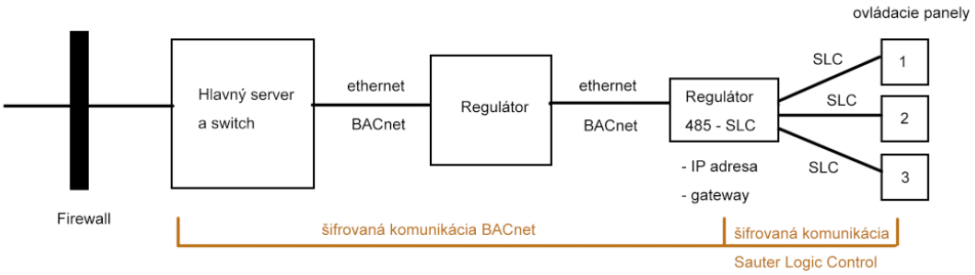
[44] http://www.bacnet.org/

(American National Standards Institute) a ISO (International Organization for Standardization). V roku 2002 získava označenie normy ISO/DIS 16484-5:2002 (Draft International Standard) a európske označenie EN ISO 16484-5. Týmto sa tento protokol stáva celosvetovým.

V budove Enterprise je protokol implementovaný skrz výrobky a systémy firmy Sauter[45].

BACnet je otvorený protokol zameraný na prenos dát po datových a komunikačných sieťach. Je nezávislý na výrobcoch a tým vzájomne kombinovateľný s inými prvkami BACnet. Tvorí decentralizovaný systém, v ktorom môže fungovať 65 535 podsietí a dohromady 4 194 305 zariadení. Adresovanie musí byť jednoznačné v celej sieti. Zariadenia BACnet sa adresujú pomocou IP protokolu, konkrétne IPv4 adries. Pri adresovaní sa dodržujú rovnaké pravidlá ako v počítačových sieťach, a teda na adresovanie zariadení sa použijú adresy z privátneho rozsahu sietí, ale je možné nastaviť aj dynamické adresovanie DHCP (zariadenie dostane volnú adresu IP pri každom zapnutí siete). Jednotlivé zariadenia sú v protokole BACnet zobrazované ako objekty a každý má svoj vlastný jedinečný identifikátor (ktorý v tomto prípade tvorí číslo zložené z posledných dvoch čísel IP adresy). BACnet vždy používa sériový port 47808 (0x BAC0). Protokol umožňuje nastaviť v rámci systému maticu priorít od 1 ako najdôležitejšej funkcie po 16 ako najnižšiu prioritu. Napríklad bezpečnostné okruhy, ako mrazová ochrana alebo maximálna teplota (kritické aplikácie) by mali byť nastavené na prioritu 5. Požiarne klapky sa nastavujú na prioritu 2. Prioritu 1 má nastavenú ochrana života, tzn. ručné ovládanie bezpečnostných funkcí.

Tento inteligentný systém je v budove Enterprise implementovaný v samostatnej sieťovej infraštruktúre, nezávislej od tej, ktorá spravuje Internetové pripojenie. Komunikácia medzi jednotlivými zariadeniami je šifrovaná a hierarchizovaná. Z centrálneho serveru, ktorý je umiestnený za hardvérovým firewallom, vedie spojenie pomocou krútenej dvojlinky k menším regulátorom a z nich na regulátori so zbernicou 485 pripojené z pomocou Ethernetu s protokolom BACnet. Každý tento regulátor má svoju IP adresu a tvorí bránu medzi protokolom BACnet a SLC. Z týchto zberníc pokračuje vedenie pod protokolom Sauter Logic Control (SLC), ktorý nie je otvorený a je šifrovaný. Na konci tohto pripojenia sa nachádzajú ovládacie panely pre jednotlivé miestnosti, ktoré umožňujú posúvať žalúzie alebo korigovať teplotu v danom teplotnom rozsahu. Jeden regulátor so zbernicou dokáže ovládať 16 miestností (obsahuje 8 portov z každej strany).



