Návrh biometrického identifikačního systému pro malou organizaci

Project of biometrical identification system for small organization

Bc. Petr Kováč

Diplomová práce
2009

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2008/2009

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Petr KOVÁČ**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Návrh biometrického identifikačního systému pro malou organizaci**

Zásady pro vypracování:

1. **Seznamte se s problematikou identifikace na základě biometrickýh znaků. Popište jednotlivé metody identifikace a jejich technické parametry**
2. **Vyberte vhodnou metodu, která by byla cenově přijatelná pro malou organizaci při zachování vysoké přesnosti identifikace**
3. **Proveďte návrh identifikačního přístupového systému. Odděleně řešte tyto dvě oblasti**
   - **ochrana dat a informací; počítačové sítě**
   - **návrh autonomního systému a návrh systému pro malou až střední organizaci**
4. **U dostupných biometrických čteček proveďte měření přesnosti systémů. Pokud to bude možné pokuste se zhodnotit/odhadnout technické parametry reálného systému a jeho chování.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **JAIN, A.K., ROSS, A., PRABHAKAR, S. An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1):420, January 2004.**
2. **ŠEBESTA, V.: Systémy procesy, signály. Skriptum VUT Brno. 1995. 79. s. ISBN 80-214-0574-0.**
3. **Biometrická čtečka otisku prstů. VPassFX. User Configuration Guide. Dostupné ze stránek výrobce www.bioscrypt.com**
4. **Systém VISION3Di. Uživatelský manuál. HoneywellAceess. ADI Olympo.**
5. **Stránky věnované biometrických systémům. http://pagesperso-orange.fr/fingerchip/biometrics/biometrics.htm**
6. **Stránky International Biometric Group. http://www.ibgweb.com/**

Vedoucí diplomové práce: **Ing. Stanislav Goňa, Ph.D.**
Ústav elektrotechniky a měření

Datum zadání diplomové práce: **20. února 2009**

Termín odevzdání diplomové práce: **22. května 2009**

Ve Zlíně dne 20. února 2009

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce probírá základní teorii o biometrické identifikaci. Úkolem je vytvořit komplexní návrh biometrické aplikace pro malou organizaci; k identifikaci byl zvolen otisk prstu. Další problematikou, kterou se práce zabývá je hodnocení parametrů u dostupných biometrických zařízení.

Klíčová slova: Biometrická identifikace, otisk prstu, návrh biometrického identifikačního systému.

ABSTRACT

This thesis discusses the basic theory of biometric identification. The objective is to develop a comprehensive proposal for biometric applications for a small organization, was chosen to identify the fingerprint. Another question, which this thesis describes, is classification parameters of available readers.

Keywords: Biometrical identification, Fingerprint, Project of biometrical identification system.

Tímto si dovoluji poděkovat své rodině za morální a finanční podporu při studiu. Také bych rád vyjádřil své poděkování Ing. Stanislavu Goňovi Ph.D. za kvalitní a odborné vedení, připomínky a poskytnuté konzultace při zpracování mé diplomové práce. Dále bych chtěl poděkovat Vlastimilu Křížovi za poskytnutí odborné pomoci při fotografování zviditelněných latentních otisků prstů a jejich následné grafické zpracovávání. Také si dovoluji poděkovat Martinu Horákovi za odbornou pomoc s leptáním DPS.

Motto:

Všechno jde a všechno je možné. Je jen na nás, co jste ochotni obětovat!

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval.

V případě publikace výsledků budu uveden jako spoluautor.

Ve Zlíně …….

Podpis diplomanta

ÚVOD

Existuje mnoho způsobů jak identifikovat člověka, respektive prokázat jeho oprávněnost k přístupu do určitého prostoru. V dnešní době se využívá různých způsobů jako: kontrola průkazu totožnosti, ověření pomocí předmětu tj. karty, čipu, ověření pomocí informace uložené v paměti tj. PINu, a také ověření biometrických údajů.

Tato práce se zabývá naposledy zmíněnou problematikou a to biometrickou identifikací člověka. Biometrie, tedy z řeckých slov bio a metric, ve volném překladu měření živého, se využívá v různých oborech jako je medicína, oděvní průmysl, v bezpečnostním aplikacích; kriminalistice, a také v oblasti zabezpečovacích systémů, respektive přístupových a docházkových systémů. Diplomová práce je zaměřena do problematiky biometrických přístupových systémů.

Práce je rozdělena do dvou celků. V první části – teoretické je rozebrána teorie biometrie, jednotlivé identifikační metody, jejich srovnání a přesnost metod. V druhé části - praktické je realizován návrh biometrických aplikací pro malou organizaci. Za malou organizaci považujme obchodní společnost či jinou organizaci o počtu osob; zaměstnanců do 200. Návrh je realizován jak v oblasti ochrany dat, počítače, počítačové sítě pomocí biometrických údajů, tak i jako biometrický přístupový systém.

Cílem práce je ukázat možnosti biometrických aplikací v každodenním životě a vytvořit návrh s ohledem na poměr cena : výkon. Dále pak provést testy dostupných biometrických čteček, poukázat na slabé a silné stránky těchto systémů.

V práci je využito především čteček otisku prstu. Teorie je věnována především identifikaci otisku prstů v oblasti komerční, nikoliv kriminalisticko-forenzní. Otisky prstu byly zvoleny po konzultaci s vedoucím práce za metodu nejschůdnější v poměru cena : výkon.

Dle normy ČSN EN 50 133 spadají biometrické přístupové systémy do třídy identifikace 2.

I. TEORETICKÁ ČÁST

1 TEORIE O BIOMETRICKÉ IDENTIFIKACI

V poslední době vzrostly požadavky na bezpečnost, ochranu dat a na spolehlivou identifikaci osob, a je prakticky jisté, že tento trend bude i v budoucnu pokračovat. Tradiční identifikační technologie jako je kontrola dokladů totožnosti, klasické přístupové systémy založené na autentizaci předmětem nebo heslem, jsou již v dnešní době na hranici svých možností. Navíc, i když vzrostly požadavky na bezpečnost, tak dostatečně nevzrostla ochota a ukázněnost uživatelů podrobovat se různým prohlídkám, omezením, učit se nazpaměť nové hesla apod. A proto jedním z vhodných řešení tohoto dilematu je nasadit biometrické technologie k identifikaci osob. O této problematice se již delší dobu hovoří, ale teprve v posledních letech dochází k aplikaci do praxe. Za dnes nejvýznamnější biometrickou aplikaci můžeme považovat použití cestovních dokladů s biometrickými údaji, které jsou dnes vyžadovány ve většině vyspělých států, i Česká republika se zařadila mezi země aplikující do cestovních dokladů totožnosti biometrické údaje - a to obličej (od září 2006) a otisk prstu (od dubna 2009).

1.1 Definice pojmu biometrie a biometrická identifikace

Biometrie je obor činnosti, který zkoumá člověka a jiné živé organismy. Již název vycházející z řeckých slov *bio* (živý) a *metric* (měřit, určovat vzdálenostní vztahy). Vypovídá o tom, že jde o obor, který se zabývá popisem a měřením anatonomicko-fyziologických a hehaviorálních znaků, tj. znaků zkoumajících chování. Mezi běžně používané metody patří identifikace otisku prstu, dlaně, obličeje, duhovky oka, sítnice oka, méně pak identifikace hlasu, geometrie žilního řečiště, dynamika podpisu, stisku kláves aj.

Existuje mnoho definic biometrie identifikace, jednou z používaných je:

„Biometrie je užití měřitelného fyzického, fyziologického znaku nebo rysu chování člověka ke zjištění identity nebo ověření jiným způsobem zadané identity.“

1.2 Kde můžeme použít biometrickou identifikaci

Mezi dnes typické oblasti, ve kterých lze využít biometrické identifikace, patří:

- kriminalistika a jiné forenzní oblasti (identifikace podezřelých, pohřešovaných, obětí trestné činnosti, vězňů a jiných zájmových osob)

- cestovní doklady, národní ID karty, jiné ID karty jako: městské karty, věrnostní programy, ID karty správních úřadů (výdej sociálních dávek, zdravotní a sociální pojištění atd.)
- automatické celní odbavení a pasová kontrola
- přístupové a docházkové systémy ACS, přístup do vozidel
- ochrana dat, počítačů, počítačových sítí a jiných datových zdrojů
- identifikace osob v davu (monitorování pomocí kamerových systémů na shromážděních, demonstracích, sportovních utkáních apod.)
- ověřování totožnosti na dálku (bankomaty, platební karty, elektronické bankovnictví, platební operace v bance, internetový obchod apod.)

1.3 Biometrický identifikační systém

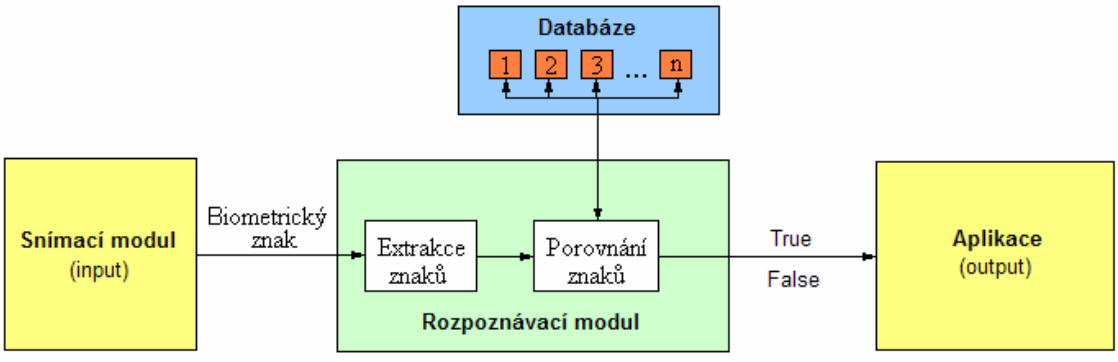
Biometrické identifikační systémy jsou aplikace biometrických technologií, které umožňují automatizovanou identifikaci nebo verifikaci osob.[5)] Tento systém se obvykle skládá z těchto částí: snímací, rozpoznávací, rozhodovací modul a databáze.

snímací modul – jde o modul, který se stará o sejmutí biometrického znaku dle použité metody a předává jej k dalšímu zpracování.

rozpoznávací modul – modul, který extrahuje znaky a porovnává je s databází.

aplikace – jde o výstupní část, komunikační prostředí nebo také zámek či jiné zařízení, které je biom. čtečkou ovládáno.

databáze – je uložiště biometrických šablon



Obr. 1. Blokové schéma biometrického identifikačního systému

1.4 Provozní stavy biometrických systémů

Biometrické identifikační systémy pracují v těchto módech:

1.4.1 Registrační mód (Enrollment)

Jde o provoz, ve kterém jsou zařazovány nové biometrické šablony do systému. Předložený biometrický znak je sejmut a je z něj extrahována porovnávací šablona, která je poté zkontrolována novým přiložením biometrického znaku. Při shodě je šablona uložena do systému. Šablona může být uložena do databáze systému nebo na externí paměťové zařízení.

- **Uložení šablony uvnitř identifikačního systému**

Šablona může být uložena uvnitř systému a to přímo v autonomním čtecím zařízení nebo v centrální databázi (např. PC); pokud se jedná o systém několika propojených neautonomních čtecích zařízení.

- **Uložení šablony na externím paměťovém médiu**

Této varianty se využívá především u verifikačních systémů. Biometrická šablona je uložena na externí paměťové médium (tokenu, čipová karta). Tato varianta nevyžaduje, aby systém měl databázi. Ale o to jednodušší je pak pokus o napadení systému padělám šablony.

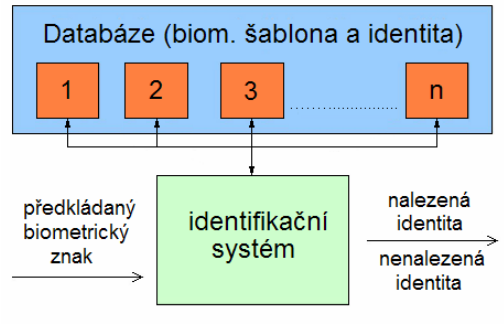
1.4.2 Provozní mód identifikace / verifikace (Identification / Verification)

Je mód vlastního přístupu do systému, kde dochází v procesu identifikace / verifikace k rozhodování o legitimnosti přístupu osoby do systému.

1.5 Identifikace, verifikace, autentizace

1.5.1 Identifikace

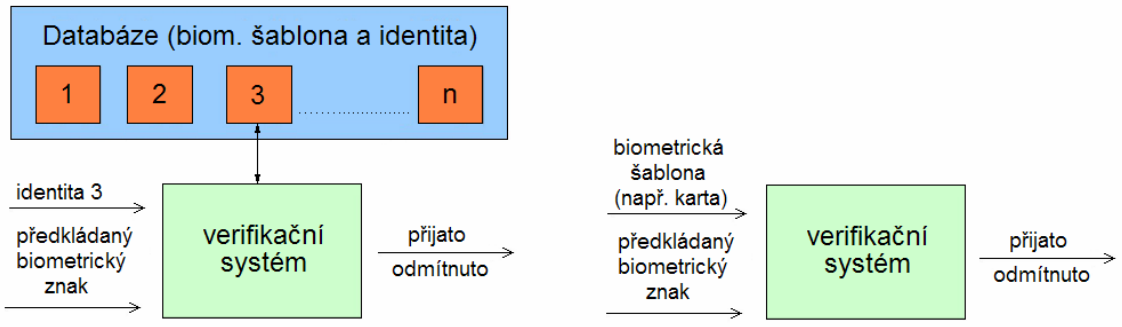
Je proces, při kterém systému předkládáme biometrický údaj a ten je porovnáván se všemi biometrickými šablonami uloženými v databázi, výsledkem porovnávání je nalezení identity či nenalezení identity. Jde o porovnávání 1: N.



Obr. 2. Schéma identifikace

1.5.2 Verifikace

Jde v podstatě o nižší stupeň identifikace, kdy porovnáváme jeden předložený biometrický údaj s jednou biometrickou šablonou uloženou v databázi systému nebo předloženou na paměťovém médiu. Výsledkem je přijato nebo odmítnuto. Jde o porovnávání 1:1.



Obr. 3. Možné podoby procesu verifikace

Pokud bude v dále v diplomové práci použit výraz identifikace, je tím myšlena i verifikace; pokud nebude uvedeno, že se jedná přímo o verifikaci.

1.6 Kritéria kladené na biometrické aplikace

Obecně lze říci, že kritéria můžeme rozdělit na ty, které jsou důležité v oblasti funkčnosti a spolehlivosti systému (tj. jedinečnost, univerzálnost, trvalost, dostupnost, přesnost a rychlost, odolnost), a ty, které jsou důležité z pohledu uživatele (tj. přijatelnost a

cena). Tyto kritéria musí splňovat jakákoliv biometrická metoda, která má uspět v oblasti identifikace osob.

- **Jedinečnost** – jedná se o vlastnost, která musí být výjimečná, a z bezpečnostního hlediska je nežádoucí, aby došlo ke shodě znaků u dvou osob. Proto je nutné vhodně zvolit metodu.
- **Univerzálnost** – musí jít o biometrické znaky, které lze měřit u co největšího počtu osob. Nemělo by se jednat o měření různých defektů a anomálií, či specifických znaků pouze pro určitá etnika.
- **Stálost** – u biometrické charakteristiky musí v průběhu stárnutí docházet k co nejmenším změnám.
- **Dostupnost** – někdy nazýváno měřitelnost. Jde o vlastnost, která udává jak složité je charakteristiku získat k měření.
- **Přesnost a rychlost** – patří mezi další důležité kritéria, udává s jakou rychlostí a přesností lze měřit a vyhodnocovat biom. charakteristiky, a tím udává pro jaké nasazení je metoda vhodná.
- **Odolnost** – parametr, který udává jaké úsilí je potřeba vynaložit k překonání systému.
- **Přijatelnost** – tato vlastnost zohledňuje míru přijetí technologie do každodenního života člověka. Člověk nesmí být nadmíru obtěžován technologií při snímání charakteristiky. Dále pak toto kritérium řeší nakolik je technologie vnímána člověkem. Určitě považujeme více přijatelné použití otisku prstu než metodu porovnávání DNA.
- **Cena** – jde o parametr, který odsouvá některé metody mimo oblast běžného každodenního použití.

Souhrn výše zmíněných kritérií udává pro jakou aplikaci a v jakém prostředí je daná metoda vhodná.

1.7 Přesnost biometrických systémů

Přesnost a výkonnost biometrických systémů hodnotí několik parametrů jako např.: pravděpodobnost chybného odmítnutí (FRR), pravděpodobnost chybného přijetí (FAR), koeficienty FMR a FNMR.

1.7.1 Falce Rejection Rate (FRR)

Chybné odmítnutí. Jde o chybu, která má za následek to, že uživatel, který má v systému zaregistrovanou biom. šablonu, je při pokusu o identifikaci odmítnut. Z bezpečnostního pohledu to není výrazná chyba, ale z pohledu uživatele ano. Pokud bude k chybě FRR docházet často, a uživatel bude opakovaně při pokusu o přístup odmítnut, tak se systémem nebude spokojen.

$$FRR = \frac{N_{FR}}{N_{EIA(EVA)}} \cdot 100 \ [\%] \quad [7]$$

N_{FR} – počet chybných odmítnutí

N_{EIA} – počet všech pokusů oprávněných osob o identifikaci

N_{EVA} – počet všech pokusů oprávněných osob o verifikaci

Někdy se můžeme setkat s označením **FNR – False NoMatch Rate** nebo **FNMR – False Non-Match Rate** (Falešné odmítnutí), jde o ekvivalent.

1.7.2 Falce Rejection Rate (FAR)

Neoprávněné přijetí. Jde o chybu, která má za následek to, že osoba, která v systému nemá zaregistrovanou biom. šablonu, je při pokusu o identifikaci přijata a je jí umožněn přístup do systému. Jedná se z bezpečnostního hlediska o fatální chybu.

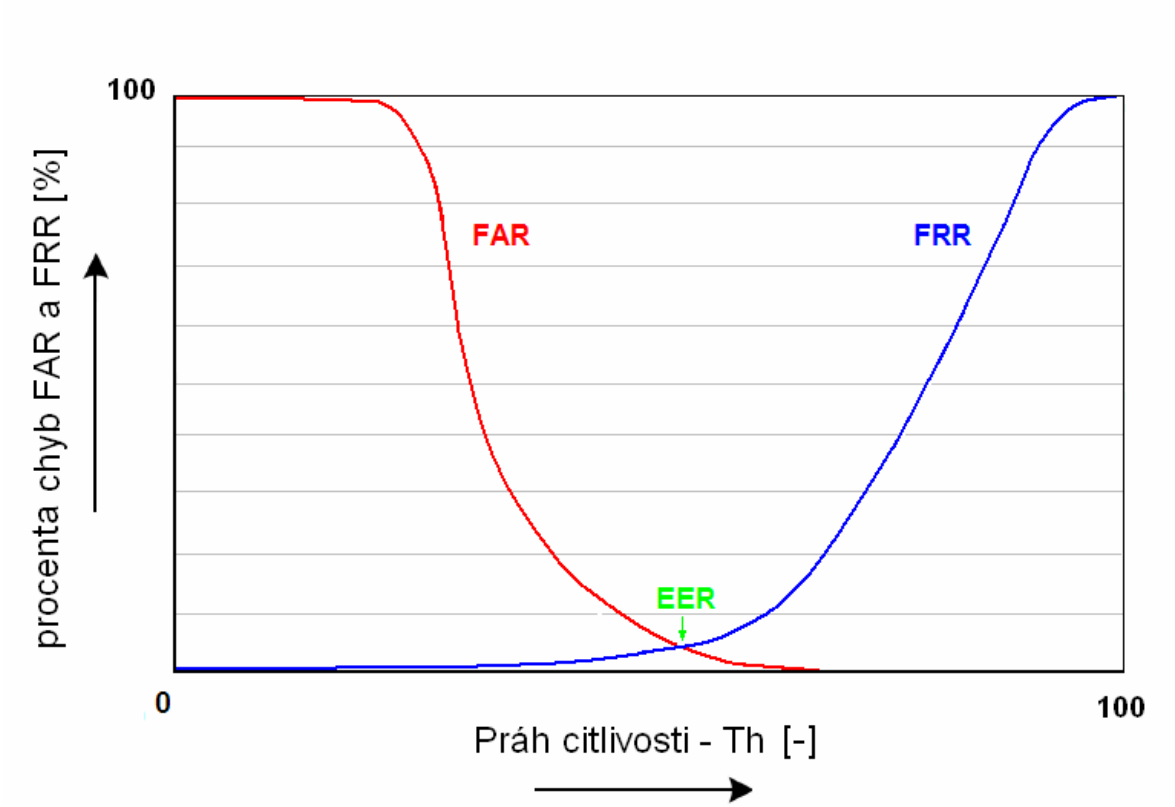
$$FAR = \frac{N_{FA}}{N_{IIA(IVA)}} \cdot 100 \ [\%] \quad [7]$$

N_{FA} – počet neoprávněných přijetí

N_{IIA} – počet všech pokusů neoprávněných osob o identifikaci

N_{IVA} – počet všech pokusů neoprávněných osob o verifikaci

Někdy se můžeme setkat s označením **FMR – False Match Rate** (Falešné porovnání), jde o ekvivalent.



Obr. 4. Vztah mezi FAR a FER

Jedinečnost, jako vlastnost, biometrických znaků je nepopiratelná, ale technologická zařízení, která vyhodnocují biometrické znaky, pracují s určitou přesností respektive nepřesností. V grafu na obrázku 4 je naznačen vztah mezi FAR a FRR. Práh citlivosti biometrické aplikace je potřeba vhodně nastavit s ohledem na použití biometrické aplikace. V bodě EER (Equal Error Rate) je vyrovnaný poměr chyb FAR a FRR. To znamená, že když nastavíme práh citlivosti do bodu EER, tak může nastat chybné přijetí se stejnou pravděpodobností jako chybné odmítnutí. Když se budeme snažit eliminovat chybu chybného přijetí, tak musíme nastavit vyšší práh citlivosti (na grafu doprava), ale to bude mít za následek zvětšení pravděpodobnosti výskytu chyby chybného odmítnutí. Pokud nám půjde o opačný případ a budeme chtít snížit chybné odmítání na co nejnižší úroveň, pak musíme snížit práh citlivosti (na grafu do leva), ale to bude mít za následek zvýšení pravděpodobnosti chybného přijetí. Graf použitý pro znázornění vztahů je pouze ilustrativní, pro každou biometrickou aplikaci je jiný.

