Univerzita Pardubice
Fakulta elektrotechniky a informatiky

Řízení přístupu

Tomáš Vondra

Bakalářská práce

2021

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Tomáš Vondra**
Osobní číslo:	**I17160**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Téma práce:	**Řízení přístupu**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování

Zabezpečení dveří mechanický zámkem patří stále k nejpoužívanějším metodám, ale krom bezpečnosti přináší určité komplikace v podobě nutnosti nosit klíč fyziky sebou, ale obzvláště v možnosti správy klíčů, kdy například ztráta klíče znamená výměnu kompletního zámku a tím i všech klíčů k němu přiřazených. Problém je výraznější v prostředích, kde je možné mít jeden klíč přiřazen k více dveřím, případně v hierarchických systémech, kde existence a ztráta tzv univerzálního neboli master klíče znamená výměnu celého systému. Tyto nevýhody dynamicky odstraňují elektronické zámkové systémy se vzdálenou správou uživatelů. Cílem práce je navrhnout přístupový systém který by vyhovoval v prostředích jako jsou učebny fakulty elektroniky a informatiky. Teoretická část práce bude obsahovat rozbor možných metod identifikace, od použití biometrických metod, po metody využívající přístupové karty, klíčenky, mobilní telefony s NFC, případně jiné metody jednoznačné identifikace. Práce jednotlivé metody porovná z hlediska implementace s ohledem na dostupnost a sw/hw podporu takových řešení a z hlediska vhodnosti pro použití v nastíněném scénáři. Praktická část bude obsahovat výběr a řešení elektronického zámku, systém pro správu uživatelů a jejich práv, identifikaci uživatelů a logování přístupů, vše s ohledem na spolehlivost a rychlost odezvy.

Rozsah pracovní zprávy: **30-60**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

[1] VÁŇA, V. Mikrokontroléry ATMEL AVR: popis procesoru a instrukční soubor. Praha: BEN technická literatura, 2003.336 s. ISBN 978-80-7300-083-0.
[2] VÁŇA, V. Mikrokontroléry ATMEL AVR: programování v jazyce C. Praha: BEN technická literatura, 2003. 216 s. ISBN 978-80-7300-102-0.
[3] VLACH, J. Řízení a vizualizace technologických procesů. Praha: BEN technická literatura, 2002. 160 s. ISBN 978-80-86056-66-X.
[4] BRTNÍK, B. Základní elektronické obvody. Praha:BEN technická literatura, 2011. 156s. ISBN 978-80-7300-408-8
[5] RIPKA, P.; TIPEK, A. Master Book of Sensors. Praha : BEN, 2003. ISBN 0-12-75218

Vedoucí bakalářské práce: **Ing. Pavel Rozsíval**
Katedra elektrotechniky

Datum zadání bakalářské práce: **31. října 2020**
Termín odevzdání bakalářské práce: **14. května 2021**

L.S.

Ing. Zdeněk Němec, Ph.D. v.r.
děkan

Ing. Jan Panuš, Ph.D. v.r.
vedoucí katedry

V Pardubicích dne 26. února 2021

Prohlašuji:

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

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

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

V Pardubicích dne 10. 5. 2021

Tomáš Vondra

PODĚKOVÁNÍ

Mé obrovské poděkování patří panu Ing. Pavlu Rozsívalovi, který se mnou neztratil nervy, a i přes časový deficit byl vždy připraven pomoci. Jeho vedení, cenné rady a konzultace byly velkým přínosem pro tuto práci.

ANOTACE

Cílem práce je navrhnout přístupový systém, který by vyhovoval v prostředích jako jsou učebny fakulty elektroniky a informatiky. Teoretická část bude obsahovat rozbor možných metod identifikace od přístupových karet po biometrické metody.

KLÍČOVÁ SLOVA

zabezpečovací systémy, řízení přístupu, zámky, RFID, NFC, biometrika

TITLE

Access control

ANNOTATION

The goal of the work is to design an access system that would suit in environments such as classroom of the Faculty of electronics and informatics. The theoretical part will include an analysis of possible identification methods from access cards to biometric methods.

KEYWORDS

security systems, access control, locks, RFID, NFC, biometric

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK

RFID	Radio Frequency Identification
NFC	Near Field Communication
REST	Representational State Transfer
API	Application Programming Interface
AJAX	Asynchronous Javascript and XML
AES	Advanced Encryption Standard
JWT	JSON Web Token

ÚVOD

Tato práce pojednává o zabezpečovacích systémech a zámcích s důrazem na řízení přístupu a na rozbory jednotlivých identifikačních metod.

Jedny z velice populárních technologií jsou RFID a NFC, která se řadí k momentálně nejpoužívanějším. Tyto technologie si dopodrobna rozebereme a poté jednu z nich použijeme při realizaci praktické práce.

První kapitola teoretické části pojednává zprvu o zabezpečovacích systémech a zámcích jako takových. Je zde vysvětleno, co to je takový zabezpečovací systém, jak vypadá a jak funguje.

V druhé kapitole jsem se zaměřil na historii zabezpečovacích systémů od počátků až po možnou blízkou budoucnost.

Dále je dopodrobna popsáno řízení přístupu včetně základních typů, principů, výzev a osvětlení známých metod.

Další kapitola je věnována principům zámků, která pojednává o mechanických a elektronických zámcích s ohledem na jejich výhody a nevýhody.

V návaznosti na elektrické zámky je v další kapitole důkladně vysvětlena technologie RFID a její konkurent, technologie NFC.

V poslední kapitole teoretické části jsem se zaměřil na trend moderních dob, a to na biometrii. Zde jsou porovnávány možnosti různých biometrických metod, jejich klady a zápory.

Praktická část je věnována vývojové části zadané práce. Nejprve představuji celkovou aplikaci jako takovou a poté se zaměřuji na každý modul zvlášť.

1 ZABEZPEČOVACÍ SYSTÉMY A ZÁMKY

Všechny zabezpečovací systémy fungují na stejném základním principu a tím je zajištění vstupních bodů – například dveří, oken či jiných objektů sloužících k zabezpečení našich cenností. Speciální výjimkou jsou systémy zaměřující se na detekci enviromentálních hrozeb jako je požár, zaplavení a kouř.

Nejzákladnější definici kteréhokoliv zabezpečovacího systému lze najít v jeho názvu. Jedná se doslova o prostředek nebo metodu, kterou je něco zabezpečeno prostřednictvím systému spolupracujících komponent a zařízeních.

Modernější domácí zabezpečovací systémy jsou sítí elektronických zařízeních spolupracujících s centrálním řídícím panelem za účelem ochrany před zloději a dalšími potenciálními vetřelci. Takový typický systém se převážně skládá z řídícího panelu, dveřních a okenních senzorů, dotykových senzorů, bezdrátových kamer a alarmů. Není to však pravidlo.

Tento bezpečnostní systém funguje na jednoduchém konceptu zabezpečení vstupních bodů pomocí senzorů, které komunikují s řídícím panelem. Řídící panel slouží k aktivaci či deaktivaci celého systému. Zároveň komunikuje s jednotlivými komponenty a reaguje na ně v případě sepnutí. Často řídící panel obsahuje klávesnici či hlasový modul pro jednoduchou správu.

Zabezpečovací systémy jsou navrženy tak, aby se při porušení bezpečnostní zóny provedl určitý úkon. Tento úkon závisí na typu systému. U profesionálně monitorovaných systémů je upozorněna bezpečnostní firma. Vyškolený bezpečnostní expert se poté snaží komunikovat s majitelem přes řídící panel nebo telefonní kontakt. V případě potvrzení nouze dojde k informování příslušného personálu – policie, hasičů nebo zdravotní služby. Neprofesionální monitorovací systémy neinformují bezpečnostní firmu, ale nejčastěji spustí alarm a kontaktují majitele systému nebo přímo bezpečnostní složky policie.

Nevýhodou těchto systémů může být vysoká cena, měsíční poplatky za provoz nebo potíže při instalaci, aktivaci a deaktivaci. Naopak největší výhodou je vysoká bezpečnost cenností, snížené riziko loupeže, vzdálený přístup a ovládání domu.

2 VÝVOJ ZABEZPEČOVACÍCH SYSTÉMŮ

2.1 Počátky a historie

První myšlenky na osobní bezpečnost a zabezpečení vznikly už za dob pravěkých lidí. Před tisíci lety se lidé vybavovali větvemi, kameny a jinými přírodními zdroji, které poté dokázali přeměnit na základní zbraně jako jsou luky, praky a šípy. Tyto zbraně pak používali k opatření potravy lovem, ale také kvůli ochraně sebe samých či jejich teritoria. Později začali vymýšlet důmyslnější taktiky, jak se zabezpečit a použili ty samé přírodní zdroje na různé pasti či alarmující spouštěče.

2.1.1 Starověké bezpečnostní systémy

Historie zabezpečovacích systémů začala v momentě, kdy si lidé stavěli své první domy. Lidský instinkt se snaží chránit naše domovy, rodiny a majetek a tento instinkt se dokázal roky rozvíjet především díky historii válek a kvůli vrozené odpovědnosti chránit jeden druhého. Tím otevřel dveře vývoji jednoduchých i složitých řešeních na ochranu našich domovů.

V dávné historii lidé používali oheň, který poskytl ochranu před nepřáteli a divokou zvěří. A jelikož oheň mnohokrát nestačil a lidé postrádali luxus komplexních systémů, museli věnovat čas a úsilí tomu, aby zvýšili svou bezpečnost všemi dostupnými prostředky. Často využívali krajinu ke svému prospěchu a stavěli své vesnice na takovém místě, které jim poskytlo určitou výhodu. Například hory sloužící jako přírodní hradba či bažina jako přírodní překážka.

