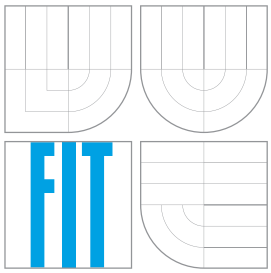
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INFORMAČNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INFORMATION SYSTEMS

BEZPEČNOSTNÍ SYSTÉM ZALOŽENÝ NA INTELIGENTNÍCH SENZORECH

SECURITY SYSTEM BASED ON INTELLIGENT SENSORS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

VOJTĚCH KUČERA

VEDOUCÍ PRÁCE
SUPERVISOR

Mgr. ROMAN TRCHALÍK, Ph.D.

BRNO 2015

Abstrakt

Cílem bakalářské práce je vytvořit návrh bezpečnostního systému na základě inteligentních seznorů a poté systém implementovat. V první části práce jsou popsány principy bezpečnostních systémů, jejich návrhu a implementace. Dále jsou přiblíženy inteligentní senzory, jejich funkce a využití. V další části práce je na základě uvedených principů vytvořen návrh bezpečnostního systému a následně je popsána jeho implementace. Bezpečnostní systém se skládá z lokálního systému, který je integrován do fyzického objektu, a serveru poskytujícího webové rozhraní. Výsledný systém monitoruje své okolí pomocí inteligentních senzorů a reaguje na bezpečnostní incidenty. V rámci webového rozhraní poskytuje přehled aktuálního stavu a historie událostí.

Abstract

The main target of this bachelor's thesis is to design and implement security system based on intelligent sensors. First part describes basic principles, design and implementation of security systems. Further are explained functions and use of intelligent sensors. The creation of design and implementation process are shown in the next part of the thesis. Security system consists of local system, which is integrated into physical building, and server providing web interface. System monitors its surroundings through intelligent sensors and responds to security incidents. Actual state and events history are available through web interface.

Klíčová slova

Bezpečnost, bezpečnostní systém, inteligentní senzory, ZigBee, návrh bezpečnostního systému, implementace bezpečnostního systému.

Keywords

Security, security system, intelligent sensors, ZigBee, security system design, security system implementation.

Citace

Vojtěch Kučera: Bezpečnostní systém založený na inteligentních senzorech, bakalářská práce, Brno, FIT VUT v Brně, 2015

Bezpečnostní systém založený na inteligentních senzorech

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením Mgr. Romana Trchalíka Ph.D. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

.....
Vojtěch Kučera
18. května 2015

Poděkování

Děkuji svému vedoucímu Mgr. Romanu Trchalíkovi Phd. za odborné vedení a informace, které mi při tvorbě této práce poskytl.

Obsah

Seznam obrázků

Seznam tabulek

Kapitola 1

Úvod

Bezpečnostní systémy jsou v dnešní době již samozřejmostí u velkých i menších společností. S pokračujícím technologickým vývojem se stávají dostupnými i pro širší veřejnost a to především do domácností. Na trhu je možné nalézt nespočet řešení od různých dodavatelů. Rozmanité jsou i technologie, které se pro implementaci bezpečnostních systému dají využít. Nicméně, ač jsou jednotlivá řešení rozdílná, všechy bezpečnostní systémy jsou postaveny na společných principech.

Cílém této práce je v první řadě popsat principy fungování bezpečnostních systémů a uvést jaké technologie se v praxi využívají. Popsána bude také funkce intelignetních senzorů v bezpečnostních systémech, jejich principy a zakomponování do systému. Hlavní částí práce je využití takto popsaných principů a technologií pro návrh a praktickou implemetaci bezpečnostního systému. Implementace si klade za cíl použít již ověřená open-source řešení, která v kombinaci s vybranými elektronickými zařízeními umožní vytvořit spolehlivý bezpečnostní systém pro obecné použití.

Podrobnosti o struktuře systému budou popsány v následujících kapitolách, k úvodu však uveďme, že dle zadání, bude vytvořený systém schopen monitorovat prostředí do kterého bude integrován, zaznamenávat definované události a dle nastaveného chování na ně reagovat např. spuštěním poplachu, informováním uživatele emailem apod. Skrze webové rozhrání pak bude uživateli umožněno prohlížet veškerou zaznamenanou historii událostí a reakcí na tyto události.

Kapitola 2

Bezpečnostní systémy s inteligentními senzory

Bezpečnostní systém je definován jako soustava koordinovaných subsystému s různou funkčností, které jsou integrovány v jeden celistvý systém. Jako příklad takových subsystémů lze uvést pohybové snímače, přístupové klávesnice, poplachové sirény nebo jiná elektronická zařízení. Hlavní úkol bezpečnostního systému je zajistit bezpečnost svého okolí a reagovat na možná ohrožení. [7]

Při návrhu a poté i při implementaci bezpečnostního systému je velmi kladen důraz na spolehlivost, která je od systému v první řadě očekávána. Na spolehlivosti těchto systémů může záviset nejen hmotný majetek(domácí zabezbečovací systémy), kapitál(bankovní systémy), ale i lidské životy(bezpečnostní systémy jaderných elektráren).[3]

2.1 Co je to bezpečnost

Bezpečnost je v širokém úhlu pohledu možné vnímat jako ochranu hodnot před potenciálními hrozbami a minimalizaci dopadu při výskytu takových hrozeb. Bepečnost lze zajistit preventivně, reaktivně a pomocí odstrašujících řešení. Při prevenci může být použito varovných oznámení a upozornění napříč dostupnými médii. Detekování ohrožení hodnot již pouze varuje na konkrétní ohrožení a minimalizuje jeho dopad. Jedná-li se o ohrožení způsobené člověkem nebo skupinou, lze je za toto chování penalizovat či potrestat, což může sloužit jako odstrašující případ pro zamezení opakování se dané situace.

V dnešním světě vnímame jako nejcennější hodnotu lidský život, který je třeba chránit před mnohými hrozbami. K dispozici máme systémy detekující přírodní katastrofy mnohdy s možností včasného varování nebo dokonce i s určitou mírou predikce, dále systémy zamezující teroristickým útokům, které pomocí kamer detekují podezřelé chování lidí nebo upozorňují na výskyt zbraní či výbušnin.

Další hodnotou, kterou se snažíme ochránit je převážně majetek, ať už se jedná o hmotné bohatství, nebo kapitál. Existuje nespočet bezpečnostních systémů střežících budovy bank, státních institucí, komerčních společností nebo i domácností. Ochrana majetku je však velmi často spojena i s ochranou životů. Bankovní bezpečnostní systémy, ač primárně ochraňující peníze, maji integrovaný i požární systém.

Neposlední, avšak velmi opomíjenou hodnotou, je naše identita. S globálním rozšířením internetu a propojením velkého množství elektronických zařízení a systémů, se dostala do ohrožení i lidská virtuální identita. To čím jsme, tedy naše pravá identita, zůstává stále

pouze naše. Naše virtuální identita, pod kterou vystupujeme na internetu, a která se stále více integurje do reálného světa, však zneužita být může. Pro příklad lze uvést odcizení elektronického podpisu. Elektronický podpis zaručuje, že elektronické dokumenty jím podepsané pocházejí z ověřeného zdroje, tedy od konkrétní osoby. Útočník, který získal přístup k elektronickému podpisu tak může vystupovat ve jménu této osoby a na základě své motivace způsobit nemalé škody. Bezpečnostní systémy tak musí v dnešní době řešit i zabezpečení virtuální lidské identity proti zneužití.[7]

2.2 Principy bezpečnostních systémů

Základním požadavkem na bezpečnostní systém je, aby zajistil spolehlivost, tedy ochraňoval naše hodnoty i přes pokusy o prolomení systému, chyby, a náhodné události, které by mohli způsobit ohrožení. [3]

V první řadě je velmi důležité si uvědomit, jaké chování je od bezpečnostního systému vyžadováno. U některých systémů je priorita chránit jejich uživatele před extrerními hrozbami, v jiném případě je prioritou systému chránit svá citlivá data před některými uživateli. Jakmile je jasně řečeno, jake jsou obecné požadavky na bezpečnostní systém, je možné začít s tvorbou bezpečnostního programu. [7]

Tvorba bezpečnostního programu je proces, kdy se postupně vytvoří seznam potenciálních hrozeb, na jehož základě se vybuduje bezpečnostní politika, která slouží k omezení výskytu a dopadu hrozeb. Jakmile je bezpečnostní politika vytvořena, dochází k praktickému ipmlementování bezpečnostních mechanizmů pro kontrolování, monitorování a vynucování bezpečnostní politiky. [9]

2.2.1 Fyzická bezpečnost

U informačních bezpečnostních systémů je při uvádění bezpečnosti především myšleno správné nastavení firewallů, šifrovaných protokolů a hesel, monitoring sítě a systémy pro prevenci a detekci síťových útoků. U bezpečnostních systému je tento přístup správný a nutný, méně už je však myšleno na fyzickou bezpečnost. Je-li objekt, ve kterém se nachází zařízení bezpečnostního systému, volně přístupný i nepovolaným osobám, může se jednodše stát, že se tato osoba dostane k zapnutému počítači, který je navíc přihlášen do systému. Tento případ je nejvíce nápadný, zkušeným útočníkům postačí nehlídaná síťová přípojka.

V rámci zajištění fyzické bezpečnosti se používá mnoha přístupů a záleží především na velikosti objektu a kritičnosti jeho zabezpečení. Obrázek si jistě každý udělá sám, když srovná fyzickou bezpečnost na terminálu letiště například s obchodem. K dispozici je mnoho technologií, které jsou buď samostatně fungující, nebo mohou být přímo spojeny s bezpečnostním systémem. Pro příklad lze uvést bezpečnostní dveře a zámky, klíče, závory nebo např. pouze zdi. Se systémem může být spojena například závora, která pak může být vzdáleně ovládána atp.

Někde na pomezí fyzické a elektronické bezpečnosti se vyskytují detekční a monitorující zařízení. Tato zařízení primárně ochraňují fyzický objekt, ale jsou implementována v rámci elektronického bezpečnostního systému. Původně tato zařízení fungovala samostatně, nicméně s technologickým pokrokem se stala součástí větších celků, které se nakonec vyvinuli do komplexních bezpečnostních systémů. Takových zařízení je velké množství, pro příklad lze však uvést detektory pohybu, kamerové systémy, poplachové systémy, různá spínací čidla detekující vloupání apod.

S vývojem bezpečnostních systémů postupem času rostlo i jejich využití. V dnešní době lze od takových systémů očekávat vysokou spolehlivost a bezproblémové fungování. Nicméně, na prvním místě je vždy třeba zvážit fyzickou bezpečnost a její dostatečnou úroveň.[7]

2.2.2 Míra ohrožení

Ještě před popisem konkrétních hrozeb, je třeba se zamyslet jaká je pravděpodobnost ohrožení hodnot, které jsou uvažovány. Důležité je uvědomit si jak důležitá je ochrana daných hodnot a kolik jsme ochotni do ní investovat.

Cena

Z ekonomického hlediska vyvstává otázka jak velké budou finanční ztráty, dojde-li k odcizení nebo zneužití dané hodnoty, a také jak velký zisk to přinese útočníkovi. S roustoucí cenou míněné hodnoty roste i riziko, že se stane předmětem přímého ohrožení. Také lze očekávat, že čim větší bude cena, tím zkušenějšího přístupu bude použito pro pokus o odcizení. Z takové závisloti lze vyvodit, že celková cena ochraňovaných hodnot se promítne do výše investice na pořízení bezpečnostního systému. Čím vyšší bude investice, tím kvalitnější pak bude výsledný systém.

Použité technologie

Samotné technologie, na kterých je systém postaven, mohou způsobit ohrožení. Pro udržení spolehlivosti systému je nutné aktualizovat dané tehcnologie a být na pozoru před výskytem chyb a zranitelností. Jen v roce 2014 bylo zveřejněno několik slabých míst u běžně užívaných aplikací, která měla obrovský globální dopad. Konkrétní a především kritické příklady takovýchto slabých míst jsou např. Heartbleed Bug [1] nebo Shellshock[2]. Alarmující u těchto zveřejnění bylo, že chyby byly v aplikacích již relativně dlouhou dobu.

Vystavení horzbám

Z praxe je známo mnoho případů, kdy došlo k narušení bezpečnosti systému nebo rovnou ke krádeži dat jen proto, že se k tomu naskytla příležitost. U některých systémů mohla příležitost vzniknout objevenou bezpečnostní mezerou v klientské aplikaci, ale může se jednat i o špatně definovanou bezpečnostní politiku, která výskyt takovéto příležitosti nijak neomezuje, ani neřeší. Při uvažování nad tím jak moc jsme vystaveni hrozbám máme na mysli především pravděpodobnost, že zrovna naše hodnoty budou ohroženy. Vhodné je se zamyslet také nad tím kdo může tyto hodnoty ohrozit a s jakým motivem. [9]

Hrozby

Hrozba je cokoli nebo kdokoli, kdo dokáže zneužít zranitelnosti systému. Také je možné hrozbu definovat jako náhodnou nebo úmyslnou událost, která může jakýmkoli způsobem ohrozit důležité hodnoty. [9]

Správně identifikovat hrozby je důležitější, než se na první pohled může zdát. Pokud se stane, že jsou některé hrozby podceněny nebo nejsou vůbec objeveny, a naopak jiné hrozby

[1] http://heartbleed.com/

[2] http://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability

jsou až prespříliš prioritní, může systém zarputile chránit místa, která ochranu vyžadují jen minimální a ponechávat bezpečnostní mezery na místech, kde je potřeba větší obezřetnosti. Na základě identifikovaných hrozeb se buduje bezpečnostní politika a pokud už hrozby jsou identifikovány nesprávně, pak i bezpečnostní politika bude nesprávná. [7]

2.2.3 Bezpečnostní prvky

Co se týče konkrétních přístupů bezpečnostních systémů pro zachování bezpečnosti objektu, každý bezpečnostní systém se skládá ze základních funkcí:

- odstrašení
- detekce
- posouzení
- reakce
- sběr evidence

Využití těchto funkcí zajišťují právě bezpečnostní prvky, ať už se jedná o metodologie, postupy, technické dokumenty, anebo přímo elektronická zařízení. Tyto prvky jsou spolu provázané a společně umožňují účinné řízení a kontrolu zachování bezpečnosti.[9]

Posouzení rizik

Posouzení rizik je soustava metod, které zajistí správné pochopení systémových ohrožení a jejich transformaci na hrozby. Je použito iterativního přístupu, kdy se uvažuje jedna část systému a postupně se analyzuje, jaká slabá místa by se zde mohla vyskytnout. Součástí posouzení je také odhadnutí pravděpodobnosti výskytu rizika. Pro posouzení mohou být použity různé metriky, nebo lze použít analýzu čistě konkrétního systému.

Bezpečnostní politika

Bezpečnostní politika je dokument, který jasně a stručně definuje jakých ochranných mechanizmů je třeba dosáhnout. Tvorba bezpečnostní politiky probíhá na základě uvědomění si možných bezpečnostních hrozeb. [7]

V bezpečnostní politice je pomocí stručných a výstižných vyjádření jasně popsáno chování systému a jeho uživatelů pro zachování jeho bezpečnosti. To může být docíleno buď preventivními, detekujícími nebo odstrašujícími opatřeními. Preventivní opatření popisují použití přístupů, které snižují pravděpodobnost výskytu bezpečnostního incidentu. Na výskyt bezpečnostního incidentu reagují detekující opatření, které se snaží co nejvíce snížit riziko dopadu takového incidentu. Ostrašující opatření se objevuje formou penalizace za porušení bezpečnostní politiky. Tato opatření jsou většinou používána u bezpečnostních systémů větších organizací. [9]

Bezpečnostní procedury

Bezpečnostní procedury konkrétně popisují jakým způsobem dosáhnout požadavků definovaných bezpečnostní politikou. Jako příklad lze uvést pravidlo bezpečnostní politiky: "Každá osoba se po vstupu do objektu autentizuje!", a procedura vztažená k tomuto pravidlu poté popisuje jakým konkrétním způsobem toto ověření identity proběhne. Ověření může

být buď pouze elektronické pomocí čipové karty, anebo pomocí fyzické karty zaměstnance, kterou je třeba ukázat vrátnému.

