Západočeská univerzita v Plzni
FAKULTA PEDAGOGICKÁ
KATEDRA VÝPOČETNÍ A DIDAKTICKÉ TECHNIKY

ZABEZPEČENÍ PŘÍSTUPU K POČÍTAČI A DATŮM POMOCÍ OTISKU PRSTŮ

BAKALÁŘSKÁ PRÁCE

Zuzana Bulková

Vedoucí práce: *Mgr. Petr Simbartl*

Plzeň, 2012

Prohlašuji, že jsem diplomovou práci vypracovala samostatně s použitím uvedené literatury a zdrojů informací.

Plzeň, 20. červen 2012

……
vlastnoruční podpis

PODĚKOVÁNÍ

Mé poděkování patří zejména panu Mgr. Petru Simbartlovi za vedení práce, jeho čas a nápady, kterými mi velmi pomohl. V neposlední řadě chci poděkovat své rodině a přátelům za jejich nekonečnou podporu.

OBSAH

1 ÚVOD

Moderní technologie, informatika, telekomunikace, počítačové sítě, miniaturizace, globalizace… Tyto pojmy a jejich význam, nás nutí jednoznačně označovat nejen hmotné a nehmotné statky, ale i člověka. Identifikace na základě určitých rysů sahá patrně až k počátku lidstva a s vývojem lidstva jsou na ni kladeny stále vyšší nároky. K jednoznačné identifikaci už nám dávno nestačí jména nebo jiné veřejné, popř. viditelné charakteristiky. Pro různé úrovně zabezpečení potřebujeme co nejjednoznačněji určit identitu osoby, která se snaží přistupovat k informacím.

A právě zde si nachází svoje místo biometrie. Moderní technologie nám umožňují automatizovaně identifikovat člověka na základě jeho vlastní jedinečnosti. Biometrická identifikace (resp. verifikace) využívá měřitelných, jedinečných, fyziologických znaků nebo projevů člověka k jednoznačnému zjištění (resp. ověření) jeho identity. [1]

Rychlému vývoji (urychlení a zkvalitnění) počítačového vyhodnocování otisků prstů přispělo především to, že tato technologie byla od počátku rozpracována pro policejně-soudní účely. Takže po bouřlivém rozvoji policejně-soudních aplikací následoval neméně bouřlivý rozvoj aplikací komerčně-bezpečnostních. Praktickému rozšíření přispěla především miniaturizace snímacích prvků, snižování výrobní ceny a rychlost oproti policejně-soudním aplikacím, které prohledávají velké množství vzorků, kdežto u komerčního využití dochází k porovnání v poměru 1:1 nebo *1:few* (malý okruh lidí).

Cílem této práce je popsat princip technologie snímání a vyhodnocování otisků, pojednání o komerčně-bezpečnostních aplikacích z hlediska bezpečnosti oproti jiným způsobům verifikace a také z hlediska zákona o ochraně osobních údajů. V závěru práce se pokusím prezentovat zařízení dostupná na běžném trhu a předvést funkce vybraného zařízení.

2 DAKTYLOSKOPIE OBECNĚ

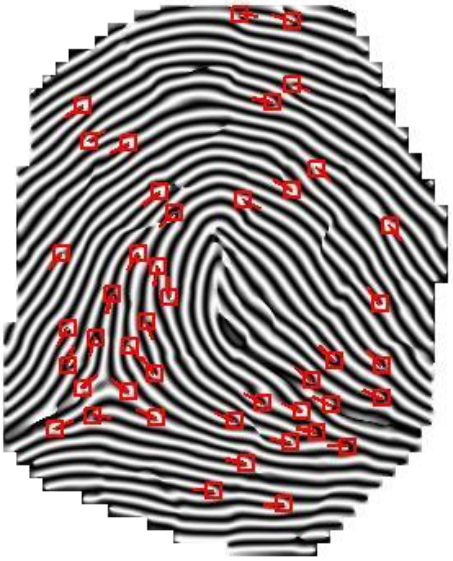
Základ daktyloskopie vychází z fyziologických vlastností kůže na lidské dlani, kde se vytvářejí papilární linie, což jsou kožní lišty na povrchu kůže.

2.1 ANATOMIE PRSTU

Papilární linie tvoří vyvýšené části pokožky, dosahující výšky 0,1-0,4 mm a šířky 0,2-0,7 mm, mezery mezi těmito liniemi se nazývají brázdy. [1] Společně tyto vyvýšeniny a brázdy vytvářejí obrazce, které jsou základem pro daktyloskopickou identifikaci osob. Tyto obrazce jsou dány geneticky a k identifikaci osob se dají využívat hlavně díky tomu, že jsou jedinečné. Pravděpodobnost, že na světě existují dva jedinci, kteří mají stejné obrazce papilárních linií, je téměř mizivá. Další výhodou je, že linie se po celý život člověka téměř nemění a jsou velmi obtížně odstranitelné. Pokud by člověk chtěl trvale znemožnit daktyloskopickou identifikaci, musel by si odstranit nejen samotné papilární linie, ale i zárodečnou vrstvu kůže.

2.2 DAKTYLOSKOPICKÉ MARKANTY

V biometrickém vzorku, otisku, můžeme najít určité charakteristiky, jež lze efektivně využít pro identifikaci člověka, tzv. markanty. V daktyloskopii tak označujeme změny v průběhu papilárních linií.



Obrázek 1: Vyznačení markant Zdroj: http://biometrics.cse.msu.edu/projects/fingerprint_reconstruct.html

2.3 HISTORIE DAKTYLOSKOPIE

Archeologické objevy dokazují, že otisky prstů byly pro identifikační účely používány již v Asýrii a Číně, minimálně 6 až 7 tisíc let př. n. l. První spis o otiscích prstů jako prostředku k zjišťování totožnosti osob pochází z Číny (618-906 n. l.), první zmínka o jejich využívání v kriminalistických procesech je z roku 1107 n. l. [1]

Základ daktyloskopii položil vědec a lékař Jan Evangelista Purkyně svojí prací z roku 1823, ve které rozlišil devět základních vzorů papilárních linií (příčné záhyby, střední podélný pruh, šikmý pruh, šikmý záliv, mandle, spirála, elipsa, kruh a zdvojený vrcholek). V roce 1880 Angličan Henry Faulds poprvé poukázal na skutečnost, že otisky prstů z místa trestného činu mohou posloužit k zjištění totožnosti zločince, v jedné ze svých prací doporučil dokonce sejmutí otisků každému zločinci, který spáchal těžký trestný čin, a uložení do sbírky pro případ, že by tento zločinec svůj čin zopakoval a udal falešné jméno. Od roku 1896 je daktyloskopie používána v kriminalistické praxi. [1]

S rozvojem vědy a techniky se začala daktyloskopie využívat i pro bezpečnostní aplikace. Jako technologie, čerstvě vyvinuté vývojáři, byly patřičně drahé, a proto si je mohly převážně dovolit jen finančně silné státní instituce. V 90. letech ale nastává bouřlivý rozvoj informačních technologií, mikroelektroniky a komunikací (Internet, osobní počítače, mobilní telefony), a proto začínají tyto technologie pronikat i do komerční sféry.

2.4 DŮLEŽITÉ POJMY BIOMETRIE

Identifikace – proces, při kterém je určována identita uživatele. Biometrický systém získá vstupní informaci, kterou porovnává se vzorky všemi uloženými v databázi (šablonami) a na základě shody identifikuje uživatele.

Verifikace – proces, při kterém se systém snaží potvrdit identitu uživatele. Biometrický systém získá biometrickou vstupní informaci a také informaci o identitě uživatele, následně porovnává pouze vstupní vzorek se vzorkem uloženým pod určitou identitou.

Autentizace – proces, při kterém je ověřovaný uživatel rozpoznán a na základě toho je mu přidělen určitý status, např. oprávněný přístup/neoprávněný přístup. [2]

3 TECHNOLOGIE SNÍMÁNÍ A VYHODNOCOVÁNÍ OTISKŮ PRSTŮ

Tato kapitola bude věnována jednotlivým senzorům, zpracování nasnímaných obrazů a negativním faktorům, které mohou ovlivnit snímání a výsledný obraz.

3.1 SNÍMÁNÍ OTISKŮ PRSTŮ

Snímání otisků prstů lze rozdělit do dvou základních skupin:

- Klasické snímání daktyloskopických stop – např. pomocí tiskařské černě
- Bezprostřední snímání daktyloskopických otisků – pomocí snímacího senzoru

My se zde budeme zabývat aplikacemi komerčně-bezpečnostního charakteru, pro které je typické bezprostřední snímání daktyloskopických otisků. Pro toto bezprostřední snímání se velmi často využívá anglický termín *live-scanning.* Pojmem *live-scanning* se v praxi rozumí všechny technologie snímání daktyloskopického otisku a jejich automatický převod do digitální podoby. Pod pojmem *live-scanner* se v praxi dnes chápou tedy všechna technologická zařízení, které buď snímají otisky z přikládaných prstů nebo dlaní ke snímači, nebo skenery, které převádějí obraz papilárních linií z daktyloskopických karet do digitální podoby.[1]

U dnešních snímačů se nejčastěji využívá dvou metod snímání otisků – statické snímání a snímání šablonováním (průtahové). Při statickém snímání uživatel pouze přiloží prst na snímač a není potřeba žádného jiného pohybu, aby byl otisk sejmut. Snímání šablonováním spočívá v tom, že uživatel přejíždí prstem přes úzký snímač, který snímá obraz papilárních linií pomocí pásů a sestavuje z nich finální podobu celého otisku prstu. U komerčně-bezpečnostních aplikací se častěji využívá metoda snímání šablonováním, především kvůli velikosti snímače, který je často integrován přímo v zařízení. [3]

Snímací senzory lze primárně rozdělit podle způsobu kontaktu snímaného povrchu tkáně se senzorem, na senzory kontaktní a bezkontaktní.