Obr. 8.3: Schéma systému v budove Enterprise

[45] https://www.sauter.cz/cz.html

Centrálny dispečink, ktorý kontroluje a ovláda stav systému, vidí na všetky regulátory v sieti. Beží na systéme Windows Server prostredníctvom špeciálnej aplikácie **novaPro Open**[46], spustenej pod účtom bežného používateľa „user“. Do tohoto účtu majú prístupové údaje len oprávnené osoby z obsluhy budovy. Samotná aplikácia vyžaduje prihlásenie používateľa buď v roli *user* alebo *admin*. Aplikácia monitoruje stav všetkých regulátorov v sieti a pomocou SQL ukladá dáta do databáz. Používateľ prihlásený do kontrolnej aplikácie, ktorý má pridelené dostatočné práva, môže manipulovať s nastavením siete a systému. Všetky jeho kroky sa zaznamenávajú do zoznamu akcií tzv. logu, ktorý je možné neskôr analyzovať.

Dáta z jednotlivých regulátorov sú ukladané na lokálnom hlavnom serveri a sú pravidelne zálohované, tak ako je zálohovaná konfigurácia systému. Pri poruche alebo napadnutí systému musí byť zásahový tím schopný reagovať a obnoviť systém do času stanoveného zmluvou (môže to byť 6hod., 24hod. a i.).

Regulátor môže byť pripojený cez gateway aj do vonkajšej siete, kde by mohol napríklad zobrazovať dáta a ovládať sa z diaľky (pomocou aplikácie novaPro Open). Tým by sa mohlo oslabiť zabezpečenie systému, útočník by mohol odpočúvať dáta posielané zo systému. Preto je vhodné použiť pri takejto konfiguráii VPN kanál, cez ktorý sa vstúpi od ovládacej aplikácie do siete, kde sú pripojené jednotlivé inteligentné prvky.

[46] https://www.sauter-controls.com/en/company-sauter/news-media-sauter/media-releases-news-media-sauter/news-details/news/sauter-novapro-open-1.html

Kapitola 9

Záver

Hlavným cieľom tejto práce bolo zhrnúť čo najviac informácií o inteligentných systémoch, podať technické informácie o spôsobe ich fungovania a uviesť riziká, ktoré hrozia pri ich používaní. Experimentom sa nám podarilo prekázať základný predpoklad, že nezabezpečený systém inteligentnej inštalácie dokáže napadnúť aj laik.

Inteligentné systémy a zariadenia IoT sa rozvíjajú závratnou rýchlosťou nielen v krajinách západného sveta, ale významne sa uplatňujú aj v rôznych špeciálnych projektoch v rozvojových oblastiach. Počet systémov a zariadení pripojených k Internetu stúpa obrovským tempom a čím ďalej tým viac ovplyvňujú život každého z nás. Preto je nutné vedieť, čo hrozí pri ich poruchách alebo napadnutiach a aké zásady bezpečnosti treba dodržiavať, tak ako v každej oblasti nášho života.

Inteligentné mestá sú nastupujúcim trendom vývoja, ktorému sa nedá vyhnúť. Priemysel 4.0 spôsobuje, že jednotlivé systémy, ktoré bývali izolované, sa teraz prepájajú, a čoskoro sa stratí hranica medzi Internetom s používaním bežných počítačov a mobilov a medzi industriálnymi systémami. Moderné elektrosúčiastky sú zraniteľné, pretože obsahujú software, a čoskoro bude každé jedno zariadenie v meste potrebovať software k vlastnej prevádzke. Je dôležité na skutočnosť reálnych hrozieb upozorňovať. V inteligentných mestách, ktoré ovplyvňujú každodenný život tisícov a miliónov ľudí, treba začať robiť aktívne kroky smerom ku kybernetickej bezpečnosti. Nie smerom špehovania občanov a všetkej komunikácie v sieti, ale smerom zabezpečenia konkrétnych systémov, školenia zamestnancov, ktorí prichádzajú do styku s týmito systémami, a pri návrhoch nových riešení počítať aj s možnosťou nebezpečenstiev, ktoré dnes ešte neexistujú, ale s exponenciálnym vývojom technológií sa môžu objaviť do niekoľkých rokov. Je nesmierne dôležité, aby nové nasadzované riešenia boli testované v reálnych podmienkach a aby sa dbalo na zálohy systémov a dát. Je rovnako dôležité zabezpečiť, aby dáta, ktoré napĺňajú databázy inteligentných miest, nemohli byť kompromitované. Ak systémy môžu byť napadnuté, dáta zmanipulované a sfalšované, predtým inteligentné mesto sa stane „hlúpym“ a nebezpečným miestom.