Kontrola dodržování bezpečnostní politiky

Kontrola dodržování bezpečnostní politiky, ale i kontrola stavu bezpečnosti v objektu nebo v jeho okolí je vykonávána pomocí elektronického bezpečnostního systému. Jedná se o bezpečnostní systém a jeho jednotlivá koncová zařízení a technologie. Kontroly může být dosaženo preventivním audiovizuálním upozorněním, spuštěním poplachu po detekci porušení bezpečnostní politiky nebo nahlášením osoby správcům objektu.

Centrální správa a monitoring

Bezpečnostní systémy spojují velké množství jednotlivých zařízení v jeden celek. V systému se vyskytují centrální zařízení, které umožňují přístup ke koncovým zařízením, jejich monitoring a správu. Monitoring zařízení v reálném čase navíc poskytuje dobrý přehled nad situací v daném objektu. Centrální přístup umožňuje rychlou reakci na vzniklé události a účinné řešení případných bezpečnostních incidentů. [7]

Centrální správa a monitoring

2.3 Mechanizmy bezpečnostních systémů

Pro splnění požadavků na zachování bezpečnosti a průběžnou kontrolu dodržování bezpečnostní politiky slouží různé mechanizmy. Mnoho takových mechanizmů má původ v armádních technologiích, pro které byly primárně vyvíjeny. V dnešní době však už tvoří standard u běžně používaných systémů a aplikací.[3]

2.3.1 Systém řízení přístupu

Obecně je systém řízení přístupu souhrn hardwaru, softwaru, organizační politiky nebo postupů, který uděluje nebo zamezuje přístup ke zdrojům, monitoruje a zaznamenává pokusy o přístup do systému, identifikuje osoby, které se snaží o přístup a rozhoduje, zda je přístup autorizovaný. [8]

Každý bezpečnostní systém musí být schopný identifikovat uživatele, který chce mít k systému přístup a poté rozhodnout jak velkou míru interakce uživateli poskytnout. Ať už se jedná o fyzický, nebo elektronický přístup, používá se mechanizmů identifikace, autentizace a autorizace. Identifikace a autentizace probíhají společně a buď uspějí obě, anebo žádná.

Identifikace

Identifikace je proces, kdy uživatel poskytne systému informaci o svojí identitě. Uživatel může tuto informaci předat pomocí uživatelského jména a hesla, magnetickou kartou, svým hlasem nebo pomocí biometrických údajů, např. otisk prstu, sken sítnice, sken obličeje apod. Systém musí poskytovat rozhraní, přes které je možné takto získat vzorek identity uživatele a podrobit jej autentizaci.

Autentizace

Při autentizaci dochází k ověření identity uživatele systémem. Systém porovná uživatelem poskytnutý vzorek identity se vzorky ve své databázi a dojde-li ke shodě, uživatel je považován za autentizovaného. Existují tři základní principy autentizace a jeden doplňkový:

- něco co víme(heslo, PIN)
- něco co máme(klíč, karta, token)
- něco čím jsme(biometrie)
- něco co děláme(intenzita úhozů na klávesnici apod.)

[8]

Autorizace

Po úspěšné autentizaci musí ještě proběhnout autorizace daného uživatele. Při autorizaci systém kontroluje, zda je uživatel oprávněn provést určitou akci nebo požadovat přístup k objektu. Oprávnění se kontroluje na základě nastavených přístupových práv. Přístupová práva mohou být přidělena přímo uživateli, anebo systémové skupině. Uživatel může patřit do více takových skupin, načež jsou na něj v rámci daných skupin nepřímo uplatňována přístupová práva. Ještě abstraktnější postavení mají role. Role se vztahuje k uživateli a je spojena s více skupinami. Uživatel s konkrétní rolí je pak členem skupin, které tato role spojuje, a má tak i výsledná přístupová práva.

Audit a účtovatelnost

Audit se stará o evidenci veškeré uživatelovi interakce se systémem. Každá událost, kterou uživatel spustí je uložena do historie pro pozdější zpracování. Tato historie se dá později použít pro analýzu chování uživatelů a odhalení případných pokusů o nepovolený přístup ke zdrojům. Díky auditu je možné uplatnit i účtovatelnost, kdy lze na základě uživatelova chování vyvozovat konkrétní následky. Příkladem může být uživatel, který nadlimitně využívá zabezpečeného komunikačního kanálu, jehož maximální délka užívání je omezena bezpečnostní politikou. Po překročení limitu tak může uživatel nést následky za své chování.

2.3.2 Bezpečnostní management

Bezpečnostní management je proces plánování a řízení dohledu nad zachováním určité úrovně bezpečnosti. V rámci bezpečnostního managementu jsou uvažovány jak hrozby, tak jejich zpracování a hlavně účinná protiopatření, která lze v případě výskytu bezpečnostních incidentů použít. Bezpečnostní management definuje tři základní entity a vztahy mezi nimi.

Událost

Událost je jakákoli změna stavu v okolí systému, kterou je systém schopný pomocí svých zařízení detekovat. Událost většinou detekuje koncové zařízení systému , které ji poté systému interpretuje pomocí předem dohodnutého protokolu. Takováto událost je systémem archivována a poté se provede její vyhodnocení v závislosti na aktuálním stavu systému. Na událost jsou postupně aplikována bezpečnostní pravidla a pokud je vyhodnocena jako událost ohrožující bezpečnost systému, považuje se za bezpečnostní incident.

Incident

Incident je událost, která ohrožuje bezpečnost objektu nebo porušuje pravidla bezpečnostní politiky. Incident je opět archivován. Pokud je možné určit viníka, tedy osobu nebo jev, který incident způsobil, tento atribut musí být zaznamenán zároveň s incidentem. Ke každému incidentu musí být definováno protiopatření, které se provede ihned po detekci incidentu.

Protiopatření

Protiopatření jeden nebo více procesů, které slouží jako explicitní rekace na detekovaný incident. Protiopatření má za úkol minimalizovat potenciální dopad na ochraňované hodnoty a pomoci předcházet podobným incidentům do budoucna.[9]

2.4 Návrh bezpečnostního systému a implementace

Návrh bezpečnostního systému sestává s několika procesů, jejichž výstupem je struktura celkového systému a jeho jednotlivých zařízení. Pro zobrazení logických návazností a vlastností zařízení jsou použity vývojové diagramy, schémata, obrázky, tabulky apod. Při návrhu se používá přístupu shora-dolů(dekompozice), kdy se první popíše celý systém na vyšší míře abstrakce a poté se přistoupí konkrétně k jednotlivým zařízením.

Identifikace hodnot

Jako první je důležité identifikovat, které hodnoty má systém ochraňovat. Od správně definovaných hodnot se pak odvíjí identifikace hrozeb, na kterých je postavena celá bezpečnostní politika. Pokud jsou hodnoty nesprávně identifikovány nebo úplně opomenuty, může být výsledný systém nespolehlivý.

Identifikace hrozeb

Při identifikaci hrozeb vycházíme z definice hrozby uvedené v předchozí kapitole. Výstupem tohoto procesu je tabulka, která obsahuje název a stručný popis hrozby. Dále jsou v tabulce uvedeny hodnoty, kterých se tato hrozba týka, popř. pravděpodobnost s jakou se může hrozba vyskytnout.

Definice bezpečnostní politiky

Bezpečnostní politika se vytváří na základě hrozeb, kterým je třeba čelit. U každé hrozby je třeba se zamyslet za jakých okolností se může vyskytnout. V rámci politiky je pak třeba v první řadě uvést pravidla, která snižují pravděpodobnost výskytu hrozby. Nesmí být však zapomenuto na přesný popis reakce na situaci, kdy se taková hrozba vyskytne a ohrozí bezpečnost systému. Dalším prvkem politiky pak může být popis chování po dané reakci, např. její zhodnocení a opatření proti opětovnému výskytu.[3]

Specifikace

Specifikace bezpečnostního systému zahrnuje veškeré požadavky na daný systém. Je zde popsán bezpečnostní systém jako celek, jeho funkce a jakých principů využívá. Popis by

měl být obecnější tak, aby bylo možné jasně určit účel systému, ale byla ponechána jistá volnost pro specifika zvolených zařízení. Často jsou používány vývojové diagramy a ilustrační obrázky.

Každý popis konkrétního zařízení obsahuje účel daného zařízení, základní funkce, prostředí, ve kterém se zařízení vyskytuje a základní atributy zařízení. Specifikace neobsahuje konkrétní zařízení, nezaměřuje se ani na konkrétní technologie či výrobce, pouze pomocí vyšší míry abstrakce popisuje jakých cílů je třeba dosáhnout a jaké postupy pro to použít.

Také je zde popsaný tzv. komunikační protokol. Tento protokol je seznam zpráv, které budou použity pro komunikaci mezi jednotlivými zařízeními. Protokol musí být implementován tak, aby zajistil spolehlivou a korektní komunikaci mezi zařízeními.

Volba technologií

Je-li systém vhodně specifikovaný, výběr konkrétních technologií pro naplnění požadavků na systém je snadnější. Při volbě technologií se stále neuvažuje o konkrétních výrobcích. V této části se mohou vyskytovat schémata propojení jednotlivých prvků. Popsáno je jaké technologie využít pro implemetaci samotných zařízení, ale i rozhraní mezi nima. Výběr by měl probíhat na základě obecně přijímané spolehlivosti dané technologie s přihlédnutím k vlastní zkušenosti.

Výběr konkrétních zařízení

Faktorů pro výběr konkrétních zařízení může být více. V první řadě by však měli splňovat bezpečnostní požadavky. Pokud má daný komponent systému komunikovat šifrovaně, musí i vybrané zařízení podporovat šifrovanou komunikaci. Dobré je zvažovat zařízení, která jsou dobře známá a v praxi běžně užívaná. Při výběru samozřejmě hraje roli i jejich cena. [7]

Implementace

Po zhotovení kompletního návrhu lze přistoupit k implementaci. Při pořizování jednotlivých součástek a zařízení je vhodné myslet na fakt, že v rámci implementace se můžou některé součástky nechtěně poničit. Je proto dobré mít jistou rezervu. Při implementaci se postupuje od tvorby jednotlivých zařízení systému, použit je přístup zdola-nahoru. Po zprovoznění každého jednotlivého zařízení je třeba jej rovnou v rámci možností otestovat.

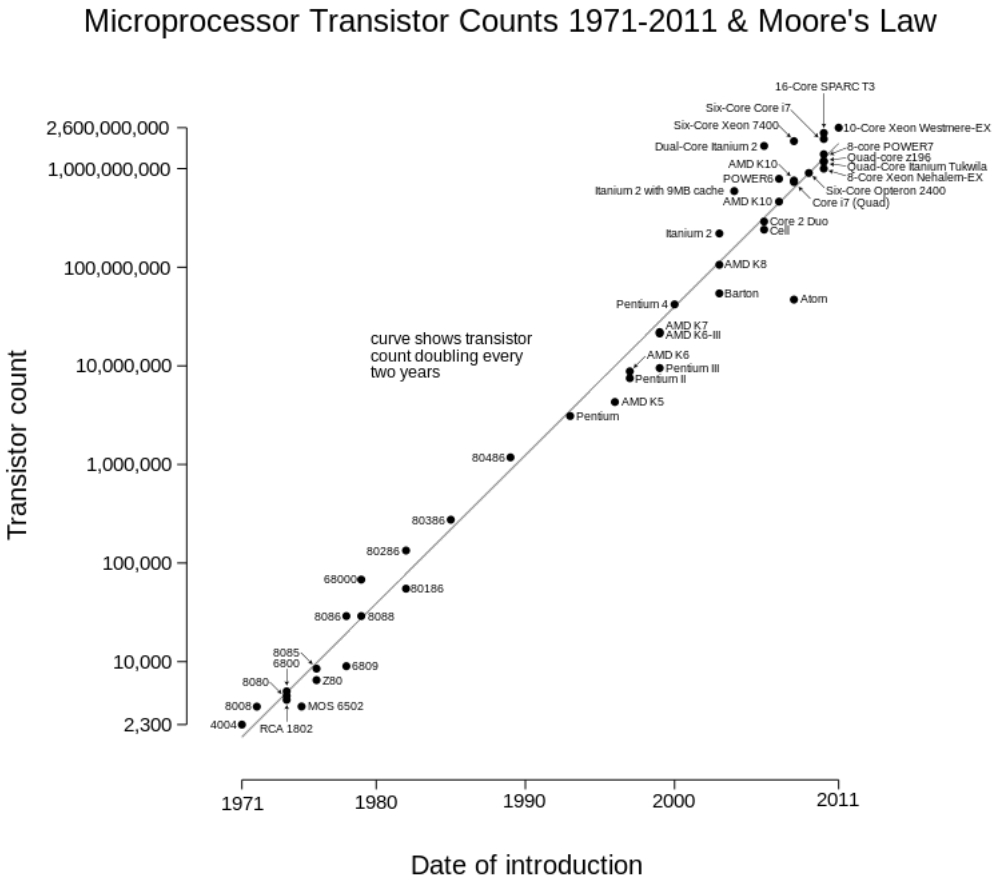
Po úspěšné implementaci a otestování jednotlivých zařízení je třeba implementovat rozhraní mezi nimi. Zde přichází v úvahu komunikační protokol, podle kterého je třeba uvést do porvozu mechanizmy pro správné zasílání zpráv mezi zařízeními. Zde je opět nutné otestovat všechna takto vzniklá rozhraní. Čím lépe jsou otestované jednotlivé části systému, tím lehčeji se pak ladí celkové chování systému při konečném testování.

V závěru implementace se všechna zařízení spojí dohromady v konečný systém a je provedeno konečné testování systému jako celku. Opravy chyb a ladění systému lze provádět právě při tomto testování. Pokud se však naskytne nějaká težce identifikovatelná chyba, je třeba se vrátit k testování jednotlivých zařízení či rozhraní a hledat tuto chybu zde.

2.5 Inteligentní senzory

Dnešní obrovské rozšíření inteligentních senzorů na trhu je znatelné. Můžeme se setkat s nepřeberným množstvím různých typů senzorů od různých výrobců. Původ jejich úspěchu můžeme nalézt připomenutím Moorova zákonu, který říká, že každý rok se na procesorech

zdvojnásobuje počet tranzistorů(Obrázek 2.1). Poukažme hlavně na ekonomický dopad Moorova zákonu, který se projevuje klesající cenou a miniaturiazcí elektronických součástek a širším spektrem jejich využití. Elektronické součástky se tak stávají dostupnějšími i širší veřejnosti.