S vyvíjející se technologií se vyvíjela i důmyslnost bezpečnostních systémů. Vládci a panovníci začlenili do svých systémů padací mosty, příkopy, hradby, věže a další vymoženosti. Takové věže by se daly brát jako předchůdci kamerových systémů.

V průběhu historie se lidé také mnohokrát spoléhali na zvířata, která je varovala či dokonce bránila před vetřelci. Hlídací psi jsou klasickou formou zvířecích zabezpečovacích systémů. Byli vytrénováni svými pány, aby je upozornili na potenciální nebezpečí nebo dokonce zaútočili a vystrašili narušitele. Dodnes jsou velmi populárním způsobem, jakým si lidé chrání své domy a majetek.

2.1.2 První důmyslné zabezpečovací systémy

První zabezpečovací systém byl vynalezen Benjaminem Franklinem ve Spojených státech amerických v 18. století. Jednalo se o tři malá zrcátka připevněná na kovové tyči v okně druhého nebo třetího patra budovy. Úhel zrcátek umožňoval z vnitřku domu sledovat, kdo byl zrovna u jejich vstupních dveří, aniž by návštěvník něco tušil. Jedna z legend praví, že tento systém vynalezl za účelem vyklouznutí z domu v případě návštěvy jeho tchyně. Toto zařízení můžete stále vidět v historických částech Filadelfie.

Obrázek 1: Ukázka Franklinových zrcátek

Ač zrcátko není příliš nápaditá metoda, ukazuje nám, že zabezpečení může být jednoduché a stále efektivní. Od těchto skromných začátků z 18. století se technologie velmi rychle vyvinula v 19. a 20. století, kdy technologie byla na začátku svého vzestupu.

V polovině 19. století jistý elektrikář z USA, Moses Farmer, využil elektromagnet, který reagoval na spojený či nespojený elektrický obvod tím, že rozezvonil zvonec. Další dva vynálezci na tomto nápadu postavili první elektromagnetické zabezpečovacím systémy.

Augustus Pope, Bostonský ministr, vymyslel systém, který využíval právě onen zmiňovaný spojený a nespojený obvod Mosese Farmera. Reagoval na otevření či zavření dveří nebo oken.

Tok proudu způsobil vibrace magnetů, které rozpohybovaly kladivo, a to mlátilo do zvonu. Další součástky poté zabránily vypnutí systému po uzavření dveří a tím i obvodu.

William Channing využil telegraf a Farmerovu technologii k aktivování celoměstského systému. Využíval se v hasičských zbrojnicích na upozornění blízkého ohně.

Na konci 19. století podnikatel Edwin Holmes vzal Popeho a Channingův vynález na širší trh a poprvé se zabezpečovací systémy prodávaly mimo Anglii. Nejvíce se cílilo na New York kvůli jeho vysoké kriminalitě a brzy většina maloobchodníků i majitelů domů používali právě jeho výstražné systémy. V momentě, kdy se tento produkt dostal na širší trh, mnoho vynálezců začalo inovovat a vyvíjet své vlastní zabezpečovací systémy.

Obrázek 2: Ukázka Holmesova zabezpečovací systému

Edward Callahan z Baltimoru udělal obrovský pokrok v roce 1871. Vyvinul systém, který umožňoval podnikům a domovům přivolat posla kontaktováním centrálního místa pomocí vzdáleného telefonního seznamu. S tímto pokrokem nově dokázaly bezpečnostní systémy varovat jak lidi v domácnosti, tak i místní bezpečnostní orgány. Jednalo se o velmi populární službu, která umožnila Callahanovi prodat svůj vynález investorům, kteří vytvořili společnost American District Telegraph – dnes známá jako ADT.

Ve 20. století vývoj nezpomaloval. Roku 1960 Marie Van Britann Brown, která se živila jako sestřička, vyvinula první video-monitorovací systém a první systém, který dokázal otevřít dveře na dálku. Rok 1990 přinesl jeden z nejvlivnějších pokroků všech dob – internet. Lidé ještě nikdy předtím nezažili takovou úroveň rychlého přenosu dat a připojení. Mohli kontaktovat další jednotlivce z celého světa, pokud byli připojení k internetu. S internetem se zabezpečení domova stalo o mnoho jednodušší a pohodlnější než kdy předtím. Kombinace video-monitorování, vzdáleného ovládání a internetu vytvořila cestu pro dnešní bezpečnostní systémy.

2.2 Současnost a moderní využití

S příchodem internetu věcí se se zabezpečovacími systémy takzvaně roztrhl pytel. Díky pohodlnosti bezdrátového připojení, rychle se vyvíjející technologii a příznivosti cen, vyskočila popularita raketově. Komplexnost systémů se rozrůstala a s tím i druhy a počet jednotlivých komponent.

Pohybové senzory jsou zařízení uvnitř domů, které se aktivují, pokud něco zaznamenají ve své cestě. Pasivní infračervené světlo a mikrovlnné zpracování poskytuje vynikající výkon bez falešných poplachů. Existují také chytré detektory citlivé na domácí mazlíčky.

Vnitřní a venkovní kamery jsou základní součástí zabezpečovacího systému. Umožňují nahrávání oblastí domu nebo zahrady. Modernější kamery umí tento záznam rovnou posílat do chytrých telefonů či tabletů.

Detektory rozbití skla jsou užitečné senzory, které sledují frekvenci zvuku tříštícího skla. Spustí alarm, pokud se někdo snaží dostat do domu rozbitím okna nebo skleněných dveří. Výhodou je, že nejsou drahé.

Dveřní a okenní detektory kontaktu jsou senzory, které detekují, zdali jsou dveře či okno otevřené. Jedná se o dva senzory – jeden na dveřích nebo oknu a druhý na rámu. Pokud jsou dveře či okno zavřené, senzory tvoří uzavřený okruh. Pokud se dveře nebo okno otevře, okruh se přeruší a typicky se sepne alarm. Je to stará, ale stále efektivní metoda, která bývá levná.

2.3 Budoucnost

Podle nedávných zpráv tvoří zabezpečovací zařízení až 18 % ze všech chytrých domácích zařízeních na světě. Čím více lidé tráví čas doma, tím více si uvědomují důležitost zabezpečovacích systémů. V posledních letech rychlý vývoj technologií způsobil, že se bezpečnostní

průmysl výrazně změnil. Nikdo nemůže s jistotou říct, jaký bude současný stav za několik let, ale zkoumáním současných trendů můžeme odhadovat, jak bude vypadat potenciální budoucnost bezpečnosti.

2.3.1 Detekce pomocí dronů

Je pravděpodobné, že kombinace létajících dronů a značkovacích sprejů pomůže zastavit všechny vetřelce ještě před tím, než se vůbec dostanou k vašim dveřím. Sprej je označí a ze střechy bude vypuštěn dron, který je bude sledovat a filmovat jejich pokus o útěk.

2.3.2 Chytré detektory

Je docela zřejmé, že inteligentní bezpečnostní kamery se budou zlepšovat. Už dnes některé kamery dokážou rozlišit, zda se jedná o hrozbu či například jen o vašeho psa. Další fáze kamer by mohla jít zase o krok dále a může zahrnout faktory prostředí ze senzorů kvality vzduchu, teploty nebo třeba i chytré rozpoznání hlasu. Systém by mohl mít schopnost učit se různé kontexty, které se u vás doma běžně dějí v závislosti na denní době a ročním období.

2.3.3 Poplašné systémy

V nepříliš vzdálené budoucnosti by poplašný systém mohl být propojen s databází zločinců a třeba i automaticky provádět rozpoznání tváře. S touto kombinací, místo hlasitého zvuku a záblesků světel, může systém okamžitě odeslat data příslušným orgánům a třeba vetřelce oslovit jménem a tím ho vyděsit.

2.3.4 Automatizovaná sousedská hlídka

Dnes jsou sousedské hlídky poměrně známé hlavně spíše v zahraničí. Jedná se o skupinu lidí, která žije ve stejné oblasti a má zájem o vytvoření bezpečnějšího sousedství. Jejich spoluprací se snaží docílit snížení kriminality v dané lokalitě.

Technologie tuto metodu posune o krok dále tím, že spolu zabezpečovací systémy budou moci komunikovat i v rámci sousedství. Pokud se objeví narušitel, upozorní všechny ostatní domy a začnou kolektivně shromažďovat důležitá data.

2.3.5 Řízení přístupu pomocí čipů

Místo tradičních klíčů již dnes můžeme odemykat dveře pomocí chytrých telefonů. Za pár let uvidíme ještě pokročilejší bezpečnostní formu, a to lidské mikročipování. Již dnes jsou na trhu dostupné čipy, které se implantují do ruky a umožňují provádění jednoduchých úkolů pomocí jediného přístupového kódu, nicméně v budoucnosti budou moci uložit mnohem více dat a umožní například otevření dveří pouhým mávnutím ruky.

2.3.6 Kamerové systémy s umělou inteligencí

Kamerové systémy se postupně stávají opravdu zajímavé, protože díky inteligentnímu sledování, rozpoznávání obličeje či rozpoznávání počtu lidí roste jejich popularita a možnosti aplikace. V nadcházejících letech se dá očekávat, že tato technologie bude mít vlastní život díky umělé inteligenci a strojovému učení. Systémy budou umět sami rozpoznat, zda se jedná o kriminální aktivitu a sami rozhodnou, jestli upozorní příslušné bezpečnostní týmy.

2.3.7 Internet věcí a bezpečnost

Alexa nebo jiní virtuální asistenti se vyskytnou na poli bezpečnosti. Mohli by působit jako recepční i bezpečnostní týmy v jednom a využívat internetu věcí k připojení zámků, kamer, světel, telefonu a dalších. Zde jsou možnosti nerozměrné.