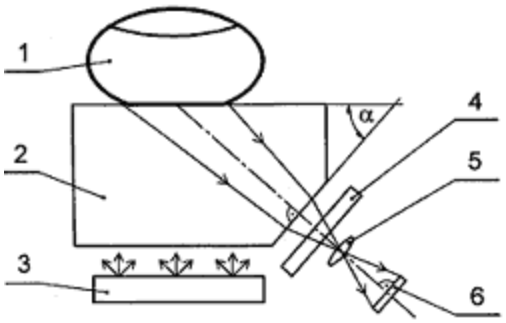
3.1.1 KONTAKTNÍ SENZORY

OPTICKÉ SENZORY

- FTIR
- Optovláknový
- Optoelektronický

Optické senzory se začaly používat v 70. letech. Tyto senzory jsou založeny na technologii *FTIR – Frustrated Total Internal Reflection*. Část prstu přiložená na plochu senzoru, skleněný nebo plastový hranol, je osvětlována laserovým paprskem a prvek CCD[1] (nebo CMOS) snímá odrážený světelný tok přes optickou čočku. Množství odráženého světla je závislé na hloubce papilárních linií a brázd. CCD prvek má nastavenou citlivost tak, aby neregistroval odraz od brázd, který je menší než odraz papilárních linií. Výsledný obraz může být ovlivněn potně-tukovým výměškem nebo také znečištěním senzoru. [1]

Nevýhodou těchto senzorů je především velikost a znečišťování senzoru. Kvalita obrazu je velmi dobrá.



1. Prst
2. Snímací hranol
3. Osvětlovací soustava
4. Optický filtr
5. Snímací objektiv
6. Maticový CCD prvek

Obrázek 2: Schéma optického senzoru Zdroj: http://www.zld.cz/cinnost/vyvoj/biometrie/sni_opt.php?p=2

Optovláknový senzor je další optický senzor založený na technologii FTIR. Hranol je nahrazen ploškou optických vláken, ke které je přímo připojen CCD nebo CMOS snímač. [4]

Optoelektronický senzor již nepracuje podle technologie FTIR, nicméně je také řazen mezi optické senzory. Tento snímač se skládá ze dvou hlavních vrstev.

[1] Elektronická součástka pro snímání obrazové informace, používaná např. ve videokamerách, fotoaparátech atd.

Horní vrstva, která je v kontaktu s kůží uživatele, je vyrobena z polymeru, který po dotyku emituje světlo závisející na přiloženém potenciálu. Polymeru se dotýkají pouze papilární linie, na rozdíl od brázd, a proto není generován stejný potenciál po celém povrchu snímače. Emitované světlo je zachyceno na druhé vrstvě, která je tvořena fotodiodovým polem. Fotodiody převádějí světelný impuls na elektrický. [4]

Tyto senzory nedosahují tak kvalitních obrazů jako senzory FTIR a jsou velmi citlivé na nečistoty.

POLOVODIČOVÉ SENZORY

- Kapacitní
- Tlakové
- Teplotní
- RF

Kapacitní senzory využívají měrné elektrické kapacity. Snímací senzor je složen z velkého množství vodivých ploch mezi sebou odizolovaných. Při dotyku kůže se senzorem se brázdy chovají jako izolant a papilární linie „přemosťují“ jednotlivé vodivé plochy. Měří se napětí a kapacitní úbytky mezi vodivými plochami. Vzniká digitální obraz papilárních linií v odstínech šedé barvy. Tyto senzory jsou citlivé na znečištění pokožky prstu, např. soli, cukry, krémy na ruce atd. Znečištění může podstatně ovlivnit vodivost kůže a tím i kvalitu snímání otisku. [1]

Výhodou těchto senzorů je velikost, vyrábí se jako plošný senzor, nebo průtahový. Senzory mohou být citlivé na elektrostatické výboje ze špičky prstu.

Tlakové senzory reagují na tlak papilárních linií na povrch senzoru. Povrch takového senzoru je tvořen elastickým, piezoelektrickým materiálem, který tlak papilárních linií transformuje do elektrického signálu. [1]

Teplotní senzory jsou založeny na rozdílných teplotách papilárních linií a brázd, které jsou způsobeny menší nebo větší vzdáleností od senzoru. Pomocí těchto senzorů lze odhalit některé pokusy o zfalšování otisku pomocí neživých napodobenin, které přirozeně nemají tak vysokou teplotu. Teplotní senzory však nedosahují tak kvalitních obrazů jako jiné.[1]

RF senzory jsou radiofrekvenční senzory, které bývají občas zaměňovány s kapacitními. „Princip činnosti spočívá v připojení generátoru střídavého signálu na dvě rovnoběžné desky (ty představují plochu snímače a ta druhá plocha otisku prstu). Jelikož je vlnová délka mnohem větší než délka desek, vyskytuje se pouze složka elektrického pole, bez pole magnetického. Pokud tedy jedna z desek bude náš otisk prstu, tvar pole se změní a bude kopírovat tvar linií, tzn. výběžky a prohlubně. Vodivé prostředí mezi prstem a plochou je docíleno pomocí vodivé plochy kolem každého snímače, to znamená, že i suché prsty nejsou problémem, jelikož se pracuje s živou tkání těsně pod povrchem pokožky. Zvlněním pole, které je způsobené přiloženým otiskem prstu, dopadá na senzory signál s rozdílnou velikostí signálu. Výběžky mají větší signál a tzv. údolí nižší signál. Kapacitní senzory tak měří rozdílnou permitivitu mezi výběžky a údolími.“ [5]

3.1.2 SENZORY BEZKONTAKTNÍ

OPTICKÉ SENZORY

Bezkontaktní optický senzor může být řešen podobným způsobem jako kontaktní s tím rozdílem, že světelný paprsek umožňuje snímat otisk prstu na vzdálenost 3-5 cm. Tyto senzory mohou být řešeny pomocí vysoce kvalitního fotoaparátu. [1]

Výhodou tohoto snímače je, že se ho uživatel přímo nedotýká, snímání je hygieničtější. Senzory dosahují vysokých rozlišení.

ULTRAZVUKOVÉ SENZORY

Pomocí ultrazvukové metody jsou snímány velice kvalitní daktyloskopické otisky. Tato metoda funguje na principu vysílání akustického signálu o vysoké frekvenci (řádově MHz) směrem k prstu a snímáním odraženého-zdeformovaného signálu přijímačem. Přijímač vyhodnocuje funkční závislost mezi vyslanými vlnami a těmi odraženými.

Vzniká kvalitní trojrozměrný daktyloskopický otisk s vysokým kontrastem. Tyto senzory nejsou citlivé na nečistotu nebo vlhkost prstu. Nevýhodou je ale velký rozměr, doba trvání snímání a také vyšší pořizovací cena.

3.1.3 PARAMETRY SENZORŮ

- Rozlišení

  - Označuje počet jednotek DPI (bodů na palec). Rozlišení v rozmezí 250-300 DPI jsou minimální rozlišení, která dovolují úspěšně lokalizovat markanty v otisku. Při použití menších rozlišení se možnost extrakce informací z otisku snižuje. [6]

- Oblast

  - Jedná se o velikost snímané oblasti. Čím větší je tato oblast, tím více informací je možné zachytit a případný otisk je lépe zřetelný. Oblast o velikosti 1x1 $inch^2$(jak požaduje specifikace FBI) nebo větší je dostatečně velká pro získání plného obrazu.[6] Komerční snímače mají oblast menší, z důvodu nižších nákladů, a proto může docházet k chybám při porovnávání se šablonou.

- Počet pixelů

  - Počet pixelů lze snadno odvodit ze vzorce $rh * rw$, kde $h(výška) * w(šířka)\ inch^2$ je velikost snímané plochy a *r* je rozlišení skeneru v DPI. [6]

- Dynamický rozsah

  - Dynamický rozsah nám určuje počet bitů nutných pro zakódování hodnoty intenzity každého pixelu. Většina skenerů snímá černobílý obraz, proto odpovídající hodnota je 8 bitů (256 úrovní šedi). [6]

- Geometrická přesnost

  - Je obvykle určena maximálním geometrickým zakřivením, které způsobuje snímací zařízení. Toto zakřivení se udává v procentech s ohledem na osu *x* a osu *y*.[6]

- Kvalita obrazu

  - Tato charakteristika bere v úvahu věci jako: zda je prst vlhký či suchý, zda jsou na prstě nějaké jizvy a další faktory. [6]

3.2 POČÍTAČOVÉ ZPRACOVÁNÍ A VYHODNOCENÍ OTISKU

Počítačové zpracování otisku se dělí do tří etap: předzpracování obrazu, extrakce markant a porovnání.