Někteří výrobci biometrických aplikací umožňují nastavení prahu citlivosti (rozhodovací úrovně), některé aplikace si volí práh v určitém rozmezím v závislosti na kvalitě biometrického vzoru a některé aplikace jej mají pevně nastaven výrobcem.

1.8 Porovnání biometrických aplikací

Na základě výše zmíněných parametrů lze vytvořit porovnávací tabulku biometrických metod (tabulka 1.). Důraz je kladen na jedinečnost, univerzálnost, přesnost, rychlost, dostupnost, cenu, odolnost.

Tab. 1. Srovnání biometrických metod [3] [4]

Biometrie	jedinečnost	univerzálnost	stálost	dostupnost	přesnost	přijatelnost	odolnost	rychlost	Cena
DNA	H	H	H	L	H	L	H	L	H
Otisk prstu	H	H	H	M	M	M	M	H	L
Geometrie ruky	H	M	M	M	L	L	L	H	M
Duhovka	H	H	H	M	H	L	H	M	M
Sítnice	H	H	H	L	H	L	H	M	M
Obličej	M	H	M	H	M-H*	H	M	M	M-H*
Geometrie žil	H	H	H	M	M	M	H	H	M
Podpis	L	L	L	H	L	H	L	M	L
Stisk kláves	L	L	L	M	L	H	M	H	L
Hlas	L	M	L	M	L	H	L	M	L

Vysvětlivky k tabulce:

H - vysoká (High) zelená – považováno za kladné

M - střední (Medium) oranžová – považováno za neutrální

L - nízká (Low) červená – považováno na nepříznivé

* - ovlivněno aplikací, pro kterou je určeno a také je důležité přihlédnutí k použité technologii.

V porovnání vyšlo v poměru cena : výkonnost nejlépe u otisku prstu. Cena těchto systémů je příznivá, přesnost poměrně vysoká, ale nejde o neomylné systémy a mají i své slabé stránky. Objevily se pokusy prolomit tyto systémy. Navíc otisk prstu není příliš vhodný pro hromadnou identifikaci ve velkých databázích (řádově tisíce až desetitisíce vzorků). Čas identifikace v těchto systémech se výrazně prodlužuje.

Další zajímavou metodou identifikace je identifikace podle duhovky. Bezesporu jde o jednu z nejbezpečnějších metod, ale má i své záporné stránky. Čas identifikace je delší než u otisku prstu, jde o nevhodnou metodu pro hromadnou identifikaci. Cena těchto systémů je oproti otisku prstu vyšší, a také je tato metoda uživateli méně vyhledávána. Lidé nejsou rádi, když jim něco snímá oko. Jde o nedůvěru k čemukoliv, o čem si uživatel myslí, že by jim mohlo ohrozit smysly respektive smyslové orgány, zvláště pak jde-li o zrak. U scanu sítnice je tomu obdobně.

Bezesporu nejbezpečnější identifikací je rozbor DNA (deoxyribonukleové kyseliny), ale tato identifikace se využívá pouze v kriminalistiky-forenzní oblasti. Čas identifikace je dlouhý, řádově dny. I kdybychom vyhodnocovací techniku zdokonalili natolik, že by identifikace trvala řádově sekundy maximálně desítky sekund, i tak by se tato metoda nestala oblíbenou mezi uživateli. Nedůvěra plyne z možnosti zneužití vzorku i k jiným než identifikačním rozborům.

Mezi další zajímavou metodu patří identifikace podle struktury žilního řečiště. Jde v porovnání s ostatními identifikacemi o novější metodu. Je to dostatečně bezpečná metoda, čas identifikace je velmi příznivý, proto jde o metodu vhodnou i pro hromadnou identifikaci. Ale jelikož jde o novou metodu, zvláště pak na evropském trhu, je cena těchto systémů zatím řádově vyšší než u otisku prstů. Lze očekávat, že se cena s odstupem času srovná s ostatními identifikacemi, kterým je schopná konkurovat.

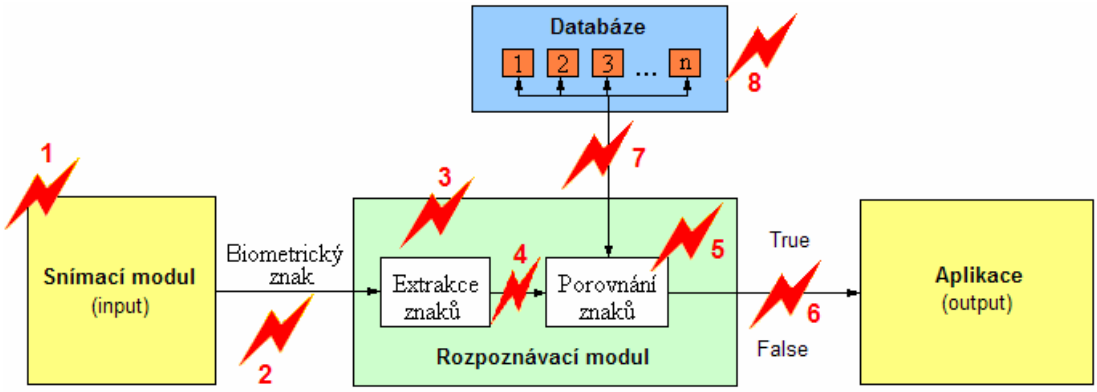
1.8.1 Výběr vhodné metody pro praktickou část

Pro praktickou část práce byly vybrány otisky prstů právě proto, že jde o nejrozšířenější a nejoblíbenější metodu mezi uživateli. Bezpečnost a cena je u této identifikace také příznivá. Na základě využití otisku prstu byl vytvořen návrh v poměru cena : výkon a byly na něm provedeny měření a detailnější prověření funkcí. Práce se dále zabývat pouze identifikací otisku prstu.

1.9 Možnosti jak překonat biometrické systémy a jejich odolnost

Stejně jako ostatní přístupové a bezpečnostní systémy, tak i biometrické, lze překonat. Je potřeba vynaložit určité úsilí a mít určité dovednosti a znalosti těchto systémů. Celý systém je tak silný a odolný vůči pokusu o prolomení, jako je odolné jeho nejslabší

místo. V následujícím obrázku č.5 je znázorněno několik slabých míst biometrických systémů.



Obr. 5. Schéma možných útoků na biometrický systém

1. Podvrh biometrického znaku

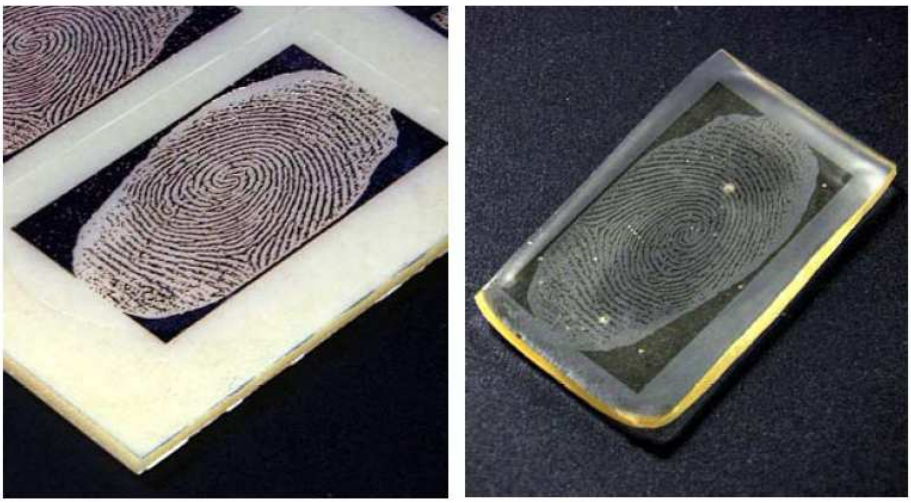
Můžeme říci, že je to jeden z nejčastějších útoků na systém. Lze říci, že se o něj může pokusit i osoba nemající podrobné znalosti systému. Existuje mnoho biometrických metod a u některých je podvrh biometrické znaku méně náročný než u jiných. Pro příklad můžeme uvést několik možných příkladů pokusu o padělání biometrického znaku: plastická operace obličeje a uší, chirurgický zákrok měnící otisky, odlévání falešného želatinového nebo silikonového otisku prstu. U nejstarších optických čteček otisku prstu se pokoušeli narušitelé padělat otisk i obyčejnou kopií prstu pořízenou v kopírce. Dokonce již ve světě nastaly i případy poškození uživatelů biometrických identifikačních systémů např. Majiteli vozidla, který měl v autě instalovanou biometrickou čtečku, byl amputován poslední článek prstu. Proto je nutné, v rámci zvyšování bezpečnosti, zdokonalovat tzv. kontrolu živosti (liveness-test).

Problematikou padělání biometrických znaků otisku prstu se zabýval výzkum profesora Tsutomu Matsumota z Yokohamské národní univerzity. Jeho tým dokázal za pomocí běžně dostupných možností, materiálů a technologií padělat otisk prstu až v 80% případů (u optických a kapacitních čteček). Je nutné zdůraznit, že tyto testy probíhaly v roce 2002 a od té doby pokročily i snímače i vyhodnocovací algoritmy. Proto se pokusím v praktické části této práce zhotovit umělý otisk prstu a otestovat dostupné biometrické čtečky.

Postup profesora Matsumota je až banálně jednoduchý. Do rozehřáté granulované plastické hmoty otiskli prst. Jakmile zhotovená forma vystydla, byla do ní nalita želatina, jakmile vystydla i želatina, byl falešný otisk hotov.[8] Je možné použít i silikon. Ale je důležité zdůraznit, že pro použití tohoto způsobu padělání musí některý z uživatelů systému s registrovanou šablonou spolupracovat.

Obr. 6. Postup zhotovení želatinového odlitku prstu [9]

Proto profesor Matsumota se svým týmem vyzkoušel i jiný způsobem padělat otisku prstu. Tentokráte se jednalo o sejmutí latentního otisku například ze skleničky. Latentní otisk vyfotografovali digitálním mikroskopem, upraven do kontrastní podoby a vytištěn na fólii, která byla přiložena na fotocitlivou PCB desku, vyvolá se a vyleptá. Následně byl vylit stejnou hmotou jako v předchozím případě.[8] Byly popsány i jiné obdobné případy. Latentní otisk lze zviditelnit pomocí kriminalistických metod, přiložit k němu měřítko a následně jej vyfotografovat další postup je obdobný jako u použití digitálního mikroskopu.



Obr. 7. Falešný otisk prstu zhotovený z latentního otisku [8]

2. Replika starých dat

Jde o napadení přenosové cesty mezi čtečkou a rozhodovacím modulem. Je zde předložen již někdy předkládaný znak, který útočník zaznamenal a v případě potřeby použil. Jako obrana proti tomuto způsobu je vhodné zabezpečit přenosové trasy. Tento způsob napadení vyžaduje velmi dobrou znalost daného systému.

3. Modifikace extraktoru znaků

Opět způsob, který vyžaduje velmi odbornou znalost systému. Obranou je zabezpečení všech komunikačních interface proti případnému nežádoucímu připojení.

4. Podvrh vektorové charakteristiky

Opět způsob, který vyžaduje velmi odbornou znalost systému. Obranou je opět zabezpečení všech komunikačních částí systému proti neoprávněné manipulaci.

5. Modifikace podsystému sloužícího k porovnávání

Také útok, který vyžaduje velmi odbornou znalost systému. Obrana je zabezpečení všech komunikačních cest systému. Dále pak oprávněný uživatel pro kontrolu může zkusit předložit biometrický vzor, který není registrován v systému, a pokud je přijat, tak to vypovídá o tom, že byl pozměněn algoritmus pro vyhodnocování, nebo práh citlivosti dané aplikace.

6. Změna výsledku porovnávání

Jde o útok, který vyžaduje odbornější znalosti a dovednosti než útok v bodě 1, ale nemusejí být na takové úrovni jako v 2-5. Toto napadení spočívá v útoku na komunikační kanál mezi biometrickým systémem a aplikací, kterou tento systém ovládá. Tato komunikace ve většině případů probíhá ve dvou logických stavech a to je True nebo False. Proto při nabourání komunikační sběrnice při znalosti základních parametrů systému není problém vytvořit falešný logický stav. Proto je nutné zabezpečit komunikační vedení a také se doporučuje ponechat vedení s co nejmenší vůlí. Aby při případném vytržení čtečky (u přístupového systému) došlo k odpojení kabelů od čtečky; případně jejich uvíznutí v montážních sloupcích či otvorech. To by pachateli zhoršilo přístup a orientaci.

7. Blokování komunikace s databází

Jde o formu útoku, která může probíhat u hlavně u databází šablon, které se nacházejí mimo čtecí zařízení. Jde o odpojení databáze a tím znemožnění získání šablony k porovnání se znakem.

8. Modifikace šablony v databázi

Jde o podobu útoku, která nevyžaduje odborné znalosti systému, postačí znalost uživatelská či administrátorská. Kdy, ať už vědomě či nevědomě, může dojít k modifikaci šablony nebo vytvoření nové šablony. Obranou je, aby administrátorský přístup do systému mělo co nejméně osob a zvolit vhodné režimové a technické opatření tak, aby se do systému nedostala nepovolaná osoba.

1.9.1 Jak tedy vhodně zabezpečit a navrhnout biometrický přístupový systém

Jde o souhrn určitých vhodných opatření, které mohou vést k zmírnění hrozeb pro biometrický systém.

1. **Zabezpečit komunikační trasy**

Je vhodné uložit datové i jiné kabely tak, aby se k nim nedalo dostat z vnější části objektu. Popřípadě uložit kabely v kabelových trasách opatřených kontakty, které se připojí do EZS a v případě narušení kabelové trasy vyvolají poplach.

2. **Použít vhodné montážní sloupky a obaly**

Výrobci nabízejí většinou velké množství příslušenství různého vzhledu a odolnosti tak, aby si zákazník mohl vybrat to ,co se mu vzhledově líbí. Ale je také potřeba myslet na bezpečnost a vyhledat výrobky v antivandal provedení.

3. **Vhodné umístění čtečky**

Čtečku je vhodné umístit tak, aby byla pokud možno v zorném poli kamerového systému (CCTV) nebo pokryta detektorem EZS. Dále pak je nutné umístit čtečku tak, aby trčela ze zdi nebo příčky pouze čtecí část a nebylo možné se např. zespod připojit ke komunikačnímu prostředí např. USB nebo COM aj. Toto bývá také slabinou některých čteček. Stává se, že čtečky jsou primárně určeny pro vnitřní použití a mají jednoduchý přístup ke komunikačnímu prostředí. Tyto čtečky bývají často použity i pro vnější použití bez vhodného ochranného krytu. Pak je k nim usnadněn přístup a plyne z toho možné riziko pro systém.

4. **Vybrat vhodnou metodu identifikace**

Pro příklad je možné uvést několik nadlehčených modelových situací. Když půjde o společnost, která se bude zabývat např. výrobou spojovacího materiálu, pak bude asi zbytečné použít biometrickou identifikaci duhovky, ale postačí nám identifikace geometrie ruky popřípadě otisku prstu. Pokud půjde o společnost zabývající se strategickým výzkumem, návrhem výpočetní techniky, hardwaru či softwaru a podobných aplikací, pak by metoda identifikace geometrie ruky nebyla příliš vhodná. V závislosti na velikosti databáze uživatelů by bylo vhodné zvolit např. otisk prstu, geometrii duhovky, geometrii žilního řečiště, 3D identifikaci obličeje, případně u high-security objektů je možné sáhnout po tzv. multiple-biomery (použití více biometrických vlastností k identifikaci). U nás tato možnost zatím není moc známa, ale je to jedna z možností.

5. **Aplikovat vhodná režimová opatření**

Je nutné vhodně proškolit uživatele a seznámit je s vhodným uživatelským přístupem. Dále pak omezit počet administrátorů spravujících systém. Čím více administrátorů, tím větší možnost úmyslného nebo neúmyslného poškození šablony nebo přidání nevyžádané šablony.

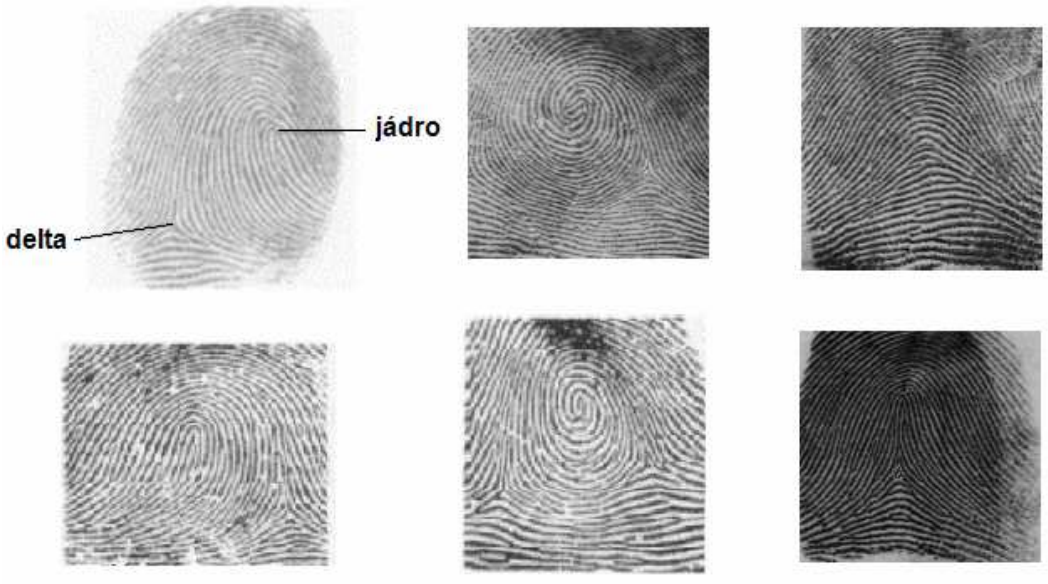
2 IDENTIFIKACE OTISKU PRSTU

Otisk prstu patří mezi nejznámější biometrické identifikační metody. Lze říci, že je nejvíce využíván jak v kriminalisticko-forenzní, tak i komerční oblasti. Původ je v kriminalistickém zkoumání otisků prstů – daktyloskopii. Jde o poměrně prověřenou metodu časem, začátek rozšiřování v komerční oblasti se datuje okolo roku 1980. Jde o identifikaci papilárních linií bříšek prstů, respektive jejich přerušení nebo ukončení tzv. markantů. Rozeznáváme tří základní klasifikační vzory (smyčka, vír, oblouk).

1 Smyčka – papilární linie zde tvoří smyčku a také mezi středem centrální oblasti a deltou se musí nacházet alespoň jedna linie. Smyčka se nachází přibližně na 65% všech otisků prstů.

2 Vír – papilární linie zde tvoří kruh, ovál, spirálu s jádrem. Vír tvoří přibližně 25% všech otisků prstů.

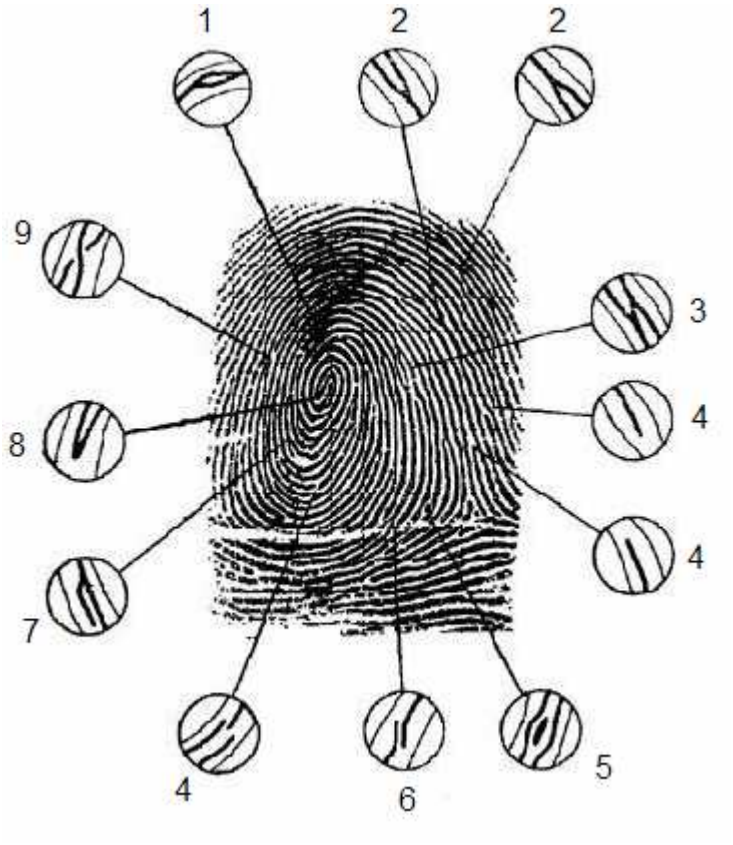
3 Oblouk – papilární linie zde tvoří jednoduché oblouky. Je nejméně častým jevem na otisku přibližně v 5-10%.



Obr. 8. Základní vzory (z leva smyčka, vír, oblouk)

Kromě základních tvarů, rozlišujeme jednotlivé přerušení nebo ukončení papilárních linií, které jsou nazývány markanty. Můžou mít následující podobu:

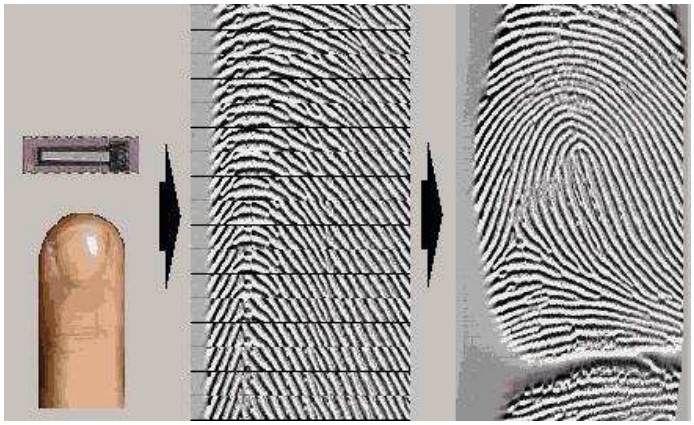
začínající/končící linie, bod, oko, hák, most, křížení, vidlice, přerušená linie, boční přerušení, ukončení aj.; tyto lze považovat za nejčastější (obr. 8).