2.4 Tabulka vývoje

Tabulka 1: Vývoj bezpečnostních systémů

Zakladatel	Datum vynalezení	Zabezpečovací systém
	Pravěk	Jednoduché dřevěné či kamenné zbraně a pasti
	Středověk	Hradby, věže, padací mosty
Benjamin Franklin	1700	„Busybody“ - zrcátka
Augustus Russell Pope	1853	Elektro-magnetický alarm
Edward Callahan	1874	První zabezpečovací společnost
Marie Van Britann Brown	1966	První monitorovací systém
Kevin Ashton	1999	Pojem internet věcí

3 ŘÍZENÍ PŘÍSTUPU

Řízení přístupu je metoda, která zaručuje to, že uživatelé jsou ti, za které se vydávají a že mají příslušné oprávnění k přístupu. Reguluje, kdo nebo co může zobrazit či používat zdroje v kybernetickém prostředí. Je to základní koncept v počítačové bezpečnosti.

Řízení přístupu můžeme rozdělit na dva základní typy:

1) Fyzický
   a) Fyzické řízení přístupu omezuje přístup do budov, místností a dalších fyzických aktiv firmy. Typickým příkladem je přístup pomocí bezpečnostní karty.
2) Logický
   a) Logické řízení přístupu omezuje připojení k počítačovým sítím, k systémům a k citlivým firemním datům jako jsou hesla zaměstnanců.

Celá metodika řízení přístupu se skládá se ze dvou základních komponent:

1) Autentizace
   a) Autentizace je technika, která se používá k ověření toho, že někdo je tím, za koho se vydává. Sama o sobě k ochraně dat nestačí. Typickým příkladem je přihlášení přihlašovacím jménem a jeho heslem na webové stránce. Správnými přihlašovacími údaji dává uživatel webové stránce vědět, kdo je (uživatelské jméno) a že je to opravdu on (heslo, které zná jen on).
2) Autorizace
   a) Autorizace určuje, zda je uživatel oprávněn k přístupu k datům nebo k provedení transakce o kterou se pokouší. Například role vedoucí má oprávnění si zobrazit karty všech zaměstnanců, kdežto obyčejný zaměstnanec pouze tu svojí.

Cílem řízení přístupu je minimalizovat bezpečnostní rizika neoprávněného přístupu ať už k fyzickým či logistickým systémům. Bez autentizace a autorizace neexistuje správné zabezpečení dat. Při zjištění narušení dat se jako první kontroluje řízení přístupu a jeho politika, protože kontroly přístupu jsou klíčovou součástí. Pokud není řízení přístupu správně implementováno, může to mít katastrofické následky. Každá organizace, jejíchž zaměstnanci se připojují k

internetu (dnes již každá organizace), potřebuje určitou kontrolu přístupu, a to platí speciálně pro zaměstnance, kteří pracují mimo kancelář a vyžadují přístup k datům a službám společnosti.

Prvky zabezpečeného řízení přístupu fungují tak, že identifikují jednotlivce nebo entitu. Ověří, zda je osobou nebo entitou jenž tvrdí, že je a zároveň ověří, že daný uživatel či entita má právo na akce spojené s danou rolí, která je přiřazena uživatelskému jménu, IP adrese či jinému identifikátoru. Po úspěšné autorizaci a autentizaci umožní přístup k povoleným prostředkům.

Řízení přístupu je proces, který musí být správně integrován do prostředí IT. To může zahrnovat řízení identit a řídících systémů. Tyto systémy by měli poskytovat software, databáze a řídící nástroje pro správu zásad kontroly přístupu a auditu. Když je uživatel přidán do systému, administrátoři by měli použít automatizovaný systém k nastavení oprávnění. Osvědčená praktika je omezení přístupu na všechny zdroje a zaměstnancům udělit minimální práva, která jsou vyžadovány k přístupu k prostředkům.

Z vysoce distribuované povahy moderního IT vychází také mnoho výzev. Je obtížné sledovat neustále se vyvíjející aktiva, která jsou fyzicky i logicky rozložena. Některé konkrétní příklady výzev:

- Dynamická správa distribuovaných IT prostředí
- Trvanlivost hesel
- Dodržování předpisů a jejich důsledné auditování.
- Centralizace uživatelských adresářů
- Správa a viditelnost údajů

V dnešní době moderní řízení přístupu potřebuje být dynamické díky trendu cloudových a hybridních implementací, který rozděluje aktiva na fyzická místa. Tradiční řízení přístupu se statickými servery není nákladově efektivní.

Organizace také často zápasí s autorizací. Příkladem je scénář, kdy jeden ze zaměstnanců opustí práci. Při špatném bezpečnostním managementu se můžou vytvořit bezpečnostní díry, protože aktivum, které zaměstnanec používal k práci, například chytrý telefon s nainstalovaným firemním softwarem, je stále připojeno do firemní interní infrastruktury.

Dalším problémem je zajištění zabezpečení každého ze zaměstnanců. Pokud je některé ze zaměstnaneckých zařízeních napadeno, hacker může získat přístup k citlivým firemním datům, protože toto zařízení je stále připojeno do firemní infrastruktury a tváří se jako ověřený uživatel.

Jedno z řešeních tohoto problému je striktní monitorování a auditování událostí, jako kdo a kdy zpřístupnil citlivé zdroje. Pokud se nalezne podezřelé chování, účet a jeho práva mohou být hned aktualizovány či zakázány. Další, často opomíjené řešení, může být uživatelská zkušenost (UX) a návrh řídících technologií. Pokud je systém složitý na použití, zaměstnanec ho může použít nesprávně, a to může vést k bezpečnostním dírám. Například pokud se špatně nastaví monitoring, bezpečnostní záznamy se nemusí vůbec zaznamenávat.

Existuje mnoho aplikací a typů řídícího softwaru pro řízení přístupu. Je běžná praxe, že několik samostatných komponent spolu spolupracují za účelem udržení vysoké bezpečnosti. Nástroje mohou běžet na vlastních serverech, na cloudu nebo hybridně v obou. Některé z typů aplikací:

- Monitorovací a hlásící aplikace
- Nástroje pro správu hesel
- Nástroje pro zajištění zdrojů
- Úložiště rolí a identit
- Nástroje pro vynucování bezpečnostní politiky

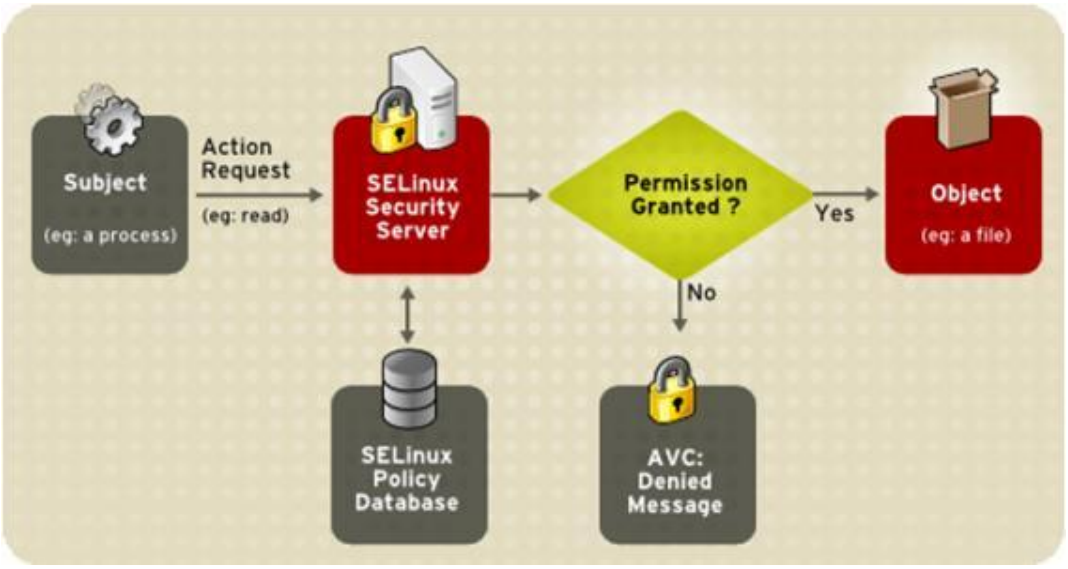
Většinu těchto nástrojů najdeme seskupené pod jedním byznysovým programem. Nejznámější je Microsoft Active Directory, který obsahuje většinu z výše zmiňovaných. Existují však i jiné nástroje od firem jako IBM, Idaptive či Okta.

3.1 Povinná kontrola přístupu (MAC)

Hierarchický model, kde jsou přístupová práva regulována centrální autoritou na základě několika úrovní zabezpečení. Je považován za nejbezpečnější model. Často využívaný ve vládě a armádě.

Všem uživatelům je přiřazena bezpečnostní úroveň, takzvaně level. Tyto uživatelé poté mohou přistupovat k objektům, které mají stejný nebo nižší level. Levely jsou typicky přiřazovány administrátorem, který je centrální autorita.

Příkladem v operačních systémech je SELinux s implementací MAC v operačním systému Linux.



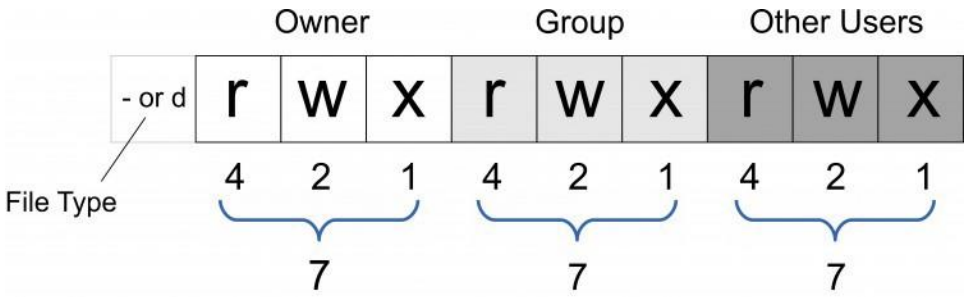
Obrázek 3: Ukázka MAC v SELinux

3.2 Volitelná kontrola přístupu (DAC)

Přístupová metoda, kdy účtu jsou přiřazena plná práva nad objektem, který vytvořil, nebo mu daná práva byla přiřazena. Tento objekt lze sdílet s vícero účty.