Výsledkom práce je rozsiahla rešerš určená pre neodbornú verejnosť a zoznam odporúčaní, ktoré eliminujú riziko napadnutí systémov hlavne v inteligentných domácnostiach, ale aj v priemyselných budovách alebo mestách.

Záverom svojej práce by som chcela poukázať na to, že zabezpečenie inteligentných systémov je často veľmi nedostačujúce, ale zatiaľ nebolo verejne zneužité tak veľmi, aby to

zarezonovalo celým svetom. To ale neznamená, že sa to nemôže stať. V dnešnom svete rýchleho vývoja a rozvoja je len otázkou času, kedy sa biznis s útokmi na inteligentné systémy rozbehne naplno a útočníci v dnešnej dobe majú, cestu často uľahčenú, buď vďaka nevedomosti a flegmatickému prístupu zodpovedných ľudí, alebo vďaka chýbajúcim bezpečnostným štandardom a inštitúciám, ktoré by ich jednotne vyžadovali, implementovali alebo kontrolovali.

Literatúra

[1] GARLíK, Bohumír. *Elektrotechnika a Inteligentní budovy.* Praha : ČVUT, 2010.

[2] LAUTERBACH, Michal. *Software pro správu a konfiguraci Z-Wave zařízení*[online]. Univerzita Pardubice, 2017. Dostupné z: <https://dk.upce.cz/handle/10195/68124>. [Online; cit.: 2018-05-28].

[3] PETERKA, Jiří. *Báječný svět počítačových sítí: Část XXIV: Wi-Fi.* EArchiv: Archiv článků a přednášek Jiřího Peterky [online], 2007. Dostupné z: <http://www.earchiv.cz/b07/b0400001.php3>. [Online; cit.: 2018-05-16].

[4] Český telekomunikační úřad. *Využívání vymezených rádiových kmitočtů.* Dostupné z: <https://www.ctu.cz/vyuzivani-vymezenych-radiovych-kmitoctu>. [Online; cit.: 2018-05-28].

[5] Webová stránka společnosti KNX. Dostupné z: <https://www.knx.org/cz/KNX-CZ/index.php>. [Online; cit.: 2018-05-20]

[6] YLONEN, T. et al. The Secure Shell (SSH) Protocol Architecture. RFC 4251, RFC Editor, 2006. Dostupné z: <http://www.rfc-editor.org/rfc/rfc4251.txt>. [Online; cit.: 2018-05-10]

[7] POSTEL, J. – REYNOLDS, J. TELNET PROTOCOL SPECIFICATION. RFC 854, RFC Editor, 1983. Dostupné z: <http://www.rfc-editor.org/rfc/rfc854.txt>. [Online; cit.: 2018-05-10]

[8] FIELDING, R. et al. Hypertext Transfer Protocol – HTTP/1.1. RFC 2616, RFC Editor, 1999. Dostupné z: <http://www.rfc-editor.org/rfc/rfc2616.txt>. [Online; cit.: 2018-05-10]

[9] RESCORLA, E. HTTP Over TLS. RFC 2818, RFC Editor, 2000. Dostupné z: <http://www.rfc-editor.org/rfc/rfc2818.txt>. [Online; cit.: 2018-05-10]

[10] KUNC, Josef. *Bezpečná a efektivní komunikace s KNX instalcí.* Dostupné z: <http://www.knxcz.cz/wp-content/uploads/2017/03/kunc2korig.pdf>. [Online; cit.: 2018-05-10].