3.2.1 PŘEDZPRACOVÁNÍ OBRAZU OTISKU PRSTU

Kromě kvality senzoru mají na kvalitu obrazu otisku vliv i další faktory, jako například různé šumy, což jsou všechny nadbytečné prvky v obrazu (jizvy, falešné markanty, atd.), nebo znečištění prstu, popřípadě senzoru.

Před samotným vyhodnocením je tedy potřeba upravit obraz tak, aby bylo možné z něj efektivně přečíst typické markantní body, které identifikují každý otisk. Hlavním cílem počítačového předzpracování je zvýšit kontrast obrazu a tím zvýraznit kresbu papilárních linií, a dále také odstranění všech nežádoucích šumů.

„V první fázi je použit tzv. adaptivní filtr. Získaný otisk prstu je rozdělen na malé, pravidelné obrazové lokality. U každé papilární linie, procházející touto pomyslnou sítí lokalit, je znázorněn její směr. Filtr je pak následně aplikován na každý obrazový bod (pixel).“ [1 s. 225]

Tato operace se nazývá prostorová konvoluce. Pixely, které se nachází ve směru papilární linie ze stejné lokality, jsou zvýrazněny a naopak pixely, které mají jinou orientaci, jsou potlačeny. Adaptivním filtrem jsme schopni odstranit nežádoucí šumy.

Po odstranění šumů se provádí binarizace, proces, při kterém se sjednocuje odstín papilárních linií na jeden odstín šedi a odstín pozadí kresby na druhý odstín. Původních 256 odstínů šedi je tedy převedeno pouze do dvou binárních hodnot.

Poslední fází předzpracování obrazu otisku prstu je tzv. skeletizace. Jedná se o ztenčování čar jednotlivých papilárních linií na šířku jednoho pixelu podle speciálních algoritmů. Pomocí skeletizace je odstraněn problém s duplicitou bodů způsobený rozvětvováním nebo ukončením tlustých čar. [1]

3.2.2 NALEZENÍ A EXTRAKCE MARKANTŮ

Základním typem markantů jsou vidlice a začátek nebo ukončení papilární linie, ostatní typy jsou od nich odvozeny, popřípadě jsou jejich kombinací.

Většina aplikací využívá právě těchto dvou základních typů markantů k vytvoření šablony, pomocí které se provádí konečné porovnání a vyhodnocování otisku.

Pomocí příslušných extrakčních algoritmů je nutné vyloučit všechny falešné markanty, které nepatří mezi základní dva typy. Vyloučeny jsou také přímočaré jizvy, jež přerušují kresbu papilárních linií a hraniční body obrazu otisku, které se tváří jako počátky (resp. ukončení). Každému nalezenému a uznanému markantu je přidělena informace o jeho orientaci, souřadnicích a typu (začátek, konec linie nebo rozvětvení, popř. jiný typ). Všechny tyto markanty tvoří tzv. šablonu markantů (*minutia template*). Jednotlivé body markantů se nejčastěji pospojují např. pomocí úseček nebo polygonů, tím se vytvoří vazby mezi markanty. Každý výrobce si může zvolit své vlastní grafické znázornění šablon.

Obrázek 3: Zpracování otisku Zdroj: https://dip.felk.cvut.cz/browse/pdfcache/polacz1_2008bach.pdf

3.2.3 POROVNÁVÁNÍ OTISKŮ

Vytvořená šablona se porovnává se šablonou uloženou v počítači. Ukládání originálních obrazů otisků prstů je u bezpečnostně-komerčních aplikací nežádoucí, především kvůli nebezpečí zneužití těchto biometrických dat. Proces porovnávání obecně spočívá v tom, že se porovnávají jednotlivé markanty a markanty, které s nimi sousedí. Tento vztah mezi nimi je vyjádřen pomocí souřadnic a směrových vektorů a lze ho využít pro porovnání. Pokud jsou všechny kombinace vyčerpány, nebo pokud byla nalezena shoda dostačujícího počtu markantů, porovnávání je ukončeno.

„Výsledkem porovnávání dvou obrazů otisků je tzv. skóre porovnávání (*match score*). Obvykle je to číslo od 0 do 1, nebo od 10 do 100, popřípadě jakýkoliv jiný celočíselný interval. Vyšší hodnota čísla, ležící v používaném intervalu, vyjadřuje vyšší pravděpodobnost (důvěru, jistotu) porovnávání. Jestliže je výsledek vyšší než předem stanovená prahová hodnota (*threshold*), říkáme, že otisky se shodují. V opačném případě ke shodě nedochází, otisky nejsou vzájemně ztotožněny.“ [1 s. 232]

Uživatel tuto prahovou hodnotu může ovlivňovat, existuje procedura zpětného přizpůsobení, nebo přizpůsobení předem.

3.3 PROBLEMATIKA IDENTIFIKACE OTISKU PRSTU

3.3.1 FAKTORY OVLIVŇUJÍCÍ IDENTIFIKACI

Správnost vyhodnocení je závislá především na kvalitě sejmutého obrazu. Čím méně kvalitní obraz otisku máme, tím menší je pravděpodobnost správné autentizace. Kvalitu obrazu ovlivňují různé faktory, např. dermatologické faktory, nebo také nevhodně zvolená technologie či chyby v procesu snímání.

DERMATOLOGICKÉ FAKTORY

Mezi dermatologické faktory, které ovlivňují kvalitu sejmutého otisku prstu, mohou patřit různá onemocnění kůže. Nejčastěji se vyskytují různé druhy ekzémů a lupénky, které mohou pokrývat celé dlaně a je téměř nemožné takto nemocnému člověku otisk prstu sejmout. Dále mezi tyto faktory patří „nadměrné pocení rukou“ (Palmární hyperhydróza) nebo nevýrazné otisky, což může být způsobeno naopak velmi suchou kůží na bříšcích prstů nebo příliš malými rozdíly mezi papilárními liniemi a brázdami. [3]

PRACOVNÍ FAKTORY

Také druh vykonávané práce může mít vliv na vrchní část kůže. Tento problém řeší především průmyslové firmy, které chtějí pomocí biometrických technologií zabezpečit přístup např. do budov firmy. Pracovníci takových firem často pracují ve velmi špinavém prostředí a často dochází k drobným poraněním, které mohou negativně ovlivnit autentizaci.

ATMOSFÉRICKÉ FAKTORY

Jak z předchozího textu vyplývá, biometrické čtečky otisků prstů jsou citlivé na vlhkost. Proto mohou snímání ovlivnit i atmosférické faktory, jako například teplota, vlhkost vzduchu, prašnost ovzduší atd.

CHYBY V PROCESU SNÍMÁNÍ OTISKU PRSTU

Chybami v procesu snímání otisku prstu jsou míněny především chyby ze strany uživatele, způsobené špatnou manipulací se čtečkou. Pro snímání může být důležitý i úhel přiložení prstu na čtečku. Vliv rotace způsobí pootočení markantních bodů o určitý úhel,

a proto se neshodují s originálem. V případě malých snímačů se může stát, že část prstu se snímače nedotkne, pokud na této části prstu jsou důležité markanty, nemůže dojít k identifikaci (resp. verifikaci). Častou chybou uživatele je také tlak s jakým uživatel prst na senzor přikládá. Lidé mají tendenci na senzory tlačit, to ale může zapříčinit slití některých papilárních linií a po následné binarizaci hrozí, že vznikne výrazně odlišný otisk prstu. Naopak pokud uživatel přiloží prst příliš zlehka, může dojít k vytvoření neúplného obrazu otisku.

Pravděpodobnost výskytu těchto chyb samozřejmě závisí na použitém typu senzoru. Výrobci mají snahu potlačit tyto chyby pomocí vhodných algoritmů v průběhu předzpracování obrazu otisku.

3.3.2 MĚŘENÍ VÝKONNOSTI BIOMETRICKÝCH SYSTÉMŮ

Tak, jako všechna ostatní zařízení, i biometrické systémy potřebujeme podle něčeho srovnávat. Běžnými kritérii při výběru čtečky otisků prstů, ale i jiných zařízení, je rychlost zpracování, cena, spolehlivost, uživatelská přívětivost, odolnost nebo třeba specifika provozního režimu. Existují ale i další, důležitější kritéria, ke kterým by uživatel měl přihlížet při výběru zařízení. A jelikož žádné zařízení není zcela dokonalé, je potřeba brát v potaz i určitou chybovost. Každé zařízení má tzv. práh citlivosti, na kterém závisí kvalita identifikace (resp. verifikace). S touto citlivostí souvisí dva důležité pojmy: [1]

- Pravděpodobnost chybného odmítnutí (FRR – *False Rejection Rate*)
- Pravděpodobnost chybného přijetí (FAR – *Falce Acceptance Rate*)

PRAVDĚPODOBNOST CHYBNÉHO ODMÍTNUTÍ – FRR

„Tato veličina udává, s jakou pravděpodobností bude biometrické zařízení chybovat a nerozpozná oprávněného uživatele nebo již dříve registrovanou osobu, která má v aplikaci uloženou svou referenční biometrickou šablonu.“ [1 s. 138]

Pravděpodobnost chybného odmítnutí je definována vztahem:

$$FRR = \frac{N_{FR}}{N_{EI(V)A}}$$

Kde:

N_{FR} – *Number of False Rejection* (počet chybných odmítnutí).