Obr. 9. Příklady markant (1 oko, 2 vidlice, 3 most, 4 začínající/končící linie, 5 bod, 6 boční přerušení, 7 hák, 8 ukončení, 9 křížení)

2.1 Snímače otisku prstu

Existuje několik typů snímačů otisku prstů, každá technologie je založená na trochu jiném principu a má své výhody i nevýhody. V této kapitole jsou rozebrány ty nejčastěji používané. Existují v principu dva postupy jak sejmout otisk první je **staticky** (kontaktně nebo bezkontaktně) nebo tzv. **šablonováním** (obr. 10) tj. přetažením prstu přes senzor. Obraz je sejmut v určitých segmentech, které jsou poté spojeny v jeden otisk pomocí příslušného algoritmu.



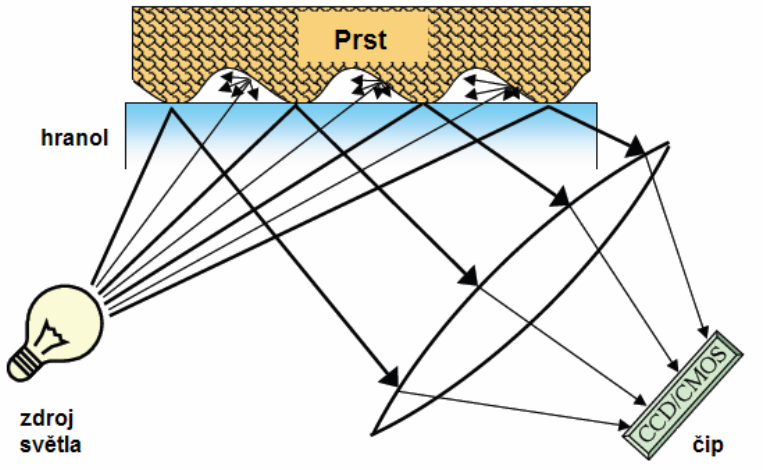
Obr. 10. Sejmutí otisku prstu šablonováním [13]

2.1.1 Optické snímače otisku prstu

Optické snímače otisku prstu jsou založeny na několika technologiích. Mezi nejvíce používané patří snímání na základě odrazu a nebo prostupu světla.

- **Optické snímače založené na principu reflekce**

Princip tohoto snímače je založen na odlišném odrazu respektive rozptylu světla. Tento optický snímač je složen ze třech hlavních částí a to: zdroji světla, hranolu a snímacího CCD/CMOS čipu. Snímání otisku se děje tak, že zdroj světla pod úhlem nasvítí hranol po přiložení prstu (od papilár se světlo odráží jinak než z prostoru mezi papilárama), a CCD nebo CMOS čip sejme obraz z hranice mezi končícím hranolem a začínajícím otiskem prstu (Obr. 11). Obraz je pak dále digitalizován.

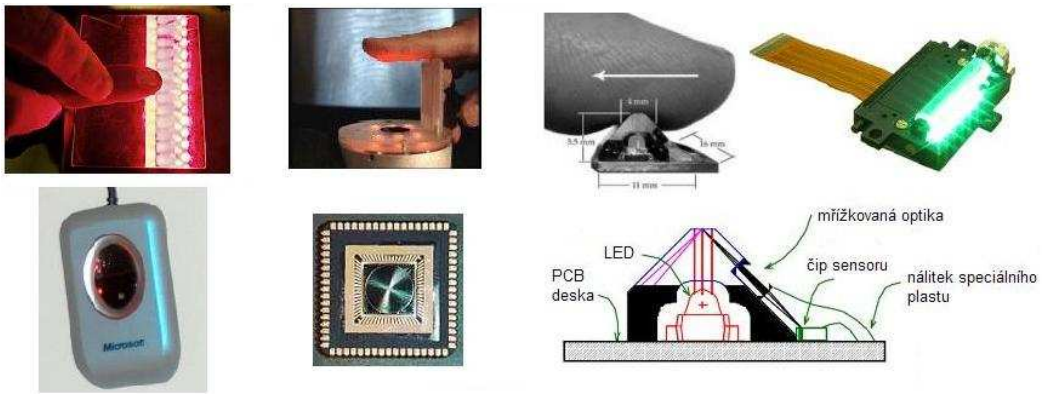


Obr. 11. Princi optického snímače na principu reflekce

Výhody - Dnes se jedná o senzory z nejvyšším rozlišením. Odolnost vůči statickým výbojům. Dále pak odolnost vůči okolním vlivům jako je teplota a vlhkost.

Nevýhody – Nečistoty nebo poranění na prstu způsobují zachycení méně kvalitních otisků (nehodí se pro manuálně pracující osoby). Další nevýhodou je, že snímání může být ovlivněno otiskem předcházejícího uživatele např. v případě více mastného otisku. Další nevýhodou je velikost snímače, takřka vylučuje použití v mobilních zařízeních jako PDA, mobilní telefon, notebook apod. Výjimkou je pouze čtečka, která snímá otisk šablonováním.

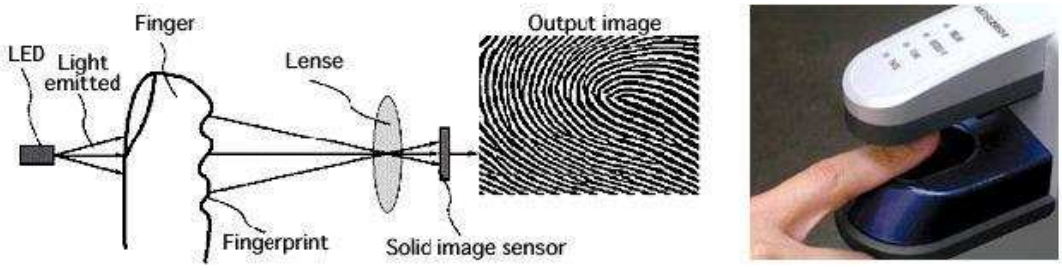
Optické senzory založené na principu reflekce mohou snímat otisk prstu staticky jak (kontaktně nebo bezkontaktně nebo šablonováním.



Obr. 12. Optická čtečka (z leva statická kontaktní, bezkontaktní, šablonovací) [10]

- **Optické snímače založené na principu transmise (světla přeneseného prstem)**

Princip tohoto optického snímače vychází z prosvícení prstu z horní části (od nehtu) a sejmutí obrazu senzorem na opačné straně. Výrobou těchto senzorů se zabývá především firma Mitsubishi.

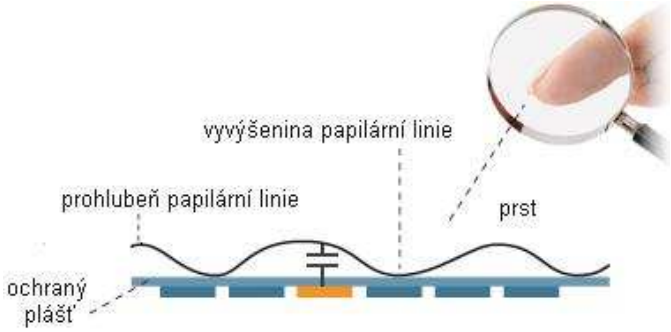


Obr. 13. Optický senzor založený na transmisním snímání [10]

2.1.2 Kapacitní snímače otisku prstu

Princip tohoto snímače vychází z měření rozdílů kapacit mezi deskou snímače a prstem (vrcholy papilár a prohlubněmi). Snímače představuje jednu desku kapacitoru a druhou představují jednotlivé části prstu. Snímací plocha je osazena velkým množstvím snímacích mikroelektrod, které vyhodnocují rozdíl kapacity mezi vrcholem papiláry a prohlubní. Obraz papilár je pořizován rovnou v digitalizované podobě.

Kapacitní snímače jsou jedny z nejpočetněji osazovaných v přístupových systémech. Velmi často tyto snímače najdeme v podobě sweep capacitive (šablonovacích kapacitních) ve výpočetní technice. Můžeme říci, že jde asi o nejrozšířenější typ senzoru používaný v noteboocích, flashdiscích a čtečkách pro přístup do PC.



Obr. 14. Princip kapacitní čtečky [10]

Výhody – Kapacitní snímače jsou poměrně levné na výrobu, jednoduchý princip funkce a malé rozměry.

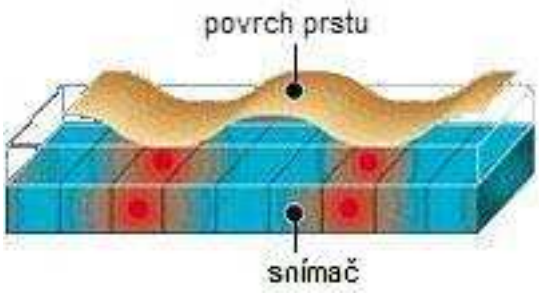
Nevýhody – Životnost snímačů je poměrně malá (často dochází k zničení statickou elektřinou). Problémy s funkčností ve vlhkém prostředí. I když snímač není zničen statickou elektřinou, tak je ho podle intenzity provozu nutné za 2-5 let vyměnit. Dále pak kapacitní čtečka špatně reaguje na prsty od cukru a solí. Stejně tak může špatně reagovat na mastnotu (krémy na ruce apod.). To podstatně mění vodivost lidské kůže.

2.1.3 Termické snímače otisku prstu

Termické snímače se ujaly nejvíce v komerčních aplikacích a nejvíce ve výpočetní a komunikační technice. Jde o nejmenší snímač otisku prstu. Proto je osazován nejčastěji do PDA, mobilních telefonů, PC periferie (např. v PC myši) apod. Literatura obecně uvádí, že jde o méně přesný typ snímače v porovnání s ostatními a je vhodné jej nasazovat

v aplikacích s menším požadavkem na bezpečnost. Avšak firma Atmel u termického snímače uvádí FAR 0,00001, což považuji za velmi přesný snímač otisku prstů, který lze řadit mezi ty nejbezpečnější.

Termické snímače otisku prstu používají jako teplocitlivý prvek malý pyrodetektor (obdobný jako u infrakamery). Princip technologie spočívá v měření rozdílu teplot mezi vrcholem papiláry a prohlubní papiláry. Rozdíl těchto teplot je takřka zanedbatelný. A jak to, že tato technologie funguje? Ve skutečnosti je prstem přejeto po teplocitlivém prvku. Vrcholy papilár jsou v kontaktu se snímací plochou, tím ji ohřejí a je sejmuta teplotní změna (změna teploty je poměrně velká, ale má krátké trvání; méně jak desetina sekundy). Zato prohlubně papilár se teplocitlivé plochy nedotknou a takřka ji neovlivní. Otisk se snímá nejčastěji šablonováním (viz. obr. 10.) takže je získán v podobě pásků, které jsou pak dle příslušného algoritmu složeny v jednotný otisk.



Obr. 15. Princip termálního snímače [10]

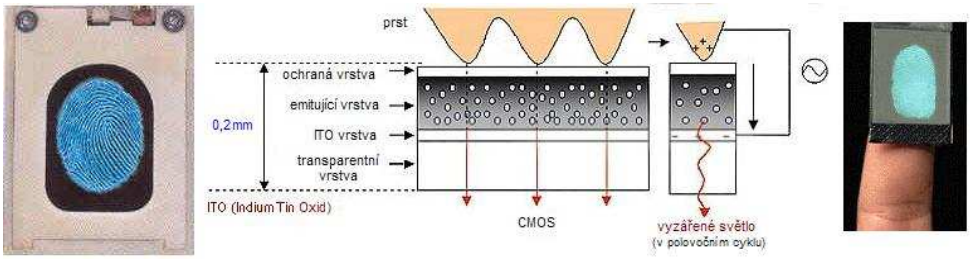
Výhody: Jde o jeden z nejlevnějších snímačů. Velmi malých rozměrů (0,4 x 14mm). Vhodný pro menší databáze otisků, popřípadě výpočetní techniku. Senzor je odolnější při styku s vodou a vzdušnou vlhkostí, pracuje přesněji než kapacitní. Je odolnější vůči otřesům a otěru. Dokáže pracovat v širokém rozsahu teplot (běžně se uvádí -40°C až 85°C).

Nevýhody: Je potřeba najít optimální postup snímání otisku tak, aby při opakovaných snímáních nebyli načítány jiné charakteristiky.

Obr. 16. Příklady termických senzorů

2.1.4 Elektrooptické snímače otisku prstu

Jde opět o jednu z novějších technologií pořizování obrazu otisku prstů. Snímač je složen z vrstveného polymeru. Princip metody vyhází z toho, že přiložením otisku prstu vrcholy papilárních linií stlačí světlo emitující vrstvou, která vyzáří světelnou energii. Toto světlo následně projde transparentní vrstvou a je sejmuto světlo citlivou vrstvou, která je složena z matice fotodiod nebo CMOS snímač (Obr. 17.)



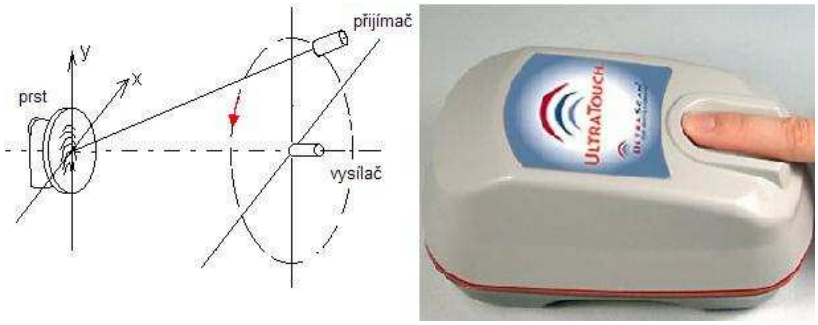
Obr. 17. Princip optoelektronické metody [10]

Výhody – Dobrá cena a rozlišení senzoru. Jde o poměrně malý snímač. Výhodou je, že pořizuje stejně kvalitní obraz i při suchém prstu.

Nevýhody – Malá odolnost vůči mechanickému poškození, to je dáno z fyzikálního principu. Dále pak menší odolnost vůči vodě a prachu.

2.1.5 Ultrazvukové snímače otisku prstu

Princip ultrazvukového snímání je takový, že se vysílá zvukový signál z pevného bodu (vysílače) na otisk prstu. Jsou snímány odražené a deformované vlny pomocí buď rotujícího přijímače okolo vysilače nebo sítí stacionárních přejímačů umístěných okolo vysilače. Měření rozeznává vzdálenější a přilehlejší linie, obraz je tedy trojrozměrný s vysokou přesností. Čtení otisku je realizováno z vrstvy pokožky jménem škára.



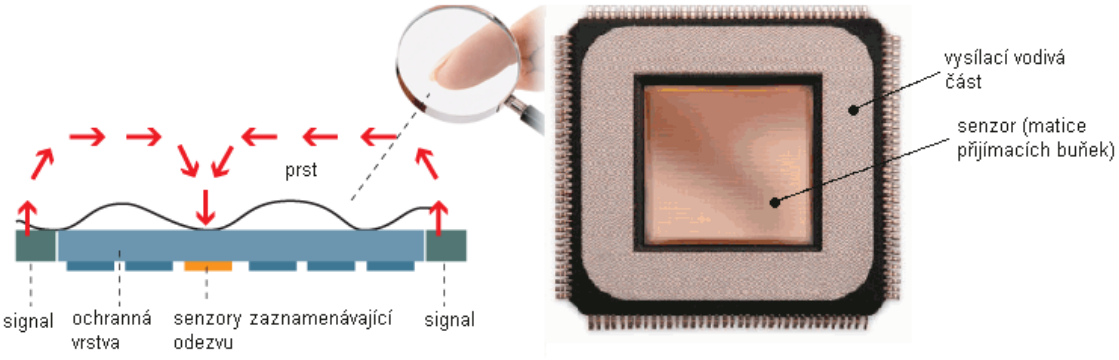
Obr. 18. Princip ultrazvukového snímače (vlevo) a příklad čtečky (vpravo)

Výhoda – Odolnost vůči vlhkosti a nečistotám, drobným oděrkám. Ultrazvukový senzor je odolný vůči podvrhům prstu, např. odlitkům prstu apod. Je možné tímto senzorem získat i otisk z mrtvého těla do určité fáze rozkladu.

Nevýhody – Mezi hlavní nevýhody patří vyšší cena a velikost snímače.

2.1.6 Radiofrekvenční snímače otisku prstu (RF Field; E Field)

Tato metoda byla vyvinuta v roce 1998, u této metody nedošlo k masivnímu rozšíření, jedná se spíše o ojedinělá řešení, která se uplatňují ve výpočetní technice. Princip této metody snímání otisku prstu spočívá v připojení generátoru střídavého signálu na dvě rovnoběžné desky. Jednou deskou je plocha snímače, tou druhou je pak otisk prstu. Jelikož otisk prstu není rovná plocha, změní se tvar elektrického pole podle výběžků a rýh na prstu. Vrcholy papilár mají větší signál a prohlubně nižší, tím vrcholy vytvoří obraz otisku. Vlnová délka je mnohem větší jako délka desek, tím je tvořeno pouze elektrické pole - bez magnetického. Signál se šíří pod povrchem pokožky. O rozšíření signálu z generátoru se stará vodivý rámeček okolo senzoru.



Obr. 19. Vlevo princip RF technologie, vpravo RF senzor [10]

Výhody – Funkci neovlivňuje nečistota, ani moc či málo mastná pokožka. Nevadí ani drobné oděrky prstu.

Nevýhody – Čas snímání otisku oproti jiným čtečkám trochu delší (cca o 1-2 s). Po přiložení prstu se vybudí pole a pak je obraz i vícekrát sejmut (dokud nedosáhne požadované kvality).

2.1.7 Tlakové snímače otisku prstu

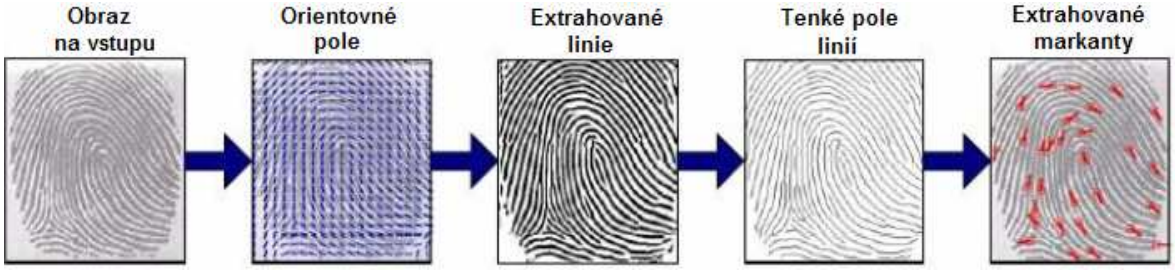
Myšlenka tlakové technologie byla jedna z nejstarších, tlačit prst vůči podložce a získat otisk. Ale piezoelektrické materiály se až v poslední době dostaly na takovou úroveň, aby mohly být použity pro identifikaci otisku prstu. Princip metody je takový, že snímač se skládá ze tří vrstev a to vodivé, nevodivé (v podobě gelu) a vodivé. Při přiložení otisku na snímač dojde ke stlačení první vodivé vrstvy v místech vrcholů papilárních linií, která projde nevodivým gelem a dotkne se spodní vodivé.

2.2 Zpracovávání a porovnávání otisku prstu

2.2.1 Snímání otisku

Pro systémy automatizovaného vyhodnocování otisku prstu se využívá pouze dvou markant a to rozbočení (vidlice) na Obr.9. reprezentované číslem 2 a začínající/končící linie reprezentované na stejném obrázku číslem 4. Vyhodnocování ostatních markantů by bylo složité, způsobovalo by inf. šum. Porovnávání by nebylo tak výkonné jako u těchto dvou markantů. Všech typů markantů se pak využívá až při ruční kriminalistické expertíze.

Obraz je po sejmutí převeden do **matice ve stupních šedi** velikosti NxN, kde je každé buňce matice přiřazen parametr intenzity pixelu. Poté je předen na **orientované pole** matice NxN a je vyjádřen směr linie v pixelu. Třetím krokem je **vytvoření mapy linií** tj. binární obrazu NxN, kde jsou rozlišeny pixely patřící linii a nepatřící linii. Každé buňce matice je přidán parametr, když má hodnotu 1 pak pixel patří linii, pokud 0 tak je to pixel neležící na linii a poté je vytvořená tenká mapa linií. Předposledním krokem je pak **detekce markant**, která je poměrně jednoduchá. V podstatě lze říci pokud má pixel linie sousedící min. 3 pixely linie jde o rozbočení (vidlici), pokud má pixel linie jednoho souseda netvořícího linii je detekováno ukončení. Poté nastává **postprocessing** což je děj, který pomocí heuristických metod vybere jen určitý počet znaků. Např. neuvažuje znaky, které mohly vzniknout nekvalitním sejmutím obrazu např. dvě ukončení orientované proti sobě (předpoklad toho, že otisk nebyl pořádně přiložen a nedošlo k prokreslení linie) nebo nedetekuje shluk většího množství markant v jednom místě (vznik šumu).



Obr. 20. znázornění algoritmu pro zpracování otisku

2.2.2 Porovnávání otisků (matching)

Skládá se ze třech celků a to: určení skóre, porovnání s mezí, a rozhodnutí.

Určení skóre jde o to, že jsou porovnány předložený znak a šablony a je jim přiřazeno skóre porovnávání (stupeň shodnosti porovnávaných vzorků). Nikdy nedosáhneme 100% shody dvou otisků, skóre se tomu může pouze blížit. Nejčastěji využíváme rozsahu 0-100. Ale není to pravidlem, a záleží na tom, jak je systém postaven.

Při procesu verifikace je pak porovnáno skóre s mezí, a je rozhodnuto. V případě identifikace, se vybere z databáze ten otisk jehož skóre bylo nejvyšší. A toto skóre je porovnáno s mezí a je rozhodnuto o schodě nebo neshodě.

Mez je parametr, který je určen administrátorem systému v závislosti na požadované přesnosti; bezpečnosti.