Obrázek 2.1: Moorův zákon
[10]

2.5.1 Cesta k inteligentním senzorům

Pro správné pochopení významu inteligentních senzorů, je třeba prvně uvést funkci klasických senzorů a jejich využití. Senzor je v tomto případě elektronické zařízení, jehož funkcí je snímání fyzikálních veličin. Snímanou veličinu poté převádí nejčastěji na elektrický signál. [1]

Pomocí senzorů je možné měřit obrovské množství veličin. Asi nejčastěji měřenou veličinou je v praxi teplota, dále pak vlhkost, tlak, pH a nespočet dalších. Velkou výhodou senzorů je nejen jejich schopnost spolehlivě snímat požadované veličiny, ale i možnost učinit měření na místech, které jsou pro pobyt člověka nepříznivé. Senzory poskytují výstupy stovky, až tísíce metrů pod mořskou hladinou, v kráteru aktivní sopky nebo v radioaktivní zóně jaderné elektrárny. [6]

Jednou z hlavních nevýhod klasických senzorů je nutnost jejich kalibrace před použitím. Nedojde-li ke kalibraci senzoru, podává pak nepřesná měření, což může být u jistých aplikací kritické. Přesnost měření pak také záleží na vzdálenosti senzoru od zařízení, které zpracovává tato měření. Čím dále je toto zařízení umístěno od senzorů, tím menší bývá přesnost měření. [6]

2.5.2 Inteligentní senzory

Narozdíl od klasických senzorů, které pouze převádí fyzikální veličinu na elektrický proud, mají inteligentní senzory jistou míru inteligence a jsou schopny snímanou veličinu zpracovat. Umožňuje jim to integrace s mikrokontrolérem, mikroprocesorem nebo logickými obvody, které se většinou nachází společně se senzory na jednom čipu. Primární funkcí může být převod analogového signálu na signál digitální pomocí AD převodníku, ale poskytovat může i funkce pro sebeidentifikaci, testy, kalibraci nebo komunikaci s ostatními zařízeními. [2]

Běžně jsou uváděny tři základní požadavky, které musí inteligentní senzory splňovat, aby dostály svému pojmenování:

1. snímací prvek, snímá jednu nebo více fyzikálních veličin, jedná se o klasický senzor popsaný výše
2. výpočetní prvek, zpracovává měřenou veličinu, převádí měření na digitální signál
3. rozhraní pro komunikaci, umožňuje zařízení komunikovat s ostatními zařízeními

[6]

Využití

Využití inteligentních senzorů nacházíme napříč všemi technickými ale i netechnyckými obory. Jako konkrétní příklady můžeme uvést automatické výrobní linky, kdy na se základě výstupů inteligentních senzorů rozhoduje, v jaké fázi se výroba nachází. U některých systému se pomocí inteligentních senzorů výroba přímo řídí.

Další využití nalezneme ve zdravotnických zařízeních, ať už jako součást zařízení pro různá vyšetření nebo přímo zařízení monitorující pacientův stav. Obecně jsou inteligentní senzory velmi rozšířene v oblastech, kde je velká potřeba monitorování a případné automatizace. To ocení firmy zabývající se logistikou a přepravou, ale také bezpečnostní.[2]

2.5.3 ZigBee

ZigBee je standard, který definuje sadu komunikačních protokolů, které umožňují bezdrátovou komunikaci nenáročnou na datový obsah a komunikační vzdálenost. Maximální rychlost přenosu dat je 250Kb za sekundu a pro přenos se využívají frekvenční pásma 868MHz, 915MHz a 2.4GHz. ZigBee technologie se používají především u aplikací, kde je kladen důraz na dlouhou výdrž zařízení, jejich nízkou cenu a nízké nároky na rychlost datového přenosu. Těchto vlastností využívají právě sítě inteligentních senzorů, protože bezdrátově potřebují komunikovat pouze velmi úsporně, senzorů je v síti větší množství, takže je zohledněna jejich cena, a konečně senzory potřebují dlouhou výdrž při napájení z baterií. Díky tomu je ZigBee vhodná technologie pro aplikace inteligentních senzorů.

ZigBee standard je vyvíjí ZigBee alliance [3], což je organizace velkého množství různých společností od softwarových firem až po výrobce elektronických součástek. Jedná se o neziskovou organizaci a kdokoli se může připojit.[5]

Typy zařízení

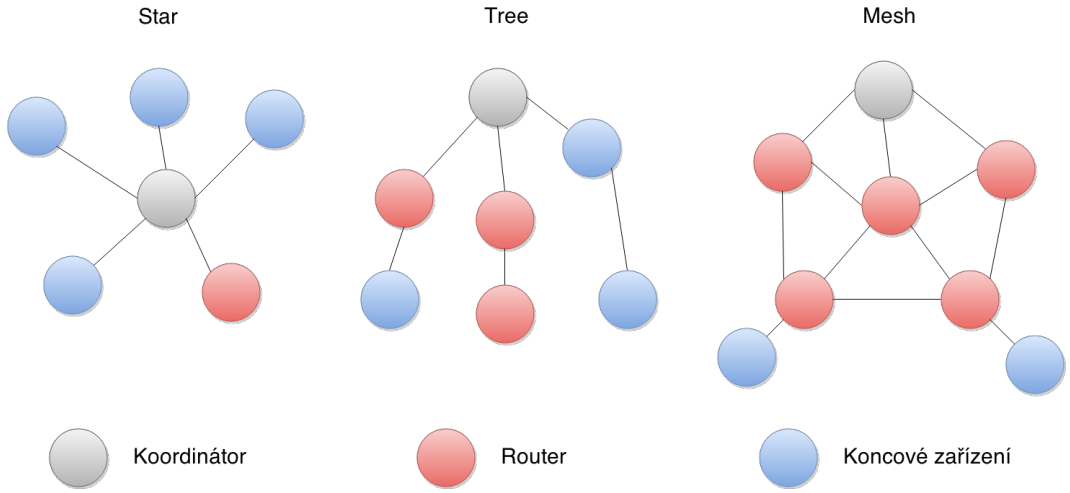
Každé ZigBee zařízení může být typu koordinátor, koncové zařízení nebo router. Koordinátor může být v síti pouze jeden a stará se o aktuální strukturu sítě a její bezpečnost. Routerů může být libovolné množství a zvětšují rozsah sítě. Koncových zařízení může být také libovolné množství a plní konkrétní úkoly v senzorové síti.[11]

Topologie sítě

Strukturu sítě popusjí tři základní topologie: hvězdice, strom a mesh. Hvězdicovitá(star) topologie obsahuje několik koncových zařízení a pouze jediný koordinátor. Koncová zařízení mohou komunikovat pouze s koordinátorem. Tato topologie je nejjednodušší na implementaci, ale pokud dojde k vyřazení koordinátoru z provozu, celá síť je nefunkční.

Ve stromové topologii(tree) se opět objevuje pouze jediný koordinátor, který je kořenem stromu. Větve tohoto stromu jsou tvořeny routery a listy koncovými zařízeními. Koncová zařízení mohou pak komunikovat pouze se svými rodiči.

V mesh topologii spolu mohou komunikovat jakékoli dva routery mezi sebou. Opět se zde vyskytuje pouze jediný koordinátor a libovolné množství routerů a koncových zařízení. Dojde-li k vyřazení nějakého zařízení, routovací protokoly zajistí alternativní cestu pro doručení zprávy na cílovou adresu. Nová zařízení lze jednoduše přidávat a rozšiřovat tak rozsah sítě.



Obrázek 2.2: Topologie ZigBee sítě

Komunikace

Každé zařízení v síti má unikátní 64 bitovou adresu, maximální počet zařízení v jedné síti je tak 2^{64}.

[3] http://www.zigbee.org/

Pro připojení zařízení k síti je třeba, aby zařízení zaslalo asociační požadavek na koordinátor. Koordinátor je tímto požadavkem upozorněn, že se zařízení chce připojit a připojení buď povolí, nebo zamítne. Chce-li zařízení opustit síť, zasílá koordinátoru disasociační požadavek. [4]

Bezpečnost

Zprávy, které jsou odesílány, mohou být zachyceny a zneužity útočníkem. Z toho důvodu ZigBee poskytuje šifrování zprávy před odesláním pomocí standardu AES [4]. Tuto zprávu je schopný rozšifrovat pouze její příjemce. Další možností narušení bezpečnosti je, že útočník zprávu pouze pozmění bez nutnosti jejího dešifrování. ZigBee tomu předchází přidáním MIC kódu do zprávy. Tento kód informuje příjemce, že zpráva nebyla pozměněna. Největší nebezpečí pro ZigBee sítě je fyzický přístup útočníka k zařízením. Pokud se útočník dostane ke konkrétnímu zařízení, může z jeho paměti přečíst bezpečnostní klíče, anebo pomocí něj přímo komunikovat se sítí. Fyzická bezpečnost zařízení se u různých výrobců liší.

Využití

ZigBee technologie má téměř neomezené možnosti využití. Nejčastěji se při konkrétních aplikacích ZigBee technologie mluví o průmyslové automatizaci, domácí automatizaci, zdravotnictví, sledování pohybu a dalších. V rámci domácí automatizace se uvádí i bezpečnostní systémy, kde kromě základních funkcí jako jsou ovládání vytápění, světel, domácích spotřebičů, obsahují systémy i detektory pohybu, tříštění skla a kamery, které jsou integrované pro splnění základních požadavků na zajištění bezpečnosti objektu.[5]

[4] Dostupný na http://csrc.nist.gov/

Kapitola 3

Návrh bezpečnostního systému

V této kapitole bude popsán návrh bezpečnostního systému. Systém bude zaměřen především na menší, až středně velké objekty, ve kterých se budou vyskytovat lidé a hmotný majetek. Důraz bude kladen na zabezpečení interiéru, ale některé bezpečnostní prvky, jako např. pohybové senzory, je možné využít i pro zabezpečení okolí objektu. Při návrhu konkrétního systému bude využito poznatků z předchozí kapitoly.

3.1 Identifikace hodnot

Jak už bylo uvedeno v kapitole 2, jako nejdůležitější hodnotu vnímáme lidský život, proto bude brána jako nejkritičtější. Další hodnotou, na kterou bude při návrhu myšleno bude hmotný majetek, tedy jakýkoli hmotný předmět uvnitř objektu, který představuje jistou finanční hodnotu. K hmotnému majetku lze ještě přidat důležité dokumenty, které by se mohly stát předmětem odcizení. Obojí bude dále uváděno pouze jako majetek. Na závěr je nutné se zaměřit na bezpečnost samotného systému a hlavně informací, které uchovává. Pokud by došlo ke krádeži těchto informací, mohly by být využity pro další škodlivou činnost. Data o bezpečnostních stavech systému by se dali využít např. pro odhadnutí, kdy je objekt obýván nebo naopak prázdný apod.

Základní hodnoty, které bude bezpečnostní systém ochraňovat jsou :

- lidský život
- majetek
- informace v bezpečnostním systému

3.2 Identifikace hrozeb

Na základě identifikovaných hodnot lze nyní uvažovat čím mohou být tyto hodnoty ohroženy.

Požáry

Jedním z nejčastějších ohrožení lidského života v objektech jsou v České republice požáry. Český statistický úřad uvádí v roce 2014 17 388 požárů, při kterých přišlo o život 114 lidí a 1 179 bylo zraněno. [14] Kromě lidského života ohrožuje požár zároveň i majetek.

Únik nebezpečných látek

Dalším ohrožením lidského života je únik nebezpečných látek. Tato práce se zaměřuje především na únik oxidu uhelnatého. Oxid uhelnatý člověk není schopen rozeznat, je bez zápachu, barvy a chuti. Vzniká při nedokonalém spalování, v praxi při používání plynového sporáku, krbových kamen apod. S rostoucí koncetrací v objektu roste i míra ohrožení lidského života. Často si postižená osoba uvědomí příčinu až v pokročilém stádiu otravy, jejíž průběh je poté velmi rychlý. [12]

Krádež

Dle českého statistického úřadu bylo v roce 2014 evidováno 49 304 krádeží vloupáním.[13] Motivací pachatele je především odcizení fyzického majetku, může však jít o krádež důležitých dokumentů a informací. Při krádeži může být ohrožen i lidský život, tuto hrozbou by však mělo primárně minimalizovat fyzické zabezpečení objektu.

Krádež dat z informačního systému

V potaz musí být brána i bezpečnost elektronických dat v bezpečnostním systému. Hlavní hrozbu představuje přímý elektronický útok na centrální server bezpečnostního systému, který uchovává citlivá data. Útok však může být veden i na jednotlivá bezpečnostní zařízení, která mohou umožňit komunikaci se serverem. Další typ útok je pak útok přímo na komunikaci. Alternativní hrozbou je fyzický útok na server, kdy je útočník schopen fyzického přístupu k serveru.

3.2.1 Hrozby

Výstupem procesu identifikace hrozeb je níže uvedená tabulka.

Hrozba	**Ohrožené hodnoty**	**Popis hrozby**
Požár	Životy, majetek	Výskyt požáru v objektu
Únik CO	Životy	Výskyt CO v objektu
Krádež vloupáním	Majetek	Vloupání do objektu s cílem odcizit majetek
Fyzický útok na server	Citlivé informace	Vloupání do objektu se serverem s cílem zneužití informací
Elektronický útok na server	Citlivé informace	Vzdálený přístup na server s cílem zneužití informací

Tabulka 3.1: Hrozby

3.3 Bezpečnostní politika

Na základě identifikovaných hrozeb bude vytvořena bezpečnostní politika.

3.3.1 Základní entity

V první řadě je třeba definovat základní entity, které se budou v systémy vyskytovat.

Bezpečnostní systém

Soustava všech elektronických zařízení sloužících k zajištění bezpečnosti objektu.

Zabezpečený stav

Stav bezpečnostního systému, kdy při pohybu osoby v objektu vyžaduje systém její autentizaci.

Nezabezpečený stav

Stav bezpečnostního systému, kdy při pohybu osoby v objektu nevyžaduje systém její autentizaci.

Objekt

Vymezený fyzický prostor, na který se uplatňují pravidla bezpečnostní politiky.

Osoba

Člověk, který se fyzicky vyskytuje v objektu.

Uživatel bezpečnostního systému

Člověk, který má fyzický přístup do objektu a zároveň elektronický přístup do bezpečnostního systému.

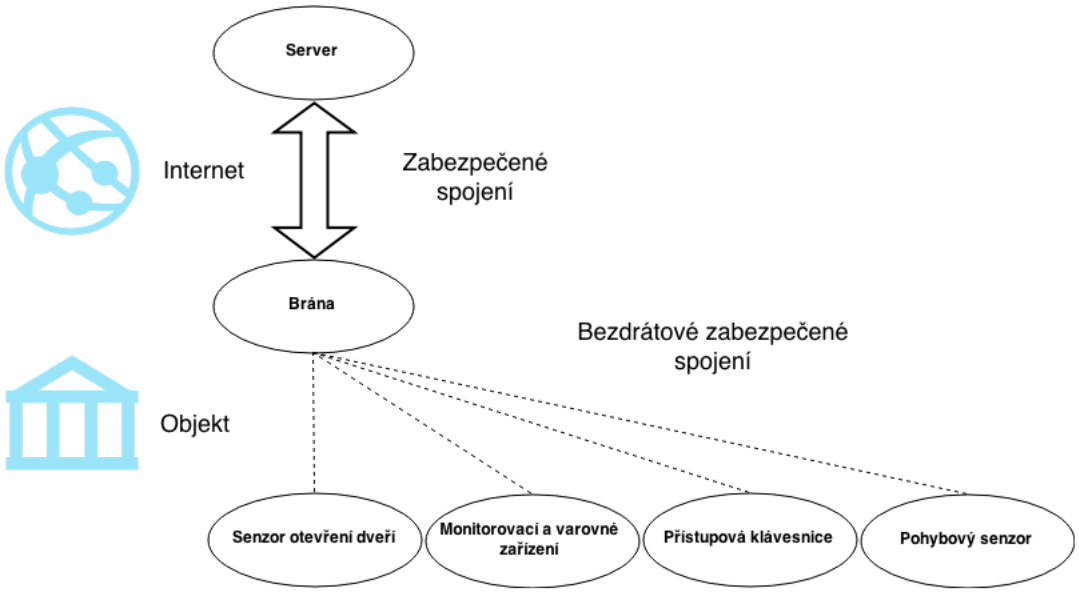
3.3.2 Jednotlivá pravidla

- v případě požáru je lokálně a zároveň vzdáleně informován uživatel bezpečnostního systému
- v případě úniku nebezpečných plynů je lokálně a zároveň vzdáleně informován uživatel bezpečnostního systému
- v případě pohybu osoby v objektu v zabezpečeném stavu je vyžadována autentizace této osoby
- není-li osoba úspěšně autentizována do daného časového limitu, je tato událost vyhodnocena jako incident vloupání
- je-li osoba úspěšně autentizována do daného časového limitu, bezpečnostní systém změní svůj stav na nezabezpečený
- v případě vloupání systém spustí lokální poplach a vzdáleně informuje uživatele bezpečnostního systému
- všechny události jsou zaznamenávány
- veškerá komunikace v rámci bezpečnostního systému je zabezpečená

Jednotlivé události, které systém detekuje jsou detekce pohybu, detekce otevření dveří, detekce teploty, detekce oxidu uhelnatého, odkódování systému, zakódování systému. Jednoltivé incidenty, které se mohou vyskytnout jsou vloupání a požár. Protiopatření, které se vztahuje k incidentu vloupání i požáru, je spuštění lokálního poplachu a informování uživatele.