$N_{EI(V)A}$– *Number of Ennrole Identification (Verification) Attemps* (počet pokusů oprávněných osob o identifikaci (verifikaci).

Uživatel, který si je jistý tím, že mu oprávnění náleží, musí pokus o identifikaci (resp. verifikaci) opakovat. Tento jev není u komerčně-bezpečnostních aplikací příliš závažný, jedná se spíše o marketingový problém. Uživatel, který je takto odmítnut, logicky ztrácí důvěru v dané zařízení. [1][3]

PRAVDĚPODOBNOST CHYBNÉHO PŘIJETÍ – FAR

FAR označuje pravděpodobnost, že biometrický systém provede autentizaci tak, že přijme nesprávnou osobu jako oprávněnou. Chybné přijetí je mnohem závažnější než chybné odmítnutí. Neoprávněná osoba získá přístup k našim datům, která může zcizit nebo poškodit.

Pravděpodobnost chybného přijetí je definována vztahem:[1]

$$FAR = \left(\frac{N_{FA}}{N_{IIA}}\right) * 100\ [\%]$$

Kde:

N_{FA} – *Number of false Acceptation* (počet chybných přijetí)

N_{IIA} – *Number of Impostor Identification Attemps* (počet všech pokusů neoprávněné osoby o přijetí)

VZTAH MEZI FRR A FAR

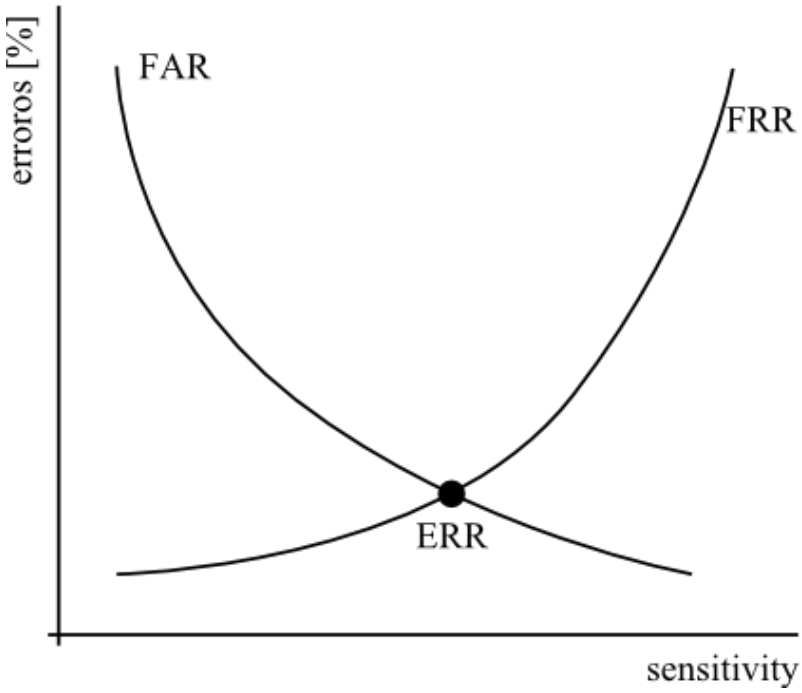
Ideální zařízení/aplikace nevykazuje žádnou chybovost, nespolehlivost. Všechny prověřované osoby jsou 100% rozpoznány; tj. neexistují ani neoprávněné odmítnuté, ani neoprávněné akceptované osoby. V tomto případě platí:

$$FAR = FRR = 0$$

„Ideální zařízení ale v praxi neexistuje. Každé reálné zařízení je různě citlivé na všechny vlivy, které ovlivňují jeho výslednou činnost. U většiny zařízení je možné

v určitém rozsahu regulovat vstupní citlivost, jež se pak odráží ve výsledcích porovnání předkládané a vzorové identity konkrétní osoby.“ [1 s. 140]

Pokud chceme vyloučit možnost, že se kvůli chybě do našeho systému dostane neoprávněný uživatel, musíme pomocí nastavení prahu citlivosti snížit pravděpodobnost FAR. Snížením hodnoty FAR se ale zvýší hodnota pravděpodobnosti chybného odmítnutí (FRR). Z toho vyplývá, že nestačí znát pouze jednu hodnotu FAR nebo FRR, ale obě hodnoty, anebo lépe - hodnotu v bodě EER. *Equal Error Rate* (EER) je bod, ve kterém se křivky FAR a FRR protínají. Tento bod slouží pouze pro porovnávání dvou zařízení. Nemá žádný jiný význam, než vztah těchto dvou křivek.



Obrázek 4: Vztah FAR a FRR Zdroj:
http://access.feld.cvut.cz/rservice.php?akce=tisk&cisloclanku=2010110002

Existují i další hodnotící kritéria, např. FMR (*False Match Rate*) vyjadřující míru chybné shody u kvalitních obrazů otisku prstu; FNMR (*False Non-Match Rate*); FTA (*Failure To Acquire Rate*) vyjadřující míru neschopnosti nasnímat; FTE (*Failure To Enroll Rate*) nebo FTM(*Failure To Match Rate*), který vyjadřuje míru neschopnosti porovnat otisk se šablonou.

4 VYUŽITÍ ČTEČKY OTISKŮ PRSTŮ PRO ZABEZPEČENÍ DAT

Jak již bylo zmíněno v kapitole 1.3, v 90. letech 20. století začaly čtečky otisků prstů pronikat do bezpečnostně-komerční sféry.

Velmi hojně se biometrických čteček využívá u docházkových systémů ve firmách. Tyto docházkové terminály mohou být řešeny více způsoby, např. jako kombinace čtečky otisků prstů a čtečky karet nebo s klávesnicí pro zadání přístupového kódu. Terminály se nejčastěji dělí na vnitřní a vnější. Mimo docházkových terminálů se můžeme setkat i se samotnými zámky s autorizací otisku prstu, tyto zámky se instalují přímo na dveře, ve většině případů fungují na baterie a nepotřebují žádné další propojení s počítačem. Dalším zajímavým využitím čteček otisků prstů je automobilový imobilizér, který po přiložení prstu odblokuje startování (startér vozu). [7]

Stále častěji se ale setkáváme s využitím biometrických čteček pro zabezpečení osobních počítačů, mobilních telefonů, tabletů atd. a dat v nich uložených.

4.1 ZAŘÍZENÍ DOSTUPNÁ NA BĚŽNÉM TRHU

4.1.1 USB ČTEČKA OTISKŮ PRSTŮ

Jednou z dostupných variant čteček otisků prstů je USB čtečka, která se připojuje k počítači pomocí rozhraní USB s využitím technologie Plug&Play.

Jako příklad zde uvádím čtečku otisků prstů firmy Suprema Inc. BioMini Plus.

Obrázek 5: BioMini Zdroj: http://www.electronicsecure.com/sites/default/files/styles/large/public/Suprema_Biomini_USB_Fingerprint_Reader.jpg

SPECIFIKACE

Snímač	Optický, povrch s odolností proti poškrábání
Rozlišení	500 DPI, 256 odstínů šedi
Snímaná plocha	15.5 x 18.8 mm
Velikost obrázku	260 – 340 px
Rozhraní	USB 2.0 High speed/Full speed, Plug & Play
OS	Windows 7, Vista, XP, 2000, ME, 98/Linux
Provozní teplota	-10~50℃
Osvědčení	CE, FCC, KCC, WHQL
Normy	ISO19794-2, ANSI-378, WSQ
Rozměr (š x d x v)	66 x 90 x 58 mm

Tabulka 1: čtečka BioMini

BioMini Plus patří mezi velmi výkonné čtečky, které dokážou rozpoznat i neživé otisky (plastické napodobeniny atd.). Cena této čtečky otisků prstů se pohybuje okolo 4 000kč. [8]

4.1.2 FLASHDISK S INTEGROVANOU ČTEČKOU OTISKŮ PRSTŮ

Tato zařízení na náš trh dodává především firma Trancend, která vyrábí řadu flashdisků JetFlash. Flashdisky zaměřené na bezpečnost a šifrování nesou označení JetFlash®220. Mají kapacitu 4, 8 a 16 GB a kromě ukládání dat umožňují i jejich šifrování a zabezpečení pomocí čtečky otisků prstů. Čtečku nemusíme využívat pouze pro zabezpečení dat na flashdisku, ale můžeme ji využívat podobně jako předchozí USB čtečku otisků, pro přihlašování na webové stránky nebo pro uzamknutí PC.[9]

Obrázek 6: JetFlash 220 Zdroj:
http://www.mytrendyphone.co.uk/images/51287_transcend2011.jpg

SPECIFIKACE

Snímač	Průtahový, kapacitní
Rozhraní	USB 2.0
OS	Windows 7, Vista, XP
Certifikace	CE, FCC, BSMI
Šifrování	AES256
Rozměry a hmotnost	70.0 mm x 20.5 mm x 11.0 mm, 13 g
Přenosové rychlosti	Čtení: 10 MB/s, zápis: 3 MB/s
Kapacita	4, 8, 16 GB