Porovnání pak je výsledkem srovnání nastavené meze se skórem. Pokud je skóre lepší než stanovená mez, je otisk označen jako matched, neboli shodný. Pokud je skóre nižší jako stanovená mez, pak je výsledkem nevyhovující otisk (neshoda).

II. PRAKTICKÁ ČÁST

3 NÁVRH BIOMETRICKÉHO IDNTIFIKAČNÍHO SYSTÉMU

Úvodem této kapitoly je představení použitých prvků pro návrh biometrické aplikace. V kapitole 3.1 jsou rozebrány prvky ochrany výpočetní techniky, poč. sítě a ochrany dat. V kapitole 3.2 jsou rozebrány prvky přístupových systémů. Samotné návrhy jsou realizovány v kapitolách 2.3 až 3.5. Varianty návrhu jsou odstupňovány vzhledem k funkčnosti, pohodlnosti, a komplexnosti řešení. Návrh u biometrického přístupového systému ACS je realizován pouze po výstupní relé, které je určeno k ovládání běžných elektromotorických, elektromechanických nebo elektromagnetických zámků, popřípadě jiných zábranných systémů. Zámky a zábranné systémy již nejsou v tomto návrhu uvažovány hlavně z toho důvodu, protože záleží na možnostech a prostoru v jednotlivých objektech, kde by tento systém mohl být realizován.

3.1 Vybrané prvky pro ochranu výpočetní techniky biometrickými prostředky

Obecně lze realizovat ochranu dat biometrickými prvky těmito třemi způsoby, a to: Ochranou přístupu do pc myšleno na bázi autonomního systému. Dále pak vyšší formou kdy je chráněna počítačová síť, respektive přístup k ní za pomoci biom. údajů. A třetí variantou je chránit data na paměťových médiích opatřených biom. prvky.

3.1.1 Prvky pro ochranu autonomního PC biometrickými prvky

Existuje celá škála produktů pro ochranu přístupu do PC biom. prvky. Nejčastěji se můžeme setkat s kapacitními šablonovacími čtečkami v různých podobách. Méně pak s optickými; těch se využívalo dříve. A ostatní typy senzorů se využívají spíše ojediněle. Je tomu z důvodu, že šablonovací kapacitní čtečka nejvíce vyhovuje dnešní výpočetní technice v poměru cena:výkon:velikost. Uvádí se, že cena tohoto snímače je cca 3$. Toto je přibližná cena, za kterou ji výrobci těchto čipů prodávají výrobcům výpočetní techniky a PC periferie. To je velmi příznivá cena, která výrazně nezmění náklady na výrobu notebooku, PC či jiných periferií. Dále pak nejčastějším údajem výrobců těchto čipů je, že přesnost, respektive chyba neoprávněného přijetí FAR je menší než 0.001% a chybného odmítnutí FRR je menší než 1%. Což už jsou v oblasti bezpečnosti poměrně solidní parametry. Třetím kladem těchto senzorů je jejich velikost, kdy velikost snímací plochy je

cca 2,5 x 11mm a velikost vyhodnocovací elektroniky cca 10 x 25 mm. To umožňuje tento senzor zabudovat takřka kamkoliv. S čtečkami otisku prstů se setkáme dnes v noteboocích pravidelně, nejčastěji se jedná právě o kapacitní šablonovací senzory. Ale u desktopových počítačů už snímače otisku prstu nejsou řešeny, proto pokud chceme realizovat ochranu PC biom. údaji musíme sáhnout po externí čtečce. U desktopových PC už se tolik nedbá na velikost snímače, proto se můžeme setkat s více typy senzorů zabudovaných v samostatné čtečce nebo jiné PC periferii jako je např. myš nebo klávesnice. V následujících dvou podkapitolách budou rozebrány dvě čtečky, které jsem zvolil pro praktický návrh.

3.1.1.1 APC Touch Biometric Pod Password Manager, EMEA

Tato čtečka je určená k ochraně PC využívá senzor typu RF Field. Proč je tento senzor vybrán pro praktickou část této práce, když byly v předcházejícím odstavci popsány a vyzvednuty kvality kapacitního šablonovacího snímače otisku prstu pro výpočetní techniku? Protože jsem se rozhodl prakticky srovnat údaje o přesnosti a uživatelské příjemnosti právě mezi technologií RF field a kapacitním šablonovacím snímačem. Této problematice se bude věnovat kapitola 5. (Měření na realizovaných biometrických systémech). Teoretické chyby FAR a FRR jsou uváděny podobně jako u kapacitních snímačů. Praktické zkušenosti budou rozebrány právě v kapitole 5. Uživatelský software disponuje obdobnými funkcemi jako ostatní softwary pro zprávu přístupu k PC za pomoci biom. údajů. Dále pak umožňuje šifrování souborů a složek. Jako u většiny těchto čteček i tato využívá šifrování zvoleným uživatelským heslem. Otisk prstu je opět jen prostředníkem pro uživatelské pohodlí a také pro zvýšení bezpečnosti tím, že nám nikdo „přes rameno“ neodečte naše heslo. Využívá software s názvem OmniPass. Databáze otisků se ukládá do PC nikoliv do čtečky.

Dále pak je nutné mít na paměti, že tyto prvky řeší pouze přístup do PC. Neřeší automatické zašifrování určitých složek jako např. dokumenty nebo plocha či jiné systémové složky. Byl by to problém a šlo by o zásah do integrity systému a navíc by šlo o digitálně nepodepsanou operaci pro MS. Někdy je možné se setkat s tím, že přístupový software vytvoří složku na HDD mimo systémové složky, která je šifrována a je dešifrována až po identifikaci. Potom je nutné data, které chceme chránit, přesunout do této složky. Tato čtečka, respektive software OmniPass nevytváří takovou složku, proto data, které chceme chránit, musíme ručně šifrovat.

Kromě přístupu do PC musíme mít na paměti i jeho ochranu před odcizením, vhodnou realizací režimových a technických opatření. Protože, jak bylo zmíněno výše, zmíněná ochrana řeší pouze přístup do PC (přihlášení). Když by byl PC (respektive pevný disk) odcizen, je možné HDD zapojit do jiného PC, a poté je přístup k nešifrovaným datům velmi jednoduchý.

Tab. 2. Parametry čtečky APC Biopod

Parametr	**Hodnota**
Velikost databáze otisků	20 otisků
Rychlost verifikace	<2s
Typ senzoru	RF field
Rozměr snímacího čipu	7 x 7 mm
Podporované operační systémy	pouze platforma MS Windows a to 98, ME, 2000, XP
Software využívaný k identifikaci	OmniPass
Hmotnost čtečky	110g
Komunikační rozhraní	USB 2.0/1.1
Rozměry čtečky	51 x 25 x 13 mm

Obr. 21. APC biopod

3.1.1.2 Identix BioTouch USB

Další z vybraných čteček je Identix BioTouch USB (technologie firmy Motorola). Jde o optickou čtečku s CMOS snímačem. Tento snímač byl vybrán záměrně, protože jej lze využít jak pro přístup pouze k jedné pracovní stanici (autonomnímu pc), tak i pro přístup k počítačové síti. Jako identifikační software je použit Biologon 3 a záleží na jeho použití, zda je nastaven a nainstalován pro použití na pracovní stanici nebo na serveru.

Velice zajímavým parametrem, který udává výrobce, je to, že při identifikaci je možno přiložit prst na čtečku jakkoliv pootočený v rozpětí 360°. To vypovídá o velmi

kvalitním zpracování jak čtečky, tak i algoritmu, který otisk vyhodnocuje. Takovou funkcí jsou vybavovány senzory méně často. Proč je tento parametr pro někoho nedůležitý a nevýznamný zmiňován? Protože jde o poměrně důležitý parametr, respektive důležitá vlastnost senzoru. Tento senzor bude mít poměrně malou chybovost FRR (chybné odmítnutí), protože je takřka jedno jak prst přiložíme a stejně dojde k jeho správnému vyhodnocení. Je odolný vůči nesprávnému uživatelskému přístupu, tím i uživatelsky přijatelnější.

Bohužel nebylo možno tuto čtečku odzkoušet, byla zvolena do praktické části pouze pro návrh ochrany počítačové sítě v kombinaci s programem Biologon 3. Ale je zařazena už v této kategorii, protože ji lze využívat jak pro přístup k jednomu PC nebo do počítačové sítě. Program Biologon 3 bude rozebrán v kapitole 3.1.2.1. Přístup k notebooku je možné řešit touto čtečkou taktéž, ale bylo by to nepohodlné. Lepší variantou pro přístup k notebooku je Identix BioTouch PC Card, které má stejné parametry jako Identix BioTouch USB, jen místo rozhraní USB je tento senzor implementován do PCMCIA karty.

Tab. 3. Identix BioTouch USB

Parametr	**Hodnota**
Typ senzoru	optický snímač CMOS DFR 200 (Motorola)
Velikost snímače otisku	17 x 17 mm
Vlastnosti senzoru	otáčení prstu 360°
Podporované operační systémy	pouze platforma MS Windows a to 95, 98, ME, NT, 2k, XP
Software užívaný k identifikaci	Biologon
Komunikační rozhraní	USB 2.0/1.1
Spotřeba energie	zapnuto 340mW, standby 120mW
Hmotnost	150g
Rozměry	96 x 60 x 31 mm
Pracovní teplota	0 - 55℃

Obr. 22. Čtečka identix

3.1.1.3 Ekey BIT

Jde o čtečku společnosti Ekey, která používá termický senzor firmy Atmel. Lze ji využívat jak k přístupu k autonomnímu PC (se softwarem ekey LOGONpro), tak i ke kontrole přístupu do počítačové sítě s programem ekey LOGONserver. Tak i pro přidávání otisků prstů pro přístupový systém ekey TOCAnet přes admin server. Na této čtečce nebyly provedeny žádná měření, slouží pouze pro návrhovou část.

Tab. 4. Parametry Ekey BIT

Parametr	**Hodnota**
Rozměry š x v x h	60 x 82 x 22 mm
Hmotnost	220g
Rozhraní	USB 1.1/2.0
Senzor	termický Atmel FingerChip
Chybovost - FAR - FRR	0,00001 0,014
Pracovní teploty	10℃ až +70℃
Ovladače	pro Windows 98 až XP (kromě NT)

Obr. 23. Čtečka Ekey BIT

3.1.2 Prvky a vybavení pro ochranu počítačové sítě biometrickými prvky

Výběr softwarového vybavení a čteček, které by umožňovaly kontroly přístupu k počítačové síti za pomocí biom. údajů, už není tak mnoho jako pro kontrolu přístupu k autonomnímu PC. Pro návrh ochrany počítačové sítě jsem vybral software Biologon 3 v kombinaci se čtečkami Identix BioTouch USB (3.1.12) a nebo Ekey LOGONserver a čtečkou Ekey Bit (3.1.1.3).

Mohla by vystat otázka proč řešit přístup do PC, když už mám např. vyřešenou ochranu autonomního PC. Jde o to, že do sítě se může připojit PC, který není takto chráněn, a pokud není poč. síť chráněna jiným klientem pro přístup (např. Novel), pak se v ní útočník může volně pohybovat. Pokud tedy budeme chtít chránit celou síť

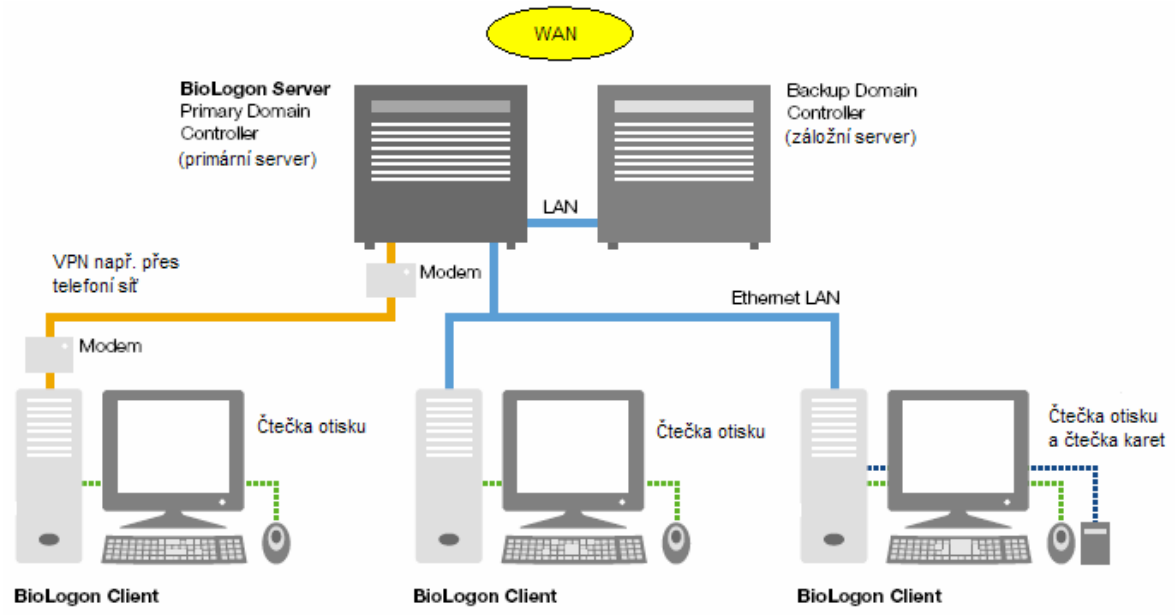
biometrickými údaji, tak můžeme zvolit např. Biologon nebo ekey LOGONserver. Softwary zde uvedené slouží pouze pro návrhovou část a bohužel na nic nebylo možné provést praktická měření.

3.1.2.1 Identix Biologon 3

Tento software umožňuje jak přístup k autonomnímu PC, tak i počítačové síti. Architektura zpracování je taková, že na serveru musí být nainstalován program Biologon Server a na jednotlivých počítačích opatřených čtečkami Identix a programem Biologon klient. Ten je dodáván ke každé čtečce zmíněné v kapitole 3.1.1.2 a může být i bez serverové verze užíván k ochraně autonomního PC.

Tab. 5. Parametry Biologon Server

Parametr	**Hodnota**
Podporované operační systémy	pouze platforma MS Windows a to NT, 2000, XP
Systémové požadavky	Pentium I 133MHz a lepší 128MB Ram a více



Obr. 24. Schéma možné architektury poč. sítě s použitím Biologonu [19]

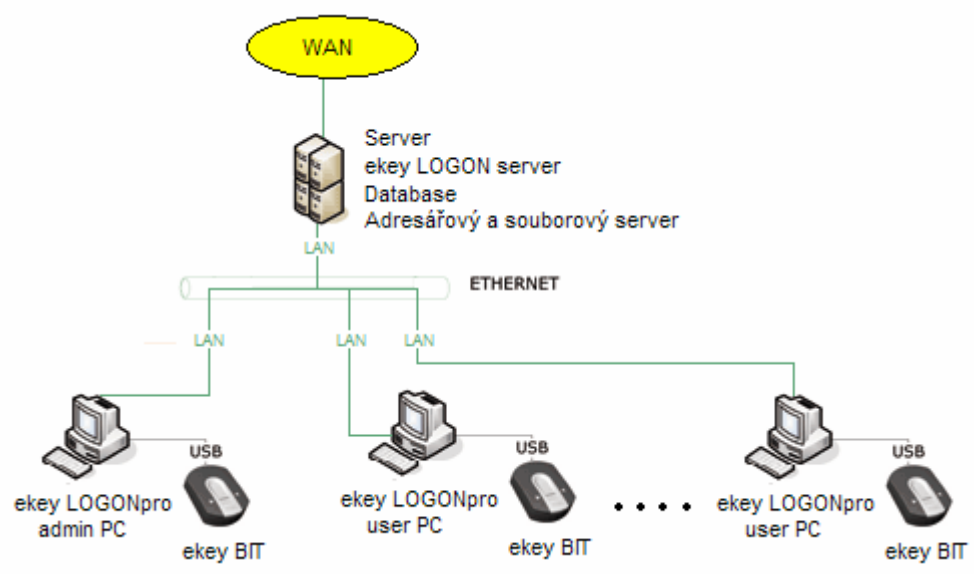
Tento software umožňuje kromě identifikace pomocí biom. údajů také identifikaci za pomocí čteček karet, které společnost Identix podporuje. Další, co umožňuje tento software, je kontrola docházky.

3.1.2.2 Ekey LOGONserver

Jde o další software umožňující kontrolu přístupu k poč. síti. Je produktem společnosti Ekey. Architektura komunikace je taková, že na serveru je instalován ekey LOGONserver a na jednotlivých uživatelských terminálech čtečka ekey BIT (kap. 3.1.1.3) a software ekey LOGONpro.

Tab. 6. Parametry ekey LOGONserver

Parametr	Hodnota
Operační systém pro server	Windows 2000 server a 2003 server
Operační systém pro pracovní stanice	Windows 2000 SP 4 a XP Professional SP1 a vyšší
Čtečka	ekey BIT nebo Siemens ID myš



Obr. 25. Možný příklad architektury se softwarem ekey LOGONserver

3.1.3 Prvky ochrany dat paměťových médií pomocí biometrických prvků

Existuje mnoho prvků, které dokáží data šifrovat pomocí biometrických údajů. Nejčastěji se využívá čteček připojených do PC přes USB nebo integrovaných v periferiích nebo notebooku. Další velmi zajímavou kategorií ochrany dat je použití flash paměťových médií opatřených biometrickým snímačem. Existuje několik typů těchto médií. Pro praktickou část této práce jsem vybral dva flash disky s šablonovací kapacitní čtečkou. Prvním je A-Data FingerPrint Disk a druhým Pretec i-Disk Touch. Jde o flash disky se stejným snímacím čipem, liší se pouze v používaném softwaru a trochu odlišných funkcích, které budou ještě rozebrány. Existují dvě podoby jak jsou data chráněny na flash

discích. První je taková, že flash disk má celý oddíl nepřístupný, „neviditelný“ a přešifrovaný (nejčastěji pomocí 2D kódu) a až po verifikaci otisku je oddíl rozšifrován a zpřístupněn. Jde o odolnější způsob řešení. Dnes méně častou metodou, spíše historicky významnější je druhý způsob ochrany dat, kdy byla na flashdisku vyčleněna jedna složka, která byla pouze šifrována za pomocí biometrických údajů či hesla. Jde o způsob, který umožňuje jednodušší pokus o prolomení tzv. „hrubou silou“, kdy lze použít generátor hesel k prolamování. Jde o způsob ochrany, který se dnes již takřka nevyužívá.

3.1.3.1 A-Data FingerPrint Disk (A-Data FP2)

Jde o první ze zmiňovaných flash disků. Pracuje se šablonovacím kapacitním snímačem. Tento fashdisk je běžně k sehnání v cenové relaci přibližně jednonásobné oproti běžným flash pamětem o stejné kapacitě. Což při ceně dnešních flash pamětí je zanedbatelná investice, která nám výrazně zvýší bezpečnost našich dat.

Pro návrh a testování jsem vybral flash disk o kapacitě 2GB, někdo by mohl namítnout, že pro dnešní dobu je to již nedostatečná kapacita. Myslím si, že pro malou až střední organizaci je to postačující pro uložení důležitých dokumentů, smluv v el.podobě, informací o zákaznících a hesel a přístupových práv (např. k internetovému bankovnictví apod.).

Tab. 7. Parametry flash disku A-Data FP2

Parametr	**Hodnota**
Kapacita	1, 2, 4, 8 GB
Rychlost čtení a zápisu	11MB/s a 10MB/s
Rychlost verifikace	<3s
Typ senzoru	šablonovací kapacitní
Velikost databáze otisků	10 otisků
Chybovost - FAR - FRR	0,001% 1%
Podporované operační systémy	pouze platforma MS Windows a to ME, 2000, XP a Vista*
Systémové požadavky	Intel Pentium III a lepší 128MB Ram a více; USB 2.0/1.1

* u systému MS Windows Vista je nutné provést nastavení kompatibility se MS Windows XP SP2

Obr. 26. USB flash disk A-Data FP2

Tento flash disk kromě znepřístupnění a zašifrování oddílu disponuje ještě několika zajímavými funkcemi, které jsou implementovány do softwaru flash disku, a je možno je využít po verifikaci prstu. Jakmile je verifikace ukončena, zpřístupní se oddíl, a spustí se příslušný software (Obr.27.). Tento software umožňuje několik podpůrných funkcí jako: IE Autologin, My Favorites, User Settings, Help, a také šifrování dat. Tyto funkce jsou společné jak pro A-data FP2 a tak i Pretec i-Disk Touch, který bude rozebrán v kapitole 3.1.3.2. Flash disk A-Data FP2 dále disponuje funkcí Flash mail, která je vhodná pro osoby (zaměstnance), kteří cestují nebo často střídají PC. Umožňuje jednoduchou správu všech mailů, bez složitého kopírování a přenášení seznamu kontaktů. Tento disk je oproti následujícímu vybaven lepším pouzdrem a krytím kapacitního snímače (Obr.26.).