3.4 Specifikace

Bezpečnostní systém na základě definovaných hodnot, hrozeb a bezpečnostní politiky rozdělíme na dvě základní části a to lokální bezpečnostní systém a server. Rozdělení musí být fyzické, abychom omezili dopady výpadků proudu a současnému ohrožení obou systémů v případě vloupání. Obecný popis architektury systému je znázorněn pomocí diagramu(Obrázek 3.1).



Obrázek 3.1: Základní architektura systému

3.4.1 Lokální bezpečnostní systém

Lokální bezpečnostní systém bude tvořit soustava elektronických zařízení, které zajistí bezpečnost požadovaného objektu. Tato zařízení budou dále uváděna jako koncová zařízení. Dle bezpečnostní politiky je třeba detekovat pohyb osob v objektu. Pro tuto činnost budou sloužit pohybové senzory a senzory otevření dveří.

Pro detekci požáru využito primárně teplotních senzorů a sekundárně i detektorů oxidu uhelnatého. Při detekci oxidu uhelnatého nelze okamžitě určit zda se jedná o požár nebo únik tohoto plynu, proto jeho detekce bude vždy považována za výskyt požáru. Pro zjednodušení návrhu a snížení nákladů budou teplotní čidlo, detektor oxidu uhelnatého a také siréna implemetnotvány jako jedno zařízení - monitorovací a varovné zařízení.

Autentizaci uživatele systémem bude poskytovat přístupová klávesnice. Ta bude umožňovat zadání uživatelského hesla pro odkódování systému. Dále bude umožňovat zakódování systému.

Koncová zařízení jsou spojena s bránou, která slouží pro spojení se serverem. Zařízení mohou komunikovat pouze s bránou. Žádné ze zařízení, kromě brány, nebude připojeno přímo k internetu.

Pohybové senzory

Hlavním úkolem senzoru bude spolehlivě detekovat pohyb a ihned odesílat informaci bráně. Pohybové senzory budou napájeny z baterií a komunikace s bránou bude řešena bezdrátově a zabezpečeně. Mezi vlastnosti senzoru bude patřit hlavně energetická úspornost a schopnost odelsat varovnou zprávu bráně o nízké úrovni napětí jeho baterie. Senzor lze umístit buď uvnitř objektu, nebo i vně objektu.

Senzory otevření dveří

Tento senzor při otevření dveří zašle zprávu o této události bráně. Jsou-li dveře zavřené, senzor bude ve stavu nízké energetické hladiny. Senzory otevření dveří budou také napájeny z baterií a komunikace s bránou opět bezdrátová a zabezpečená. Požadované vlastnosti jsou energetická úspornost a varování o nízké úrovni napětí. Senzor lze umístit buď uvnitř objektu, nebo i vně objektu.

Monitorovací a varovné zařízení

Toto zařízení bude schopné provádět měření teploty a oxidu uhelnatého ve stanovených intervalech a odesílat informace o měření bráně. Dále bude schopno zvukově upozorňovat před možnými ohroženími. Komunikace s bránou bude bezdrátová a zabezpečená. Vzhledem k výše uvedeným požadavkům může být napájeno buď z elektrické sítě, anebo z baterií, pokud to bude efektivní. Zařízení bude umístěno uvnitř objektu.

Přístupová klávesnice

Autentizaci uživatele systémem bude poskytovat přístupová klávesnice. Na základě bezpečnostní politiky bude klávesnice sloužit uživateli systému k autentizaci, pokud se bezpečnostní systém nachází v zabezpečeném stavu. Naopak, pokud je stav nezabezpečený, klávesnice bude umožňovat systém uvést do zabezpečeného stavu. K zabezpečení systému dojde s přednastaveným zpožděním, aby nedošlo k planému poplachu. K dispozici bude numerická klávesnice, pomocí které se zadá a odešle bezpečnostní kód. Komunikace s bránou bude bezdrátová a zabezpečená. Tento prvek bude napájen přímo z elektrické sítě a umístěn uvnitř objektu.

Brána

Brána bude sloužit jako prostředník mezi jednotlivými bezpečnostními zařízeními a serverem. Bude přijímat zprávy od jednotlivých zařízení a přeposílat je na server. Pokud je server nedostupný, musí být brána schopnat vyhodnotit přijímané zprávy, a jedná-li se o incident, okamžitě reagovat. Z tohoto důvodu je logika vyhondocování incidentů implementována právě v bráně. Brána komunikuje s konkrétními zařízeními na základě jejich adres. Komunikace je bezdrátová a zabezpečená. Propojení s internetem je řešeno drátově a komunikace do internetu je opět zabezpečená. Brána je napájena přímo z elektrické sítě a umístěna uvnitř objektu.

Na bráně bude kvůli náročnějším požadavkům na její funkce implementovaný open-source operační systém, který bude zajišťovat její správnou funkčnost a bezpečnost. Hardware může být libovolný, splňuje-li požadavek na zprovoznění operačního systému.

3.4.2 Server

Server je od lokálního bezpečnostního systému fyzicky oddělen pro zvýšení bezpečnosti. Server komunikuje s bránou lokálního bezpečnostního systému a tato komunikace je zabezpečená.

Hardwarové požadavky

Bezpečnostní systém bude multiuživatelský a schopný obsluhovat více lokálních bezpečnostních systémů. Dle počtu obsluhovaných bezpečnostních systémů se budou odvíjet hardwarové požadavky na server. V případě obsluhy jednoho systému bude server vybaven jedním procesorem, pamětí s minimální kapacitou 2GB, pevným diskem s minimální kapacitou 10 GB.

Operační systém

Server bude mít nainstalovaný aktuální open-source operační systém, který zajistí bezpečnou komunikaci s lokálním bezpečnostním systémem. Systém musí poskytovat základní funkce elektronického zabezpečení a tyto funkce musí být správně nastaveny a používány.

Databázový server

Na serveru bude nainstalována open-source databáze, která bude uchovávat data pocházející jak z lokálního bezpečnostního systému, tak i serveru samotného. Databázový server musí být schopen běžet i na jiném stroji, než se nachází webové rozhraní.

Webové rozhraní

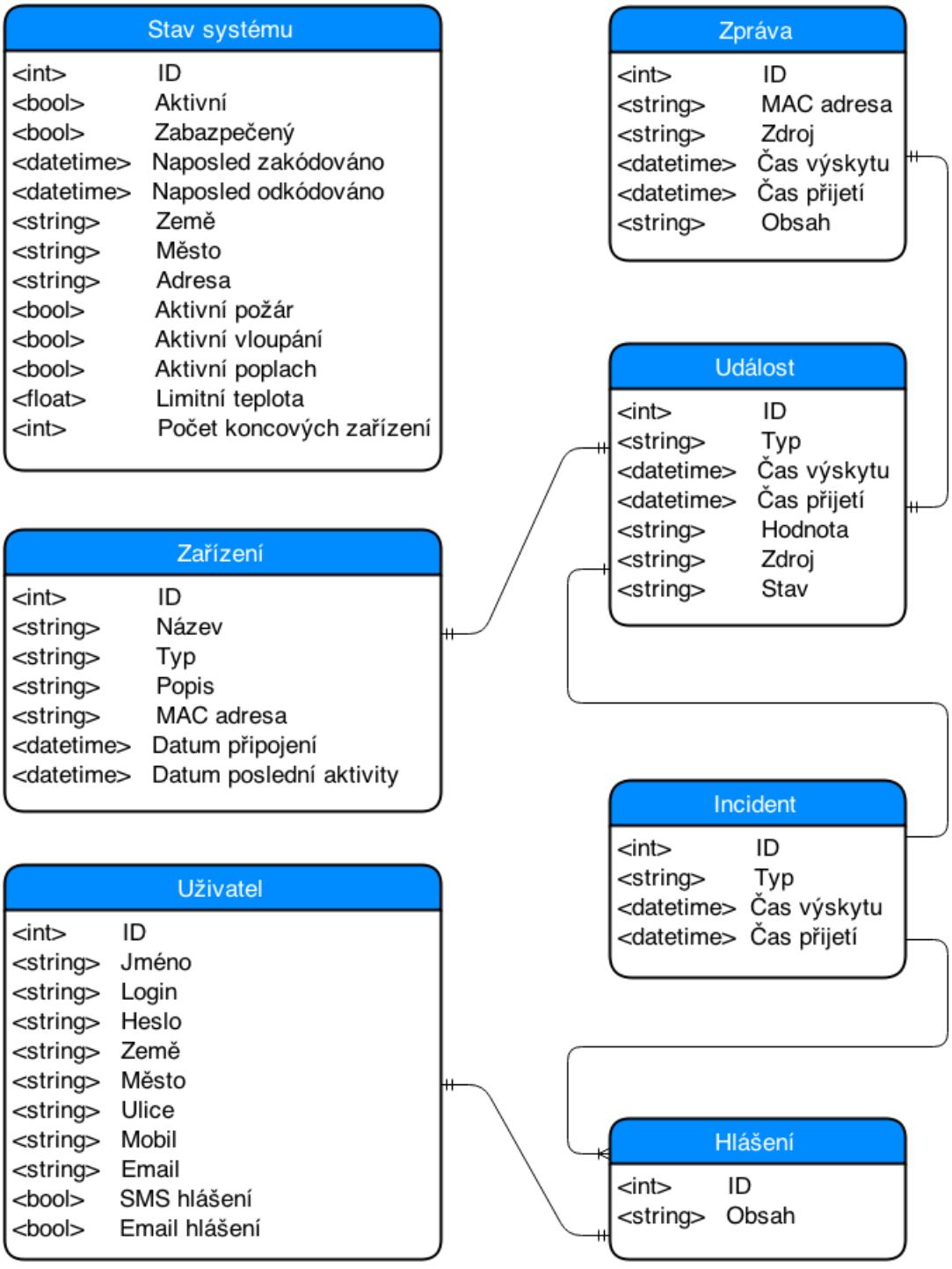
Webové rozhraní bude implementováno v rámci open-source přostředí. Bude propojeno z databází a poskytovat databázová data autorizovaným uživatelům. Rozhraní bude zajišťovat autentizaci a autorizaci uživatelů. Bezpečnostní systém bude multiuživatelský a bude poskytovat základní role pro administrátora, který bude schopen měnit většinu nastavení bezpečnostního systému, a roli pro uživatele bezpečnostního systému, který bude moci upravovat jen některá nastavení bezpečnostního systému.

Datový model

Tvorba datového modelu bezpečnostního systému bude vycházet z managementu událostí, který je popsán v kapitole 2. Základními entitami jsou tedy událost, incident a protiopatření. O tom zda je událost zároveň incidentem se bude starat aplikační logika na bráně. V datovém modelu je však uvedena událost a incident rozděleně, kdy každá událost může mít buď žádný, nebo právě jeden incident. Při vytváření incidentu se automaticky provede i protiopatření.

V aplikaci budou také uloženy informace o uživatelích, kteří budou mít přístup do webového rozhraní. Dále zde budou informace o jednotlivých koncových zařízeních a uchovávat

se bude celkový stav systému. Uložení dat v systému a jejich závislost je popsána diagramem(Obrázek 3.2).



Obrázek 3.2: Datový model serverové aplikace

3.4.3 Komunikační protokol

Zprávy, které jsou používány pro komunikaci mezi všemi zařízeními bezpečnosntího systému, jsou ve formě ASCII řetězců s maximální délkou 128 bytů. Textový řetězec má formu python slovníku, na který je při zpracování převeden. Základní atribut je atribut "command", který identifikuje o jakou zprávu se jedná. Dalšími atributy mohou být hodnoty senzorových měření apod. Tento protokol používá server a všechna zařízení lokálního bezpečnostního systému kromě pohybových detektorů a detektorů otevření dveří. Tyto detektory komunikují pouze pomocí zigbee protokolu kvůli zachování minimálních energetických nároků.

Formát	**Popis**
{'command':'secure_system'}	uvádí systém do zabezpečeného stavu
{'command':'unsecure_system'}	uvádí systém do nezabezpečeného stavu
{'command':'temperature_humidity','tvalue':value,'hvalue':value}	poskytuje naměřené hodnoty teploty a vlhkosti koncovým zařízením
{'command':'co_detection'}	informuje o detekci oxidu uhelnatého koncovým zařízením
{'command':'movement_detection'}	informuje o detekci pohybu koncovým zařízením
{'command':'door_opened'}	informuje o detekci otevření dveří koncovým zařízením
{'command':'access_granted'}	informuje zařízení o korektním odkódování systému
{'command':'access_denied'}	informuje zařízení o zadání neplatného hesla při odkódovávání systému
{'command':'trigger_alarm'}	spouští alarm v lokálním bezpečnostním systému
{'command':'stop_alarm'}	vypíná aktivní alarm v lokálním bezpečnostním systému

Tabulka 3.2: Komunikační protokol

3.5 Vybrané technologie

V kapitole 2 u návrhu bezpečnostního systému je uvedeno, že u výběru technologií se ještě nemluví o konkrétních výrobcích. U velkých projketů při návrhu bezpečnostního systému to má zajisté své opodstatnění. V případě této práce však bude přehlednější uvést jednotlivé technologie a zároveň vybraná zařízení dohromady. Dle specifikace bude popis vybraných technologií opět rozdělen pro jednotlivé části systému a to lokální bezpečnostní systém a server.

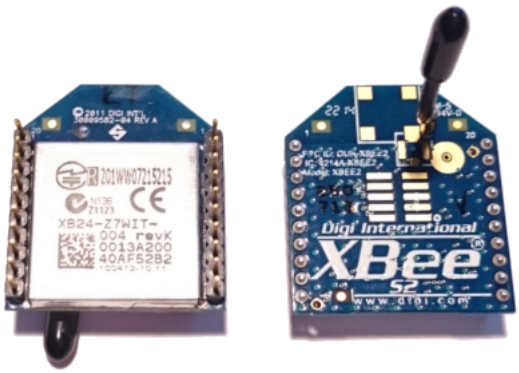
3.5.1 Lokální bezpečnostní systém

Bezdrátová komunikace

U brány a jednotlivých senzorů je jedním z hlavních požadavků bezdrátová zabezpečená komunikace. Dále je kladen důraz na energetickou úspornost. Oba tyto požadavky splňuje technologie ZigBee. Ta umožňuje spolehlivou šifrovanou komunikaci mezi zařízeními, dostatečný rozsah a poměrně velkou škálovatelnost sítě. ZigBee moduly jsou zároveň energeticky velmi úsporné.