Tabulka 2: JetFlash 220

Software této čtečky také umožňuje vytvoření soukromého chráněného oddílu na disku. Cena JetFlash®220 se pohybuje v rozmezí 250 – 600 Kč. [10]

4.1.3 ZAŘÍZENÍ S INTEGROVANOU ČTEČKOU OTISKŮ PRSTŮ

Zařízení s integrovanou čtečkou otisků, se kterým se nejčastěji setkáme, jsou notebooky. První notebook s integrovanou čtečkou představila v roce 2004 firma IBM (dnes Lenovo), byl to model ThinkPad T 42. Notebooky ThinkPad se už v té době řadily mezi velmi kvalitní a čtečka otisků prstů nebyla jediným bezpečnostním prvkem. Tyto notebooky byly například vybaveny technologií APS (Active Protection System), která chrání pevný disk při pádu notebooku. Uvnitř ThinkPadu je čidlo, které rozpozná zrychlující se pohyb notebooku, který by mohl odpovídat pádu, v tomto případě APS spustí parkování hlav pevného disku tak, aby při případném nárazu nepoškodily roztočené plotny. Dalším zajímavým bezpečnostním prvkem je čip ESS (Embedded Security Subsystem), který zajišťuje ochranu dat šifrováním obsahu. ThinkPad T42 firmy IBM nezůstal dlouho jediným notebookem se čtečkou otisků na trhu, postupně se přidali i další výrobci notebooků. Dnes se kromě značky Lenovo velmi často setkáme s notebooky HP, a dále také Acer, Toshiba nebo například Fujistsu.[11]

Obrázek 7: čtečka otisků ThinkPadu L420 Zdroj: http://www.lenovoblog.cz/2011/09/thinkpady-l420520-otisk-prstu-misto.html

U většiny těchto zařízení se využívá průtahového snímače teplotního, kapacitního nebo RF. Velkou výhodou těchto snímačů je jejich malý rozměr, proto se s nimi můžeme setkat i na malých zařízeních jako jsou tablety, mobilní telefony nebo počítačové myši. Na druhou stranu jsou ale některé tyto snímače citlivé na znečištění pokožky prstu nebo její vlhkost, a proto se může stát, že snímač otisk vyhodnotí nesprávně.

4.2 AUTHENTEC

Nejčastěji se u notebooků, ale i jiných přenosných zařízení, setkáme se čtečkami otisků prstů společnosti AuthenTec. Tato společnost se zabývá komplexním zabezpečením organizací a jednotlivců prostřednictvím otisků prstů. Na trh dodává velké množství senzorů, které do svých zařízení integrují společnosti jako Alcatel-Lucent, Cisco, Fujitsu, HBO, HP, Lenovo, LG, Motorola, Nokia, Orange, Samsung, Sky, a Texas Instruments. Kromě výroby senzorů AuthenTec vyvíjí i software pro správu identity nebo také šifrovací technologie pro širokou škálu aplikací a VPN[2].

[2]Virtuální privátní síť

Nejnovějším senzorem společnosti AuthenTec je AES2665. [12]

SPECIFIKACE

Snímač	Průtahový, RF
Rozlišení	500 DPI
Provozní teplota	0 - 70° C
Povrch	Odolný proti nárazu a poškrábání
Šifrování	AES256
Rozměry	22 x 14,6 x 3,1 mm
Rozhraní	USB

Tabulka 3: AuthenTec AES2665

Obrázek 8: AES2665 Zdroj: http://authentec.com/a/Production/smartsensors_pc/AES2665.aspx

4.3 SOFTWARE

Abychom mohli se čtečkou otisků pracovat, potřebujeme k ní přistupovat pomocí ovládacího softwaru. Uživatel má možnost využívat software dodaný výrobcem, nebo si může zakoupit jiný, který jeho čtečku otisků podporuje. Běžný software umožňuje registraci jednoho a více uživatelů, kteří se mohou pomocí čtečky otisků přihlašovat do operačního systému nebo uzamykat počítač. Další funkce závisí na konkrétním programu, jako příklad uvedu funkci One Touch Internet programu DigitalPersona Fingerprint Suite, která umožňuje přihlásit se k internetovým stránkám a k heslem chráněným programům.[13]

5 POHLED NA OTISKY PRSTŮ Z HLEDISKA OCHRANY OSOBNÍCH ÚDAJŮ

„Osobní údaje se mohou stát bránou do soukromí všech. Je jen na každém z nás, koho necháme vstoupit, koho necháme projít a koho necháme před těmito pomyslnými branami stát.“ [14]

V době, kdy se informační technologie staly každodenní součástí našich životů, se stále více setkáváme s problematikou ochrany osobních údajů. Abychom mohli využívat nějakou službu na Internetu, je po nás stále častěji vyžadována registrace, při které zadáváme více či méně osobních údajů, tyto údaje jsou uchovávány v databázích, stejně tak jako údaje, které poskytujeme jiným organizacím (členství v nějakém klubu, mobilní operátoři, atd.). Kdyby tyto databáze byly veřejné a mohl s nimi kdokoli jakkoli nakládat, byl by to zásah do našeho soukromí, který by nám byl velmi nepříjemný.

5.1 OSOBNÍ ÚDAJE A OCHRANA OSOBNÍCH ÚDAJŮ

„Osobní údaje (někdy též osobní data) jsou jakékoli informace vztahující se ke konkrétní fyzické osobě. Nemusí jít vždy o údaje identifikační (jméno, příjmení, rodné číslo, fotografie, otisky prstů), ale i o jiné údaje, které souvisejí se životem určité fyzické osoby (např. velikost oblečení, členství v politické straně, vlastnictví nemovitostí, provozování koníčků).“ [14].

Ochrana osobních údajů je definována zákonem č. 101/2001 Sb., o ochraně osobních údajů a o změně některých zákonů a dalšími právními předpisy. Tento zákon se převážně zabývá zpracováním osobních údajů, definuje povinnosti správce (zpracovatele) a práva subjektu údajů (osoby, jejíž osobní údaje jsou zpracovávány). [14]

5.2 OTISKY PRSTŮ

Otisky prstů, ale i ostatní biometrické údaje, patří mezi naše citlivé osobní údaje, a proto je jejich ochraně věnována zvýšená pozornost. Nelze se ale spoléhat na to, že každý udělá přesně to, co mu zákon ukládá, a proto bychom se měli vždy zajímat o to, komu své biometrické údaje svěřujeme, jaké bude jejich využití a jak budou chráněny, aby nedošlo ke zneužití těchto údajů. Pokud někdo získá nějaký náš PIN nebo klíč, je to něco úplně jiného, než když jsou nám zcizeny otisky prstů. PIN nebo klíč si můžeme

kdykoli zvolit jiný, kdežto otisk prstu máme po celý život jen jeden a v nejhorším případě může dojít i ke zcizení identity.

Pokud chráníme naše data a počítač pomocí otisků prstů, je potřeba si uvědomit, jak a kam si program ukládá šablonu otisku prstu, aby mohlo být provedeno porovnání při autentizaci. Ukládání celých šablon otisků prstů do počítače není bezpečné a v případě většího množství uživatelů mohou šablony zabírat velké množství místa na disku. Proto se často využívá ukládání a porovnávání kódu, který se z otisku vygeneruje, z tohoto kódu pak nelze zpětně vytvořit grafickou podobu otisku. Nedochází tak tedy k žádnému shromažďování citlivých osobních údajů ani jinému nakládání s otisky, a proto je takový způsob řešení, z hlediska ochrany osobních údajů, v pořádku. [15]

Výše uvedené se týká především soukromých čteček otisků, kde tato citlivá osobní data poskytujeme dobrovolně z vlastní vůle. Více diskutované jsou biometrické přístupové terminály, kterými zaměstnavatelé kontrolují přístup především zaměstnanců na pracoviště. Pokud totiž zaměstnanec odmítne dát souhlas ke zpracování citlivých údajů, může zaměstnavatel využití výjimky z povinnosti získat souhlas zaměstnance podle § 9 písm. h) ZOOÚ – tedy zpracování, které je „nezbytné pro zajištění a uplatnění právních nároků“.[14] Ona nezbytnost je potom posuzovaná individuálně.

5.3 NĚKTERÉ DŮLEŽITÉ VÝŇATKY ZE ZÁKONA O OCHRANĚ OSOBNÍCH ÚDAJŮ

§ 9 „Citlivé údaje je možné zpracovávat, jen jestliže

a) subjekt údajů dal ke zpracování výslovný souhlas. Subjekt údajů musí být při udělení souhlasu informován o tom, pro jaký účel zpracování a k jakým osobním údajům je souhlas dáván, jakému správci a na jaké období. Existenci souhlasu subjektu údajů se zpracováním osobních údajů musí být správce schopen prokázat po celou dobu zpracování. Správce je povinen předem subjekt údajů poučit o jeho právech podle §12 a 21“

a v několika dalších případech, jako je např. při zajišťování zdravotní péče, ohrožení osob, odhalování trestné činnosti atd.