Přístupová oprávnění jsou uložená v seznamu řízení přístupu (ACL). Tento seznam lze generovat automaticky, když uživatel někomu udělí přístup, nebo jej může vytvořit správce.

Příkladem jsou přístupové práva na Unixových systémech. Vlastník souboru může ostatním uživatelům přiřadit práva přístupu k tomuto souboru.

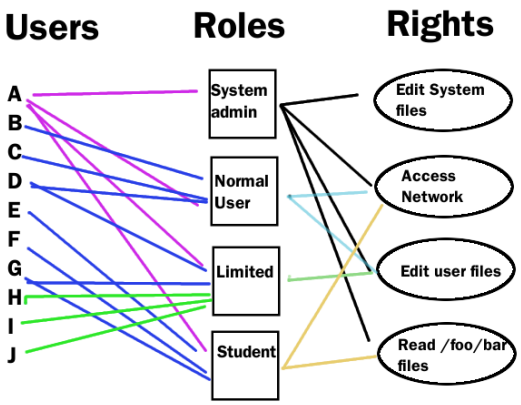


Obrázek 4: Ukázka DAC v Unixových právech

3.3 Řízení přístupu na základě rolí (RBAC)

Jedná se o široce rozšířený mechanismus řízení přístupu k počítačovým prostředkům na základě uživatelské role. Uživatelská role poté určuje, jaká přístupová práva účet bude mít.

Příkladem, role zaměstnanec má přístup pouze k prostředkům, které jsou nutné pro vykonávání jeho práce. Role administrátor bude mít práva obvykle vyšší, jako například správu těchto zaměstnanců.



Obrázek 5: Ukázka RBAC v systému

3.4 Řízení přístupu na základě pravidel (RuBAC)

V tomto bezpečnostním modelu administrátor definuje pravidla, která řídí přístup k prostředkům. Tyto pravidla můžou mít různé parametry jako třeba přístup pouze z určité IP adresy nebo země.

Konkrétním příkladem může být omezení přístupu k firemním datům pouze v pracovní době či ve zvoleném intervalu.

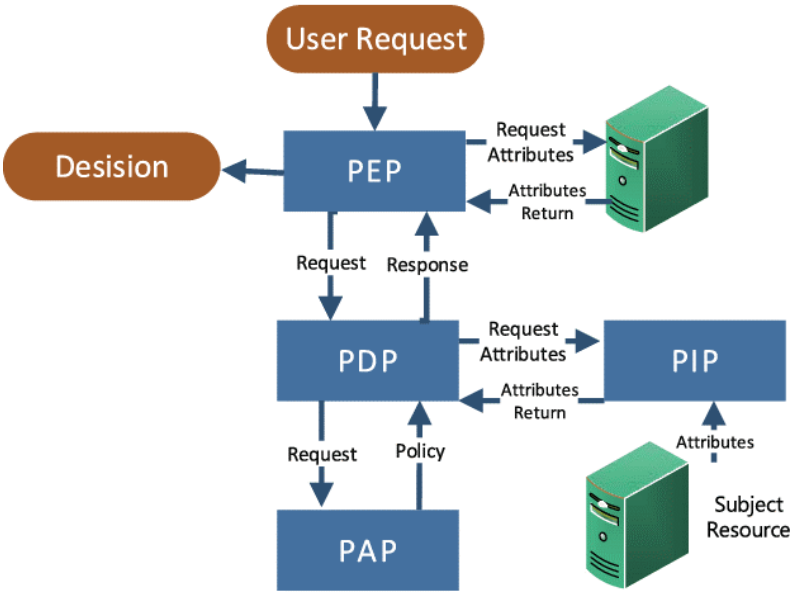
No.	Protocol	Source IP	Destination IP	Dest. Port	Action
1	TCP	10.1.1.1	20.1.1.1	80	Accept
2	TCP	10.1.1.2	20.1.1.1	80	Deny
3	TCP	10.1.1.0/24	20.1.1.1	80	Deny
4	TCP	10.1.1.3	20.1.1.1	80	Accept
5	TCP	10.2.2.0/24	20.2.2.5	80	Deny
6	TCP	10.2.2.5	20.2.2.0/24	80	Deny
7	TCP	10.3.3.0/24	20.3.3.9	80	Accept
8	TCP	10.3.3.9	20.3.3.0/24	80	Deny
9	IP	0.0.0.0/0	0.0.0.0/0	0-65535	Deny

Obrázek 6: Ukázka RuBAC v iptables

3.5 Řízení přístupu na základě atribut (ABAC)

Tento autorizační model vyhodnocuje atributy k určení přístupu. Cílem je zabránit přístupu uživatelům, kteří nemají schválené charakteristiky definované bezpečnostní politikou.

Příkladem modulu ABAC je umožnění přístupu do mzdového systému pouze uživatelům, kteří mají nastavený atribut *type=employees* a atribut *department=HR*.



Obrázek 7: Ukázka architektury ABAC.

4 ŘÍZENÍ PŘÍSTUPU A PRINCIPY ZÁMKŮ

Pokud se budeme bavit o fyzickém řízení přístupu, narážíme na elektronické zabezpečovací systémy. Obvykle využívají nějakou formu identifikátoru, jako jsou přístupové karty, které lidé využívají k autorizaci při vstupu do budovy. A protože tyto systémy dokážou zaznamenat kdo, kde a kdy se snažil autorizovat, poskytují velmi užitečná bezpečnostní data.

Mechanické klíče jsou nejjednodušší formou fyzického přístupu a tuto formu stále mnoho menších organizací využívá. Nicméně tento způsob má několik nedostatků a omezení.

- Lidé ztrácejí klíče
  - Pokud někdo ztratí klíč, musí se vyměnit celý zámek a nechat vyrobit nové klíče pro všechny, kteří mají přístup.
- Klíče se nedají sledovat
  - Nedá se sledovat kdo a kdy otevřel tyto dveře.
- Klíče je obtížné spravovat
  - Pokud má někdo přístup do několika budov a místností, potřebuje velké množství klíčů.

Využíváním elektronického řízení přístupu se vyhnete těmto problémům, a navíc získáte mnohem větší kontrolu.

- Kdo má a nemá přístup
- Ke kterým dveřím mají přístup
- Řízení časovaného přístupu
- Podmínky přístupu

Čím více kontroly, tím lepší přístupový systém. Dobrý přístupový systém by měl umět nastavit parametry pro jednotlivce a zároveň je rychle a snadno aktualizovat, pokud je potřeba.

Přístupové karty jsou stále nejvíce populární volbou. Přiložíte kartu ke čtečce a pokud jsou splněny podmínky uložené v systému, vstup je povolen. Existují i jiné metody, které dokonce nabízejí větší úroveň zabezpečení.

Klíčové identifikační metody jsou:

- Něco, co máte
  - přístupová karta nebo jiná identifikační známka.
- Něco, co víte
  - heslo nebo PIN kód.
- Něco, co jste
  - biometrické identifikátory jako je otisk prstu.

Každá metoda má své pro a proti a výběr spočívá na situaci. Volba se může lišit například pro venkovní dveře a dveře uvnitř budovy. Je zde i možnost kombinovat tyto metody za účelem zvýšení bezpečnosti. Typickým příkladem jsou dvoufázové ověření – nejdříve se ověříte heslem (něco, co víte) a poté vám přijde PIN kód na váš telefon (něco, co vlastníte)

4.1 Mechanické zámky

Pokud se mluví o zámcích, s největší pravděpodobností se mluví o mechanických zámcích. Jsou to standardy dveřního zabezpečení. Existují již stovky let a vždy budou volbou jednoduchého zabezpečení. Na rozdíl od elektronických zámků, nevyžadují k provozu elektřinu.

4.1.1 Zadlabací zámky

Tento typ je velmi typický a často používaný. Vyžaduje vyvrtání „kapsy“ do dveří, kam se poté umístí. Poskytuje velmi slušné zabezpečení, nicméně instalace tohoto typu je poměrně obtížná.

4.1.2 Válcové zámky

Další běžný typ mechanického zámku. Díky různým formátům vložek nabízejí různé úrovně zabezpečení. Tyto zámky však mohou být zranitelné vůči prasknutí a zámek může být rozbit, pokud na něj bude vyvíjen velký tlak.

Výhody mechanických zámků:

- Vysoká spolehlivost už mnoho let
- Dlouhá životnost
- Nepotřebuje elektřinu
- Odolný vůči počasí
- Jednoduchost
- Relativně nízká cena

Nevýhody mechanických zámků:

- Nejsou tak moderní pro tuto dobu
- Chybí audit při otevření dveří
- Pokud se ztratí klíč, celý zámek musí být vyměněn

4.2 Elektrické zámky

Elektrické zámky eliminují potřebu fyzického klíče a přidávají další funkce jako vzdálené odemykání a auditování přístupu. Můžou být dokonce řízeny či spravovány z chytrého telefonu.

4.2.1 Vstup na kód

Velmi rozšířený typ elektrických zámků. Před dveřmi je umístěna klávesnice a pro odemčení dveří se musí zadat správný kód.