[11] SEDLÁK, Jan. *Nesahat, hlavně že to funguje. Průmyslové a energetické systémy jsou v ČR výrazně děravé.* 2017. Dostupné z: <https://www.lupa.cz/clanky/nesahat-hlavne-ze-to-funguje-prumyslove-a-energeticke-systemy-jsou-v-cr\-vyrazne-derave/>. [Online; cit.: 2018-05-10].

[12] PETERKA, Jiří. *Na počátku byl ARPANET .....* EArchiv: Archiv článků a přednášek Jiřího Peterky [online]. Dostupné z: <http://www.earchiv.cz/a95/a504c502.php3>. [Online; cit.: 2018-05-28].

[13] MALIK, Yogesh. *Smart, Connected and IoT Based Devices. What's The Difference?.* Dostupné z: <https://medium.com/all-technology-feeds/smart-connected-and-iot-based-devices-whats-the-difference-36fc1bdc36b2>. [Online; cit.: 2018-05-20].

[14] GAMROT, Daniel. *Automatizace práce prostřednictvím IFTTT.* Dostupné z: <http://danielgamrot.cz/automatizace-prace-prostrednictvim-ifttt/>. [Online; cit.: 2018-05-20].

[15] *Referenční model ISO/OSI.*[online]. Dostupné z: <https://cs.wikipedia.org/wiki/Referen%C4%8Dn%C3%AD_model_ISO/OSI>. [Online; cit.: 2018-05-28].

[16] Česká republika. *Trestný zákoník, Část druhá, Hlava V §230.* zakonyprolidi.cz. Dostupné z: <http://zakony.centrum.cz/trestni-zakonik/cast-2-hlava-5-paragraf-230>. [Online; cit.: 2018-05-10]

[17] THIBODEAUX, Todd. *Smart Cities Are Going to Be a Security Nightmare*[online],2017. Dostupné z: <https://hbr.org/2017/04/smart-cities-are-going-to-be-a-security-nightmare>. [Online; cit.: 2018-03-10].

[18] YOUNG, Angelo. *Smart cities can be vulnerable: That Dallas emergency siren hack is a warning of things to come*[online],2017. Dostupné z: <https://www.salon.com/2017/04/14/smart-cities-can-be-vulnerable-that-dallas-emergency-siren-hack-is-a\-warning-of-things-to-come/> [Online; cit.: 2018-03-10].

[19] LEYDEN, John. *Polish teen derails tram after hacking train network*[online],2008. Dostupné z: <https://www.theregister.co.uk/2008/01/11/tram_hack/>. [Online; cit.: 2018-03-10].

[20] CHEREPANOV, Anton, LIPOVSKY, Robert. *Industroyer: Biggest threat to industrial control systems since Stuxnet*[online],2017. Dostupné z: <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/?utm_source=twitter&utm_medium=social&utm_campaign=fanpage>. [Online; cit.: 2018-03-10].

[23] CHEREPANOV, Anton. *BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry*[online],2016. Dostupné z: <https://www.welivesecurity.com/2016/01/03/blackenergy-sshbeardoor-details-2015-attacks-ukrainian-news-media-electric>. [Online; cit.: 2018-03-10].

[22] CERRUDO, Cesar. *An Emerging US (and World) Threat:Cties Wide Open to Vyber Attacks.* 2015.

[23] Antonini A., Maggi F., Zanero S. *A Practical Attack Against a KNX-based Building Automation System*[online],2014. Dostupné z: <https://ewic.bcs.org/upload/pdf/ewic_icscsr14_paper7.pdf>. [Online; cit.: 2018-04-15].

[24] KLADIVOVÁ, Barbora. *Česko v boji proti kyberkriminalitě zaostává. Každá třetí firma čelí hackerskému či hospodářskému útoku* [online],2018. Dostupné z: <https://www.irozhlas.cz/ekonomika/kyberkriminalita-v-cesku-hackerske-utoky-na-firmy_1803230730_jak>. [Online; cit.: 2018-05-28].