Obr. 27. Software pro A-Data FP2vlevo a software pro Pretec vpravo

Popis uživatelských funkcí:

- **IE Autologin** – tato funkce je velice zajímavá v tom, že nám umožňuje v kombinaci s aplikací MS Internet Explorer 6 a vyšší vytvořit databázi internetových stránek, přihlašovacích jmen a hesel. Tak můžeme jednoduše spravovat svého web manilového klienta, přístup k internetovému bankovnictví, internetovým obchodům a jiným internetovým aplikacím, které vyžadují login a heslo.
- **My Favorites** – opět funkce vhodná pro osoby, která často střídají počítače. Je kompatibilní taktéž pouze s IE. Umožňuje vytvořit databázi používaných internetových stránek a uložit ji na v tomto paměťovém médiu.
- **User Settings** – přes tuto záložku můžeme spravovat databázi otisků prstu (max. 10 otisků) a heslo k přístupu a šifrování.
- **Help** – nápověda k uživatelským funkcím tohoto disku
- **Flash Mail** – Jak bylo již výše zmíněno jde o manilového klienta. Který umožňuje příjem i odesílání mailů, správu adresáře. Maily jsou v systémové složce flash disku uloženy v šifrované podobě, zpětně je lze exportovat do aplikací Outlook. Celý software včetně manilového klienta jsou pouze v anglicko jazyčné verzi, ale uživateli se znalostí základních anglických slov nedělá problém tyto funkce ovládat.
- **Šifrování dat** – tímto flash diskem můžeme zašifrovat jakoukoliv složku či soubor i mimo tento flash disk. Kliknutím pravým tlačítkem myši nad souborem či složkou se a vybráním možnosti Encrypt file/folder provede zašifrování; odšifrování pak Decrypt file/folder. Touto funkcí můžeme udržovat chráněné i data mimo tento flash disk. Ale musíme mít na paměti, že šifrování je zde prováděno ne otiskem prstu, ale kódem uloženým na flash disku. Proto je doporučené toto heslo volit co nejsložitější. Utvořit např. náhodnou kombinaci velkých a malých písmen doplněnou číslicemi (max. 16 znaků), kterou pak uložíme např. do trezoru, abychom si ji nemuseli pamatovat. Osobně doporučuji heslo zvolit co nejsložitější, aby jej nebylo možno v rozumném čase prolomit „útoky hrubou silou“. Dále pak bych doporučil toto heslo uložit na vhodném místě (např. v trezoru) a nespoléhat pouze na otisk prstu nebo svou paměť. Protože většina výrobců šablonovacích kapacitních senzorů garantuje (nebo spíše udává) životnost okolo 1 milionu přejetí prstu po senzoru. Musíme mít na paměti, že

velkým nepřítelem kapacitních čteček otisku prstu je statická elektřina. A tak můžeme i nevědomky tento snímač zničit dříve jak po 1 milionu sejmutí otisku prstu.

Jinou variantou biometrických šifrátorů jsou tzv. hardwarové šifrátory. Tyto šifrátory nevyužívají k šifrování uživatelem zvolené heslo. Ale jedinečný kód získaný sejmutím charaktericky otisku prstu. Jde o bezesporu mnohem složitější kód, ale pozor šifrování a dešifrování je nutné provést stejným prstem. Proto při větším poranění či amputaci prstu přijdeme o data. Hardwarový biometrický šifrátor nebyl pro praktickou část této práce vybrán. Důvody jsou dva a to: protože softwarové šifrování složitějším (16. místným) kódem považuji za plně dostačující. Druhým důvodem je cena. Hardwarové šifrátory jsou běžně v cenách deseti tisíc až několika desítek tisíc.

3.1.3.2 Pretec i-Disk Touch

Jde o další variantu flash disku s ochranou dat pomocí biometrických prvků. Je do něj implementován stejný typ šablonovacího kapacitního senzoru jako v médiu FP2. Tento disk používá i takřka stejný vyhodnocovací software, jen se odlišuje v několika uživatelských funkcích. A právě proto jsem ho vybral pro praktickou část této práce jako druhou variantu. Tento flash disk sice postrádá funkci Flash Mail, ale zase disponuje taktéž velmi zajímavou funkcí PC Lock, která bude ještě rozebrána.

Tab. 8. Parametry flash disku Pretec i-Disk Touch

Parametr	**Hodnota**
Kapacita	512MB, 1 , 2, 4, 8 GB
Rychlost čtení a zápisu	max. 12MB/s
Rychlost verifikace	<3s
Typ senzoru	šablonovací kapacitní
Velikost databáze otisků	10 otisků
Chybovost - FAR - FRR	0,001% 1%
Podporované operační systémy	pouze platforma MS Windows a to ME, 2000, XP a Vista*
Systémové požadavky	Intel Pentium III a lepší 128MB Ram a více; USB 2.0/1.1

* u systému MS Windows Vista je nutné provést nastavení kompatibility se MS Windows XP SP2

Obr. 28. Pretec i-Disk Touch 2GB

Popis uživatelských funkcí:

Funkce jsou stejné jako u A-Data FP2 kromě Flash Mailu, tato funkce je nahrazena jinou zajímavou funkcí a to PC Lock.

- PC Lock – Funkce umožňující zamknout PC a umožnit přístup až po přiložení otisku. Nevýhodu shledávám v tom, že PC lze dle nastavení uzamykat pouze na: 1, 2, 3, 6, 12 a 24 hodin. Zámek funguje i po restartu a uspání PC. Je to vhodná metoda k uzamykání PC, pokud nebudeme chtít investovat do samostatné čtečky. Nasazení je vhodné tam, kde jsem nucen odcházet od zapnutého pc a nechceme, aby někdo nahlížel do dat ložených v něm (různá obchodní oddělení, úřady apod.).

3.2 Vybrané prvky pro přístupové biometrické systémy

U přístupových systémů již oproti výpočetní technice je rozmanitější výběr biometrie, jak různých metod identifikace, tak i různých typů snímačů otisků. Taktéž je i rozmanitější výběr možných typů zpracování, lze aplikovat jak autonomní systémy, tak i systémy s různými typy centrální správy. Návrh v oblasti

3.2.1 Prvky pro autonomní systémy

Jde o systém, který je reprezentován takovou teorií: co přístupový bod, to vlastní čtečka bez jakéhokoliv společného řídícího členu. Jde o prvky, které mají vše potřebné pro svoje rozhodování v jedné čtečce. I většina online systémů může pracovat autonomně v případě výpadku řídících členů (disponují svou pamětí). Nebo existují případy autonomních čteček, které po sběrnicích jako RS232 či 485 nebo wiegand posílají

informace a stavy do centrálního záznamového prvku, ale v opačném směru není čtečka nikterak ovládána.

3.2.1.1 FPL – 250 nebo FPL – 255

Jde o kombinaci biometrické čtečky a mech. zámku v jednom „kování“. Vhodné aplikace jsou například pro domácnost i kanceláře u verze 255 i hotely. Komunikace může probíhat přes RS232,485 u verze 255 i přes TCP/IP. Jelikož jde o kombinaci čtečka a zámek, nemáme již další náklady při budování autonomního přístupového bodu. Přístup je možný ve třech variantách a to pomocí otisku prstu, hesla nebo kombinace heslo plus otisk.

Tab. 9. Parametry biom. zámku FPL – 250 (255)

Parametr	**Hodnota**
Senzor	Optický
Rozlišení	500 DPI
Čas snímání	<1s
Chybovost - FAR - FRR	0,0001% 0,001%
Velikost databáze otisků	300 otisků
Paměť událostí	30 000
Napájení	5 x baterie AA (6V DC)
Odběr proudu - klidový - provoz	12µA 100 - 250mA
Komunikace	RS 232, RS 485, u verze 255 TCP/IP
Provozní teplota	-30 až + 80℃
Relativní vlhkost	20 až 80%

Obr. 29. FPL – 250

Hodí se pro menší systémy tam, kde nepožadujeme kontrolu docházky a chceme ušetřit nemalé peníze, které bychom museli investovat do složitějších systémů. Další výhodou je, že tento systém lze osadit na takřka jakékoliv dveře a zvládne jej středně zručný člověk namontovat sám. Toto zařízení bylo použito pouze pro návrh bez měření v praktické části.

3.2.1.2 V-Pass FX MV 1610

Čtečka V-Pass je z produkce firmy Bioscrypt. Tato čtečka je opatřena kapacitním snímačem otisku. Jde o čtečku, která je autonomní a je vhodná pro použití v malých až středních aplikacích s maximálně 200 při identifikaci respektive 500 otisky při verifikaci. Čtečka sama o sobě neobsahuje spínací relé, takže nemůže přímo spínat zámek. Ale je vybavena několika komunikačními rozhraními, přes které je možné spínat door controler a případně data posílat dále. Čtečka sama osobě nemá paměť událostí, tak pokud od ní požadujeme nějakou vyšší funkci, je potřeba například pomocí sběrnice wiegand, ji připojit do nějakého vyššího systému. Když tuto čtečku aplikujeme do systému, je to taková přechodová varianta mezi autonomním a online systémem. Správou se jedná o autonomní systém, ale při použití vhodných řídících prvků dostaneme online systém vhodný pro sledování docházky apod.

Tato čtečka byla, pro praktickou část vybrána, protože je instalována v laboratoři D309, a lze na ní tudíž provést praktická měření. Čtečka nepatří k těm nejlepším na trhu, spíše k průměrným čtečkám neposkytujících velkou přesnost, ale pro běžné použití je postačující. Není vhodná pro aplikace, u kterých požadujeme vysokou bezpečnost. Čtečku shledávám vhodnější pro použití ve vnitřních prostorech a v prostorech pod dohledem. Případně v kombinaci s vhodným ochranným krytem. Protože její nevýhodou je, že komunikační interface přes USB je volně k dispozici ze spodní části čtečky, kryt je zajištěn šroubkem. Sice po připojení USB kabelu a nainstalování VeriAdminu nelze v čtečce změnit nastavení bez znalosti kódu umístěného běžně ze zadní strany čtečky. Ale plyne z toho možné riziko zneužití pachatelem, naším zaměstnancem či pracovníkem montážní firmy.

Tab. 10. parametry čtečky V-Pass FX

Parametr	**Hodnota**
Rozměry d x š x h	130 x 50 x 63,5 mm
Rychlost verifikace	<1s
Typ senzoru	kapacitní
Velikost databáze otisků	200 (1:N), 500 (1:1)
Velikost šablony	2500b (1:N), 350b (1:1)
Chybovost - FAR - FRR	0,20% 1%
Komunikační rozhraní	RS 232 RS 485 wiegand USB AUX port
Provozní napětí	9 - 24V DC
Proud	0,2A v zátěži max. 0,5A
Provozní teplota	0 - 60℃
Software pro nastavení čtečky	VeriAdmin

Obr. 30. Čtečka V-Pass FX (MV 1610)

3.2.2 Prky pro neautonomní (online) systémy

Jde o systém jedné nebo více čteček, které jsou propojeny s nějakým centrálním řídícím a rozhodovacím prvkem nebo vzájemně mezi sebou s různými stupni inteligence a komunikace. Pro návrh v praktické části jsem vybral systém firmy Ekey modelové řady TOCAnet. Jde opět jen o návrh, na systému nebyla prováděna praktická měření.

3.2.2.1 Ekey TOCAnet

Tento produkt jsem vybral, protože ho lze použít komplexně pro online systém. Je jednoduchý na použití a disponuje mnoha doplňky. Tento přístupový systém je použit v nejvýkonnější variantě návrhu.

Čtečky využívají termického senzoru firmy Atmel s označením FingerChip. Čtečka se skládá ze dvou částí a to: vnitřní a vnější jednotky. Vnitřní jednotka se stará o zpracovávání informací, rozhodovaní, ovládání zámku (přístupového místa), komunikací se serverem, tak i komunikací s vnější jednotkou (snímacím senzorem).

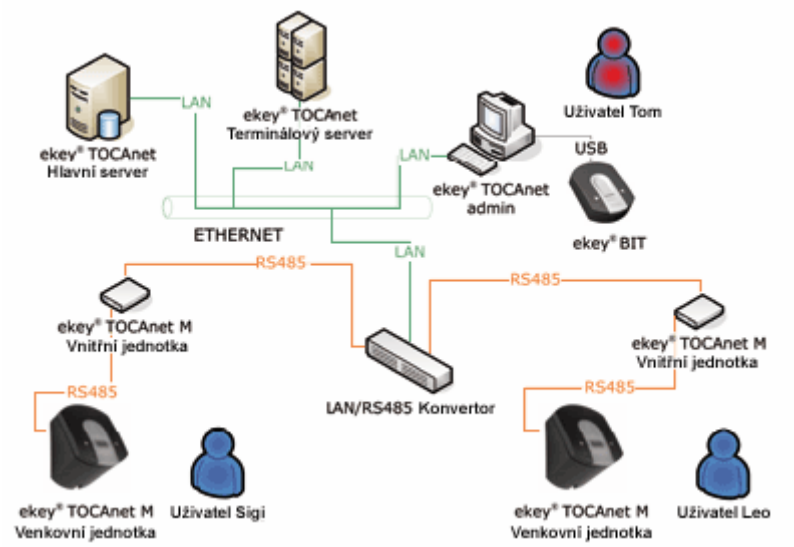
Tab. 11. Parametry systému ekey TOCAnet

Parametr	**Hodnota**
Rozměry - vnitřní jednotka (š x v x h) - vnější jednotka	140 x 128 x 48 mm 60 x 95 x 55 mm
Typ senzoru	termický Atmel FingerPrint
Databáze otisků – offline (dle verze) - online	200 otisků verze M, 40 otisků u S a 2000 otisků u L "neomezeně"
Chybovost - FAR - FRR	0,00001 0,014
Napájení	z 220/110V na 9 nebo 12 V DC venkovní jednotka napájená z vnitřní
Příkon	2,2W
Relé	3x až 230V max. 5A
Komunikace	RS 485 přes konvertor LAN (Ethernet)
Pracovní teploty	-40 až +85 ℃
Relativní vlhkost	max. 95%
Krytí - vnitřní jednotka - vnější jednotka	IP 54 IP 43

Architektura systému je taková, že otisk je přes čtečku ekey BIT zapojenou v administrátorské stanici nahrán na ekey TOCAnet server odkud je pomocí LAN sítě respektive konvertoru LAN/RS 485 nahrán do ekey TOCAnet jednotky (vnitřní). Při identifikaci může tento systém pracovat v režimu online, kdy předkládaný biom. vzor porovnává s databází šablon na ekey TOCAnet serveru (neomezený počet šablon). V případě výpadku serveru nebo některého komunikačního prvku může pracovat v režimu offline, kdy je předkládaný biom. vzor porovnán s databází šablon v ekey TOCAnet M vnitřní jednotce (200 otisků). Když se čtečka po výpadku uvede zpět do režimu online, jsou zaslány všechny informace z čtečky na server. Umožňuje tvořit různé přístupové úrovně, časové režimy apod. Další výhodou je, že na jednu vnitřní jednotku můžeme připojit až 6

čteček otisku prstu (vnějších zařízení). Vnitřní jednotka obsahuje 3 releové výstupy, tudíž lze ovládat najednou více prvků např. dveře, vrata, zabezpečovací ústřednu apod.

Obr. 31. vnější část Ekey TOCAnet M



Obr. 32. Schéma systému Ekey TOCAnet [20]

3.3 Základní varianta návrhu

Tato varianta se zabývá nejzákladnější formou návrhu. Je zde kladen velký důraz na nižší náklady, ale ne na úkor bezpečnosti. Dále pak není požadována evidence docházky. Tento návrh vychází z výchozího stavu, kdy není aplikována žádná kontrola vstupu ACS. Ochrana výpočetní techniky je realizována běžným hardwarovým a softwarovým vybavením. V oblasti ochrany výpočetní techniky je požadována zabezpečit data biom. prvky (není přímo vyhrazeno, kde data mají být ukládána). Není potřeba řešit kontrolu přístupu do všech PC pomocí biom. prvků. Jen je doporučné použít biometrickou čtečku pro přístup k PC u vedoucích pracovníků, kvůli uživatelskému pohodlí a jiným

doplňkovým funkcím Dále je pak požadována kontrola přístupu biom. prvky k serveru. Je obecný předpoklad, že server je postaven na MS Windows 2000 server nebo 2003 server, jako je tomu dnes u většiny malých organizací.

3.3.1 Vybrané prvky pro realizaci základní varianty návrhu

Z výše zmíněných požadavků a absence předchozího přístupového systému jsem vybral pro přístup prvek **FPL – 250** (kap. 3.2.1.1). Jako u jediné varianty v rámci úsporných opatření jde o kombinaci biom. čtečky a zámku v jednom prvku. Lze jej namontovat na takřka jakékoliv dveře. Parametry pro použití v malé organizaci má velmi uspokojivé a databáze otisků je také více jak dostatečná. Pro přístup k PC pro vedoucí pracovníky, administrátora a přístupu na server byl vybrán **APC Touch Biometric Pod Password Manager z kapitoly** 3.1.1.1. Tento biopod umožňuje jak ochranu přístupu k PC, tak i management přihlašovacích údajů a hesel pro různé aplikace a také umožňuje šifrování dat. Pro ochranu dat je ke každému PC navržen USB flash disk **Pretec i-Disk Touch** (kap. 3.1.3.2). Tento flash disk byl zvolen hlavně z důvodu funkce PC Lock (uzamčení PC). Touto funkcí můžeme dočasně (pouze pro určitou dobu nejdéle pak 24h) uzamknout PC a bez správné verifikace otisku nelze v PC provádět žádné uživatelské úkony. Díky tomu můžeme uzamykat PC, když od něj budeme odbíhat a budeme jej chtít zabezpečit aniž bychom se museli odhlásit (i při úsporném režimu a režimu spánku funkce zůstává aktivní).

Jde o návrh, který příliš neoslní, ale splní všechny základní modelové požadavky (uvedené v pro základní návrh) při zachování vyššího standartu bezpečnosti.

3.3.2 Architektura základní varianty návrhu

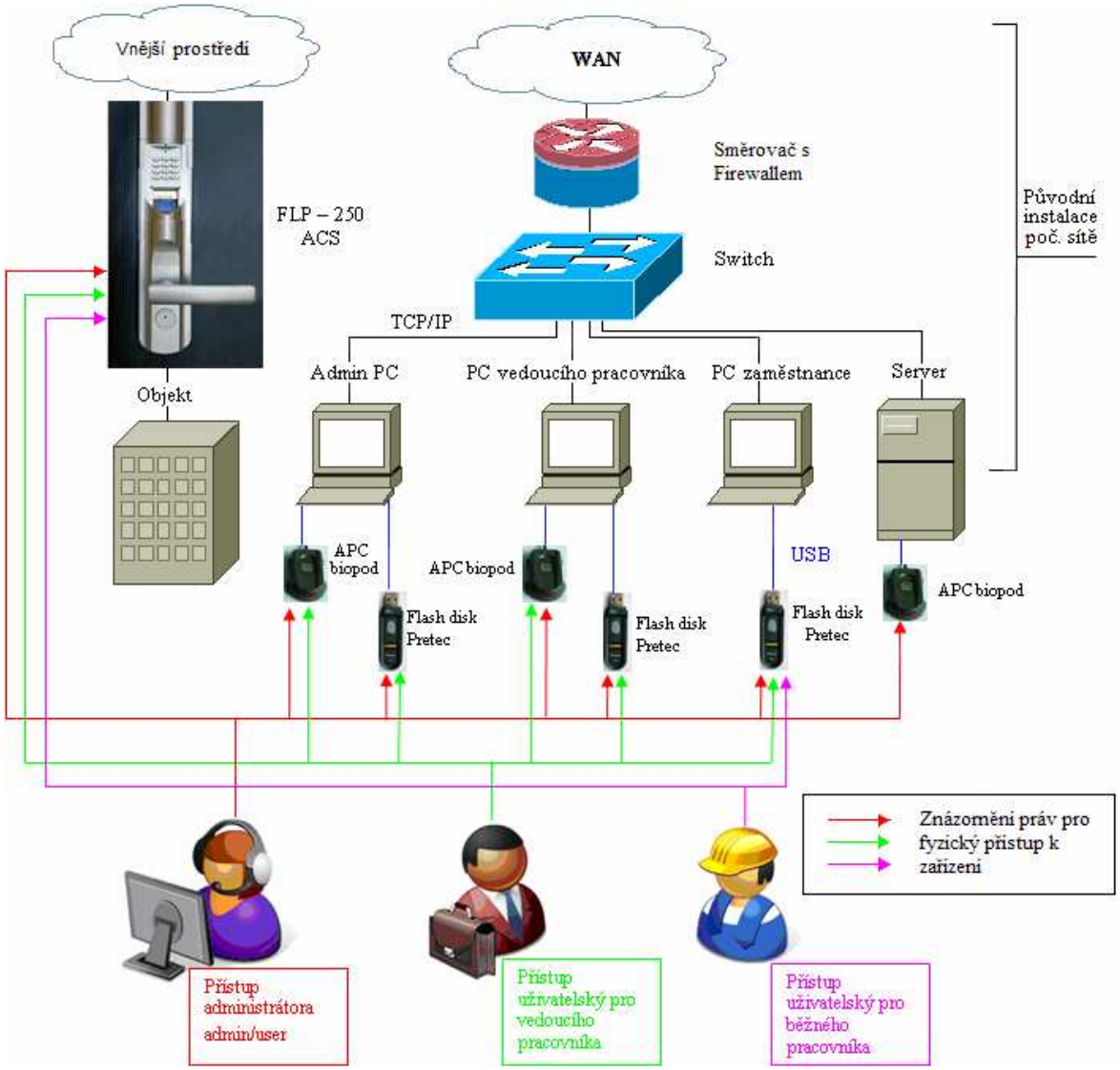
Jelikož jde o nejlevnější variantu návrhu, která mezi sebou není nijak provázána. Jedná se zde vysoký stupeň autonomity. Uživatelsky to není nijak důležité. Ale z hlediska administrátora jde o systém s vyšší složitostí na přehlednost a ovládání. Prodlužuje administrátorské úkony přidání, či změny uživatele aj. Administrátor těchto systémů musí s osobou, které je udělován přístup, projít všechny typy přístupových bodů a nahrát do nich šablonu. Nelze v reálném čase zjišťovat, kde se zaměstnanec nachází apod. Jde o vhodnou varantu řádově pro desítky zaměstnanců, nejvíce však okolo 50, a nejlépe jedním, nebo co nejméně přístupovými body do objektu. Při větším počtu zaměstnanců v této variantě

vzniká problém se složitostí systému, respektive špatné orientaci v tomto systému, a také se výrazně narůstá čas vynaložený na servisní úkony.

Přístup přes přístupový terminál FPL – 250 je udělen přístup každému zaměstnanci. Přístup přes APC biopod pak vedoucím pracovníkům do jejich PC a také administrátorovi systému k jeho PC a serveru. A na flash disk pro ochranu dat doporučuji přidat tři sady otisků a to: zaměstnance jemuž je přidělen, nadřízenému pracovníkovi a administrátorovi. Jde jak o vhodný postup pro případ kontroly a také pro případný servisní úkon.

Tento návrh je výhodný v tom, že síť LAN nemusí být vybudována tak, jak je znázorněna ve schématu architektury základního návrhu. Její existence pro základní návrh není nutná. Využíváme již stávající instalaci výpočetní techniky a připojíme pouze čtečky a flash disky, nevyžaduje další úpravy. Je zde řešen pouze přístup k PC nikoliv síti. Další výhodou je, že nemusíme k přístupovému bodu do objektu přivádět zdroj el. energie. Biometrický zámek využívá jako zdroj energie 5 AA baterií, které vydrží cca 6 měsíců při 50 použitích denně. Z důvodu úsporného řešení jsou pro přístup do objektu vybrány pouze jedny dveře a druhé slouží pouze jako nouzový východ, který lze otevřít pouze z vnitřní strany objektu.