4.2.2 Zámek ovládaný chytrým telefonem

Jak již název napovídá, tyto zámky vyžadují aktivaci z nějakého chytrého zařízení jako je telefon. Tyto zámky lze aktivovat odkudkoliv a obvykle potřebují aplikaci. Prostřednictvím aplikace můžeme předem nastavit časy zamykání, odemykání a další funkce, jako upozornění, pokud se někdo dveře pokusí otevřít.

4.2.3 Biometrické zámky

Biometrické zámky se ovládají pomocí jedinečných znaků biologické charakteristiky. Nejznámější přístup je pomocí otisku prstu. Stačí přiložit prst na zámek a pokud se otisky shodují s těmi v systému, získáte přístup. Mezi další biometrické možnosti patří oční skenery či aktivace hlasem. Tyto metody jsou považovány jako jedny z nejbezpečnějších, avšak můžou být velice drahé.

4.2.4 Přístupové karty

Zámky na přístupové karty jsou čtečky karet, ke kterým se přiloží identifikační karta či tag a dveře se aktivují podle nahraných informacích na kartě. Jedná se o momentálně nejrozšířenější elektronický zámek.

Výhody elektrických zámků

- Schopnost monitorovat přístup
- Možnost samo-obslužných zámků
- Zvýšené zabezpečení zámku
- Jednoduchá správa

Nevýhody elektrických zámků

- Nutnost elektřiny

5 RFID A NFC ZÁMKY

5.1 Radio Frequency Identification – RFID

RFID je zkratka pro radio-frequency identifikation, česky identifikace na rádiové frekvenci. Označuje technologii, při níž jsou digitální data zakódovaná v RFID štítcích, snímána čtečkou pomocí rádiových vln. Informace jsou elektronicky ukládány na takzvaný tag (štítek), který je přidružený k danému objektu. Tag je aktivován, pokud je poblíž čtečky, což mu umožňuje sdílet informace, které v sobě má.

Systémy RFID se skládají ze tří složek: RFID tagu, RFID čtečky a antény. Tagy obsahují integrovaný obvod a anténu, která se používá k přenosu dat do čtečky. Čtečka poté převádí rádiové vlny na použitelnější formu dat. Tyto informace z tagů jsou obvykle poté přeneseny přes komunikační rozhraní do hostitelského systému, kde se data ukládají do databáze a používají později.

Technologie RFID se běžně používá v systémech řízení přístupu. Nejběžnější použití je ve vstupních systémech pro zaměstnance. V tomto případě se tagy obvykle používají na velmi základní úrovni, což poskytuje jednoduché řešení pro jakoukoliv společnost, která řízení přístupu využívá.

RFID aplikace pro identifikaci personálu běžně pracují na nízké frekvenci 140kHz. Informace o držiteli karty či objektu jsou ukládány na tagy, ty však mohou uchovávat pouze malé části informací jako jsou identifikační čísla.

RFID tagy jsou velmi odolné a fungují za jakéhokoliv počasí. Na druhou stranu existuje jistá nespolehlivost, protože cokoliv vysílá signál může být odchyceno. Existuje možnost, že kdokoliv vybavený čtečkou RFID by mohl přistupovat k vloženým informacím na cizí kartě a ty poté zneužít. „Nepřátelská“ čtečka může navíc čtecí rozsah ještě rozšířit pomocí zesilovače. Pokud dojde ke krádeži informací na kartě, je velmi jednoduché tyto informace naklonovat na novou kartu. RFID karty jsou navíc náchylné k elektromagnetickému rušení, které může pocházet z jiných RFID karet nebo jiného zmagnetizovaného zařízení. To znamená, že se můžou snadno zaseknout či ztratit schopnost přenášet informace.

5.1.1 RFID Tagy

Jak již bylo zmíněno výše, RFID štítky se skládají z integrovaného obvodu a antény. Také jsou však složeny z ochranného materiálu, který drží kousky pohromadě a chrání je před různými podmínkami prostředí. Ochranný materiál závisí na dané aplikaci. Například zaměstnanecké odznaky jsou obvykle vyrobeny z odolného plastu a tag je vložen mezi plastové vrstvy. Nejčastěji se jedná o karty nebo klíčenky.

RFID Tagy přichází ve dvou typech – pasivní nebo aktivní.

- Pasivní tagy jsou nejpoužívanější, protože jsou menší a jejich implementace je levnější. Před přenosem dat musí být pasivní tagy „zapnuty“ čtečkou RFID.
- Aktivní tagy nepotřebují být „zapnuty“ čtečkou RFID, protože v sobě mají zabudovaný napájecí zdroj (třeba baterii), což jim umožňuje kdykoliv přenášet data.

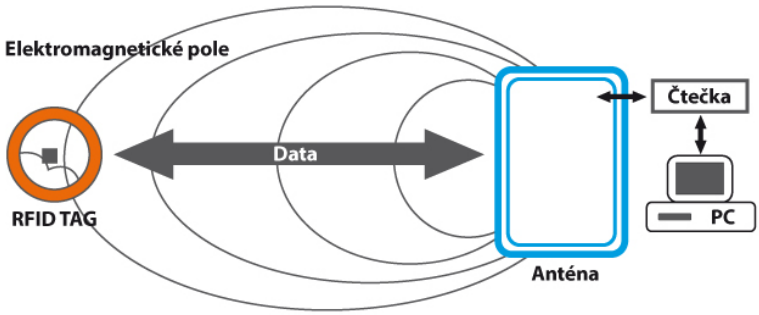
Tagy může přijímač detekovat z poměrně vysoké vzdálenosti, takže jsou ideální pro řízení přístupu do budov s vysokým počtem zaměstnanců.

5.1.2 RFID čtečka

Každá čtečka RFID je vybavena malou anténou, která vysílá vlastní rádiové vlny za účelem detekce tagů ve svém rozsahu. Tento rozsah se může lišit v závislosti na frekvenci rádiových vln, které vydává, od deseti centimetrů až do jednoho metru. Čtečka dekóduje unikátní informace, které jsou emitovány z odpovídajícího RFID tagu, a odesílá signál do svého hostitelského softwaru, který uživateli buď uděluje nebo odepírá přístup.

5.1.3 Anténa

Účelem antény je absorbovat rádiové vlny ze signálu čtečky a odesílat a přijímat data. Výkon pasivního RFID tagu závisí právě na anténě – čím větší anténa, tím více může nashromáždit energie a tím zvýšit čtecí rozsah. Nízkofrekvenční antény jsou obvykle cívky, protože tyto frekvence jsou magnetické.



Obrázek 8: Ukázka RFID technologie.

5.2 Near Field Communication – NFC

NFC neboli Near Field Communication (komunikace na blízko), umožňuje komunikaci na krátkou vzdálenost mezi kompatibilními zařízeními. Je to velmi podobná technologie jako RFID, akorát že modernější.

I když funkce je podobná RFID, NFC se běžněji vyskytuje v mobilních systémech řízení přístupu, ve kterých je tag v chytrém telefonu a může se chovat jak jako přijímač dat, tak jako vysílač dat. Klíčový rozdíl je však omezený rozsah, který je oproti RFID technologii o dost menší.

RFID umožňuje identifikaci pomocí rádiových vln. NFC je postaveno na těchto standardech a posouvá je o krok dále. Umožňuje nejen identifikaci položek, ale také umožňuje bezpečnou výměnu dat prostřednictvím bezkontaktní peer-to-peer komunikace. Navíc zařízení NFC může fungovat jako tag i jako čtečka. Každé zařízení je buď pasivní nebo aktivní stejně jako u RFID.

Pasivní zařízení NFC zahrnují tagy a další malé vysílače, které mohou odesílat informace do jiných zařízení NFC bez nutnosti vlastního zdroje napájení. Nezpracovávají však žádné informace odeslané z jiných zdrojů a nemohou se připojit k jiným pasivním zařízením.

Aktivní zařízení jsou schopna odesílat i přijímat data a mohou komunikovat navzájem i pasivně. Smartphony jsou zdaleka nejběžnější formou aktivního zařízení NFC. Dobrým příkladem této technologie jsou také čtečky karet veřejné dopravy a dotykové platební terminály.

NFC funguje stejně jako Bluetooth, Wi-Fi a všechny ostatní bezdrátové signály. Pracuje na principu odesílání informací přes rádiové vlny. Je standardem pro bezdrátové datové přenosy, což znamená, že zařízení musí dodržet určité specifikace, aby mohly správně komunikovat. Technologie je založená na starších myšlenkách RFID, které k přenosu informací používaly elektromagnetickou indukci.

Výhody oproti klasickému RFID

- Není potřeba fyzických tagů, karet
  - Díky NFC technologii můžeme jako tag využít náš chytrý telefon, pokud však tuto možnost podporuje.
- Nenáročnost na údržbu
  - Snadno začlenitelné do cloudových systémů. Přidávání a odebírání uživatelů je snadné, chyby v zabezpečení jsou minimální a celková správa vyžaduje mnohem méně prostředkům
- Zvýšené zabezpečení
  - V případě krádeže by zloděj musel odcizit celý chytrý telefon, který má sám o sobě několik vrstev zabezpečení.

Nevýhody oproti klasickému RFID

- Kratší rozsah
  - RFID mají dosah několik stop, kdežto NFC jsou omezena na několik palců.