Při výběru konkrétního výrobce je dispozici celkem dost možností. Pro implementaci byla nakonec zvolena společnost Digi a její Xbee moduly. Digi poskytuje na svých webových stránkách kvalitní podporu ke svým produktům a také kolem této společnosti vznikla silná komunita, která pomocí diskuzních fór sdílí své zkušenosti s ostatními.

Konkrétní modulem, který byl vybrán pro implementaci koncových zařízení, je Xbee modul XB24-Z7WIT-004(Obrázek 3.3). Tento modul sice neobsahuje žádné měřící prvky pro měření teploty, CO a dalších veličin, které je dle specifikace nutno detekovat, ale poskytuje jednoduché analogové a digitální rozhraní pro napojení libovolných senzorů. Kombinací tohoto modulu s různými senzory je dosaženo široké škály vužití. Takovéto použití Xbee modulu navíc umožňuje jednoduchou rozšířitelnost bezpečnostního systému o další typy senzorů, které nejsou specifikovány, ale v budoucnu by mohly být vyžadovány. Konkrétní senzory, které budou použity v kombinaci s Xbee moduly budou popsány níže u jednotlivých zařízení.

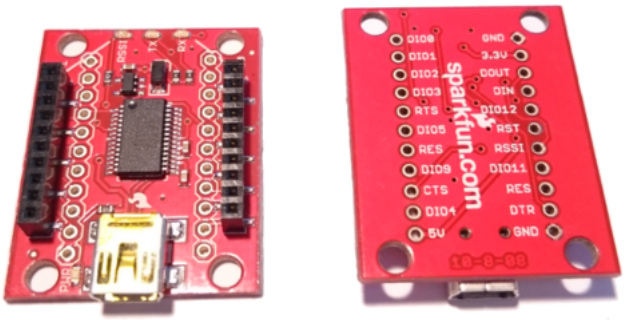


Obrázek 3.3: XBee modul XB24-Z7WIT-004

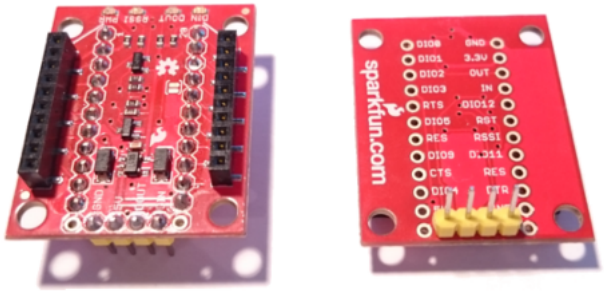
Xbee modul XB24-Z7WIT-004 je možné využívat samostatně, ale pro jeho praktické použití je dobré využít regulátoru. Jako regulátor byla vybrána zařízení XBee Explorer Regulated(Obrázek 3.5) a XBee Explorer USB(Obrázek 3.4) od společnosti SparkFun. Tyto regulátory jsou kompatibilní se zařízeními XBee série 1 i série 2.

XBee Explorer USB je pro práci s XBee moduly jistou nutností. Pomocí tohoto zařízení lze XBee modul spojit s počítačem skrz USB rozhraní, což je potřebné pro naprogramování modulu. Kromě samotného naprogramování zapojeného modulu lze i komunikovat s ostatními zařízení v sítí, popř. vzdáleně programovat tato zařízení přímo z PC. Ke komunikaci skrze USB rozhraní slouží aplikace X-CTU od společnosti Digi.

V případě zařízení XBee Explorer Regulated lze XBee modul napájet napětím 5V, které poskytuje např. USB rozhraní nebo také platforma arduino a většina napájecích



Obrázek 3.4: SparkFun XBee Explorer USB



Obrázek 3.5: SparkFun XBee Explorer Regulated

článků. Další výhodou tohoto zařízení je možnost připájet kontakty pro jednoduché vložení do breakboardu. Jednotlivé piny XBee modulu lze pak jednodušeji propojit s ostatními zařízeními.

Brána

Dle specifikace musí brána splňovat požadavky na komunikační rozhraní mezi koncovými zařízeními a serverem a zároveň musí být schopno vyhodnocovat události z koncových zařízení.

Na základě zvýšených požadavků na toto zařízení bylo rozhodnuto pro implementaci brány použít open-source řešení openWRT. OpenWRT systém bude instalován na routeru TP-link model TL-WDR4300. Toto konkrétní zařízení je systémem openWRT oficiálně podporováno.

Brána bude pomocí USB rozhraní propojená s modulem XBee v roli koordinátoru a bude tak umožňovat komunikaci s koncovými zařízeními. Se serverem bude brána komunikovat za pomocí VPN rozhraní, kde bude vystupovat jako klient.

O komunikaci mezi koncovými zařízeními a serverem a zároveň o logiku vyhodnocování

událostí se bude starat samostatná aplikace. Tato aplikace bude napsána v jazyce Python. Základní funkcí aplikace je příjem a zasílání zpráv od a do koncových zařízení pomocí XBee koordinátoru.

Pohybové senzory

Pro implementaci pohybových senzorů byla zvolena technologie PIR senzoru, konkrétně bude použit senzor HC-SR501(Obrázek 3.6) Tento senzor má dle technické specifikace dosah až 10 metrů, úhel snímání 110°a je u něj možné nastavit citlivost snímání a dobu po které bude senzor sepnutý v případě detekování pohybu. Informaci o detekci pohybu poskytuje digitálně a je-li detekován pohyb je výstupem logická 1.

Tento senzor je spojený s Xbee modulem, který je defaultně v režimu spánku a probouzí se pouze pokud je detekován pohyb. Poté odesílá zprávu bráně o detekované události a opět usíná. Protože Xbee modul probouzí logická 0 na pinu 9(pin hibernate), je třeba toto zařízení doplnit o logický člen invertor, který bude invertovat signál pohybového senzoru pro probuzení Xbee modulu logickou hodnotou 0.

Obrázek 3.6: Pohybový senzor HC-SR501

Senzory otevření dveří

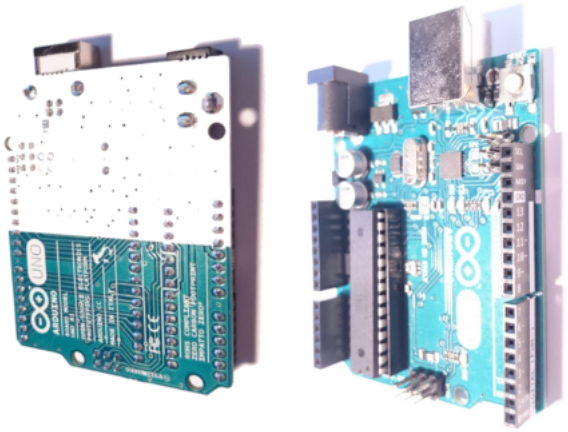
Nejčastěji využívanými senzory jsou magentické kontakty. Tyto senzory budou použity i v této práci a to konkrétně magnetický kontakt MEDER MK04-1A66B-500W(Obrázek 3.7). Tento magnetický kontakt je opět spojený s Xbee modulem, který je ve stavu spánku. Pro detekci a ohlášení otevření dveří je využíváno přímo principu magnetického kontaktu. Pokud jsou dveře zavřené, kontakt vede proud, drží se proud 5V na XBee pinu pin hibernate, čímž se Xbee modul udržuje ve stavu spánku. Dojde-li k otevření dveří, rozepnutí kontaktu, proud na pinu hibernate poklesne na 0, čímž se modul probudí a odešle zprávu o této události bráně.

Monitorovací a varovné zařízení

Protože toto zařízení potřebuje integrovat více senzorů různých typů a může být dle specifikace napájeno i z elektrické sítě, bude implementováno pomocí platformy arduino. Jako konkrétní model bylo vybráno arduino Uno(Obrázek 3.8). Arduino je schopno vykonávat

Obrázek 3.7: Magnetický kontakt MEDER MK04-1A66B-500W

uživatelem nahraný kód v jazyce C. V kódu je možno spravovat analogové i digitální vstupy a výstupy, čehož bude využito pro propojení senzorů, sirény a Xbee modulu pro komunikaci s bránou.

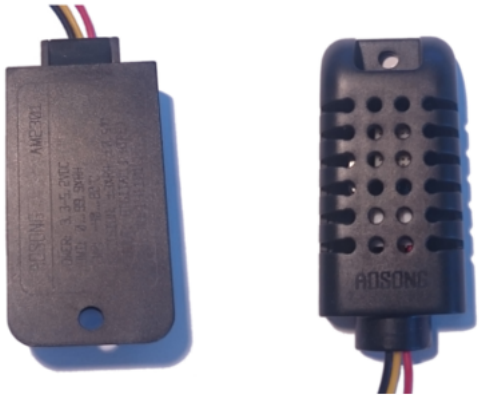


Obrázek 3.8: Arduino Uno

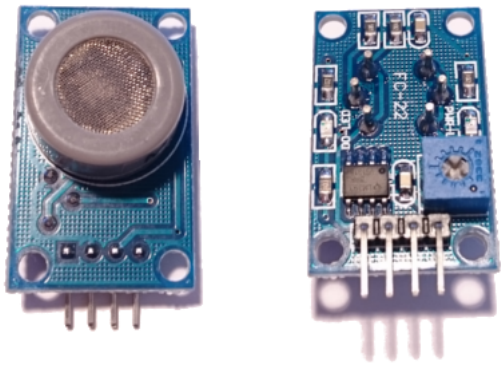
Funkci teplotního senzoru pro monitorovací zařízení plní zařízení AM2301(Obrázek 3.9). Senzor má digitální výstup a na platformě Arduino pro něj existuje podpora v rámci samostatné knihovny, což přispívá ke snadné integraci. Teplotní senzor je kalibrován s přesností 0.5 stupně Celsia, což pro požadavky bezpečnostního systému postačuje. Tento senzor je navíc schopen měřit i relativní vhkost vzduchu, která má však v systému pouze informativní charatker.

Pro detekci oxidu uhelnatého bude použit detektor typu MQ7, který je integrovaný na obvodu FC-22(Obrázek 3.10) navrženém přímo pro arduino. Senzor poskytuje velmi přesné a citlivé měření CO v okolí. Citlivost lze nastavit pomocí potenciometru na obvodu. Tento senzor pracuje při napětí 5V, což opět dodává Arduino, a poskytuje digitální i analogový výstup. Pro účely bezpečnostního systému postačí digitální výstup, který pouze nabude logické hodnoty 0 při detekování CO v okolí. [**?**]

Pro zvukovou signalizaci incidentů bude součástí monitorovacího zařízení piezosirénka



Obrázek 3.9: Senzor AM2301



Obrázek 3.10: Senzor oxidu uhelnatého MQ7

KINGSTATE KXG-0905C(Obrázek 3.11). Ke svému provozu potřebuje napětí v rozmezí 4 - 7 V, které ji poskytne Arduino. Při tomto napětí sirénka vyvine akustický tlak cca 85 dB ve vzdálenosti 10 cm od sirénky. To je v rámci jedné místnosti dostatečné.

Přístupová klávesnice

Přístupová klávesnice bude implementována pomocí mobilního zařízení se systémem android. Na zařízení bude k dispozici aplikace, která umožní zadání číselného kódu a jeho odeslání bráně k autentizaci. Po úspěšné autentizaci je systém odkódován.

3.5.2 Server

Pro server bude využito virtuálního server hostingu. Tímto bude zajištěno fyzické oddělení serveru od lokálního bezpečnostního systému. Tím je sníženo riziko kombinovaného útoku na server a lokální bezpečnostní systém. Jako operační systém bude použita linuxová distribuce Ubuntu 14.04 LTS.

Obrázek 3.11: Piezoelektrická sirénka KINGSTATE KXG-0905C

Odoo webové rozhraní

Pro webové rozhraní bylo zvoleno využití open-source řešení Odoo v8[1]. Toto řešení je primárně určeno pro tvorbu byznys aplikací jako jsou CRM(Customer relationship management) a ERP(Enterprise Resource Planning) systémy ,ale díky jeho modularitě a flexibilitě jej lze využít pro široké spektrum projektů. V základní verzi je předinstalováno několik základních modulů, které plní různé funkce. Takovéto moduly lze vytvořit i vlastní a poté nainstalovat do Odoo.

Odoo poskytuje základní rozhraní pro práci s databází, systém pro správu uživatel a základní funkce pro autentizaci a autorizaci. Dále je k dispozici funkční a efektivní vizuální rozhraní, které lze dále upravovat podle potřeb projektu. Funkce, komunikace s databází a základní logika je psána v jazyce Python. Uživatelské rozhraní je implementováno pomocí xml šablon, které lze jednoduše upravovat, popř. vytvořit úplně nové.

Pro bezpečnostní systém bude vytvořen samostatný modul, který bude využívat pouze základní předinstalované moduly Odoo platformy. Veškerá logika bude implementována pouze v rámci tohoto modulu, takže v konečném důsledku pro zprovození webového rozhraní postačí nainstalovat Odoo a posléze nainstalovat modul bezpečnostního systému.

Odoo nativně používá open-source databázi PostgreSQL, takže v rámci implementace bezpečnostního systému se použije také. Je však možné použít i jiné databáze a to např. MySQL.

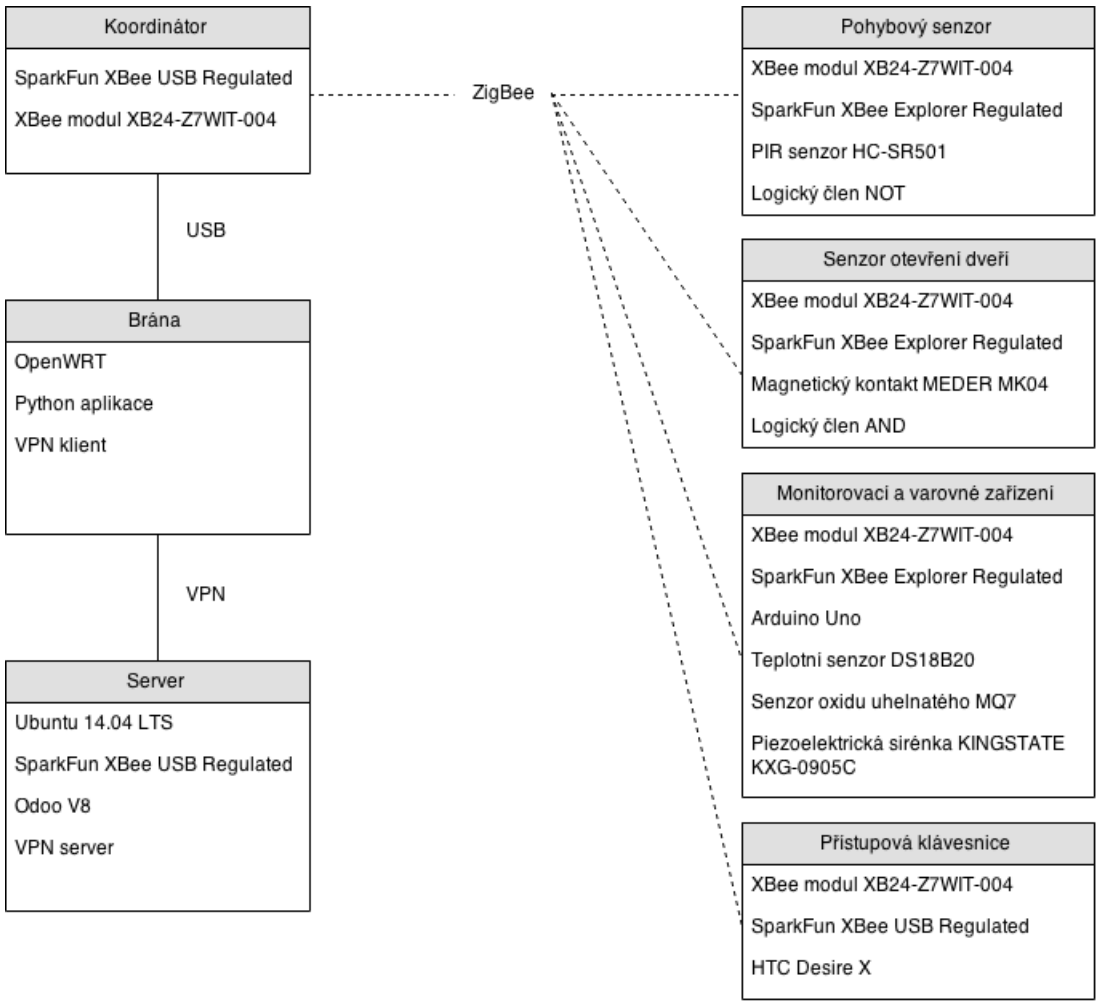
3.5.3 Komunikace

Komunikace mezi serverem a lokálním bezpečnostním systémem má být zabezpečená. Nejvhodnějším řešením tohoto požadavku je použití technologie VPN(Virtual Private Network), virtuální privátní sítě. Server bude propojen s bránou pomocí VPN tunelu, kde server bude vystupovat zároveň jako VPN server a brána bude VPN klient. Vešekerá komunikace mezi bránou a serverem bude probíhat pouze skrz VPN tunel. Jako VPN aplikace bude použita open-source aplikace openvpn.