V rámci dalšího úsporného opatření se předpokládá, že administrátor používá pro svůj PC a Server set jednoho monitoru, klávesnice a myši připojené přes přepínač. Proto přes tento přepínač realizováno připojení i čtečky pro přístup. Celkový počet čteček pro přístup k PC je o jednu méně než je součet PC, pro které jsou určeny.



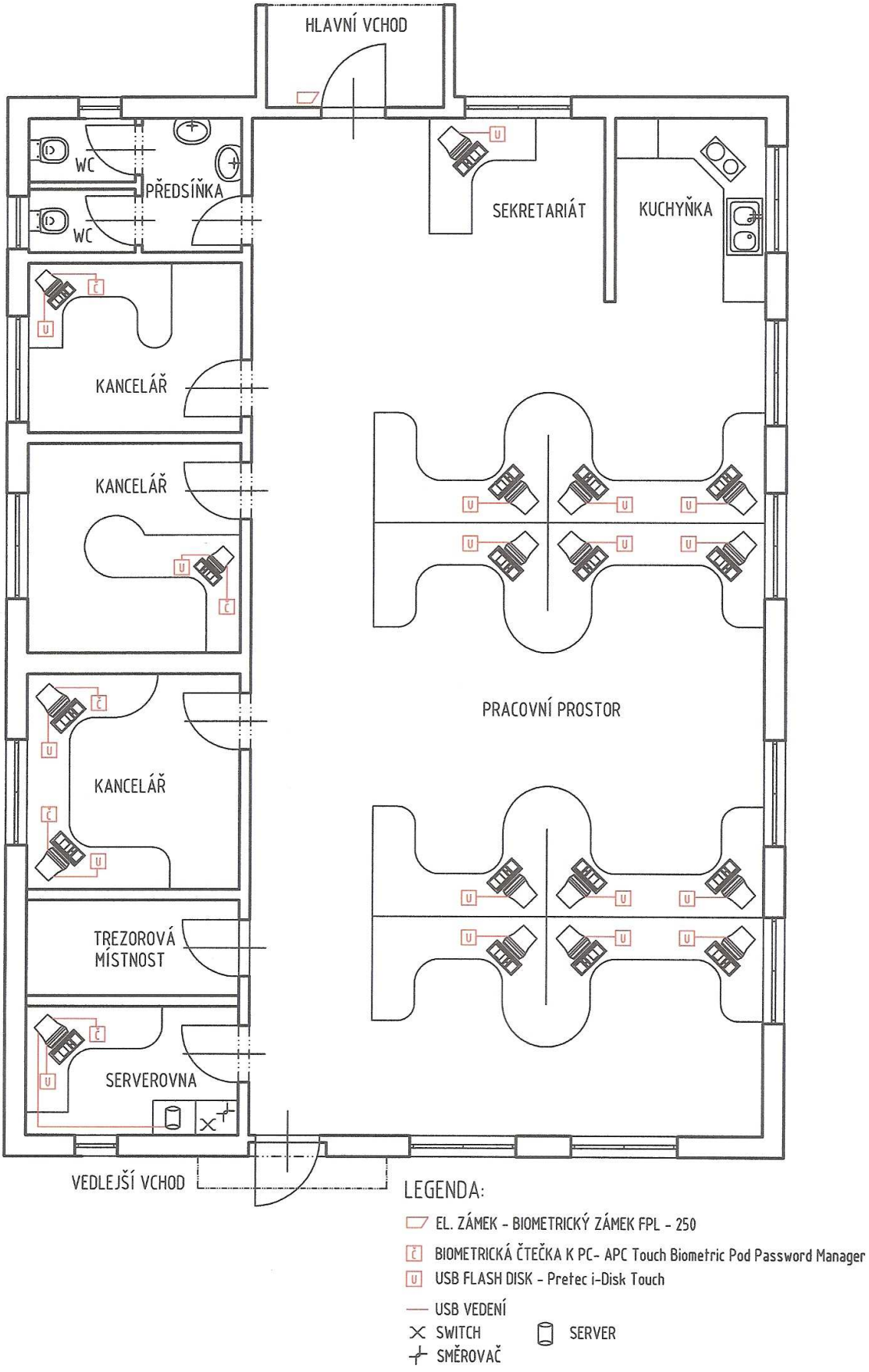
Obr. 33. Schéma architektury základního návrhu

3.3.3 Základní návrh pro modelovou organizaci

Modelová organizace má 18 zaměstnanců, z toho 4 vedoucí pracovníky, jednoho správce výpočetní techniky a 13 ostatních pracovníků.

Náklady na zřízení: (Náklady na vybudování kabeláže nejsou počítány)

1x FPL – 250	14 995
5x APC Touch Biometric Pod Password Manager z kapitoly	5x 1 000
18 x Pretec i-Disk Touch 2GB	18x 400
Celkem bez DPH Kč:	**27 195**



Obr. 34. Zobrazení základního návrhu pro modelovou organizaci

3.4 Vyvážená varianta návrhu

Tato varianta návrhu se zabývá optimálně vyváženým návrhem. Kdy již je aplikován kartový přístupový a docházkový systém a je požadováno jej v rámci úsporných opatření pouze upravit a doplnit o čtečky biometrických charakteristik na všech vstupech do objektu. Ochrana výpočetní techniky je realizována běžnými metodami. Je zde požadováno zabezpečit přístup do poč. sítě pomocí biometrických prvků. Není kladen důraz na značku systému a komplexnost řešení.

Předpokládá se, že je instalován např. systém **APS 400 nDocházka**, **s řídící modulem MCA168.1E**, na vstupech do objektu a přístupu do kanceláří **čtecí modul MREM 53** a u hlavního vchodu **docházkovým čtecím modulem MRED 53**, pro kontrolu vstupu do trezorové místnosti je použit čtecí **modul + PIN MREP 53** vše od firmy TechFass. Dále pak předpokládáme již vybudovanou **LAN síť** v objektu.

3.4.1 Vybrané prvky pro vyváženou variantu návrhu

Jelikož již je aplikován určitý přístupový a docházkový systém, je nutné vhodně zvolit čtečku. Je nutné zvolit čtečku, která podporuje komunikační rozhraní daného systému a je v ní umístěno relé pro ovládání např. dveří. Bývá většinou dost velkým problémem, abychom splnili jak vhodné komunikační prostředí, tak i ovládací prvek (relé) a zároveň splnění vhodných biom. parametrů v jedné čtečce při zachování rozumné ceny. U některých systémů ani takovou biometrickou čtečku nemusíme nalézt. Proto je potřeba nalézt vhodný převodník komunikačního interface, který disponuje pamětí pro určitý počet ID a také datovým vstupem o stejném typu, jaký má biometrická čtečka. Proto jsem vybral čtečku **V-Pass FX MV 1610** (kap. 3.2.1.2) a jako převodník pro daný systém jsem zvolil **WGD 44** od firmy TechFass. Jehož parametry jsou: 500 ID, 2x wiegand vstup, 4 log. vstupy a 4 výstupní relé, komunikuje po RS 485 a je vhodný pro APS 400. Pro ochranu počítačové sítě biom. prvky jsem zvolil software **Identix Biologon 3** (kap. 3.1.2.1) se čtečkami **Identix BioTouch** (budou osazeny na každém PC). Popis těchto čteček je uveden v kapitole 3.1.1.2. Software Biologon umožňuje jak přístup k poč. síti, PC, tak i management hesel a přihlašovacích údajů do jiných aplikací. I když je toto už komplexnější řešení, tak stále musíme myslet i na ochranu dat, které může náš zaměstnanec přenášet. Proto jsem se do tohoto návrhu rozhodl zařadit i flash disk s biometrickými prvky **A-Data FingerPrint Disk (A-Data FP2)** z kapitoly 3.1.3.1. Tento flash disk může zaměstnanec

využívat při přenášení dat, které může zpracovávat doma, případně přenáší mezi pobočkami, či kooperujícími firmami. Navíc si na tomto flash disku může zaměstnanec udržovat chráněná svou e-mailovou komunikaci.

3.4.2 Architektura vyváženého varianty návrhu

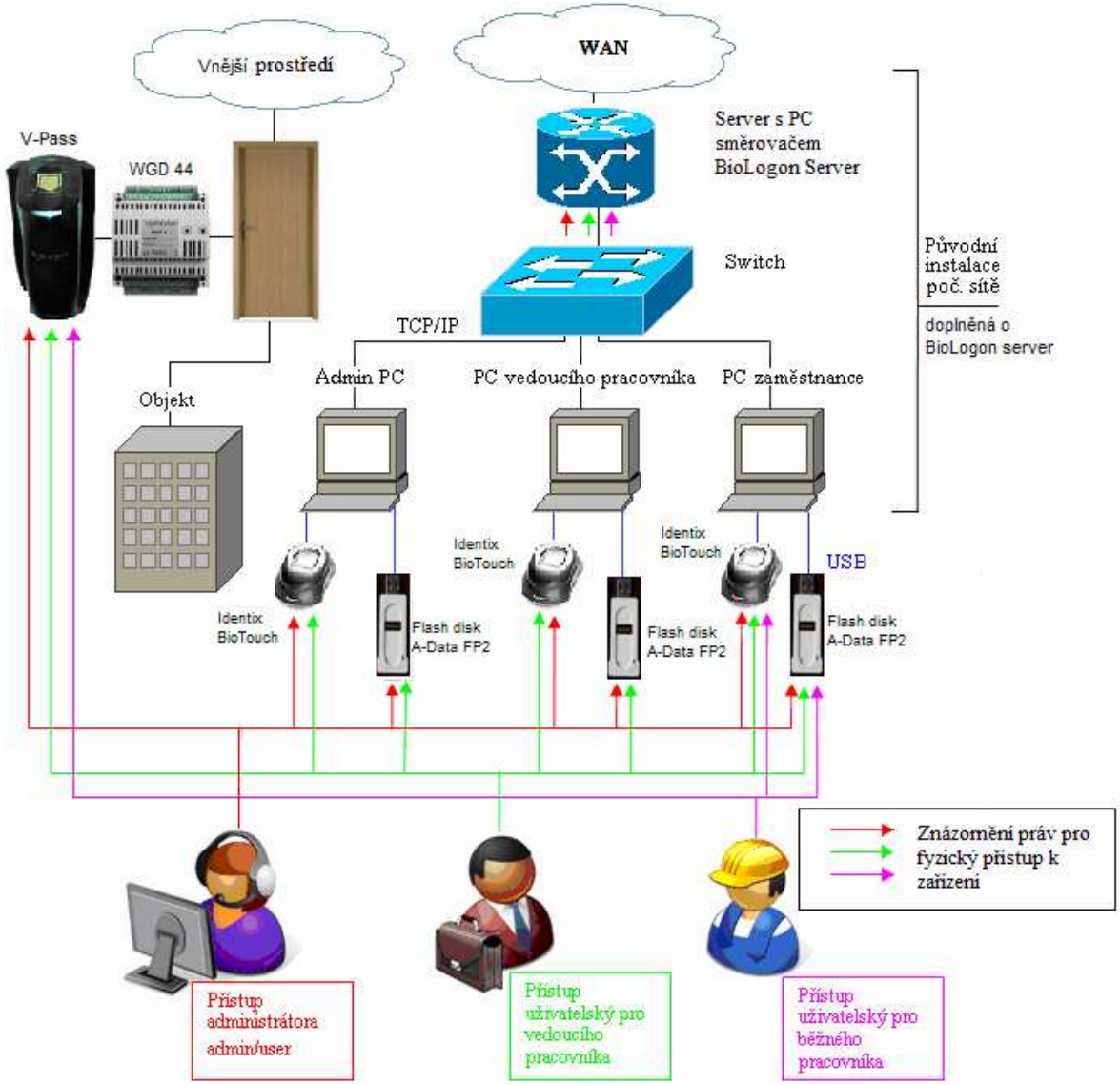
Návrh je vyřešen tak, že řídící jednotka MCA168 je propojena s PC (serverem) přes TCP/IP (LAN síť). Na PC je nainstalován APS 400 nDocházka. Do jednotky MCA168 jsou po sběrnici RS 485 připojeny čtecí moduly MREM 53 (čtečka), MRED 53 (docházka), MREP 53 (čtečka + PIN); na jedné lince můžeme realizovat maximálně 32 zařízení. To je stávající modelový přístupový systém. Do tohoto systému jsem zvolil jako převodník WGD 44, který je připojen na sběrnici RS 485. Do tohoto převodníku je přes rozhraní wiegand připojena čtečka V-Pass. Nejjednodušším způsobem jak zprovoznit komunikaci je tak, že čtečce V-Pass k biom. šabloně přiřadíme ID, které je stejné jako ID karty daného uživatele ve stávajícím systému. Popřípadě můžeme přidat uživateli další číslo karty, pokud to systém umožňuje, ale to považuji za složitější způsob. Spíše pak může nastat stav, že my si vymyslíme číslo, které může časem začít kolidovat s některou novou kartou, která předtím v systému nebyla. Tento systém pak funguje online, případně i autonomně. Správu karet pak lze realizovat online, pouze přidávání biom. šablon musí být realizováno u každé čtečky zvlášť.

Pro ochranu sítě byl zvolen Biologon, ten již umožňuje administrátorovi pohodlnou správu a přidávání uživatelů z jednoho PC. Čtečky BioTouch pracují se softwarem Biologon mohou pracovat i autonomně při výpadku síťových prvků. Architektura je taková, že na lokálním PC je nainstalován Biologon klient v jehož databázi jsou pro případ výpadků sítě uloženy jen otisky uživatelů, kteří mají přístup do dané pracovní stanice. Na serveru je pak nainstalován software Biologon server, v jehož databázi jsou uloženy šablony všech uživatelů sytému.

Do každého flash disku je pak doporučeno nahrát tři sady otisků a to: administrátora, vedoucího zaměstnance a zaměstnance, pro kterého je flash disk určen. Jak již bylo zmíněno v kap. 3.3.2.

Správu systému pak lze až na malé výjimky provádět z administrátorského PC. Jedinou výjimkou je čtečka V-Pass, do které je nutno na místě zadat biom. šablonu a ID.

Zajímavostí je, že docházku pak můžeme řešit jak z kartového systému, tak i z čteček BioTouch, respektive softwaru Biologon Server. Tento návrh je už vhodný i pro pohodnou a efektivní správu v malé organizaci i o maximálním počtu 200 zaměstnancích, jak bylo zvoleno v úvodu práce.



Obr. 35. Schéma vyváženého návrhu

3.4.3 Vyvážený návrh pro modelovou organizaci

Modelová organizace stejná jako v předcházejícím případě tj. 18 zaměstnanců, z toho 4 vedoucí pracovníky, jednoho správce výpočetní techniky a 13 ostatních pracovníků. Řídící modul WGD bude použit jeden pro dvě čtečky, protože disponuje dvěma wiegand vstupy, dále pak 4 logickými vstupy (2 mag. kontakt, 2 odchodové tlačítka)

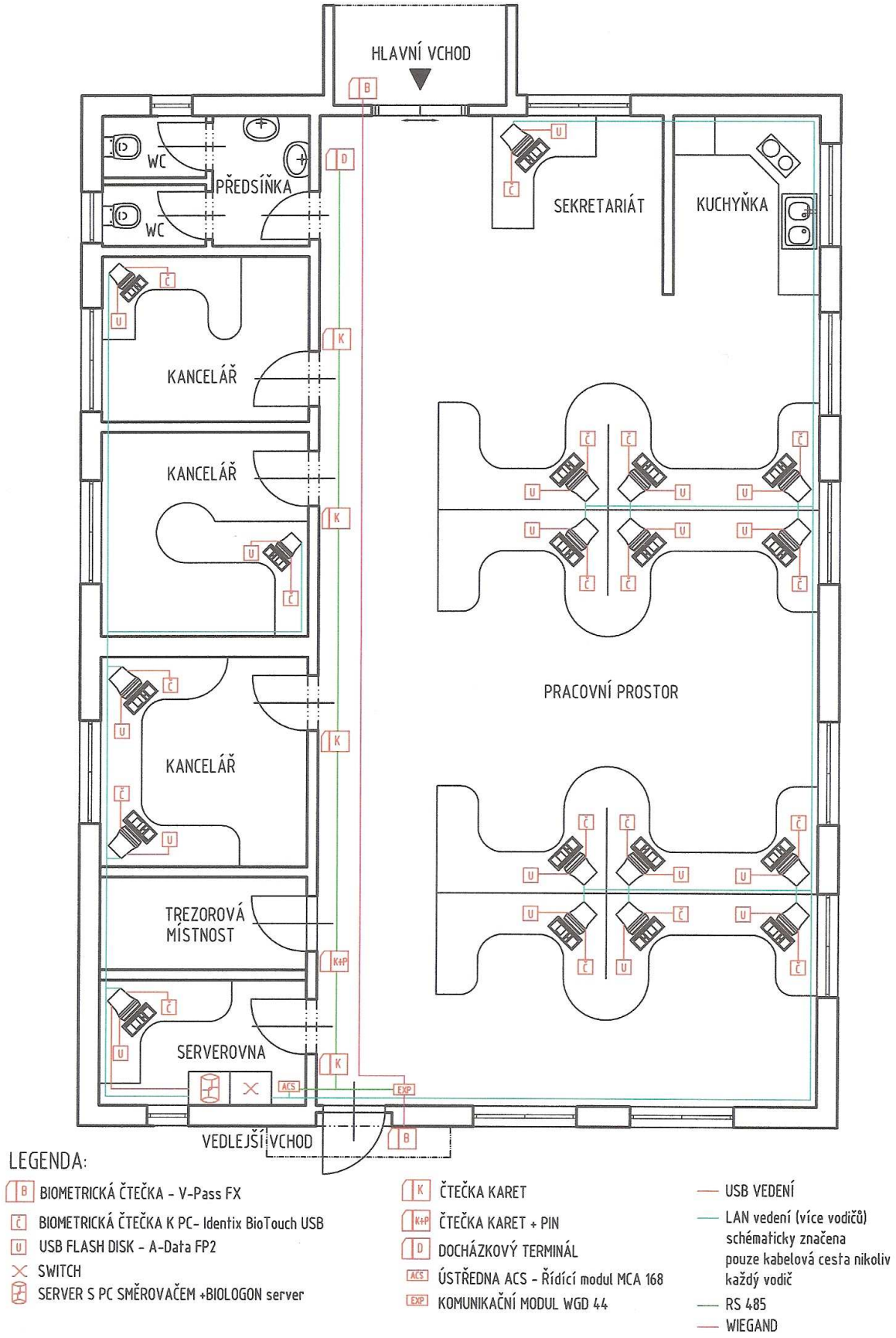
a 4 výstupními relé NC/NO, tudíž postačuje pro ovládání 2 dveří. Odchod z kanceláří je řešen odchodovým tlačítkem, v návrhu není znázorněno. Návrh pro danou fiktivní organizaci je uveden v následujícím výkrese.

Náklady na zřízení: (Náklady na vybudování kabeláže nejsou počítány)

2 x V-Pass FX	2x 28 900
1x WGD44 komunikační modul	9 950
18x Identix BioTouch USB	18x 4 650
1x Identix BioLogon Server pro 25 uživatelů	22 500
18 x A-Data FP2- 2GB	18x 400
Celkem za doplnění stávajícího systému bez DPH Kč:	**181 150**
Cena stávající instalace*:	
1x APS 400 nDocházka + Administrátor (do 50 ID)	9 620
1x řídící modul MCA168.1E	22 060
4x čtecí modul MREM 53	4x 6 700
1x docházkový čtecí modul MRED 53	7 480
1x čtecí modul s klávesnicí PIN MREP 53	7 480
Celkem stávající instalace bez DPH Kč:	**73 440**
Celkem stávající instalace + doplnění o biometrii bez DPH Kč:	**254 590**

*Se stávající instalací se počítá, že již je instalována v objektu, ale slouží jako celkový porovnávací údaj s nejvýkonnější variantou návrhu a jejich následnému srovnání.

Druhou variantou tohoto návrhu by mohl být lepší cenový kompromis. Kdy bychom pro přístup k počítačové síti a PC využili software Biologon v kombinaci se čtečkami BioTouch. K ochraně dat flash disky A-Data FP2. Ale k přístupu do objektu by byly využity dva biometrické zámky FPL – 250. Pod podmínkou použití běžných otevíracích dveří, nikoliv posuvných nebo otočných. Další podmínkou by bylo to, že tento zámek by nebyl propojen se stávajícím systémem. Cena této varianty doplnění by pak byla 143 390 Kč bez DPH, což je úspora 52 755 Kč.



Obr. 36. Zobrazení vyváženého návrhu pro modelovou organizaci

3.5 Nejvýkonnější varianta návrhu

Jde o „nejlepší“ variantu návrhu. Kdy je v objektu nějakým způsobem zajištěna kontrola přístupu ACCESS i ochrana výpočetní techniky a poč. sítě. Instalace je však pro dnešní dobu již zastaralá. Proto je požadováno kompletní přebudování systému, vytvoření komplexní biometrické aplikace s mnoha i nadstandardními funkcemi. Je kladen důraz na jednoduchost systému, vzájemnou kompatibilitu a uživatelskou příjemnost. Předpokládáme vybudovanou síť Ethernet 100Mb/s. Opět je předpokladem, že na serveru běží operační systém MS Windows 2000 server nebo 2003 server jako je tomu v dnešní době ve většině menších organizací.

3.5.1 Vybrané prvky pro nejvýkonnější variantu návrhu

Krom flash disku **A-Data FingerPrint Disk (A-Data FP2)** z kapitoly 3.1.3.1, který má v tomto návrhu složit k zabezpečení přenášených dat jsou všechny ostatní prvky od společnosti Ekey. Produkty této společnosti je vyřešen jak přístupový systém do objektu, tak i přístup do počítačové sítě. Jde o komplexní řešení. Je možné z jednoho administrátorského PC (ekey TOCAnet admin) s jednou čtečkou a jedním uživatelským prostředím spravovat databázi šablon a přístupových práv přístupového systému do objektu, tak i přístupu k poč. síti. Pro přístupový systém byly zvoleny čtecí zařízení **Ekey TOCAnet** (rozebrané v kapitole 3.2.2.1). Přístup k poč. síti je realizován softwarem **Ekey LOGONserver** (kap. 3.1.2.2), jemuž slouží jako přístupové čtečky **Ekey BIT**, jejíž parametry byly popsány v kapitole 3.1.1.3.