§13 (1) „Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.“

Na ochranu práv subjektů údajů a kontrole plnění povinností správce a zpracovatele osobních údajů byl zřízen Úřad na ochranu osobních údajů.[14]

§29 (1) „Úřad

a) provádí dozor nad dodržováním povinností stanovených zákonem při zpracování osobních údajů,

b) vede registr zpracování osobních údajů,

c) přijímá podněty a stížnosti na porušení povinností stanovených zákonem při zpracování osobních údajů a informuje o jejich vyřízení,

d) zpracovává a veřejnosti zpřístupňuje výroční zprávu o své činnosti,

e) vykonává další působnosti stanovené mu zákonem,

f) projednává přestupky a jiné správní delikty a uděluje pokuty podle tohoto zákona,

g) zajišťuje plnění požadavků vyplývajících z mezinárodních smluv, jimiž je Česká republika vázána, a z přímo použitelných předpisů Evropských společenství,

h) poskytuje konzultace v oblasti ochrany osobních údajů,

i) spolupracuje s obdobnými úřady jiných států, s orgány Evropské unie a s orgány mezinárodních organizací působícími v oblasti ochrany osobních údajů. Úřad v souladu s právem Evropských společenství plní oznamovací povinnost vůči orgánům Evropské unie.[25a]“ [16]

6 JINÉ PŘÍSTUPY K DATŮM A POČÍTAČŮM A JEJICH SROVNÁNÍ S OTISKY PRSTŮ

Tato kapitola bude věnována dalším používaným metodám autentizace uživatelů. Jednotlivé přístupy budou porovnávány z hlediska bezpečnosti a komfortu.

Metody autentizace mohou být založeny na něčem, co uživatel zná (např. heslo, PIN), co uživatel vlastní (nějaký token, např. čipová karta) nebo čím uživatel je (biometrické informace, např. otisk prstu). [17]

6.1 VLASTNICTVÍ

Mezi identifikační charakteristiky založené na vlastnictví řadíme identifikační čísla, kódy, karty, čipy, biočipy, ale také osobní doklady nebo jméno a příjmení. Tyto charakteristiky si člověk dobrovolně vybírá a přivlastňuje, nebo jsou mu přiděleny, např. státem nebo zaměstnavateli.

6.1.1 IDENTIFIKAČNÍ ČÍSLA A KÓDY

Identifikační čísla a kódy se staly nedílnou součástí našeho života. Máme identifikační čísla (resp. kódy – kombinace znaků a čísel) pro domy, automobily, veškeré zboží a také pro lidi. Cílem personálních identifikačních kódů je jednoznačné vyjádření identity osoby a jsou tvořeny podle určitých algoritmů, např. rodné číslo je kombinací data narození, pohlaví a čísla za lomítkem. [1]

Tyto identifikační kódy jsou často jednoúčelové, slouží především pro vyhledávání v databázích, např. lékařských nebo zaměstnaneckých, pro vedení záznamů atd.

6.1.2 PLASTOVÉ IDENTIFIKAČNÍ KARTY A ČIPY

Karty jsou jedním z nejběžnějších tokenů současnosti. Téměř každý kdo využívá bankovní účet, využívá i platební kartu, která mu byla přidělena. Nejjednoduššími kartami jsou karty s *magnetickým proužkem*, kde magnetický proužek slouží jako paměťové médium, informace je zapisována do 2 až 3 stop a zakódována. Tyto karty se využívaly především jako platební a dnes jsou již na ústupu a jsou nahrazovány *čipovými kartami*. Čipové karty existují kontaktní a bezkontaktní, kontaktní karta musí být při své činnosti zasunuta ve čtecím zařízení, zatímco bezkontaktní čipové karty používají pro styk s okolím elektromagnetické vlnění a jsou napájeny z tohoto vlnění pomocí indukční smyčky, a tak se čipová karta pouze přiloží k terminálu. Můžeme se s nimi setkat například

v městské hromadné dopravě, kde slouží k zakoupení jízdenky. Čipové karty mohou být pouze paměťové, paměťové se speciální logikou (ochrana PINem atd.) nebo procesorové čipové karty tzv. smartcard. Smartcard obsahují kromě paměti i jednočipový procesor, díky kterému umožňují i kryptografické operace. [1][17][19]

Čipové karty jsou řízeny kódem, operačním systémem, který je implementován výrobcem. Operační systém je uložen zpravidla v paměti typu ROM a určuje, k čemu je možné čipovou kartu používat. Karty určené pro zabezpečení počítače a dat umožňují především přihlášení do OS, do VPN, elektronický podpis emailů a dokumentů včetně šifrování a propojení s www prohlížeči.[18]

Obrázek 9: OmniKey čtečka čipových karet CardMan3021
Zdroj: http://www.scardi.com/contents/en-us/d16_-omnikey-smart-card-readers.html

ÚROVEŇ ZABEZPEČENÍ

Aplikační zabezpečení – autentizace držitele karty (PIN), přístupová práva k datům, čtení a zápis dat kryptografickým klíčem

Zabezpečení čipu – neduplikovatelný čip, paměť nelze smazat ani modifikovat, ochrana proti fyzickému útoku

Možnost odcizení – relativně vysoká. Většina lidí má karty uschované v peněžence, které je snadno odcizitelná. U většiny karet je vyžadován PIN, ale pokud se jedná o cílený útok, útočník může nejdříve PIN vypozorovat a pak až kartu majiteli odcizit.

OSTATNÍ ASPEKTY

Rychlost autentizace – u kontaktních čipových karet je rychlost dána především rychlostí čtecího zařízení.

Komfortnost – karta je malá, skladná, ale uživatel ji musí nosit u sebe a chránit se proti zcizení nebo ztrátě.

Kromě karet existují i jiné tokeny, jako například klíčenky nebo USB tokeny, které také obsahují čip a jsou založeny na stejných technologiích. Další možností identifikace osob by mohly být biočipy, jsou to samostatné čipy, které jsou implementovány do těla jedince, např. do zubu. Hlavní nedostatky biočipové technologie nejsou ani tak technologické, jako spíše etické, morální a právní. „Jakkoliv označovat určité osoby (byť „jen“ trestance, přistěhovalce apod.) má diskriminační charakter. Navíc nelze předvídat důsledky, kdy kriminálně jednající osoby se budou chtít zmocnit biočipu někoho jiného s cílem páchání např. finančních podvodů, zakrývání své vlastní identity apod.“ [1 s. 87]

6.2 ZNALOSTI

Nejčastěji používanými prostředky identifikace na základě znalostí jsou hesla nebo PINy.

6.2.1 PIN

Hlavním rozdílem mezi heslem a PINem je ten, že při zadávání PINu máme pouze omezený počet pokusů na uhádnutí správné hodnoty, obvykle má uživatel povolena dvě špatná zadání, pokud se mu nepodaří ani na po třetí zadat PIN správně, systém se zablokuje a na jeho odblokování je potřeba použít složitější mechanismus, jako např. delší alternativní PIN (někdy označován jako PUK) nebo je vyžadován osobní kontakt se zákaznickým centrem, např. pobočkou banky, a předložení jiných identifikačních dokladů.

PIN se obvykle skládá pouze z číslic a jeho délka je 4 až 8 znaků. PIN se využívá u dvoufaktorové autentizace, kdy je potřeba ještě navíc vlastnit autentizační předmět – token. [17]

6.2.2 HESLA

Hesla jsou v dnešní době nejběžnějším způsobem autentizace, ale zároveň nepříliš bezpečným. Uživatel pro přihlášení do systému potřebuje znát své uživatelské jméno (login) a heslo.

Běžné statické heslo je řetězec 5-10 znaků, ideálně ale 8-12 znaků, který je uživatelem snadno zapamatovatelný. Právě zapamatovatelnost hesla bývá nejčastějším kamenem úrazu. Běžný uživatel, používající slabá hesla, volí slova, která si snadno pamatuje, nejčastěji informace ze svého blízkého okolí, např. jména dětí, data narození, předměty jejich citů a zájmů atd. Tato hesla nejsnáze podlehnou útoku, ať už hrubou silou (speciální software generuje různé kombinace znaků pomocí obsáhlého slovníku), nebo sociálnímu útoku, kdy útočník využije informací získaných o uživateli.

Za silné heslo lze považovat takové heslo, které je dostatečně dlouhé (výše zmiňovaných 8-12 znaků), a které obsahuje znaky z různých skupin – číslice, malá i velká písmena nebo speciální tisknutelné znaky. Není vhodné používat jedno heslo pro přihlašování se do více systémů, ani používání stejného hesla příliš dlouhou dobu.

Kromě statických hesel existují ještě hesla dynamická. Takové heslo je použito pouze jednou a pro další použití je podle určitého algoritmu změněno. „Dynamická hesla se mění např. v závislosti na čase a místě použití hesla.“ [1 s. 88] Uživatel si může změnu hesla vypočítat sám, nebo pomocí speciálního softwaru, který je zabudován např. do čipové karty.

Dále existují jednorázová hesla. Tato hesla také nelze použít více než jednou, ale nejsou odvozována od původního hesla, jsou náhodně generována. S tímto principem se můžeme setkat např. u elektronického bankovnictví, kdy je uživateli zaslán autorizační kód na mobilní telefon, který je platný pouze pro jednu transakci a pouze na omezenou dobu.