V rámci VPN tunelu bude brána pro komunikaci se serverem používat rozhraní xmlRPC. Toto rozhraní je základním prvkem pro interakci s Odoo aplikací, která je aktivní na serveru.

[1]Další informace ohledně Odoo jsou k nalezení na webových stránkách www.odoo.com

Server bude pro komunikaci s bránou používat standardní http požadavky. Na bráně bude v rámci python aplikace běžet jednoduchý http server, který bude přijímat http požadavky od Odoo aplikace. Zprávy mezi bránou a lokálním bezpečnostním systémem jsou definovány v komunikačním protokolu. Komunikace mezi konkrétními zařízeními a použité technologie jsou zobrazeny pomocí diagramu(Obrázek 3.12).



Obrázek 3.12: Schéma systému s konkrétními zařízeními

Kapitola 4

Implementace

V této části práce bude popsána praktická implementace bezpečnostního systému dle návrhu z předchozí kapitoly. Narozdíl od návrhu, který byl tvořen pomocí přístupu shora-dolů, pro implementaci bude použit přístup zdola-nahoru. Nejdříve budou tedy implementována jednotlivá zařízení, která budou poté spojena v jednotný celek. Pro přehlednost budou tato zařízení opět rozdělena pro lokální bezpečnostní systém a server.

4.1 Lokální bezpečnostní systém

Lokální bezpečnostní systém budou tvořit zařízení umístěná ve fyzickém objektu, který má být chráněn.

4.1.1 Pohybový senzor

Nastavení XBee modulu

XBee modul pro pohybový senzor nastavíme pomocí aplikace X-CTU jako ZigBee End Device v režimu API. Dále nastavíme základní parametry pro správné fungování(Tabulka 4.1).

Pro upřesnění je třeba dodat, že první tři parametry(Product family, function set, firmware version), které se nachází v tabulce se nastavují již při aktualizaci XBee firmwaru. Pro přehlednost jsou uvedeny zároveň s ostatními parametry, v tabulce jsou však graficky odděleny. Po aktualizaci firmwaru na nejaktuálnější verzi a odpovídající funkční set nastavíme parametry pro implementaci pohybového senzoru.

Parametr ID je nastaven na číslo 20 (HEX). Tento parametr udává, ke které síti se má XBee modul připojit. Na všech koncových zařízeních bezpečnostního systému je hodnota tohoto parametru shodná.

Pro zajištění bezpečné komunikace nastavíme parametr EE na honotu 1 a KY vyplníme náhodnou hodnotou v rozsahu 0 - 32 hexadecimálních znaků. [1] Tento klíč se využije pro autentizaci XBee modulů a zaslání síťového klíče, který se poté použije na zašifrování komunikace. KY parametr nastavíme na hodnotu 1a2bc3 a tato hodnota musí být na všech koncových zařízeních shodná.

Aby koncové zařízení bylo ve stavu spánku zajistí nastavení parametru SM na hodnotu 1(pin hibernate). Tato hodnota uvede XBee modul do stavu spánku. K probuzení dojde,

[1] Parametr KY je dostupný pouze pro zápis, po zapsání klíče a znovunačtení parametrů již nebude viditelný, ale v modulu bude stále uchovaný

je-li na pinu 9(pin hibernate) detekován pokles napětí z 5V na 0V. Dokud je toto napětí udržováno na hodnotě 0V, modul je aktivní a vykonává svou funkci. Pokud je na pin 9 opět přivedeno napětí 5V, modul setrvá v aktivním stavu ještě tak dlouho jak definuje hodnota parametru ST a poté se přepíná zpět do stavu spánku.

Pro zaslání zprávy po probuzení modulu, tedy informování brány, že došlo k detekci pohybu, nastavíme parametr IR na hodnotu 3H8. Tato hodnota určuje v jakém intervalu se zasílá informace o aktivovaných měřených vstupech. Bráně není nutno zasílat hodnotu tohoto vstupu, protože samotná zpráva od tohoto zařízení se vyhodnotí jako detekce pohybu. Je však třeba rozlišit zda se jedná o zařízení pohybového senzoru anebo senzoru otevření dveří. Pro detektor pohybu nastavíme parametr D4 na hodnotu 4. V poslední řadě nastavíme parametr PR na hodnotu 0, což deaktivuje pull-up rezistor na vstupech, a parametr V nastavíme na hodnotu 0a00 pro zaslání varování při poklesu napětí na zařízení.

Parametr	**Hodnota (HEX)**
Product family:	XB24-ZB
Function set:	ZigBee End Device API
Firmware version:	29A7
ID:	18
JN:	1
EE:	1
KY:	1a2b3c
SM:	1
D4:	4
PR:	0
IR:	3E8
V:	0A00

Tabulka 4.1: Nastavení XBee modulu pro pohybový senzor

Zapojení

XBee modul je zasazený do sparkfun regulátoru. Napájecí kontaky pohybového senzoru jsou připojeny k odpovídajícím napájecím kontaktům na SparkFun regulátoru a logický výstup je napojen na vstupní pin logického členu INVEROTR. Výstup invertoru je napojen na pin DTR regulátoru SparkFun(Obrázek 4.1).

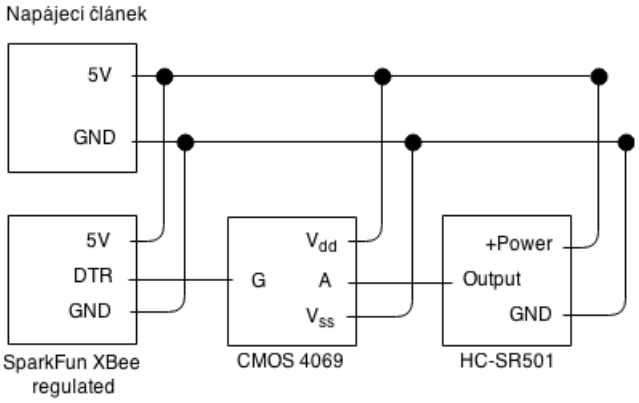
4.1.2 Senzory otevření dveří

Nastavení XBee modulu

Nastavení XBee modulu pro senzor otevření dveří je stejné jako pro pohybový senzor, až na parametr D4. Pro rozlišení tohoto senzoru od pohybového senzoru je nastaven parametr D5 na hodnotu 4(Tabulka 4.2).

Zapojení

XBee modul je zasazený do SparkFun regulátoru. Jeden konec magnetického kontaktu je zapojen do napájení a druhý přiveden na vstup logického členu AND. Na zbylý vstup je



Obrázek 4.1: Schéma zapojení pohybového čidla

Parametr	**Hodnota (HEX)**
Product family:	XB24-ZB
Function set:	ZigBee End Device API
Firmware version:	29A7
ID:	18
JN:	1
EE:	1
KY:	1a2b3c
SM:	1
D5:	4
PR:	0
IR:	3E8
V:	0A00

Tabulka 4.2: Nastavení XBee modulu pro senzor otevření dveří

přivedeno napětí 5V. Výstup AND členu je spojený s pinem DTR na regulátoru. Člen AND je připojený k napájení(Obrázek 4.2).

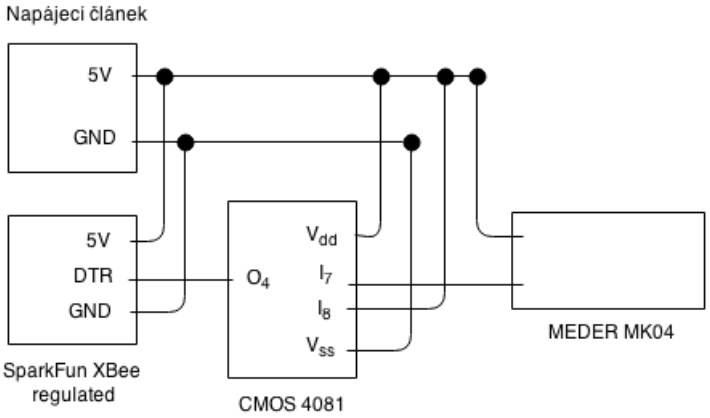
4.1.3 Monitorovací a varovné zařízení

Nastavení XBee modulu

XBee modul pro toto zařízení má nainstalován firmware router v AT módu. Router vyžaduje pouze základní nastavení a to pouze parametr ID pro přídání se do sítě, parametr JN a parametry EE, KY pro šifrovanou komunikaci(Tabulka 4.3).

Zapojení

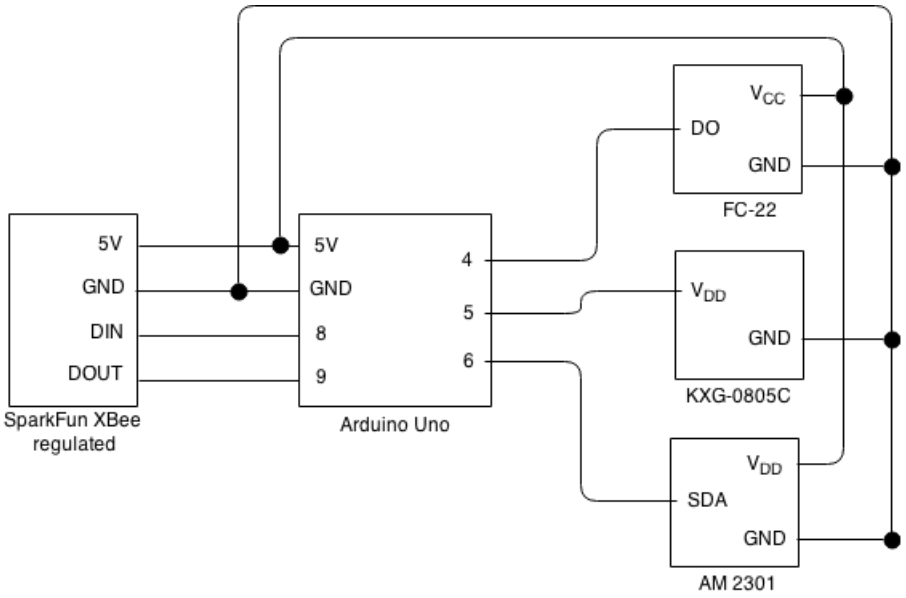
Jednotlivé senzory jsou napájeny přímo z arduina a jejich výstupy jsou připojeny k vyznačeným vstupům na arduinu(Obrázek 4.3). Arduino je napájeno pomocí USB kabelu.



Obrázek 4.2: Schéma zapojení senzoru otevření dveří

Parametr	**Hodnota (HEX)**
Product family:	XB24-ZB
Function set:	ZigBee Router AT
Firmware version:	22A7
ID:	18
JN:	1
EE:	1
KY:	1a2b3c

Tabulka 4.3: Nastavení XBee modulu pro monitorovací a varovné zařízení



Obrázek 4.3: Schéma zapojení součástí monitorovacího a varovného zařízení

4.1.4 Přístupová klávesnice

Nastavení XBee modulu přístupové klávesnice je shodné jako nastavení u monitorovacího zařízení(Obrázek 4.4). Modul XBee je přes SparkFun USB Explorer pomocí USB kabelu

připojen k mobilnímu zařízení.

Parametr	**Hodnota (HEX)**
Product family:	XB24-ZB
Function set:	ZigBee Router AT
Firmware version:	22A7
ID:	18
JN:	1
EE:	1
KY:	1a2b3c

Tabulka 4.4: Nastavení XBee modulu pro přístupovou klávesnici

4.1.5 Brána

Instalace OpenWrt

Pro zprovoznění brány je třeba zapnout router TL-WDR4300 a propojit jeho ethernetový port pomocí síťového kabelu s libovolným počítačem. Nyní lze pokračovat instalací systému OpenWrt.[2] Na počítači ve webovém prohlížeči zadáme adresu 192.168.1.1, která zobrazí nativní administrační rozhraní routeru. V menu "System Tools"vybereme možnost "System Upgrade"a v souborovém manageru vybereme soubor s obrazem OpenWrt systému. Po kliknutí na "Upgrade"dojde k instalaci OpenWrt systému.

Po úspěšné instalaci je nutné provést update repozitářů na aktuální verzi. Toho lze docílit provedením příkazu opkg update.

Instalace a nastavení VPN klienta

Instalace VPN klienta se provede příkazem opkg install openvpn. Po instalaci je třeba vytvořit vlastní inicializační skript pro automatické spuštění po startu a restartu routeru.

Pro korektní fungování VPN spojení je nutné mít na klientovi k dispozici veřejné klíče vygenerované VPN serverem. Toto generování bude popsáno níže v popisu nastavení serveru. Na klientovi se poté klíče uvedou v konfiguračním souboru. V kombinaci s použitím klíčů je také v rámci nastavení nutné nakonfigurovat firewall. Primárně je třeba povolit port 1194 pro openvpn spojení.

Po korektním nastavení klienta a jeho spuštění se v systému objeví nové síťové rozhraní tun0, které lze standardně využívat. Server je dostupný na IP adrese 10.8.0.1 a zařízení brány má nastaveno IP na 10.8.0.6. Všechny součásti bezpečnosntího systému na bráně komunikují pouze s tímto rozhraním.

Aplikace

Aplikace vykonávající funkce brány je napsána v jazyce python a uložena v domácím adresáři /root pod názvem gate_app.py. Pro tuto aplikaci je vytvořen incializační skript pro automatický start po startu a restartu routeru. Pro interpretaci je třeba nainstalovat python

[2]Veškeré informace o instalaci OpenWrt na router TL-WDR4300 jsou k nalezení na webových stránkách http://wiki.openwrt.org/toh/tp-link/tl-wdr4300

verze 2.7 a také knihovny, které nejsou dostupné ve standardní instalaci. Jedná se o knihovny xbee [3] a pyserial [4]. Lze je doinstalovat pomocí příkazu pip install [nazev_knihovny].

Aplikace je rozdělena do několika částí. Tyto části jsou reprezentovány jednotlivými třídami. Každá třída je rozšířením třídy Thread, která dělí vykonávání aplikace do vláken. Využity jsou principy pro práci se sdílenou pamětí a to především zámky(Lock) a fronty(Queue).