3.5.2 Architektura nejvýkonnější varianty návrhu

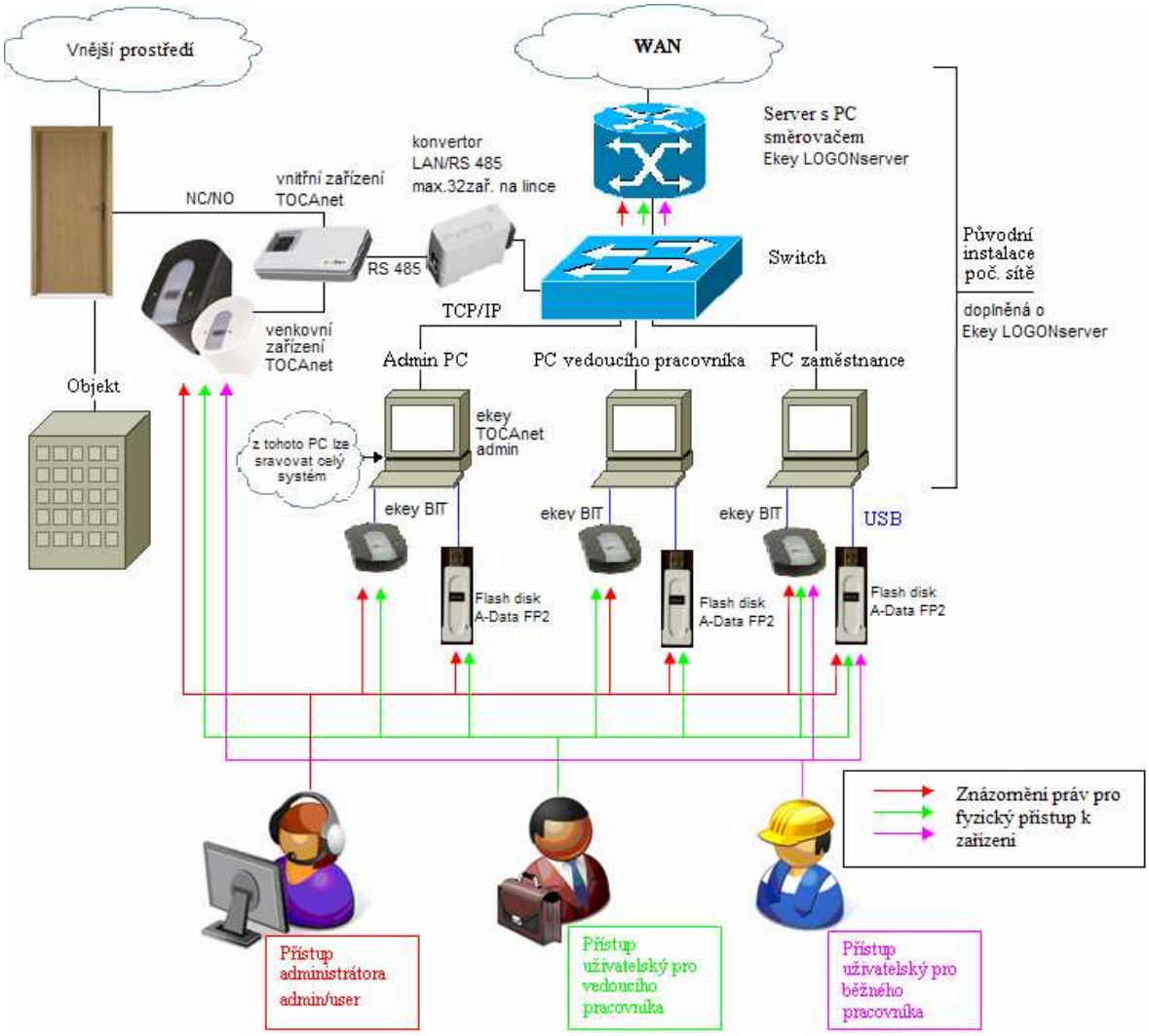
Je zde předpoklad existující LAN sítě, pokud by nebyla bylo by nutné ji vybudovat. Přístupový systém je velmi modulární a lze jej využít i pro více objektů navzájem propojených. Dále pak můžou jednotlivé čtecí terminály pracovat i autonomně, ale pouze s omezeným počtem uživatelů (a dle verze). Systém umožňuje i dvouúrovňový serverový koncept řízení. Kdy Ekey TOCAnet Masterserver je hlavním serverem (může být i vzdálený) a jsou na něm umístěny všechny šablony a přístupová práva celého systému. Na tento masterserver jsou připojeny jednotlivé terminálové servery. Ke každému terminálovému serveru jsou připojeny přes LAN/RS 485 konvertor jednotlivé přístupové terminály (max. 32 na jeden konvertor). Dále pak lze využít i USB/RS 485 konvertor.

Připojením příslušného počtu konvertorů lze dosáhnout požadovaného počtu přístupových terminálů; takřka neomezeně (jsme omezeni rozsahem sítě a kapacitou serveru). Jednotlivé terminálové servery mají uloženy pouze šablony a práva pro soubor jim podřízených přístupových terminálů. Pro příklad malé organizace si vystačíme pouze s jednoúrovňovým konceptem. Kdy k hlavnímu serveru jsou připojeny všechny přístupové terminály. Dále pak na server nainstalujeme Ekey LOGONserver, k přístupu do PC se pak využívá čtečky ekey BIT. Tato umožňuje přístup do sítě přes LOGONserver, tak i k autonomnímu PC pomocí programu přes program LOGONpro. Tento program pak dále umožňuje na pracovní stanici management přihlašovacích údajů a hesel k jiným aplikacím. LOGONpro je používán s nebo bez LOGONserver.

Jak již bylo zmíněno v úvodu této kapitoly jde o komplexní řešení od jednoho výrobce, který nám umožňuje efektivní správu a nevyvstávají problémy s kompatibilitou a nastavováním systému.

Dále pak samostatně fungujícím prvkem je právě flash disk A-Data FP2, který nemá správou s výše uvedeným systémem nic společného, ale je do tohoto návrhu zařazen stejně jako u předchozího návrhu kvůli ochraně dat, které mohou být přenášeny mezi pobočkami organizace nebo kooperujícími organizacemi apod.

Opět je to, jako předchozí varianta návrhu, systém již vhodný pro 200 uživatelů i více, dle použitých prvků a počtu zakoupených licencí apod.



Obr. 37. Schéma nejvýkonnějšího návrhu

3.5.3 Nejvýkonnější návrh pro modelovou organizaci

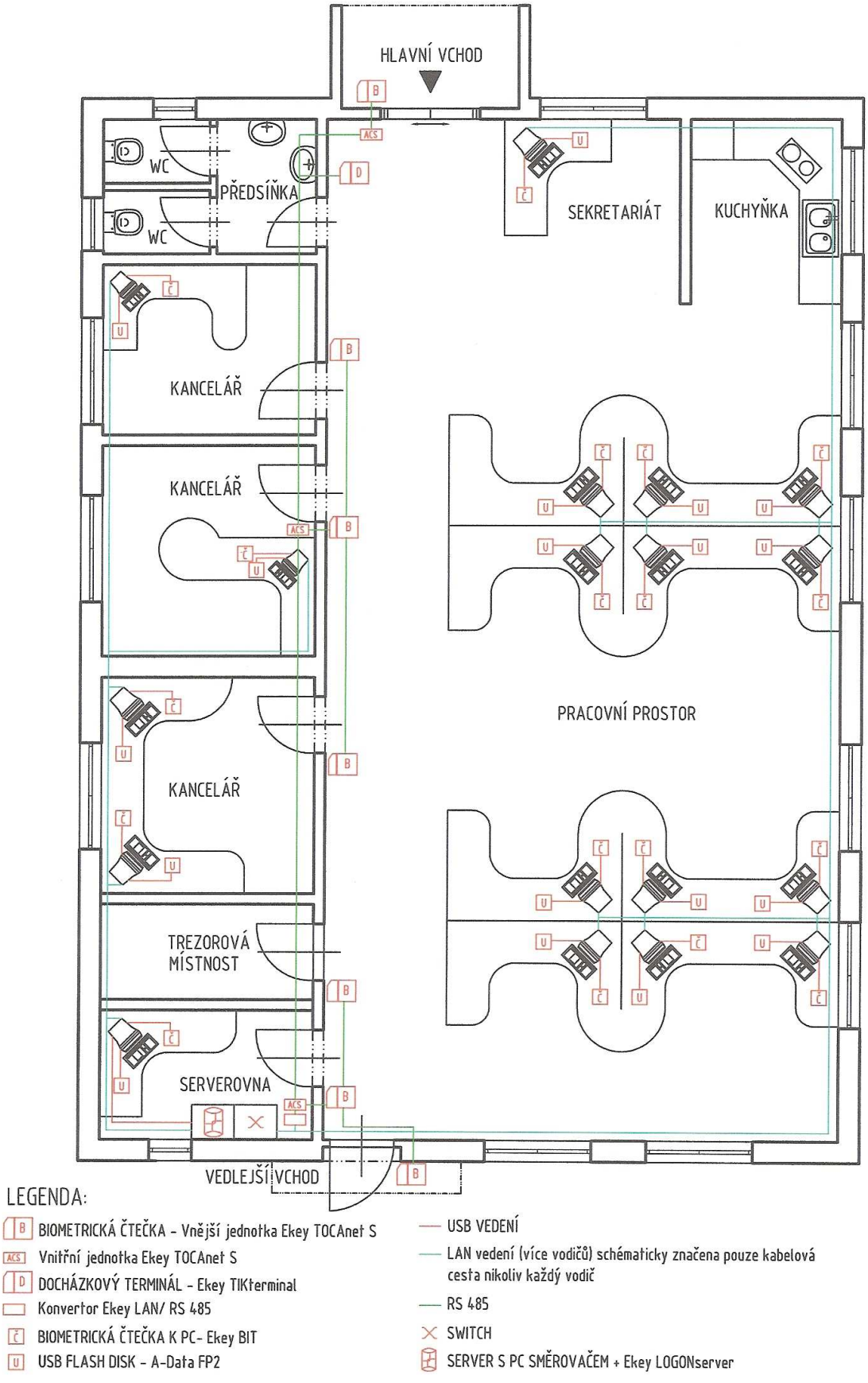
Jak již bylo zvoleno v předchozích dvou případech, tak modelová organizace má 18 zaměstnanců, z toho 4 vedoucí pracovníky, jednoho správce výpočetní techniky a 13 ostatních pracovníků. Přístupový terminál bude u obou vchodů do objektu, dále pak u všech vstupů do kanceláří, servrovny a trezorové místnosti. Na tři čtečky (vnější jednotky s čtečkou otisku), bude použita jedena vnitřní jednotka, která bude ovládat troje dveře. Odchod řešen tlačítkovým spínačem, opět neuvedeno ve výkrese. Pro docházku bude využit terminál TIK, který bude umístěn u hlavního vchodu. Čtečky pro kontrolu přístupu k poč. síti budou rozmístěny u všech PC. Pokud by tomu tak nebylo a někteří uživatelé se přihlašovali heslem, pak by tento návrh pozbýval význam. Dále pak bude k dispozici

každému zaměstnanci flash disk A-Data FP2 pro zabezpečení dat, které bude zaměstnanec přenášet.

Náklady na zřízení: (Náklady na vybudování kabeláže nejsou počítány)

3x Ekey TOCAnet S komplet	3x 19 800
(3x vnější jednotka-čtečka a 3x vnitřní jednotka) SW TOCAadmin zdarma	
4x Ekey TOCAnet S pouze čtečka (vnější jednotka)	4x 8 100
1x docházkový set TIKterminal + SW pro docházku (do 200 ID)	60 000
1x konvertor ekey LAN/RS 485	4 200
18x Ekey BIT + LOGONpro	18x 1 900
1x Ekey LOGONserver + 5 klientských licencí	16 800
+ 15 klientská licence pro LOGONserver	9 800
18 x A-Data FP2- 2GB	18x 400
Celkem bez DPH Kč:	**224 000**

Když si srovnáme celkové náklady z předchozího návrhu, vyvážené varianty, 254590 Kč bez DPH za kartový + biometrický systém a náklady tohoto nejvýkonnějšího návrhu (čistě biometrického) 224000 Kč bez DPH. Tak jasně vyplývá, že náklady na tento návrh jsou nižší. Nevyplatí se tvořit nový hybridní systém karta a biometrie. Ať už z důvodu ceny, tak i kompatibility, komplexnosti a uživatelského pohodlí. Tvořit tyto hybridní systémy má cenu pouze tam, kde se jedná o doplnění již stávajícího klasického přístupového systému o biometrické prvky.



Obr. 38. Zobrazení nejvýkonnějšího návrhu pro modelovou organizaci

4 MĚŘENÍ NA REALIZOVANÝCH BIOMETRICKÝCH SYSTÉMECH

4.1 Měření chybovosti FRR, uživatelské příjemnosti a dalších funkcí

Mohlo by se zdát, že chybovost FRR není zase tak důležitá, ale opak je pravdou, pokud biometrické prvky budou odmítat uživatele příliš často ovlivní to jeho přístup k těmto systémům. Proto je zajímavé porovnat měření této chybovosti na několika čtečkách; respektive typech senzoru. Dalším zajímavým parametrem jaké chybné odmítání má uživatel proškolený v technologii, a jaký poměr chybného odmítání má uživatel, který nebyl proškolen v přístupu k těmto systémům a byl mu pouze udělen přístup.

Reálné měření chybovosti FRR je vyšší než laboratorní měření, protože uživatelé ne vždy přistupují ideálně k čtečce. Dále je tato statistika u některých typů čteček ovlivněna okolními vlivy a podobně.

4.1.1 Měření na šablonovacím kapacitním senzoru (A-Data FP2 a Pretec i-Disk Touch)

Jelikož mají i oba flash disky A-Data FP2 a Pretec I-Disk Touch osazený stejný typ snímače, bylo měření reálné chybovosti FRR prováděno na obou discích. Měření provádělo více uživatelů, ale jen ode dvou jsou spolehlivé data o počtu měření. První uživatel je znalý technologie. Druhému uživateli byl přidán otisk do databáze, bylo mu vysvětleno, jak má s flash diskem zacházet a zbytek byl ponechán na jeho dovednostech a schopnostech učit se z chyb.

- Statistika chybných odmítnutí u uživatele znalého technologie

$$FRR = \frac{N_{FR}}{N_{EIA(EVA)}} \cdot 100 = \frac{53}{475} \cdot 100 = 11{,}2\%$$

- Statistika chybných odmítnutí u uživatele neznalého technologie

$$FRR = \frac{N_{FR}}{N_{EIA(EVA)}} \cdot 100 = \frac{61}{151} \cdot 100 = 40{,}4\%$$

U uživatele znalého technologie je chybovost FRR 11.2% v reálných podmínkách přijatelná. Avšak u uživatele, který nemá přehled o technologii, je chybné odmítání na

hodnotě 40,4%, což je absolutně nepřijatelný parametr. U tohoto uživatele vznikl ke čtečce odpor a nevyhovovalo mu její používání. Proto je důležité proškolit uživatele v používání biom. senzorů. Zvláště pak u šablonovacích senzorů všech typů je proškolení nutné. Kapacitní šablonovací senzory jsou velmi kvalitní v oblasti bezpečnosti, ale je nutné k těmto snímačům vhodně přistupovat.

4.1.1.1 Vhodný postup při používání šablonovacího kapacitního senzoru

Po zkušenostech s používáním těchto senzorů bych doporučil následující postup:

1. Při šablonování (přejíždění prstem po snímači) nevychylovat prst do stran oproti vertikální ose o víc než 3-5°.

2. Je nutné mít na paměti, že příliš suchý nebo příliš mastný prst zhoršuje proces snímání otisku

3. Rychlost přejetí článku prstu přes snímací plochu bych doporučoval asi 0,5-0,75s. Při příliš rychlém přejetí se charakteristika vůbec nenačte (kapacitní snímač dostatečně rychle nezareaguje) nebo naopak při velmi pomalém přejetí obraz splyne a je nečitelný a rozmazaný.

4. Tlak vynaložený na senzor musí být asi takový, že při přejíždění prstem ucítíme menší protitlak ve flash disku, asi takový, že se disk mírně prohne v USB portu. Při lehkém přejetí prstem senzor nezareaguje a nedojde k změření žádné charakteristiky. U příliš silného stlačení se obrazec papilárních linií slije (poznáme ze zobrazovaného obrázku otisku).

5. Při enroll procesu (nahrávání šablony) musíme dbát na to, abychom při přejíždění prstem přes senzor zabrali co největší část charakteristiky prstu. Abychom poté při následných pokusech o verifikaci nesnímali hluché místa, pro které není nahrána šablona.

6. Pozor na vlhkost a mokré prsty, na ty senzor takřka nereaguje.

Při správném dodržení procesu nahrávání šablony a následně dodržení doporučení pro verifikaci je kapacitní šablonovací snímač uživatelsky velmi příjemný a rychlý pro verifikaci.

4.1.2 Měření na RF-Field senzoru (APC Biopod)

Sama myšlenka RF technologie není špatná, ale senzor není zdaleka tak uživatelsky příjemný jako kapacitní šablonovací snímač. Snímací plocha je poměrně malá cca 7x7 mm a prst není na této čtečce pořádně stabilizován. Proto dochází velmi často k snímaní míst na prstu, pro které není uložena vhodná šablona. Při vytváření šablony musíme na tuto problematiku dbát a vhodně přikládat prst k senzoru. Této problematiky si je pravděpodobně vědom i výrobce, proto identifikační software vyžaduje při nahrávání šablony přiložit prst 8x, aby byla sejmuta co největší charakteristika. U jiných typů senzoru stačí většinou nejvíce 3x přiložit prst pro vytvoření kvalitní charakteristiky.

Měření chybovosti FRR bylo prováděno pouze osobou znalou technologie, i tak chyba FRR nastávala výrazně více jako u kapacitní šablonovací čtečky.

- Statistika chybných odmítnutí u uživatele znalého technologie

$$FRR = \frac{N_{FR}}{N_{EIA(EVA)}} \cdot 100 = \frac{48}{271} \cdot 100 = 17{,}7\%$$

Je potřeba najít vhodný postup jak přikládat prst na senzor. Když si osvojíme vhodný postup, chyba FRR nastává méně.

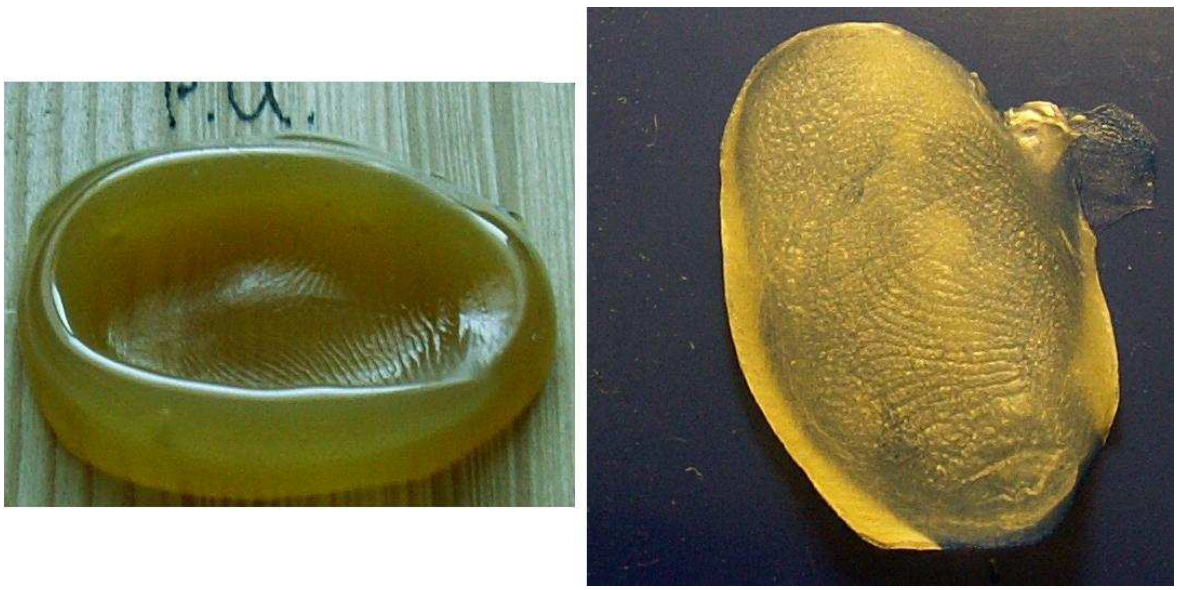
I přes tyto neduhy čtečka poskytuje zajímavý produkt pro přístup k PC a managementu hesel a přihlašujících údajů a ochraně dat.

4.2 Pokus o překonání dostupných biometrických zařízení

Tuto kapitolu jsem se rozhodl zařadit, protože jsem chtěl prakticky ověřit odolnost dostupných biom. systémů proti padělání. Obecně se považuje za nejjednodušší způsob jak tyto systémy padělat - předložit jim padělek biom. znaku. V roce 2002 byl uveřejněn výzkum profesora Tsutomu Matsumota jak vytvořit pomocí „běžně“ dostupných metod, nástrojů a možností podvrh biom. znaku. Od roku 2002 pokročily biom. technologie dále, proto jsem se kvůli nedostatku další literatury a praktických pokusů rozhodl vyzkoušet vytvořit odlitek biom. znaku z běžně dostupných možností. Postup je trochu upraven, protože např. digitální mikroskop nepovažuji za běžně dostupný předmět apod. Byl vykonán pokus jak vytvořit odlitek z otisku ve hmotě (kap. 4.2.1), tak i ze zajištěného latentního otisku (kap 4.2.2).