ÚROVEŇ ZABEZPEČENÍ

Bezpečnost/prolomení hesla – Je důležité vytvořit opravdu silné heslo, jehož prolomení by zabralo příliš mnoho času, než aby se to útočníkovi vyplatilo. K vytváření silných hesel se často využívají různé mnemotechnické pomůcky. Takovou pomůckou může být převedení určitého sloganu nebo oblíbeného díla, který si uživatel

pamatuje, na řetězec. Např. Michal Viewegh: Báječná léta pod psa, 1992 převedeno na „MV:Blpp,92“. [20]

Možnost odcizení – vysledování, odhadnutí (u slabých hesel), z počítačového souboru, kde je heslo uloženo atd.

OSTATNÍ ASPEKTY

Rychlost/dostupnost – pokud heslo nosíme v hlavě, obyčejně k němu nepotřebujeme nic dalšího, přihlášení je rychlé. Dalo by se říct, že se zvyšováním zabezpečení, se zvyšuje i doba přihlašování.

Velké množství hesel – různá hesla pro různé systémy. Je náročné zapamatovat si více složitých řetězců (u silných hesel), možným řešením je ukládání do souboru, který je potřeba adekvátně chránit a přenášet.

6.3 BIOMETRIKY

Autentizace pomocí biometrik je založena na tom, čím daný uživatel je, jeho jedinečnosti. Kromě otisků prstů se pro autentizaci používá i velké množství jiných fyziologických vlastností. Autentizační technologie může být založena i na chování jedince, např. dynamika psaní na klávesnici.

Biometrické systémy nemohou absolutně určit identitu člověka. Říkají, že s určitou pravděpodobností se jedná o daného jedince. Není problém vytvořit systém, který povolí přístup jedinci pouze se 100% shodou, ale je potřeba určitou variabilitu povolit, protože výsledky měření nejsou vždy naprosto stejné, např. u otisků prstů uživatel nikdy nepřiloží prst na senzor úplně stejně, jako to udělal poprvé při snímání šablony.[17]

6.3.1 PŘEHLED ZÁKLADNÍCH BIOMETRIK POUŽÍVANÝCH V BĚŽNÉ PRAXI

OČNÍ DUHOVKA

Oční duhovka, viditelný interní orgán oka, umožňuje spolehlivou identifikaci s velkou přesností. Barevný kruh kolem zorničky se skládá z náhodně rozmístěných barevných struktur, které se s časem nemění. Ke snímání oční duhovky se používá monochromatické CCD kamery. Tato kamera využívá blízké infračervené pásmo o vlnových délkách 700nm až 900nm, které je neinvazivní pro uživatele.[1]

OČNÍ SÍTNICE

Sítnice je vrstva oka, která se nachází na zadní straně oční bulvy a slouží k detekci světla na ni přicházejícího skrze čočku. Sítnice je prokrvována pomocí cév, které tvoří jakousi mapu, která se téměř s časem nemění. Pokud je snímán obraz oční sítnice, je snímáno řečiště těchto drobných žilek a cévek. Sítnice je snímána pomocí infračerveného světla a specializovaných kamer. Systémy snímání oční sítnice jsou nasazeny především u státních bezpečnostních nebo výzkumných organizací, kde je vyžadována vysoká úroveň zabezpečení.[1]

Obrázek 10: Snímání oční sítnice Zdroj: http://www.thesolutionspk.com/site/index.php?option=com_content&view=article&id=2&Itemid=2

GEOMETRIE RUKY

„Podstatou této metody je dvou nebo třírozměrné měření délek nebo šířek jednotlivých prstů, kloubů nebo kostí.“ [1 s. 112] Kombinace těchto rozměrů a obrysu je pro každého dospělého člověka jedinečná. Uživatel položí ruku na scanner, ta je osvícena nejčastěji infračervenými LED diodami. Světlo, které je odražené od ruky, dopadne na soustavu zrcadel, od kterých se odrazí do snímací kamery. Výsledkem je silueta ruky (shora, z boku). Na této siluetě jsou následně vyhledávány identifikační markanty, podobně jako u otisků prstů.[1]

Tato metoda paří k prvním metodám užívaným pro bezpečnostně-komerční účely a také je to první biometrická metoda použitá pro počítačovou verifikaci. Je to prostředek

pro rychlou verifikaci, nikoli identifikaci. Používá se především pro kontrolu přístupu osob do budov.

Obrázek 11: Snímač geometrie ruky Zdroj: http://www.ir-ssi.com/contents/144/386.html

ROZPOZNÁNÍ HLASU

Rozpoznávání osob na základě charakteristik hlasu a řeči se hojně využívá v kriminalistice a soudnictví, tento obor byl označen jako forenzní fonetika. Kriminalisté se nejčastěji snaží identifikovat osobu z telefonátů a nahrávek odposlechů, což je nelehký úkol, především kvůli kvalitě nahrávek.

Obecné systémy pro rozpoznávání mluvčího můžeme klasifikovat podle toho, zda jsou textově závislé (systém po uživateli vyžaduje stejný text při registraci i při následné autentizaci), nezávislé (žádný konkrétní text, pro odposlechy) nebo s textovou výzvou (systém si vyžádá přečtení náhodné sekvence slov). [1]

Rozpoznávání hlasu je často označováno jako méně přesné, ve srovnání s ostatními biometrikami, na druhou stranu se ale uživatel nemusí ničeho dotýkat nebo se někam dívat. K autentizaci mu stačí, když promluví, což je pro člověka přirozené.

TVÁŘ

„Lidská tvář obsahuje identifikační body, které jsou specifické a časové neměnné.“ [1 s. 113] Pro rozpoznání tváře existuje velké množství metod, ale ve srovnání s otisky prstů, mají tyto metody nižší identifikační jednoznačnost. Rozpoznávání obličeje je snadno

využitelné pro zabezpečení počítače a dat, k jeho snímání nám totiž stačí obyčejná web kamera a příslušný software, který většinou umožňuje i vícefaktorovou autentizaci (rozpoznání hlasu, heslo, propojení s jiným biometrickým zařízením atd.).

PODPIS

S vývojem moderních technologií už podpisy nejsou jen statickým objektem zkoumání grafologů a personalistů. Dnešní technologie už se nezaměřují pouze na výsledný obraz, ale i na kompletní proces vytváření podpisu – rychlost psaní, tlak hrotu pera, směr a posloupnost čar atd. Podpis je realizován pomocí speciálního bezdrátového pera nebo je snímání řešeno na obrazovce PDA zařízení, pomocí speciálního psacího hrotu.[1]

Obrázek 12: Podpis Zdroj: http://www.advancedsourcecode.com/neuralsignature.asp

DNA

Patrně nejspolehlivějším způsobem identifikace jedince je pomocí analýzy jeho deoxyribonukleové kyseliny (DNA). Vybrané znaky ve struktuře DNA jsou převedeny na vyhodnotitelné genetické profily, které jsou jedinečné u každého člověka. Použití této identifikace je limitováno především složitým technologickým postupem, který může trvat několik hodin. Proto se tato biometrická metoda používá především ve forenzních vědách, kde doba ověřování identity není až tak rozhodující. [1]

ÚROVEŇ ZABEZPEČENÍ

Biometrické metody jsou, až na některé výjimky, velmi spolehlivé. Do velké míry ale záleží na kvalitě snímače/scanneru/pera/… a na jeho variabilitě.

OSTATNÍ ASPEKTY

Dostupnost – Pokud je systém založen pouze na biometrické autentizaci, uživatel si nemusí pamatovat žádné heslo resp. PIN, ani nemusí mít připraven žádný token.

Uživatelská přívětivost – Biometrické metody založené na otiscích prstů, ruky, popř. ucha, nepotřebují žádnou speciální spolupráci uživatele, jen pouhé přiložení. Co se uživatelské přívětivosti týče, jsou nejméně oblíbené snímače oční sítnice resp. duhovky, vyžadují totiž, aby uživatel sledoval určité body po dobu 10-15 vteřin, což může být pro někoho nepříjemné nebo náročné (uživatel může mít oční vadu, která mu znesnadňuje sledování bodů).

7 PRAKTICKÁ ČÁST

Tato část bude věnována vyhodnocení dotazníku (viz. Příloha č. 1) a testování dvou vybraných zařízení se čtečkou otisků prstů.

7.1 DOTAZNÍK

Cílem dotazníkového šetření bylo zjistit rozšíření čteček otisků prstů, spokojenost s nimi a do jaké míry jim respondenti důvěřují. Otázky v dotazníku byly sestaveny co nejjednodušeji a nejstručněji, aby byla zajištěna co největší návratnost. Dotazník byl tvořen pomocí dotazníkové služby Vyplnto.cz a vyplnilo jej 72 respondentů. Výsledné grafy jsou k nahlédnutí v příloze č. 2.

7.1.1 CHARAKTERISTIKA RESPONDENTŮ

V otázce č. 1 byl zjišťován věk respondentů. Dotazník byl šířen především mezi studenty, a proto více než 50% respondentů patří do věkové skupiny 19-25 let.

7.1.2 VYHODNOCENÍ DOTAZNÍKU

OTÁZKA Č. 2

Na otázku „Setkali už jste se někdy s čtečkou otisků prstů?“ odpovědělo kladně 45 respondentů. Mezi odpověďmi „Ano“ měly zástupce všechny věkové skupiny. Pokud respondent zvolil odpověď „Ne“, byl přesměrován na otázku č. 11.