Třída **XBEE_receiver** plní funkci serveru pro XBee zařízení. V neblokujícím režimu poslouchá na sériovém rozhraní, ke kterému je připojen XBee koordinátor a při dostupné komunikaci zpracovává příchozí zprávy. Při přijetí zprávy je obsazen zámek xbee_received_lock a zpráva vložena do fronty xbee_received_que. Po vložení zprávy do fronty je uvolněn zámek.

Třída **XBEE_sender** zajišťuje zasílání zpráv na koncová zařízení. Její kód se provádí v nekonečné smyčce, kdy se v každém cyklu kontroluje, zda existují data ve frontě xbee_send_que. Pokud je tato fronta neprázdná, uzamkne se zámek xbee_send_lock a všechny záznamy z fornty se postupně vyberou a odešlou na sériové rozhraní XBee koordinátoru. Veškeré informace potřebné k odeslání jsou obsaženy v záznamu. Po odeslání se opět uvolní zámek.

Třída **WEB_receiver** slouží pro příjem komunikace ze serveru. V nekonečném cyklu je v neblokujícím režimu naslouchán na portu 5000, který slouží pro komunikaci se serverem. To zajišťuje standardní síťový socket. Jsou-li na socketu dostupná data, uzamyká se zámek web_received_lock a data jsou uložena do fronty web_received_que. Poté je uvolněn zámek.

Třída **WEB_sender** zasílá zprávy zpět na server. V nekonečném cyklu je kontrolována fronta web_send_que. Pokud je fronta neprázdná, dojde k uzamknutí zámku web_send_lock a všechny záznamy z fronty jsou postupně odeslány na server. Po odeslání se uvolní zámek. K odeslání zpráv na server je využito knihovny xmlRPC, která se používá v rámci Odoo aplikace pro komunikaci se serverem. Nastavení xmlRPC rozhraní je definováno na začátku aplikace. V rámci zprávy přes toto rozhraní je třeba uvést uživatelské jméno, heslo, url serveru, název databáze a url odkazy na rozhraní na serveru. Tyto informace jsou zasílány v plain textu, proto je důležité komunikovat pouze přes nastavené VPN rozhraní. Jako url je tedy nastavena IP adresa VPN rozhraní a také port 8069, na kterém poslouchá Odoo serverová aplikace.

Třída **Data_cracker** zpracovává veškerou komunikaci. V nekonečné smyčce jsou kontrolovány fronty web_received_que a xbee_received_que. Pokud je fronta web_received_que neprázdná, jedná se o přijetí zpráv ze serveru. Tyto zprávy jsou z fornty vybrány a předány funkci web_command(). Jedná-li se o zprávu pro některé z koncových zařízení, je tato uložena do fronty xbee_send_que odkud je posléze odeslána na konkrétní zařízení. Pokud se jedná o zprávu pro bránu, provede se příkaz, který je ve zprávě uveden. Je-li neprázdná fronta xbee_received_que, jedná se o zprávu z koncových zařízení. Zpráva se předá funkci xbee_interpreter. Tato funkce provádí zpracování zprávy a pokud se jedná o incident, hlásí jej serveru a spouští lokální příkazy pro varování.

Třída **Counter** zajišťuje zpoždění při detekci pohybu nebo otevření dveří, když je bezpečnostní systém v zabezpečeném stavu. Po vzniku takovéto události se čeká 30 sekund a poté je zkontrolován bezpečnostní stav systému. Pokud je stav nezabezpečený, znamená to, že došlo ke korektnímu odkódování systému. Pokud je systém po uplynutí limitu stále v zabezpečeném stavu, znamaná to, že nedošlo ke korektnímu odkódování a jedná se tedy o bezpečnostní incident. Tento incident je nahlášen serveru a v objektu je lokálně supštěn

[3] Bližší informace jsou k nalezení na webových stránkách https://code.google.com/p/python-xbee/ . Knihovna je dostupná pod open-source licencí.

[4] Bližší informace jsou k nalezení na webových stránkách http://pyserial.sourceforge.net/

poplach. Další funkcí je zpoždění při zabezpečování systému. Po zakódování systému se čeká 60 sekund a teprve poté je systém uveden do zabezpečeného stavu.

Natavení XBee modulu pro bránu

XBee modul pro bránu bude jako jediný nastavený jako koordinátor. Všechny ostatní XBee moduly budou komunikovat pouze s tímto koordinátorem. Kromě firmwaru je však nastavení modulu shodné s nastavením XBee routerů.

Parametr	**Hodnota (HEX)**
Product family:	XB24-ZB
Function set:	ZigBee Coordinator API
Firmware version:	22A7
ID:	18
JN:	1
EE:	1
KY:	1a2b3c

Tabulka 4.5: Nastavení XBee modulu pro bránu

4.2 Server

4.2.1 Zprovoznění cloudového serveru

Server u poskytovatele nemá nastavené doménové jméno a lze se na něj připojit pouze přes jeho IP adresu. Server má již od poskytovatele předinstalován operační systém Ubuntu 14.04 LTS. Po prvním přihlášení je však nutné systém aktualizovat pomocí apt-get update a poté apt-get upgrade.

4.2.2 Spuštění VPN serveru

Aplikace pro zprovoznění VPN sítě openvpn se nainstaluje ze standardních repozitářů pomocí příkazu apt. Po instalaci je třeba vygenerovat kořenový CA klíč pro podepisování certifikátů, kořenový CA certifikát, certifikát pro server, klíč pro server a konečně klientský certifikát a klientský klíč. Kořenový CA certifikát a klientský certifikát a klíč je nutné pomocí ssh tunelu přenést na zařízení brány. Zbytek vygenerovaných souborů zůstává na serveru.

Po vygenerování certifikátů lze vytořit konfigurační soubor ve složce /etc/openvpn s příponou .conf. Tento soubor je upravený ukázkový konfigurační soubor, který poskytuje openvpn pro rychlou konfiguraci. Do souborou jsou pouze doplněny cesty k certifikátům a klíči, zapsána IP adresa VPN klienta s defaultním portem 1194 a povoleno bezpečnější nastavení pro uživatele a skupiny.

Automatické spouštění VPN serveru zajistí defaultní nastavení openvpn, které při instalaci vytvoří inicializační skript. Při startu a restartu tento skript spouští VPN server s konfiguračním souborem s příponou .conf, který nalezne ve složce /etc/openvpn. Po spuštění VPN serveru je v systému vytvořeno nové síťové rozhraní s názvem tun0 a zařízení brány je dostupné přes toto rozhraní na IP adrese 10.8.0.6. Detaily instalace a podrobný návod je popsán v příloze této práce.

4.2.3 Instalace Odoo

Před samotnou instalací je nutné nainstalovat postgreSQL databázi verze 9.3 a python verze 2.7.6 nebo novější. Odoo je možné nainstalovat dvěma způsoby. První je jednodušší a rychlejší, ale poskytuje pouze základní funkce. Tímto způsobem je instalace balíčku z repozitáře pomocí příkazu apt-get. Tímto se nainstaluje Odoo aplikace a všechny nutné závisloti. Daleko užitečnější je však instalace přímo ze zdrojových souborů. Instalace je delší a náročnější, ale v konečném důsledku poskytuje větší kontrolu nad výsledným systémem a přístup ke zdrojovým souborům. Tento způsob byl použit při instalaci Odoo pro bezpečnostní systém.

Ke zdrojovým souborům se lze dostat buď stáhnutím archivu, anebo pomocí aplikace git. Použití gitu je rozhodně vhodnější, protože pro update Odoo aplikace pak stačí zadat jediný příkaz. Pro naklonování repozitáře na server je třeba se přesunout do složky /opt a zde spustit příkaz git clone https://github.com/odoo/odoo.git . Tento příkaz vytvoří podsložku /opt/odoo a do ní umístí všechny soubory potřebné pro spuštění Odoo aplikace.

Dalším krokem je vytvoření systémového uživatele odoo a jeho přidání do skupiny odoo. Uživatel odoo musí být vytvořen i v postgreSQL databázi. Nakonec je třeba doinstalovat potřebné python moduly, které Odoo vyžaduje. Seznam těchto modulů se nachází v souboru requirements.txt v kořenovém adresáří Odoo aplikace. Po doinstalování modulů lze aplikaci spustit pomocí souboru odoo.py v kořenovém adresáři aplikace. Pro spuštění aplikace po restartu serveru je třeba vytvořit inicializační skript a uložit jej do adresáře /etc/init.d. Podrobný návod na instalaci Odoo je k nalezení v příloze této práce.

4.2.4 Modul bezpečnostního systému

Aplikace bezpečnostního systému spuštěná na serveru je implementována jako modul v platformě Odoo [5]. Modul má vlastní složku pojmenovanou názvem modulu, která obsahuje veškeré soubory potřebné pro daný modul. Rodičovská složka tekvýchto složek je poté uvedena v konfiguračním souboru Odoo /etc/odoo-server.conf. Po zkopírování složky modulu do rodičovské složky je třeba restartovat Odoo server pomocí incicializačního skriptu /etc/init.d/odoo restart. Po restartu lze ve webovém rozhraní v menu Settings kliknout na položku Update Module List čímž se zaktulizují moduly uložené na pevném disku. V podmenu Local Modules pak bude k dispozici vytvořený modul MSS. Po rozkliknutí jeho detailu je možné modul nainstalovat.

Zprávy

Třída **Message** slouží pro příjem zpráv od brány lokálního bezpečnostního systému. Při přijetí zprávy z brány pomocí xmlRPC rozhraní je vytvořen objekt této třídy a v rámci jeho vytvoření se na základě XBee MAC adresy detekuje, zda jde o první komunikaci s tímto zařízením. Pokud ano, vytvoří se nový záznam pro zařízení a vyplní se informace o tomto zařízení jako MAC adresa, typ zařízení, název zařízení a popis zařízení. Pokud je již zařízení v systému zaznamenáno, zpráva se pouze předá dále ke zpracování třídě Event.

[5] Principy fungování Odoo modulu jsou názorně vysvětleny na webových stránkách https://www.odoo.com/documentation/8.0/howtos/backend.html

Události

Třída **Event** obsahuje základní logiku pro zpracování událostí. V první řadě se rozliší, zda událost pochází z lokálního systému nebo z webového rozhraní. Z webového rozhrnání mohou přijit pouze události pro online zakódování a odkódování systému. Po přijetí takovýchto událostí je systém uloží do historie a přepošle je jako zprávy lokálnímu systému, který podle nich provede vlastní operace pro zakódování popř. odkódování systému.

Událostí původem z lokálního systému je více. První dvě jsou opět zakódování a odkódování, dochází k nim, když je lokální systém uveden do zabezpečeného respektivě nezabezpečeného stavu skrz přístupovou klávesnici.

Další událostí je měření teploty a vlhkosti, jejichž hodnoty jsou uloženy do historie. Pokud naměřená teplota překročí nastavenou limitní hodnotu teploty, je událost vyhodnocena jako incident výskytu požáru. Zpracování incidentu je implementováno ještě v rámci třídy Event a bude popsáno níže. Incident výskytu požáru vytváří i událost detekce oxidu uhelnatého, u které se však neprovádí žádné kontroly a incident je vytvořen hned po přijetí této události.

Událost otevření dveří se opět ukládá do historie. Pokud je však systém v zabezpečeném stavu, je vytvořen objekt třídy ir_cron, který po nastaveném časovém limitu opět zkontroluje bezpečnostní stav systému. V případě, že nedošlo ke změně ze zabezpečeného stavu na nezabezpečený, tedy systém nebyl korektně odkódován, je událost vyhodnocena jako incident vloupání. Naprosto identické chování má i událost detekce pohybu.

Incidenty a hlášení

Zpracování incidentu probíhá ve dvou fázích. V první fázi se vytvoří objekt **Incident** do kterého se uloží informace o incidentu. Základní informace jsou datum výskytu, datum přijetí serverem a typ incidentu. V druhé fázi je vytvořeno hlášení o incidentu a provedeno protiopatření. V rámci vytváření hlášení, jsou odeslány přednastavené zprávy k danému typu incidentu pomocí emailu, popř. sms zprávy všem uživatelům systému, kteří mají nastaven odběr hlášení konkrétního typu incidentů. Objekty Event, Incident a Report jsou mezi sebou provázány pro uchování v historii.

Stav systému

Aktuální stav a informace o systému je uložen v objektu třídy **State**. Atributy tohoto objektu můžeme rozdělit na statické a dynamické. Statické může měnit pouze uživatel a jedná se především o fyzické umístění lokálního systému. Další atributy již podléhají dynamickému chování systému. Nejdůležitějšími jsou pak stav zabezpečení state_secure, který indikuje v jakém bezpečnostním stavu se sytém aktuálně nachází, a stav indikující aktivitu lokálního systému. Lokálnímu systému jsou cyklicky zasílány zprávy a pokud na ně server nedostane odpověď, vyhodnotí systém jako neaktivní(nedostupný). Dalšími atributy jsou časové známky posledního zakódování a odkódování systému. Atributy incident_fire, incident_brekein indikují vzniklé incidenty, alarm_on informuje o aktivním spuštěném alarmu v objektu. Stav systému, který je přístupný na serveru koreluje se stavem lokálního bezpečnostního systému.

Zařízení a uživatelé

Zařízení ani uživateli není třeba implementovat žádne chování v rámci jeho objektu. Objekty zařízení třídy Device na serveru nemají žádnou jinou funkci, kromě uchovávání in-

formací o zařízení. S objekty třídy User je situace identická, protože veškeré chování je již defaultně implementováno v rámci Odoo aplikace. Uživatelé však mohou mít v systému dvě základní role. Uživatelé s rolí user mají přístup k většině objektů, avšak měnit mohou jen pár atributů. Uživatelé s rolí admin pak mohou měnit bezpečnostní a systémová nastavení.

Grafické rozhraní

Grafické webové rozhraní je postaveno na základě Odoo xml šablonovací struktury. Základními prvky této struktury jsou pohledy a menu položky. Pohled je vždy vázaný ke konkrétnímu objektu a je schopný zobrazit pouze atributy tohoto objektu, popř. atributy, na které má tento objekt odkaz. Čtyři základní typy pohledů jsou tree, form, kanban, graph. Tree pohled zobrazuje záznamy jako seznam s možností označení více záznamů, které lze hromadně mazat nebo exportovat. Form zobrazuje detail jednoho konrétního záznamu a umožňuje měnit jeho atributy. Kanban zobrazuje opět seznam několika záznamů, kde však každý záznam může být graficky upraven pro přehlednější uspořádání. Pohled graph umožňuje záznamy vynést do grafu na základě vybraných závislostí. Menu položky jsou spojené s konkrétními pohledy, které jsou po kliknutí na položky zobrazeny.

Grafické prostředí je rozděleno na hlavní oblasti pomocí menu položek Monitoring, Devices, State, Users a Settings. V menu Monitoring se nachází seznamy událostí, incidentů a jejich hlášení. Tyto záznamy nemohou být nijak upraveny ani vytvořeny nové, pouze uživatel s rolí admin je může mazat. V menu Devices je zobrazen kanban pohled s názvy a obrázky všech zařízení v systému. Po kliknutí na konkrétní záznam se zobrazí pohled form, kde jsou k nalezení konkrétní informace o daném zařízení. State menu obsahuje v rámci form pohledu informace o stavu systému a možnost upravovat některá bezpečnostní nastavení jako např. limitní teplotu pro detekci požáru. V tomto pohledu lze také dálkově měnit bezpečnostní stav systému. V menu Users jsou k nalezení záznamy systémových uživatelů v kanban pohledu. Po rozkliknutí konkrétního uživatele se zobrazí form pohled s doplňujícími informacemi. Některé si může uživatel sám upravovat. Poslední menu Settings obsahuje veškerá nastavení týkající se Odoo aplikace. Pro aplikaci bezpečnostního systému jsou tato nastavení zbytečná, až na jeden konrétní případ a tím je aktualizace modulu pro bezpečnostní systém. Z toho důvodu je toto menu přístupné pouze uživateli s rolí admin.