Ačkoliv používání mobilních telefonů pro přístup má výhody, je zde několik úvah:

- Méně pohodlí
  - Chcete-li použít systémy řízení přístupu na bázi NFC, lidé často předpokládají, že stačí mít svůj mobilní telefon. Není tomu ale tak, protože musí být splněna jistá kritéria. Telefon musí být:
    - Smartphone
    - Vybaven správnou aplikací
    - Zapnutý, s dostatečnou baterií a se zapnutou funkcí NFC
- Technologické limity
  - Jelikož různé operační systémy jako Android a Apple mají pravidelné aktualizace, starší smartphony nemusí mít NFC aplikaci vůbec nainstalovanou. U některých telefonů dokonce nemusí být k dispozici dostatek příslušného místa pro tuto aplikaci.
  - Pokud také někdo smartphone vymění za nový, musí si znova stáhnout tuto NFC aplikaci a požádat o nové přihlašovací údaje.
  - Pokud někdo přijde ke dveřím a dojde mu baterie v telefonu, musí existovat nějaký záložní plán.
- Kybernetická rizika a hacking
  - Některá mobilní ověření jsou obyčejná čísla uložená v aplikaci a přenášena prostřednictvím NFC, takže zde existuje riziko, že tato čísla mohou být zachycena a použita k trestné činnosti.

6 BIOMETRICKÉ ZÁMKY

Rychlý vývoj technologie biometrického rozpoznávání vedl k tomu, že už se biometrické bezpečnostní systémy nepoužívají jen v místech s vysokým zabezpečením, jako jsou banky, ale také v prostředích, které nepotřebují až takovou míru zabezpečení, třeba kanceláře. Biometrické systémy otevírají zcela nové příležitosti ke zlepšení ochrany lidí, míst a majetku a zároveň nabízejí lidem uživatelsky přívětivější způsoby, jak se identifikovat.

Biometrie je věda, která provádí biologické měření za účelem identifikace jednotlivců. Zahrnuje použití biometrického bezpečnostního softwaru k automatickému rozpoznávání lidí na základě jejich chování nebo biologických charakteristik.

Klíčová výhoda biometrických bezpečnostních zařízeních je vysoké zabezpečení. Je mnohem těžší zfalšovat otisk prstu než přístupovou kartu. K ještě větší úrovni zabezpečení lze biometrické údaje použít také k ověření více faktorovým ověřením. Další značnou výhodou je pohodlí uživatelů. Je snadné zapomenout klíč nebo kartu, ale své biometrické údaje máte stále u sebe. A úrovně uživatelského pohodlí se zase dají posunout o úroveň výše – například pokud se jedná o obličejové rozpoznání na dálku, můžete prostě projít a systém vám sám naskenuje obličej v momentě, co budete procházet.

Zásadní nevýhoda biometrických bezpečnostních zařízeních je přesnost, která není zaručena. Každá technologie biometrického rozpoznávání má svou vlastní míru přesnosti a falešné odchylky. Další z nevýhod je sběr osobních údajů. Je důležité je uchovávat v souladu s místními předpisy – GDPR. Nutno také vytknout faktory jako jsou mokré prsty, nejasné otisky či onemocnění sítnice v oku. Všechny tyto faktory můžou zapříčinit nemožnost použití. A pro některé případy je nevýhoda i to, že uživatel musí být fyzicky přítomen při registraci do systému.

Možnosti řízení přístupu pomocí biometrie se nyní pohybují od rozpoznání tváře až po rozpoznávání vzorců krevních cév. Rozpoznání pomocí DNA je velmi blízko realitě. Pokud jde o výběr biometrické technologie, záleží na vyvážení zabezpečení, které potřebujeme, a finančních prostředcích, které jsme schopni obětovat.

6.1 Otisk prstu

Rozpoznání otisků prstů je považováno za jeden z nejstarších a nejrozvinutějších typů biometrického rozpoznávání. Skener otisků prstů pořídí vylepšený obraz s mřížkami. Tento obraz je

převeden do šablony ukazující charakteristiky otisku prstu. Tato šablona se poté porovnává s přiloženým prstem.

Výhody:

- Poměrně dobrá přesnosti
- Relativně nízká cena
- Známá a ověřená technologie

Nevýhody:

- Špína, vlhkost či oděrky v prstu mohou mít vliv na přesnost.

6.2 2D rozpoznání obličeje

Kamera vyfotí obraz obličeje osoby. Tento obraz je převeden do matematického kódu, který slouží jako šablona. Tato šablona se poté porovnává s obličejem člověka, který žádá přístup.

Výhody:

- Snadné použití
- Rychlost rozpoznání
- Lze využít v monitorovacích systémech ke sledování osob na černé listině

Nevýhody:

- Nepříliš velká přesnost

6.3 3D rozpoznání obličejem

Je vytvořena trojrozměrná mapa obličeje pomocí infračervených mřížek nebo sloučením několika obrazů.

Výhody:

- Uživatelsky přívětivá
- Rychlost rozpoznání
- Vyšší přesnost než 2D

Nevýhody:

- Brýle a vousy mohou snížit přesnosti
- Ještě stále není tak přesná jako třeba otisk prstu

6.4 Rozpoznání duhovky (oka)

Oko je vyfoceno a uloženo do obrázku. Obrázek je převeden do matematického kódu a uložen jako šablona, která se poté porovnává.

Výhody:

- Vysoká přesnost
- Dnes již vzdálenost může být i přes 2 metry

Nevýhody:

- Méně uživatelsky přívětivá – je třeba dobré osvětlení
- Nerozpozná brýle

6.5 Geometrie ruky

Čtečka pořídí trojrozměrný obraz ruky a měří tvar a délku. Tyto 3D měření se poté převedou na matematický identifikátor a vytvoří se šablona.

Výhody:

- Špína a vlhkost neovlivní přesnost

Nevýhody:

- Přesnost není až tak vysoká

6.6 Rozpoznání žil

Unikátní vzor žil každého člověka je zachycen pomocí infračerveného světla. Tento vzor je pak rozpoznán čtečkou, která svítí infračerveným světlem na ruku nebo prst, aby žíly byly viditelné.

Výhody:

- Přesnost
- Špína nemá vliv na přesnost

Nevýhody:

- Méně uživatelsky přívětivé – poloha ruky musí být umístěna přesně.
- Studené teploty ovlivní přesnost

6.7 DNA

Uloží se vzorek DNA a poté se porovnává při pokusu o přístup.

Výhody:

- Hodně vysoká přesnost

Nevýhody:

- Ač se technologie vyvíjí, stále ještě není použitelná kvůli dlouhé době analýzy.

7 REALIZACE PRAKTICKÉ PRÁCE

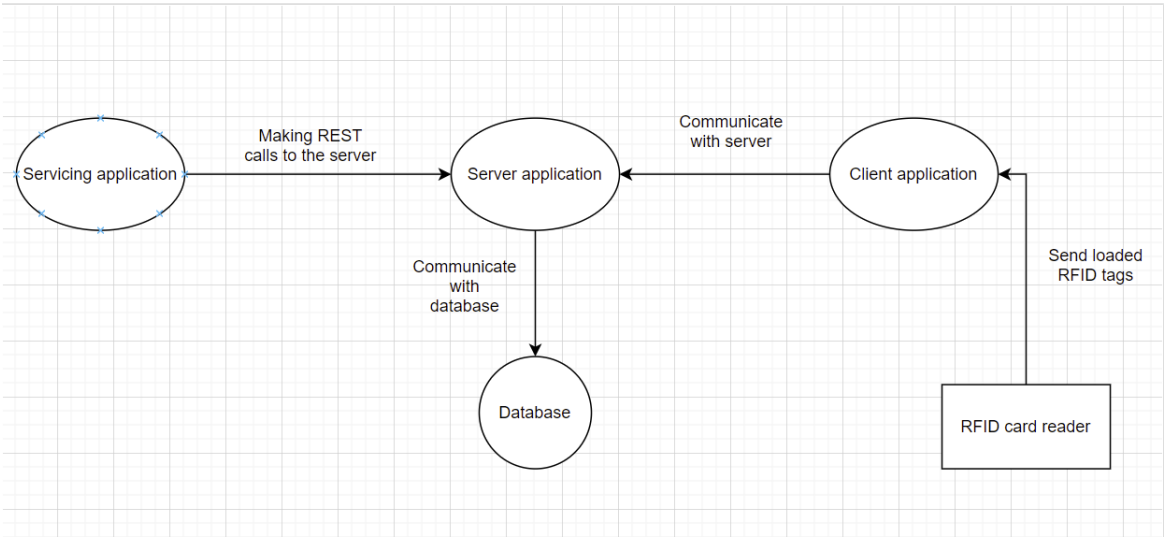
V této poslední kapitole se budu věnovat realizaci praktické práce. Celkové řešení se skládá z jednotlivých modulů, které popíšu dopodrobna v podkapitolách. Zaměřím se především na použité technologie, hardwarové komponenty, softwarové závislosti, dané funkce kódu, vývojové prostředí, konfigurovatelnost, zabezpečení a širší pohled na moduly jako takové.

Pro danou práci jsem využil znalosti a zkušenosti z firemního odvětví, tudíž je alespoň serverová část napsána konfigurovatelně a s ohledem na možné rozšiřování. Také jsem se snažil držet principů čistého kódu s využitím „best practices“.

Celkové řešení využívá klient-server architektury. Klient, modul ESP32, slouží k obsluze dveří a načítání RFID karet. Zasílá načtené RFID tagy serveru, který je porovná s těmi, které jsou uložené v databázi, a zašle zpět informaci o úspěchu či neúspěchu autorizace.

Databáze funguje odděleně. Může se jednat o jakoukoliv relační databázi a může běžet jak lokálně, tak kdekoliv jinde v síti či internetu. Musí se však nastavit v konfiguračním souboru serverové aplikace.

Serverová aplikace je napsána ve stylu REST architektury, tudíž potřebuje obslužného klienta, který bude posílat požadavky na koncové adresy této aplikace. Tento klient může být napsán v jakémkoliv jazyce. Je nezávislý na platformě a může ho napsat kdokoliv se znalostí API serverové aplikace.