[25] ČÍŽEK, Jakub. *Mnozí zákazníci UPC stále riskují. Jejich Wi-Fi modemy jsou často špatně zabezpečené*[online],2016. Dostupné z: <https://www.zive.cz/clanky/mnozi-zakaznici-upc-stale-riskuji-jejich-wi-fi-modemy\-jsou-casto-spatne-zabezpecene/sc-3-a-181708/default.aspx>. [Online; cit.: 2018-05-28].

Dodatok A

Zoznam použitých skratiek

APCI application protocol control information

BAS Building Automation Systems

BMS Building Management Systems

CCTV uzavreté kamerové systémy/televízia

CERT Computer emergency response team

CMS City Management Systems

DALI Digital addressable Lighting Interface

DDoS Distributed Denial of Service

DNS Domain Name Server

DoS Denial of Service

EMCS Emergency Management and Control Systems

EMS Emergency Management System

EPS protipožiarne systémy

EZS elektronické zabezpečovacie systémy alebo signalizácie

FMS Facility Management Systems

IANA Internet Assigned Numbers Authority

iBMS Intelligent Building Management Systems

IEEE Institute of Electrical and Electronics Engineers

IFTTT If This Then That

IoT Internet of Things

IP Internetový protokol

IRC Individual room control

LAN Local Area Network

LPWAN Low Powered Wide Area Network

M2M Machine to Machine

M2M Machine to machine

MAN Metropolitan Area Network

Meranie a regulácie MaR

MITM Man in the middle

NAT Network Address Translation

OSI Open Systems Interconnection

P2P peer-to-peer

PAN Personal Area Network

SaaS Software as a service

SCADA Supervisory Control and Data Acquisition

SLC Sauter Logic Control

TZB technických zariadení budov

VPN Virtual Private Network

WAN Wide Area Network

Prehľad ľudí o bezpečnosti inteligentných systémov

Prehľad ľudí o bezpečnosti inteligentných systémov

*Povinné pole

1. **Pohlavie** *
   Označte jen jednu elipsu.
   - ◯ muž
   - ◯ žena

2. **Vek** *
   Označte jen jednu elipsu.
   - ◯ 0-19
   - ◯ 20-29
   - ◯ 30-39
   - ◯ 40-49
   - ◯ 50-59
   - ◯ 60-viac

3. **Zaujímate sa o akékoľvek témy súvisiace s informatikou a novými technológiami?** *
   Označte jen jednu elipsu.
   - ◯ áno
   - ◯ nie

4. **Ako uchovávate svoje dôležité heslá?** *
   Dôležité heslá môžu byť heslá k internetovému bankovníctvu, k e-mailu, osobnému Facebooku, k dôležitej aplikácií, atď... Heslá k náhodnej internetovej službe, ktorú nepoužívate pravidelne a ktorá nemanipuluje s vašimi osobnými údajmi nie sú pre túto anketu dôležité.
   Zaškrtněte všechny platné možnosti.
   - ☐ pamätám si ich
   - ☐ uložené v prehliadači
   - ☐ napísané na papieri
   - ☐ uložené v dokumente v počítači
   - ☐ uložené v dokumente na flash disku alebo inom externom úložisku
   - ☐ používam správcu hesiel (software na výrobu a ukladanie hesiel)
   - ☐ Jiné: _____

5. **Ako často si meníte svoje dôležité heslá?** *
Označte jen jednu elipsu.

- nikdy
- raz za niekoľko rokov
- raz za rok
- raz za pol roka
- raz za 3 mesiace
- raz za mesiac
- častejšie

6. **Ako veľmi veríte, že je silné heslo dôležité?** *
Označte jen jednu elipsu.

- veľmi dôležité - s dobrým heslom sa mi takmer nič nemôže stať
- stredne dôležité - silné heslo je základ a väčšinou stačí
- málo dôležité - je to takmer zbytočné
- vôbec

7. **Používate pre rôzne dôležité služby rovnaké heslá?** *
Dôležité služby sú myslené služby, ktoré majú prístup k vašim peniazom, osobným dátam a identite (bankovníctvo, email, Facebook, účet v leteckej spoločnosti na nákup leteniek, atď)
Označte jen jednu elipsu.