4.3 Testování

Testování systému probíhalo v rámci jednoho dne v bytě o dvou pokojích. Přístupová klávesnice a detekční senzory byly umístěny u vchodových dveří a monitorovací zařízení v pokoji. Do objektu měly přístup dvě osoby, z nichž pouze jedna měla možnost autentizace systémem. Systém byl na 3 hodiny v zabezpečeném stavu a po zbytek testování v nezabezpečeném stavu. Pro testování byl použit hardware a software uvedený v příloze této práce.

Po ukončení testováni byla data systému vyhodnocena a zapsána do tabulky(Tabulka 4.4). Zaznamenán je celkový počet událostí. Z tabulky lze vyčíst, že při zabezpečeném stavu systému došlo k incidentu vloupání, protože osoba nacházející se v bytě nebyla systémem korektně autentizována. Dále se v tabulce nachází i incident požáru. Tento incident byl ovšem způsoben zvýšenou koncentrací oxidu uhelnatého pocházejícího z výfukových plynů, protože byt se nachází na rušné ulici. Použitý senzor byl nastaven na vysokou citlivost, proto došlo k detekci oxidu uhelnatého.

Po vyhodnocení testu bylo pozměněno nastavení senzoru oxidu uhelnatého, aby senzor nespouštěl planý poplach při detekci výfukových plynů.

Název události	**Počet událostí v nezabezpečeném stavu**	**Počet událostí v zabezpečeném stavu**
Detekce pohybu	163	13
Detekce otevření dveří	6	1
Detekce CO	9	0
Detekce teploty	252	36
Detekce vloupání	0	1
Detekce požáru	1	0
Zakódování systému	1	0
Odkódování systému	0	1

Tabulka 4.6: Výsledky testování systému

4.4 Možnosti rozšíření

Systém je vytvořen tak, aby v budoucnu umožňoval jednoduché přidávání nových druhů koncových zařízení. Pro rozšíření bezpečnostních funkcí systému je možné ho rozšířit o další detekční zařízení. Použity mohou být bezpečnostní kamery, fotopasti, laserové závory, detektory tříštění skla, optické detektory kouře a další zařízení pro zabezpečení objektu. Kromě bezpečnosntích funkcí může být systém rozšířen i o prvky domácí automatizace jako např. inteligentní spínače světel, senzory pro ovládání vytápění a klimatiazce, ovládání domácích spotřebičů apod. Dále lze uvažovat o využití domácích zdravotnických zařízení např. pro měření tepové frekvence nebo aktivity. S ohledem na využití inteligentních senzorů jsou možnosti rozšíření v tomto směru téměř neomezené.

Co se týče použitých technologií a jejich možností, rozšířením může být použití typu ZigBee mesh sítě namísto použitého typu multipoint. Mesh síť poskytne větší fyzický rozsah, protože zařízení mohou komunikovat mezi sebou. V případě spících koncových zařízení však může vyvstat potřeba rozšířit síť o zařízení typu router, což může zvednout náklady na systém. Pro intuitivní a dynamické přidávání nových typů zařízení bez nutnosti zásahu do kódu a restartu systému je možné implementovat komunikační protokol a metody pro jeho chování do databáze. Pro identifikaci nového zařízení a nastavení komunikace s ním pak bude stačit vytvořit nové záznamy v databázi skrz webové rozhraní.

Kapitola 5

Závěr

Výstupem této bakalářské práce je funkční prototyp bezpečnostního systému. Systém se skládá z lokálního bezpečnostního systému, který je integrovaný do fyzického objektu, a serveru, který je od lokálního systému oddělený. Systém je schopný spravovat více fyzických objektů a podporuje přidání nových koncových zařízení. Lokální systém monitoruje okolí objektu pomocí inteligentních senzorů založených na standardu ZigBee. Každou událost, která je senzory detekována, systém vyhodnotí. Je-li událost vyhodnocena jako bezpečnostní incident, systém spouští lokální poplach a varuje uživatele systému pomocí emailu nebo sms. Aktuální stav, historie všech událostí a statistiky jsou uživatelům přístupné skrz webové rozhraní, které je implementováno na serveru. Ve webovém rozhraní lze také měnit stav zabezpečení systému, přidávat nové uživatele a měnit základní nastavení. Pro ovládání systému z koncového zařízení slouží pouze přístupová klávsnice, která umožňuje po zadání hesla autentizovat osobu a měnit stav zabezpečení.

ZigBee standard a hlavně konkrétní XBee zařízení se při implementaci systému ukázali jako velmi spolehlivé řešení. Při použití těchto zařízení se nevyskytly žádné kritické problémy a zařízení splnila veškerá očekávání. Efektivní práce byla také s platformou Odoo, která díky osvědčeným principům velmi urychlila implemetaci. Nejobtížnější částí implementace byla optimalizace OpenWrt systému na routeru. Problém se týkal hlavně menší podpory požadovaných knihoven a aplikací pro zprovoznění především python aplikace pro komunikaci s XBee moduly. U budoucích projektů bych v závisloti na požadavcích energetické úspornosti možná zvážil platformu PC.

Systém lze použít čistě jako bezpečnostní systém, ale v rámci implementace bylo myšleno také na jeho snadné rozšíření. Může tak sloužit jako počáteční platforma pro vývoj podobných projektů. V rámci implementace bylo použito pouze open-source řešení.

Literatura

[1] *Sensor Technology Handbook*. Burlington: Elsevier, 2005, iSBN 0-7506-7729-5.

[2] *Measurement, instrumentation, and sensors handbook*. Second edition. Boca Raton: CRC Press, 2014, iSBN 978-1-4398-4889-0.

[3] ANDERSON, Ross: *Security engineering: a guide to building dependable distributed systems*. 2nd ed. Indianapolis: Wiley Publishing, 2008, iSBN 978-0-470-06852-6.

[4] CALLAWAY, E: *Wireless sensor networks*. Vyd. 1. London: CRC Press, 2004, iSBN 08-493-1823-8.

[5] FARAHANI, Shahin: *ZigBee wireless networks and transcievers*. Elsevier; Newnes, 2008, iSBN 978-0-7506-8393-7.

[6] HUDDLESTON, Creed: *Intelligent sensor design using the microchip dsPIC*. Amsterdam: Elsevier/Newnes, 2007, iSBN 978-0-7506-7755-4.

[7] NORMAN, Thomas L: *Integrated security systems design: concepts, specifications, and implementation*. Amsterdam: Elsevier Butterworth-Heinemann, 2007, iSBN 978-0-7506-7909-1.

[8] STEWART, James Michael, Ed TITTEL, Mike CHAPPLE: *CISSP: Certified Information Systems Security Professional Study Guide. 3rd ed.* San Francisco: SYBEX, 2005, iSBN 0-7821-4443-8.

[9] TIPTON, Harold F a Micki Krause NOZAKI: *Information security management handbook*. 6th ed. Boca Raton: Auerbach Publications, 2007, iSBN 978-0-8493-7495-1.

[10] Wgsimon: Creative Commons - Graf počtu transistorů na různých procesorech během času [online]. [cit. 2015-05-5]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Moore%C5%AFv_z%C3%A1kon#/media/File:Transistor_Count_and_Moore%27s_Law_-_2011.svg>.

[11] ZigBee Alliance: ZigBee PRO with Green Power [online]. [cit. 2015-04-22]. Dostupné WWW: <http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeepro/>.

[12] ČESKÁ SPOLEČNOST HYPERBARICKÉ A LETECKÉ MEDICÍNY ČLS JEP: Upozornění obyvatelům ČR na nebezpečí otravy oxidem uhelnatým [online]. [cit. 2015-05-1]. Dostupné z WWW: <http://www.cshlm.cz/aktualne/upozorneni-obyvatelum-cr-na-nebezpeci-otravy-oxidem-uhelnatym-95>.

[13] ČESKÝ STATISTICKÝ ÚŘAD: Kriminalita podle krajů v 1. až 4. čtvrtletí 2014 [online]. [cit. 2015-05-1]. Dostupné z WWW: <https://www.czso.cz/documents/10180/20549143/33008614q4p2.pdf/8968364c-4d36-4e27-b4ba-7210d973686d?version=1.3>.

[14] ČESKÝ STATISTICKÝ ÚŘAD: Požáry podle krajů v 1. až 4. čtvrtletí 2014 [online]. [cit. 2015-05-1]. Dostupné z WWW: <https://www.czso.cz/documents/10180/20549143/33008614q4p5.pdf/97aaacac-6dd9-48fb-9cdf-e0797874db8f?version=1.3>.

Příloha A

Instalace a konfigurace Odoo

- na čistě nainstalovaném systému Ubuntu 14.04 LTS první aktualizujeme software

```
sudo apt-get update
sudo apt-get upgrade
```

- nainstalujeme git pro stáhnutí a pozdější údržbu Odooo

```
sudo apt-get install git
```

- naklonujeme Odoo repozitář do složky /opt/odoo

```
git clone https://github.com/odoo/odoo.git /opt/odoo
```

- vytvoříme systémového uživatele odoo, kterého přidáme do skupiny sudo a přiřadíme domácí adresář /opt/odoo

```
sudo useradd -g sudo -d /opt/odoo/ odoo
```

- instalace postgreSQL databáze a vytvoření databázového uživatele odoo

```
sudo apt-get install postgresql
sudo su - postgres -c "createuser -s odoo"
```

- instalace pip manageru a knihoven vyžadovaných Odoo aplikací

```
sudo apt-get install python-pip
sudo apt-get install postgresql-server-dev-9.3 libxml2-dev
libxslt1-dev libevent-dev libldap2-dev libsasl2-dev
python-dev libjpeg-dev
sudo pip install -r /opt/odoo/requirements.txt
```

- změna vlastníka a vytvoření složky pro inicializační skript

```
chown -R odoo /opt/odoo
mkdir /var/run/odoo
chown odoo /var/run/odoo
```

- konfigurační soubor Odoo aplikace odoo-server.conf uložíme do složky /etc

```
[options]
admin_passwd = 123456
db_user = odoo
db_password = password
logfile = /var/log/odoo/odoo-server.log
addons_path=/opt/odoo/addons
lang = cs_CZ
secure = True
unaccent = True
xmlrpcs = True
xmlrpc = True
xmlrpc_port = 8069
```

- inicializační skript uložíme do složky /etc/init.d/ , nastavíme mu právo pro spuštění a nastavíme jej pro automatické spuštění po restartu

```
sudo cp odoo /etc/init.d/odoo
sudo chmod +x /etc/init.d/odoo
update-rc.d odoo defaults
```

- pro spuštnění, zastavení a restart Odoo serveru používame inicializační skript

```
/etc/init.d/odoo start
/etc/init.d/odoo stop
/etc/init.d/odoo restart
```

- do složky addons_path uvedené v konfiguračním souboru zkopírujeme složku s modulem bezpečnostního systému
- v menu Settings klikneme na položku Update Modules List a popup okně klikneme na tlačítko update
- v menu settings klikneme na položku Local Modules v pravém horním rohu zrušíme aktivníá filtr a zadáme jméno modulu mss pro vyhledání
- klikneme na tlačítko Install a počkáme na dokončení instalace

Příloha B

Instalace a konfigurace openWrt

Instalace openWrt

Instalace je popisována s využitím operačního systému debian 8, veškeré příkazy, které jsou uváděny z PC jsou myšleny právě pod tímto systémem.

- Obraz operačního systému openWrt Barrier Breaker lze stáhnout z
- Router zapojíme do elektrické sítě, zapneme a propojíme přes síťový kabel s PC, na routeru je třeba zapojit kabel do portů pro lokální síť
- V prohlížeči zadáme adresu 192.168.0.1 a přihlásíme se do administračního rozhraní
- V menu System Tools vybereme Firmware Upgrade a pomocí adresářového manageru vybereme stažený obraz systému a klikneme na Upgrade
- Po úspěšné instalaci a zrestartování routeru se připojíme pomocí telnet klienta na adresu 192.168.1.1

  ```
  telnet 192.168.1.1
  ```

  po připojení změníme heslo uživateli root

  ```
  passwd
  ```

  a restartujeme router

  ```
  reboot
  ```

-

Instalace podpůrných aplikací

- instalace python interpretu

  ```
  opkg install python python-openssl
  ```

- instalace pip manageru

  ```
  opkg install distribute
  easy_install pip
  ```

- instalace python modulů pro komunikaci s XBee přes sériové rozhraní

```
pip install xbee
pip install pyserial
```

- instalace python interpretu

```
opkg install python python-openssl
```

Instalace a konfigurace openvpn

- instalace openvpn

```
opkg install openvpn-openssl openvpn-easy-rsa
```

- vytvoření konfiguračního souboru myvpn.conf ve složce /etc/openvpn, tento soubor je automaticky načten při spuštění openvpn

```
client
dev tun0
proto udp
resolv-retry infinite
nobind
persist-key
persist-tun
verb 5
ca /etc/openvpn/ca.crt
cert /etc/openvpn/wrt.crt
key /etc/openvpn/wrt.key
remote 185.56.37.101 1194
remote-cert-tls server
comp-lzo no
```

- konfigurace firewallu

```
uci set network.vpn0=interface
uci set network.vpn0.ifname=tun0
uci set network.vpn0.proto=none
uci add firewall rule
uci set firewall.@rule[-1].name=Allow-OpenVPN-Inbound
uci set firewall.@rule[-1].target=ACCEPT
uci set firewall.@rule[-1].src=*
uci set firewall.@rule[-1].proto=udp
uci set firewall.@rule[-1].dest_port=1194
uci add firewall zone
uci set firewall.@zone[-1].name=vpn
uci set firewall.@zone[-1].input=ACCEPT
uci set firewall.@zone[-1].forward=ACCEPT
uci set firewall.@zone[-1].output=ACCEPT
```

```
uci set firewall.@zone[-1].network=vpn0
uci add firewall forwarding
uci set firewall.@forwarding[-1].src='vpn'
uci set firewall.@forwarding[-1].dest='wan'
uci commit network
/etc/init.d/network reload
uci commit firewall
/etc/init.d/firewall reload
```

Příloha C

Seznam použitého hardwaru a softwaru

- XBee modul XB24-Z7WIT-004
- SparkFun XBee Explorer USB
- SparkFun XBee Explorer Regulated
- PIR senzor HC-SR501
- magnetický kontakt MEDER MK04-1A66B-500W
- CMOS 4069 DIP14 NXP
- CMOS 4081 DIP14 STM/THOMSON
- Arduino Uno
- senzor teploty a vlhkosti AM2301
- senzor oxidu uhelnatého MQ7
- piezoelektrická sirénka KINGSTATE KXG-0905C
- TP-Link TL-WDR 4300
- Ubuntu 14.04 LTS
- OpenWrt Barrier Breaker 17.07
- Odoo V8
- OpenVPN 2.3.2

Příloha D

Obsah CD

Dokumentace	Programová dokumentace a uživatelská příručka
Zdrojove_Kody	Zdrojové kódy pro OpenWrt aplikaci, arduino a přístupovou klávesnici
Modul_Odoo	Všechny soubory Odoo modulu
BP_Zdroj	Zdrojové texty bakalářské práce pro LaTeX a obrázky
BP_Bezpecnostni_System.pdf	Pdf soubor této práce