Obrázek 9: Ukázka systému jako celku

Scénář:

1. Klient se připojí k Wi-Fi, spustí svůj webový server a vyčkává na žádost o registraci. Do té doby nemůže číst RFID karty či přijímat jiné žádosti.
2. Uživatel přes obslužnou aplikaci zadá IP adresu a název klienta. Ta zašle REST požadavek serverové aplikaci, která se pokusí klienta zaregistrovat a vrátí odpověď. Na tu obslužná aplikace reaguje a zobrazí hlášku.
3. Klient obdrží žádost o registraci a pokud je vše v pořádku, uloží si adresu serverové aplikace pro případnou komunikaci.
4. Pokud je v dosahu RFID čtečky karta, aplikace jí načte, zvaliduje, a nakonec pošle serveru její tag id v hexadecimální podobě.
5. Server se podívá do databáze, zda obsahuje tag id, které jí bylo zasláno. Pokud ano, vrátí kladnou autorizační odpověď.
6. Klient reaguje na autorizační odpověď sepnutím či nesepnutím dveří.

7.1 Serverová aplikace

Serverová aplikace je jádrem celého systému. Obstarává registraci, komunikaci a správu klientů. Zároveň komunikuje s databází a spravuje povolené RFID tagy. Pro snadnější identifikaci případných chyb loguje celkový běh aplikace do souborů a komunikaci s klientem loguje externě do databáze. V neposlední řadě je aplikace vysoce konfigurovatelná.

7.1.1 REST architektura

Jedná se o webovou službu, která byla napsána podle pravidel REST architektury. Díky REST architektuře můžeme konat jednotlivé příkazy pomocí jednoduchých HTTP volání na dané koncové body. V aplikaci jsou využity metody HTTP popsané níže, nicméně existuje jich více.

Metody:

- GET metoda
  - Požadavek sloužící k získání určitého prostředku. Případné data lze zaslat přes URL adresu.
- POST metoda

- Požadavek sloužící k zaslání dat na server.

- DELETE metoda
  - Požadavek sloužící k smazání prostředku na serveru.

7.1.2 Zabezpečení

K zabezpečení koncových bodů a zabránění neautorizovaného volání jsem zvolil otevřený standard JSON Web Token (JWT), který slouží k zabezpečenému přenosu informací mezi stranami. Tyto informace jsou důvěryhodné a lze je ověřit, protože jsou digitálně podepsané.

Při autentizaci uživatel zašle své přihlašovací údaje serveru a pokud jsou správné, server vrátí speciální token. Tento token poté slouží k autorizaci a tím pádem nám odpadne starost neustále posílat přihlašovací údaje s každým novým požadavkem.

7.1.3 Koncové body aplikace:

- /login [POST]
  - Slouží k zaslání přihlašovacích údajů v podobě JSON formátu
  - Při úspěšné autentizaci vrátí JWT token, který je potřeba použít v hlavičce při volání zabezpečených koncových bodů.
  - Všechny koncové body jsou zabezpečené kromě bodu /login, který slouží neautorizovanému uživateli pro možnost přihlášení, a bodu /api/v1/openRequest, na který klient zasílá požadavky na kontrolu načteného tagu.
- /api/v1/registration/register/{ip} [GET]
  - Odešle požadavek registrace na danou IP adresu klienta.
  - Vrací status registrace.
- /api/v1/registration/revoke/{ip} [GET]
  - Odešle požadavek odregistrace na danou IP adresu klienta.
  - Vrací status registrace.
- /api/v1/clients/ [GET] / [POST]

- [GET] Vrací registrované klienty.
- [POST] Přijímá JSON objekt klienta, kterého přidá do databáze.

- /api/v1/clients/{clientIp} [DELETE]
  - Odstraní klienta z databáze.
- /api//v1/history [GET]
  - Vrací historii požadavků na klienty.
- /api/v1/tags [GET] / [POST]
  - [GET] Vrací uložené RFID tagy v databázi
  - [POST] Přijímá JSON objekt tagu, který přidá do databáze.
- /api/v1/tags/{tagId} [DELETE]
  - Odstraní tag z databáze.
- /api/v1/{ip}/open [GET]
  - Odešle požadavek na IP klienta, který slouží k otevření dveří.
  - Vrací status o úspěšnosti.
- /api/v1/openRequest [POST]
  - Přijímá JSON požadavek od klienta.
  - Slouží k autorizaci tagu.

7.1.4 Konfigurovatelné parametry:

Aplikační konfigurovatelné parametry:

- ACDuino.username [povinné]
  - Nakonfiguruje jméno defaultního uživatele, který se propíše do databáze.
- ACDuino.password [povinné]
  - Nakonfiguruje heslo defaultního uživatele
- jwt.security.secret [nepovinné]
  - Nakonfiguruje tajemství zabezpečení JWT.
- jwt.security.expiration [nepovinné]
  - Nakonfiguruje expiraci JWT tokenu.
  - Defaultní hodnota 30 minut v milisekundách.
- aes.security.salt [povinné]
  - Nakonfiguruje sůl AES zabezpečení
- aes.security.password [povinné]
  - Nakonfiguruje heslo AES zabezpečení

Spring konfigurovatelné parametry:

- spring.datasource + spring.jpa
  - Konfigurace databáze
- server.port
  - Konfigurace portu aplikace.
- logging
  - Konfigurace logování aplikace.

7.1.5 Vývoj

Použité technologie:

- Java (JDK 11)
- Spring framework
- Spring Boot framework

Vývojové prostředí a nástroje:

- Intellij IDEA Ultimate
- Insomnia

Závislosti:

- Spring-boot-starter-web
- Spring-boot-starter-test
- Spring-boot-starter-data-jpa
- Spring-boot-starter-security
- Spring-security-test
- Jjwt-api
- Jjwt-impl
- Jjwt-jackson
- Mysql-connector-java

7.2 Klientská aplikace

Klientská aplikace je modul, který se stará o načítání RFID karet a o ovládání dveří. Čtečka načte RFID tag, který aplikace zašle serveru. Server ověří jeho autorizaci a vrátí odpověď. Aplikace poté reaguje na danou odpověď a podle úspěchu či neúspěchu autorizace sepne elektrický zámek.

Při prvním spuštění klient vyčkává na požadavek k registraci. Po úspěšné registraci je připravena přijímat další příkazy jako třeba vynucené otevření dveří či odregistrace. Také aktivuje čtečku RFID karet a je připravena číst a odesílat tagy serveru.

7.2.1 Hardware

- ESP-WROOM-32
  - Jedná se o IOT modul s dvoujádrovým procesorem, Wi-Fi a Bluetooth konektivitou
  - Celý kód je nahrán právě do tohoto mikrokontroleru. Řídí tedy celý systém klienta.
- RFID čtečka RDM6300
  - RFID čtečka s externí anténou.
- LED diody
  - Vizuální reprezentace konaných operací.

7.2.2 Software

- Třída ACDuinoHardwareController
  - Stará se o celkovou obsluhu připojených modulů do ESP32.
  - Spíná dveře, bliká LED diodami, obsluhuje RFID čtečku
- Třída ACDuinoWifi
  - Konfiguruje připojení k Wi-Fi síti.
- Třída ACDuinoWifiClient
  - Zasílá požadavky serveru.
  - Odesílá RFID tagy a čte odpověď serveru
- Třída ACDuinoWifiServer
  - Naslouchá požadavkům serveru.
  - Čeká na požadavek o registraci, poté na požadavky na odregistraci a otevření.

7.2.3 Vývoj

Použité technologie:

- Wiring

Vývojové prostředí a nástroje:

- Visual Studio Code
- Arduino IDE

Závislosti:

- ArduinoJSON

7.3 Obslužná aplikace

Obslužná aplikace je aplikace, která zasílá požadavky na server a tím pádem ho nám umožňuje intuitivně řídit. Mohla by být napsána v jakémkoliv jazyce nezávisle na platformě. Dokonce můžeme mít vícero obslužných aplikací jako třeba aplikace na desktopu či mobilní aplikace.

Pro tuto práci jsem zvolil jednoduché řešení, a to aplikaci napsanou v Javascriptu. Ta zasílá požadavky pomocí technologie AJAX a přes html kód reprezentuje grafickou podobu stránku.

7.3.1 Vývoj

Použité technologie:

- HTML
- CSS
- Javascript

Vývojové prostředí a nástroje:

- Visual Studio Code

- Intellij IDEA Ultimate

Závislosti:

- jQuery
- Bootstrap

7.4 Databáze

Databáze funguje zcela nezávisle na serverové aplikaci. Může se zvolit jakákoliv relační databáze a může být umístěna kdekoliv, odkud na ní serverová aplikace vidí. Ostatní moduly s ní vůbec nekomunikují.

Pro tento projekt jsem zvolil externí MySQL databázi, která běží v docker kontejneru.

7.4.1 Docker

Docker je otevřený softwarový nástroj, jehož cílem je izolovat aplikace do kontejnerů jak na Linuxu, tak na Windows nebo Mac OS.

Kontejnery umožňují zabalit aplikaci se všemi závislostmi, které potřebuje. Díky tomu si můžeme být jisti, že aplikace bude spuštěna na jakémkoliv počítači bez ohledu na jeho vlastní nastavení, které by se mohlo lišit od počítače, kde byla aplikace napsána

7.5 Možné rozšíření / co se nestihlo

- Zabezpečená komunikace s klientem pomocí AES šifrování.
- Lepší grafická stránka obslužného klienta / přepsání do frameworku React
- Obslužný klient běžící i na telefonu.
- Rozšířené REST služby jako třídění výsledků, paginace.
- Jednotkové testy

ZÁVĚR

Cílem práce bylo navrhnout a zhotovit přístupový systém, který by pracoval na stanovištích jako jsou školní učebny či firemní místnosti. Popsat různé metody identifikace a zvolit takovou, která bude vhodná pro učebny Fakulty elektrotechniky a informatiky.
Nejdříve jsem tedy popsal zabezpečovací systémy jako takové a zanalyzoval jejich vývoj v průběhu historie. Poté jsem osvětlil řízení přístupu a nastínil jeho nejznámější metody. Při porovnávání identifikačních metod byl kladen důraz na jejich silné a slabé stránky. Nejvíce populární metody RFID či NFC byly vysvětleny podrobněji, avšak čitelně pro všechny čtenáře.