- áno
- nie

8. **Čo si predstavíte pod pojmom Inteligentná budova / domácnosť?** *
Stačí stručná odpoveď jednou vetou. Ak nemáte predstavu, použite "neviem, nie som si istý" a pod.

9. **Čo si predstavíte pod pojmom IoT (Internet of Things)?** *
   Stačí stručná odpoveď jednou vetou. Ak nemáte predstavu, použite "neviem, nie som si istý" a pod.

10. **Napíšte kľúčové slová, ktoré vám napadnú pri spojení "počítačová bezpečnosť"** *
    Názvy technológií, dôležité pojmy, čokoľvek. Napr. "heslá, šifrovanie dát" a podobne. Nepíšte viac než 10 slov.

11. **Máte doma zariadenie, ktoré je IoT / Smart?** *
    Označte jen jednu elipsu.

    - ◯ áno
    - ◯ nie
    - ◯ neviem

12. **Ak áno, aké?**

13. **Máte na váš domáci router pripojené aj iné zariadenie, než je počítač/notebook?** *
    Označte jen jednu elipsu.

    - ◯ áno
    - ◯ áno (je to len tiskárna)
    - ◯ nie
    - ◯ neviem

14. **Ak áno, aké?**

15. **Požívate doma bezdrôtovú šifrovanú sieť (Wi-Fi)?** *
Označte jen jednu elipsu.

- ◯ áno
- ◯ nie
- ◯ neviem

16. **Aké zabezpečenie vaša domáca sieť používa?** *
Označte jen jednu elipsu.

- ◯ WPA-PSK
- ◯ WPA2-PSK
- ◯ WEP
- ◯ neviem
- ◯ Jiné: _____

17. **Používa vaša domáca sieť prednastavené SSID z výroby - názov Wi-Fi?** *
Má vaša WiFi názov, ktorý jej zostal z výroby?
Označte jen jednu elipsu.

- ◯ áno
- ◯ nie
- ◯ neviem

18. **Aktualizujete pravidelne firmware svojho domáceho routeru?** *
Označte jen jednu elipsu.

- ◯ áno
- ◯ nie
- ◯ neviem

19. **Ohodnoťte stupeň dôležitosti každého z nasledujúcich pojmov (1 - najmenej dôležité, 5 - veľmi dôležité)** *
Označte jen jednu elipsu na každém řádku.

	1	2	3	4	5
dlhé heslo					
heslo ktoré obsahuje veľké a malé písmená, čísla, špeciálne znaky					
šifrovanie dát na úložisku doma					
šifrovanie komunikácie					
používanie software správcu hesiel					
zmena prednastaveného hesla v routeri (heslo k wifi)					
zmena prednastaveného názvu siete (SSID) v routeri					
zmena hesla každý mesiac					
pravidelné aktualizácie software, firmware					
zmena prednastaveného hesla do administrácie routeru					

20. **Stretli ste sa osobne s nejakými následkami po počítačovom útoku alebo s narušením počítačovej bezpečnosti?** *
Označte jen jednu elipsu.

- nie
- nie osobne, ale videl som v médiách / čítal som o tom
- nie, ale niekto z mojich známych áno
- áno

21. **Ak áno, s akými?**

22. **Myslíte si, že je dôležité dodržiavať zásady bezpečnosti na počítači?** *
Označte jen jednu elipsu.

- áno
- nie
- neviem

23. **Myslíte si, že je dôležité dodržiavať zásady bezpečnosti pri IoT a Inteligentných domácnostiach?** *
Označte jen jednu elipsu.

- áno
- nie
- neviem

24. **Myslíte, že sa s nejakým útokom alebo narušením PC bezpečnosti reálne stretnete v budúcnosti?**
Označte jen jednu elipsu.

- áno
- nie