4.2.1 Vytvoření odlitku otisku prstu z otisku ve hmotě

Pro otisk do hmoty bylo zvoleno několik materiálů. Výzkum uvádí, že použili rozpuštěný granulovaný plast, některé české překlady pak uvádí, že lze využít klasické modelíny. Proto pokusy začaly právě modelínou, ta je však absolutně nevhodná, a při nalití teplé tekoucí želatiny dojde k zdeformování otisku. Dále pak výběr padl na modurit, který se vytvrzuje vypečením nebo vyvařením. Tento materiál se zdál docela vhodný, ale nastal problém při vytvrzování, kdy hmota výrazně změnila tvar a otisk byl nepoužitelný. Dalšími použitým materiálem byly Kera plast, plast z tavné pistole a sklenářský kyt. V těchto materiálech již otisk papilárních linií zůstává poměrně kvalitní. Následně byly ve formě vylity želatinové otisky. Nejlepší kvalita odlitku byla pořízena z otisku lepidla tavné pistole. Dle očekávání nebyl tento želatinový otisk na čtečce APC biopod funkční, vychází z principu technologie RF field. U šablonovacího kapacitního senzoru dle předpokladu došlo k setření otisku. U kapacitní čtečky V-Pass taktéž neprošel. Dokud odlitek není suchý ovlivňuje funkci kapacitních senzorů, jakmile vyschne, začne se drolit a je takřka nepoužitelný. Bylo by možné, že by mohl tento odlitek projít u optických čteček, ale nebylo možné to ověřit. Stejné výsledky jako želatina měl i silikonový odlitek.



Obr. 39. Forma na falešný otisk z lepidla do tavné pistole(vlevo), falešný otisk (želatinový)

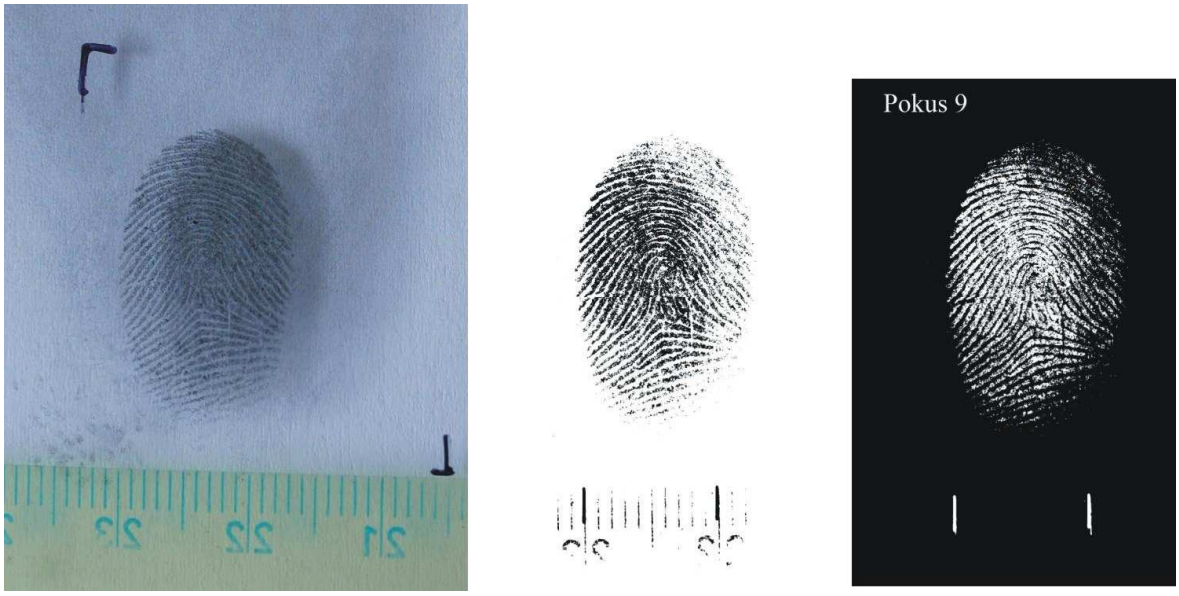
4.2.2 Vytvoření odlitku otisku prstu ze zajištěného latentního otisku

Při postupu jak vytvořit odlitek prstu z latentního otisku jsem se nechal inspirovat ve výzkumu prof. Matsumota (v kap. 1.9). Jen tento postup byl upraven, protože digitální

mikroskop není úplně nejběžnějším nástrojem. Proto bylo využito digitální zrcadlovky s makro objektivem, která byla stabilizována na stativu. K zviditelněnému otisku bylo přiložené přesné měřidlo, aby mohly být prováděny s otisky úpravy v reálném rozměru. Aby byl postup zajišťování otisku co nejjednodušší, bylo použito rovné sklo, za které byla vložena bílá podložka pro zvýšení kontrastu mezi zviditelněnýma papilárama a prostorem mezi nimi.

Obr. 40. Focení zviditelněného otisku, fotografické vybavení

Pro zviditelnění otisku nebyly použity kriminalistické prášky, ale pokusil jsem se vystačit si s běžně dostupnými materiály. Jako první byl použit mazací práškový grafit, ten se neosvědčil, sice na otisku ulpěl, ale nezvýraznil papilární linie v dostatečné kvalitě. Jako další prášek pro zviditelnění byl použit kreslící uhel, který byl rozdrcen na velmi jemný prášek. Jako třetí materiál bylo využito rozdrcených očních stínů na prášek. Oba tyto materiály již na otisku ulpěly dobře a poměrně kvalitně zvýraznily papilární linie. Zviditelněný otisk byl následně upraven několika grafickými operacemi jako: Vyvážení jasu a kontrastu, odbarvení, vyhlazení šumu, nalezení a vyznačení okrajů kontury a invertace barev. Invertaci je nutno provést, protože chceme zvýraznit vrcholy papilární linie a ne prohlubně pap. linií. Respektive chceme vysvítit na desku právě linie, aby se nám na desce vytvořili po vyleptání vytvořil zajištěný otisk prstu, do kterého odlijeme odlitek otisku. Zpět k postupu, co se zpracovaným obrazem otisku prstu. Ten vytiskneme na průhlednou fólii a přiložíme k světlocitlivé PCB (DPS) desce, a necháme vysvítit pod UV lampou (bylo použito horské slunce), poté vyvoláme v roztoku hydroxidu sodného (NaOH) a vyleptáme v roztoku chloridu železitého (FeCl3). Poté desku osušíme a můžeme do ní odlívat želatinový odlitek otisku.



Obr. 41. Nafocený otisk (z leva), otisk po zpracovávání před invertací barev, otisk po invertaci barev

Při tomto postupu nastal mnou očekávaný výsledek, kdy došlo k podleptání i nevyvolaných míst. I když byl obraz kvalitně zpracován a vysvícen, jde už o leptání velmi jemných vlásečnic (cca 0,2 mm tj. rozměr papilár), čehož je běžnými amatérskými a poloamatérskými metodami výroby DSP nedocílitelné. S výrobou DSP jsem se obrátil na Střední průmyslovou školu, kterou jsem navštěvoval, na elktrodílnu odborného výcviku. Tady se nepodařilo otisk ani nasvítit a vyvolat. Proto jsem se pokusil o tuto činnost i já, a obrátil jsem se s žádostí o pomoc na velmi dobrého známého, který má v leptání vlásečnicových spojů poměrně dobré zkušenosti. Podařilo se nám již za výše uvedeného postupu kvalitně nasvítit a vyvolat otisk, ale při leptání došlo k poměrně velkému podleptání vlásečnicových nevyvolaných míst viz. Obr. 42. Z těchto dvou postupů bylo usouzeno, že za běžných amatérských a poloamatérských podmínek je padělek otisku tímto způsobem nevytvořitelný. Domnívám se, že vhodnější postup než leptání do DPS by bylo gravitování laserem takto zviditelněného otisku. Což není běžně dostupná metoda, tak nemá cenu se jí dále zabývat.

Obr. 42. Vyvolaný otisk na DPS (vlevo), vyleptaná DPS s otiskem (vpravo)

Fotograficky bylo zajištěno cca 150 fotografií otisku, ze kterých bylo vybráno cca 11 nejkvalitnějších. Ty byly následně pomocí výše zmíněných grafických operací zpracovávány a vytisknuty na průhlednou fólii. Leptání již pak bylo prováděno pouze na dvou otiscích (pokus 9,10), protože jiné nebyly vyvolány. A výsledek je vidět na Obr. 42. Všechny zpracovávané otisky jsou vytištěny na fólii a vložené jako příloha PI. Dovoluji si tvrdit, že literatury, které uvádějí (bez praktického odzkoušení), že lze sejmout otisk ze skleničky a nebo čtečky, je scestné. A že šablonovací čtečky mají výhodu oproti normálním, že na nich nezůstává otisk, který je možné sejmout a použít k padělání apod. Protože jsem se pokoušel zajistit i otisk ze čtečky. Kupodivu fotografie byla velmi kvalitní (Obr. 21.), ale nedošlo ani k vyvolání otisku na DSP desku. Došlo pouze k částečnému vyleptání otisku otisknutého na sklo (pokus 9,10). Podotýkám, že otisk byl vytvářen vědomě za takřka laboratorních podmínek, a byl zajišťován z rovné, nikoliv oválné plochy. Běžně zanechané otisky obsahují šmouhy a nejsou tak kvalitně prokreslené aby s nimi šlo provádět tyto operace. Jejich zajištění většinou postačuje pouze pro kriminalistickou identifikaci příslušným softwarem (a ne vždy jsou otisky dostatečné kvality i pro krim. identifikaci). Nikoli pak pro průmyslové zpracovávání.

Soupis potřebného vybavení a stráveného času nad tímto pokusem:

Digitální zrcadlovka Canon EOS 300D, objektivy objektiv Canon zoom lens EF 38-76mm f/4.5-5.6 s makro čočkou 52 mm 4+ a objektiv Canon EF-S 18-55 mm f/3.5-5.6 IS

s reverzivním makroadaptérem, dálkové ovládání k řadě fotoaparátů EOS, stativ. Toto vybavení v dnešní době vyjde na cca 20tisíc. Fotografování a zajišťování otisku trvalo 6h.

Dále pak bylo zapotřebí počítač grafickými editory (Adobe Photoshop CS, Corel PhotoPaint aj.) To je při dnešních cenách cca 100 tisíc s licencemi. Výběr a zpracovávání fotografií cca 28h. Přípravy a leptání trvalo cca 3h. Náklady na pořízení všech potřebných věcí cca 600 Kč (UV lampa a roztok na vyvolání a leptání). Čas strávený na pokusu o výrobu podvrhu je cca 40h, protože následné vylití želatinou zabere zanedbatelný čas. Náklady jsou na tento pokus variabilní a záleží na dostupných zdrojích, ale pokud by se mělo pořizovat vše pak okolo 120tis.

4.2.3 Shrnutí k problematice padělání otisku a vytváření umělého odlitku otisku

Stejně jako i jiné systémy budou i biometrické oklamatelné falešným podvrhem. Ale tento podvrh nelze amatérsky nebo poloamatérsky vytvořit tak, aby byl funkční. Jako i překonávání jiných systémů a prvků platí pravidlo tří a to: pachatel musí mít **motiv** čin spáchat, pak **znalosti a dovednosti,** a poslední podmínkou je, že pachatel musí mít **prostředky** (jak materiální tak finanční).

Pokud někomu neotisknu prst kvalitně do plastické hmoty, tak nemá takřka šanci vytvořit použitelný odlitek otisku.

Otisk zfalšovat není tak jednoduché, jak jsem se prakticky přesvědčil. A navíc, dnes jsou k dispozici i nové technologie, které jsou vůči těmto pokusům odolné. Výrobci zavádí do senzorů takzvaný test živosti, který odliší živý prst od neživého. Dle mého názoru je důležitější než řešit umělé odlitky a podobně, kvalitně vyřešit ochranu komunikačního vedení těchto systémů. - Tak aby nemohlo dojít k nežádoucímu nabourání do systému. Důležitá jsou pak i režimová opatření a přístup k administrativě systému.

ZÁVĚR

Biometrická identifikace je dynamicky se rozšiřujícím oborem. Existuje mnoho metod identifikace, trh je velmi rozmanitý. Bezesporu nejvíce rozšířenou identifikací je ověřování otisku prstu. V dnešní době jde o dostupnou metodu identifikace. Cena čteček se dostává do rozumné cenové relace. Většinou jsou čtečky otisku prstu mnohem levnější, při zachování stejného stupně přesnosti, než čtečky založené na jiné biometrické metodě.

Hlavním cílem práce bylo prozkoumat možnosti nasazení biometrické identifikace pro malou organizaci. Byl vybrán právě otisk prstu, protože vychází nejlépe v poměru cena : výkon. Byly vytvořeny tři modelové typy návrhu. První se zabýval pouze vyřešením přístupu do objektu pomocí biometrických prvků a základní ochranou dat. Jde o návrh, který neoslní, ale splní základní požadavky. Druhou variantou návrhu bylo doplnění stávajícího kartového přístupového systému o biometrické prvky a vytvoření komplexnějšího řešení ochrany výpočetní techniky a dat. Jde o návrh, který je již poměrně moderní a vyznačuje vyšším stupněm bezpečnosti. Třetí variantou návrhu je pak vytvoření plně kompatibilního systému, jak pro přístup, tak i pro ochranu výpočetní techniky a dat. Systém je vytvořen na produktech jedné společnosti. Na dostupných čtečkách bylo provedeno měření spolehlivosti a prověření uživatelských funkcí.

Biometrie nám přináší, jak zvýšení uživatelského pohodlí, tak bezesporu navýšení bezpečnosti. A metody překonání „ala gumový medvídek z želatiny“ jsou v dnešní době pro padělání těchto systémů nepoužitelné.

Lze očekávat, že se bude biometrická identifikace i nadále rozšiřovat do běžných aplikací. A budeme se s ní v brzkých letech setkávat čím dál tím více.

ZÁVĚR V ANGLIČTINĚ

Biometric identification is a dynamically growing industry. There are many methods of identification, the market is very diverse. Without identifying, the most widespread, the verification of fingerprints. The method's of identification are the available today. Price readers enter the reasonable price. Most fingerprint readers are much cheaper, while maintaining the same degree of accuracy than the reader, based on other biometric method.

The main objective of this work was to explore the use of biometric identification for a small organization. It was chosen by the fingerprint, it is preferably in the ratio of price to performance. They were the three types of model design. The first dealt with only by addressing access to the building using biometrics, and basic data protection. This is a proposal which unamazed, but meets the basic requirements. The second option was to complement the existing card access card system for biometric features and the creation of comprehensive solutions to protect computer equipment and data. This is a proposal, which is already quite advanced and has more safety. The third variant of the proposal is the creation of a fully compatible, how to access, as well as for the protection of computer technology and data. The system is created on the products of one company. The available readers were made measurements of reliability and verification of user functions.

Biometrics brings us to increase user comfort, and certainly increase security. A method of overcoming the "as the rubber bear from gelatin", is today for the forgery of such systems useless.

It can be expected that biometric identification will continue to expand into mainstream applications. And we will be in the early years to meet increasingly with her.

SEZNAM POUŽITÉ LITERATURY

[1] BITTO, Ondřej. *Šifrování a biometrika : aneb tajemné bity a dotyky*. [s.l.] : Computer Media s.r.o., 2005. 168 s. ISBN 80-86686-48-5.

[2] RAK, Roman. *Biometrie a identita člověka : ve forenzních a komerčních aplikacích*. [s.l.] : [s.n.], 2008. 664 s. ISBN 978-80-247-2365-5.

[3] JAIN, Anil, ROSS, Arun, PRABHAKAR, Salil. An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology*. 2004, vol. 14, no. 1.

[4] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi*. , 2008. 58 s. Dostupný z WWW:

<http://www.fbi.vsb.cz/shared/uploadedfiles/fbi/biometricke_metody.pdf>

[5] *Pracovní dokument o biometrii* [online]. 2003 [cit. 2008-04-14]. Dostupný z WWW:
<http://www.uoou.cz/index.php?l=cz&m=left&mid=08:02:08:03&u1=&u2=&t=>

[6] KOTYK, Josef. Zabezpečení informačních technologií. *Automatizace* [online]. 2008, roč. 51, č. 5 [cit. 2009-04-15]. Dostupný z WWW: <http://www.automatizace.cz/article.php?a=2222>.

[7] RAK R., MATYÁŠ V., ŘÍHA Z. *Biometrické docházkové systémy a měření jejich výkonnosti*, Security magazín, roč. XII, 2/2005, Family media, spol. s. r. o., Praha, ISSN 1210-8723

[8] MATSUMOTA, Tsutomu. Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies: A Case Study for User Identification. In *ITU-T Workshop on Security, Seoul*. [s.l.] : [s.n.], 2002.

[9] HOLČÍK, Tomáš. Čtečku prstů překoná gumový medvídek. *Živě cz* [online]. 2002, [cit. 2009-04-19]. Dostupný z WWW: <http://www.zive.cz/Clanky/Ctecku-prstu-prekona-gumovy-medvidek/sc-3-a-106728/default.aspx>.

[10] *Biometrics* [online]. 2007 [cit. 2009-04-23]. Dostupný z WWW: <http://pagesperso-orange.fr/fingerchip/biometrics/biometrics.htm>.

[11] *Fingerprint structure imaging based on an ultrasound camera* [online]. 2009 [cit. 2009-04-23]. Dostupný z WWW: <http://www.optel.pl/article/english/article.htm>.

[12] *BIOMETRIKY* [online]. 2008 [cit. 2009-04-23]. Dostupný z WWW: <http://www.comfis.cz/biometrie>.

[13] COUFAL, Tomáš. *Co je to FingerChip* [online]. 2007 [cit. 2009-04-29]. Dostupný z WWW: <http://hw.cz/teorie-praxe/art2020-co-je-fingerchip.html>.

[14] *V-Pass FX* [online]. [cit. 2009-05-05]. Dostupný z WWW: <213.181.36.29/ap/datasheet.php?product=V-PASS-FX&loc_code=CZ>.

[15] *WGD 44E* [online]. 2007 [cit. 2009-05-05]. Dostupný z WWW: <http://www.euroalarm.cz/zabezpecovaci-technika/kotrola-pristupu-a-dochazka/interface-a-prevodniky/wgd-44e-s16199017>.

[16] *Nobility Series FP2 Flash* [online]. c2007 [cit. 2009-05-03]. Dostupný z WWW: <http://www.adata.com.tw/en/product_show.php?ProductNo=AFP2ZZZWH>.

[17] *I-Disk Touch* [online]. c2006 [cit. 2009-05-04]. Dostupný z WWW: <http://www.pretec.com/epages/Store.storefront/?ObjectPath=/Shops/Store.Pretec/Products/UFUXXX>

[18] *APC Touch Biometric Pod Password Manager, EMEA* [online]. [cit. 2009-05-03]. Dostupný z WWW:

<http://www.apc.com/resource/include/techspec_index.cfm?base_sku=BIOPOD-EC&tab=features>.

[19] *Digitus - software* [online]. 2009 [cit. 2009-05-06]. Dostupný z WWW: <http://www.digitus.cz/pristup_pc.php>.

[20] *Ekey* [online]. [cit. 2009-05-10]. Dostupný z WWW: <http://www.ekey.cz/produkty/>.

[21] *FINGER-PRO* [online]. 2007 [cit. 2009-05-09]. Dostupný z WWW: <http://www.fingerpro.cz/zamky-na-otisk-prstu.html>.

[22] *Euroalarm - Kontrola přístupu a docházka* [online]. c2007 [cit. 2009-05-10]. Dostupný z WWW: <https://www.euroalarm.cz/zabezpecovaci-technika/kotrola-pristupu-a-dochazka/>.

[23] *E.J.C. ČR s.r.o. - Přístupové systémy* [online]. c2007 [cit. 2009-05-16]. Dostupný z WWW: <http://www.ejc.cz/access.html>.

[24] *ADI - Access* [online]. c2008 [cit. 2009-05-10]. Dostupný z WWW: <http://www.adi-olympo.cz/iiWWW/cz/produkty130.nsf/wp/index>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

PC	Počítač
USB	Universal serial bus – univerzální sériová sběrnice
RS 232	Jde o sériové komunikační rozhraní
RS 485	Jde o specifikaci dvoudrátového poloduplexního multibodového sériového spoje
COM	Sériový port pro rozhraní RS 232
ACS	Přístupový systém
EZS	Elektronická zabezpečovací signalizace
CCTV	Uzavřený okruh průmyslové televize
FAR	Chybné přijetí neoprávněné osoby
FRR	Chybné odmítnutí oprávněného uživatele
IE	MS Internet Explorer
MS	Microsoft
HDD	Pevný disk (harddisk) počítače
VPN	Virtual privat network - Virtuální privátní síť
NC	Normal close
NO	Normal open
DC	Stejnosměrný proud
ID	Jedinečné identifikační číslo / identita
LAN	Local area network - lokální síť, místní síť
WAN	Wide Area Network – síť většího geograf. rozsahu (kraj, stát, i internet)
TCP/IP	Sada protokolů pro komunikaci v počítačové síti
PIN	Personal identification numer – jedinečný kód v paměti uživatele
PCB (DPS)	Deska plošných spojů

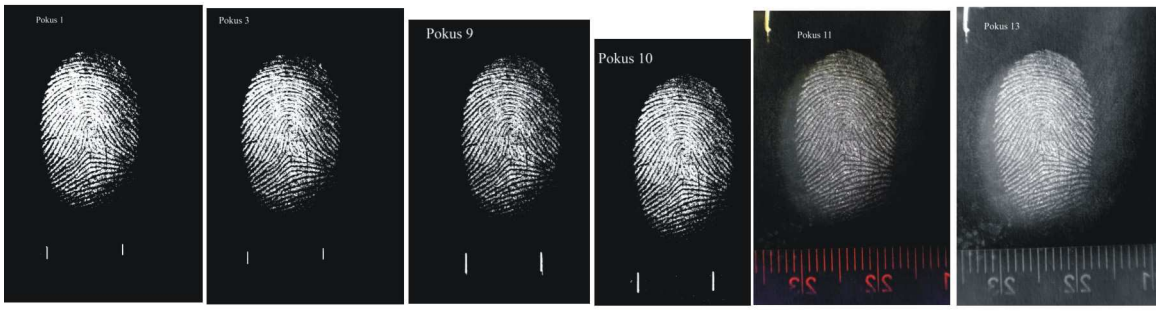
SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: OTISKY TIŠTĚNÉ NA FÓLII

Pokus 9 Pokus 10



Otisky zajištěné z čtečky

(Zde nejsou vloženy v rozměru 1:1, tisk proveden na fólii přímo z grafického editoru.)