Praktická část obsahuje náhled do struktury celkového řešení aplikace. Práce byla rozdělená na jednotlivé moduly z důvodů rozdělení odpovědností. Nejdůležitější je serverová aplikace, která má na starosti komunikaci s modulem, který čte RFID karty a ovládá příslušné dveře. Pro ni jsem zvolil REST API architekturu za účelem jednoduché komunikace přes HTTP protokol a možnosti naprogramovat obslužného klienta v jakémkoliv jazyce. HTTP protokol však běží nezabezpečeně, tudíž jsou zde potenciální problémy se zabezpečením. Ty však lze vyřešit pomocí AES šifrování. Hardwarový modul běží na mikrokontroleru ESP32, který umožnil komunikaci přes Wi-Fi. Využívá čtečku RFID karet RDM6300, která je díky své externí anténě vhodná k zabudování. Nakonec jsem ještě musel zvolit, jakou použiji databázi a jelikož nepředpokládám velké množství dat, vyřadil jsem NoSQL databáze a držel se osvědčené relační databáze. Ta běží v docker kontejneru pro lehkou přenositelnost, nicméně je velice jednoduché jí přenasadit na nějaký server či cloud.

POUŽITÁ LITERATURA

[1] VODA, Zbyšek. *Průvodce světem Arduina*. Vydání druhé. Bučovice: Martin Stříž, 2017. ISBN 978-80-87106-93-8.

[2] DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. [Brno: M. Drahanský], 2011. ISBN 978-80-254-8979-6.

[3] DOBKIN, Daniel Mark. *The RF in RFID: UHF RFID in practice*. 2nd ed. Oxford: Elsevier/Newnes, 2013. ISBN 978-0-12-394583-9.

Internetové zdroje

[4] SAFEWISE TEAM. *What Is a Security System and How Does it Work?* [online]. 15.10.2020 [cit. 15.3.2021]. Dostupný na WWW: https://www.safewise.com/home-security-faq/how-do-security-systems-work/

[5] TORREST, Katherine. *8 Benefits to Owning a Home Security System* [online]. 22.10.2020 [cit. 15.3.2021]. Dostupný na WWW: https://www.safewise.com/blog/top-8-reasons-get-home-security-system/

[6] SAFEWISE TEAM. *How Do Home Security Systems Protect Against Fire and Floods?* [online]. 09.09.2020 [cit. 15.3.2021]. Dostupný na WWW: https://www.safewise.com/home-security-faq/home-security-protects-fire-flood/

[7] SMITH, Steven. *The History of Security Systems* [online]. [cit. 29.3.2021]. Dostupný na WWW: https://www.hoyles.com/blog/history-security-systems/

[8] ABUS AUGUST BREMICKER SÖHNE KG a kol. *History of the Alarm System - Alarm systems - Break-in* [online]. [cit. 29.3.2021]. Dostupný na WWW: https://www.abus.com/eng/Guide/Break-in-protection/Alarm-systems/History-of-the-alarm-system

[9] LLOYD SECURITY INC. a kol. *The History of Security Systems in the United States* [online]. 05. 01. 2021 [cit. 29.3.2021]. Dostupný na WWW: https://www.lloydsecurity.com/history-security-systems/

[10] STANILAND, Lane a kol. *History and Timeline of the Home Security System* [online]. 27. 02. 2020 [cit. 29.3.2021]. Dostupný na WWW: https://www.boydsecurity.com/history-and-timeline-of-the-home-security-system/

[11] ALARM.ORG a kol. *The History of Home Security* [online]. 23. 08. 2019 [cit. 29.3.2021]. Dostupný na WWW: https://alarm.org/the-history-of-home-security/

[12] COX, Sarah a kol. *Society Hill Mirrors Pay Tribute To Philandering Forefather* [online]. 21. 03. 2013 [cit. 29.3.2021]. Dostupný na WWW: https://philly.curbed.com/2013/3/21/10261688/society-hill-mirrors-pay-tribute-to-philandering-forefather

[13] UNCHARTEDADAM a kol. *The busybody: Benjamin Franklin's greatest "invention"?* [online]. 02. 07. 2020 [cit. 29.3.2021]. Dostupný na WWW: https://unchartedlancaster.com/2020/07/02/the-busybody-benjamin-franklins-greatest-invention/

[14] SAFEWISE TEAM. *What Are Common Components of a Security System?* [online]. September 09, 2020 [cit. 13.4.2021]. Dostupný na WWW:

[15] ELLY, Suzanne. *Traditional vs modern: the better security systems* [online]. July 08, 2018 [cit. 13.4.2021]. Dostupný na WWW: https://www.asmag.com/showpost/25806.aspx https://www.safewise.com/home-security-faq/security-system-components/

[16] WELCOME GATE. *3 Predictions on how Security Will Change by 2021* [online]. [cit. 13.4.2021]. Dostupný na WWW: https://welcomegate.com/3-predictions-on-how-security-will-change-by-2021/

[17] WISENBAKER-SCHEEL, Courtni. *Security 2030: What the future holds for home protection* [online]. July 25, 2017 [cit. 13.4.2021]. Dostupný na WWW: https://www.ifsecglobal.com/global/security-2030-future-holds-home-protection/

[18] LUTKEVICH, Ben. *What is Access Control?* [online]. September, 2020 [cit. 16.4.2021]. Dostupný na WWW: https://searchsecurity.techtarget.com/definition/access-control

[19] TUNGGAL, Abi Tias. *What is Access Control? The essential cybersecurity practice* [online]. March 22, 2021 [cit. 16.4.2021]. Dostupný na WWW: https://www.upguard.com/blog/access-control

[20] ZHANG, Ellen. *What is Role-Based Access Control (RBAC)? Examples, Benefits, and More* [online]. December 1, 2020 [cit. 16.4.2021]. Dostupný na WWW: https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more

[21] BEILMAN, Bryon. *RBAC: Rule-Based vs. Role-Based Access Control* [online]. March 28, 2019 [cit. 16.4.2021]. Dostupný na WWW: https://blogs.iuvotech.com/rbac-rule-based-vs.-role-based-access-control

[22] CASEY, Keith. *What Is Attribute-Based Access Control (ABAC)?* [online]. September 29, 2020 [cit. 16.4.2021]. Dostupný na WWW: https://www.okta.com/blog/2020/09/attribute-based-access-control-abac/

[23] NEDAP N.V. *Access Control System; What is it? | Nedap Security Management* [online]. [cit. 16.4.2021]. Dostupný na WWW: https://www.nedapsecurity.com/insight/what-is-access-control/

[24] OPURUM, Paulynn. *Mechanical Door Locks vs. Electronic Door Locks* [online]. November 12, 2020 [cit. 20.4.2021]. Dostupný na WWW: https://fieldedge.com/blog/mechanical-vs-electronic-door-locks/

[25] AB&R. *What is RFID and How Does RFID Work?* [online]. [cit. 22.4.2021]. Dostupný na WWW: https://www.abr.com/what-is-rfid-how-does-rfid-work/

[26] AB&R. *Types of RFID Tags* [online]. [cit. 22.4.2021]. Dostupný na WWW: https://www.abr.com/passive-rfid-tags-vs-active-rfid-tags/

[27] KISI. *Comparing RFID and NFC Access Control Systems* [online]. [cit. 22.4.2021]. Dostupný na WWW: https://www.getkisi.com/guides/rfid-access-control

[28] NEDAP N.V.. *Near-field communication (NFC) for access control: the benefits & challenges* [online]. [cit. 22.4.2021]. Dostupný na WWW: https://www.nedapsecurity.com/insight/near-field-communication-nfc-for-access-control-the-benefits-challenges/

[29] VERKADA INC.. *What is RFID and NFC Access Control?* [online]. [cit. 22.4.2021]. Dostupný na WWW: https://info.verkada.com/door-access-systems/rfid-vs-nfc-access-control-guide/

[30] TRIGGS, Robert. *What is NFC and how does it work* [online]. June 30, 2019 [cit. 22.4.2021]. Dostupný na WWW: https://www.androidauthority.com/what-is-nfc-270730/

[31] NEDAP N.V.. *Is biometric security something to consider for your access control system?* [online]. [cit. 20.4.2021]. Dostupný na WWW: https://www.nedapsecurity.com/insight/biometric-security/

[32] NEDAP N.V.. *Which is the best biometric access control solution for you?* [online]. [cit. 20.4.2021]. Dostupný na WWW: https://www.nedapsecurity.com/insight/biometric-access-control/

[33] PINTO, Amiram. *Understanding the Types of Biometrics* [online]. November 12th, 2019 [cit. 20.4.2021]. Dostupný na WWW: https://www.nice.com/engage/blog/rta-understanding-the-types-of-biometrics-2513/

[34] CODECADEMY. *What is REST?* [online]. [cit. 20.8.2021]. Dostupný na WWW: https://www.codecademy.com/articles/what-is-rest

[35] JWT.IO. *Introduction to JSON Web Tokens* [online]. [cit. 20.8.2021]. Dostupný na WWW: https://jwt.io/introduction

[36] RED HAT, INC.. *What is Docker?* [online]. [cit. 20.8.2021]. Dostupný na WWW: https://opensource.com/resources/what-docker

PŘÍLOHY

Příloha A – Abstrakt systému