Odpověď	Počet respondentů	% globálně
Ano	45	62,5%
Ne	27	37,5%

Tabulka 4: Otázka č. 2

OTÁZKA Č. 3

Třetí otázka měla za cíl zjistit, kolik respondentů vlastní čtečku otisků prstů (nebo jakékoli zařízení se čtečkou). Na otázku „Vlastníte nějaké zařízení se čtečkou otisků prstů?“ odpovědělo kladně pouze 13 respondentů, ale dalších 8 má ve svém okolí někoho, kdo čtečku vlastní.

Odpověď	Počet respondentů	% globálně
Ano	13	18,06%
Ne	24	33,33%
Já osobně ne, ale někdo z mých blízkých takové zařízení vlastní	8	11,11%

Tabulka 5: Otázka č. 3

Pokud respondent zvolil odpověď „Ano“, byl přesměrován na otázku č. 6, pokud „Ne“, byl přesměrován na otázku č. 4.

Na otázku č. 4 „Uvažujete o koupi zařízení se čtečkou otisků prstů?“ odpovědělo všech 24 respondentů záporně, a proto se k otázce č. 5 „O jaké zařízení by se jednalo?“ žádný respondent nedostal. Bohužel, osm respondentů, kteří u otázky č. 3 odpověděli, že zařízení sice nevlastní, ale někdo jejich blízkých ano, nebyli na otázku č. 4 přesměrováni kvůli nedopatření při nastavováni dotazníku.

OTÁZKA Č. 6

Nejčastější odpovědí na otázku „Jaké zařízení vlastníte?“ byl notebook. Zde se potvrdila má hypotéza, že mezi běžnými uživateli budou nejvíce rozšířená zařízení, ve kterých je čtečka integrována, než samostatné čtečky.

Odpověď	Počet respondentů	% globálně
Notebook	10	13,89%
Flashdisk	1	1,39%
USB čtečka otisků prstů	1	1,39%
Jiné: Otvírač dveří	1	1,39%

Tabulka 6: Otázka č. 6

OTÁZKA Č. 7

U otázky č. 7 „Jste s tímto zařízením spokojeni?“ měl respondent záměrně povoleny jen odpovědi „Ano“ nebo „Ne“, abychom získali souhrnnou odpověď, vycházející z pocitu respondenta.

Odpověď	Počet respondentů	% globálně
Ano	8	11,11%
Ne	5	6,94%

Tabulka 7: Otázka č. 7

OTÁZKA Č. 8

Otázka č. 8 měla hodnotící charakter. Respondent vlastnící čtečku otisků měl za úkol oznámkovat své zařízení z hlediska vzhledu, rychlosti a funkčnosti. Pouze dva respondenti byli se svou čtečkou naprosto spokojeni.

	Průměr
Vzhled	2,077
Rychlost autentizace	2,385
Funkčnost	2,923

Tabulka 8: Otázka č. 8

OTÁZKA Č. 9

„Funguje vaše zařízení dokonale, nebo jste se již setkali s nějakou chybou?“

Odpověď	**Počet respondentů**	**% globálně**
Často chybuje	5	6,94
Zatím bez problémů	4	5,56
Občas chybuje	4	5,56

Tabulka 9: Otázka č. 9

Na tuto otázku navazovala nepovinná otázka č. 10 „S jakými chybami jste se setkali:“, respondent zadával odpověď do textového pole. Na otázku odpovědělo celkem 8 respondentů, přičemž nejčastější odpovědí bylo chybné načtení – nerozpoznání otisku.

Odpovědi:

„dokáže mě identifikovat až na několikátý pokus“

„Chybné načtení otisku.“

„Je třeba pečlivé přiložení prstu, při mírném náklonu nepustí dále.“

„Možná je chyba na mé straně, ale z 10 pokusů o načtení otisku uspěju tak v 1 případě.“

„Neexistence ovladačů pro linux. A nemožnost jejich vývoje díky šifrovanému proprietálnímu protokolu“

„nepoznává můj otisk“

„samo se spousti; je treba casto opakovat“

„zřejmě chyba software, zablokování se... nutnost restartu“

OTÁZKA Č. 11

Otázka č. 11 měla za cíl zjistit důvěru respondentů ve snímače otisků prstů. Absolutní nedůvěru projevili pouze 3 respondenti z celkových 72.

„Myslíte si, že jsou tato zařízení důvěryhodná?“

Odpověď	Počet respondentů	% globálně
Spíše souhlasím	33	45,83%
Souhlasím	19	26,39%
Spíše nesouhlasím	9	12,5%
Nevím	8	11,11%
nesouhlasím	3	4,17%

Tabulka 10: Otázka č. 11

OTÁZKA Č. 12

Otázky č. 12 a 13 měly zjistit, jak velkou důvěru respondenti otiskům prstů přikládají obecně a ve spojitosti s financemi.

„Dokázali byste si představit, že jsou otisky prstů nahrazena veškerá hesla a piny?“

Odpověď	Počet respondentů	% globálně
Ne	37	51,39%
Ano	35	48,61%

Tabulka 11: Otázka č. 12

OTÁZKA Č. 13

„Dokázali byste si představit nahrazení PINu u platebních karet otisky prstů?“

Odpověď	Počet respondentů	% globálně
Líbila by se mi kombinace otisků a pinu	27	37,5%
Ne	25	34,72%
Ano	20	27,78%

Tabulka 12: Otázka č. 13

7.1.3 ZÁVĚR

Respondentů nebylo takové množství, abychom ze získaných informací mohli vyvozovat nějaké zásadní závěry.

9 ze 13 respondentů vlastnících zařízení se čtečkou otisků odpovědělo, že jejich zařízení chybuje, přičemž nespokojenost projevili majitelé notebooku, flashdisku i USB čtečky otisků.

7.2 ZAŘÍZENÍ: FLASHDISK HIRSCHMANN

Po připojení flashdisku se nám otevře okno s menu. Pokud otevřeme průzkumníka, vidíme, že se flashdisk si vytvořil virtuální jednotku CD-ROM a vyměnitelný disk, který když chceme otevřít, tak vrátí výzvu o vložení disku.

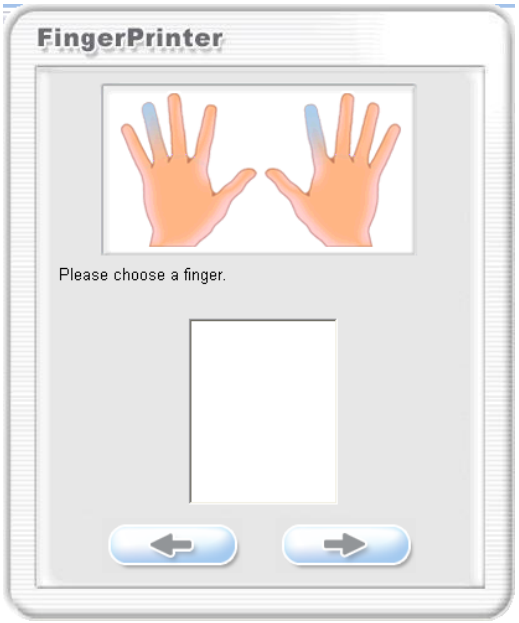
Obrázek 13: FingerPrinter 01

Po kliknutí na FP Manager, máme možnost zaregistrovat nového uživatele. Po zadání nového uživatelského jména nás FingerPrinter vyzve k vybrání prstu, který budeme chtít snímat.

Můžeme uložit až 10 otisků, následně se přihlašujeme kterýmkoliv z nich. Tuto volbu můžeme po odemknutí kdykoli změnit, otisky lze přidávat a mazat. Patrně nejjednodušší je přihlašování se pravým nebo levým ukazovákem. Na druhou stranu je to ale předvídatelné chování a otisky těchto prstů necháváme na mnoha místech (počítačová myš, sklenice,…), takže v případě, že si někdo bude chtít zhotovit falešný otisk

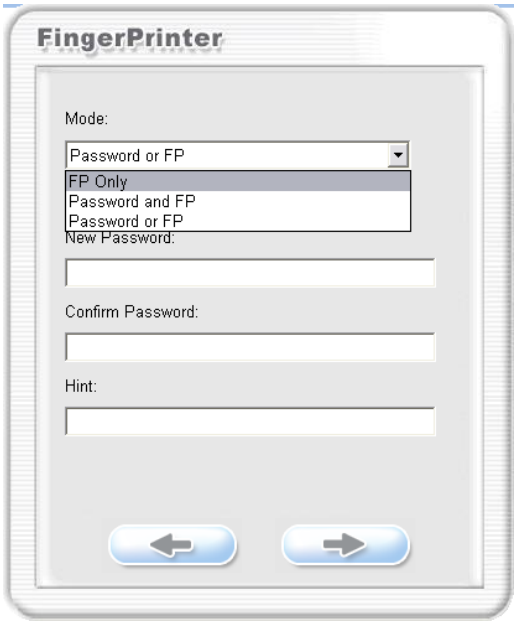
našeho prstu, jako první půjde po ukazováku a jeho otisk najde téměř na všem, čeho se běžně dotýkáme.

Po vybrání prstu nás FingerPrinter vyzve, abychom daným prstem přejeli po čtečce. Prst musíme přes senzor protahovat opravdu pomalu, aby se otisk načetl správně. Pokud je otisk neúplný, musíme snímání opakovat, dokud otisk nebude kompletní.



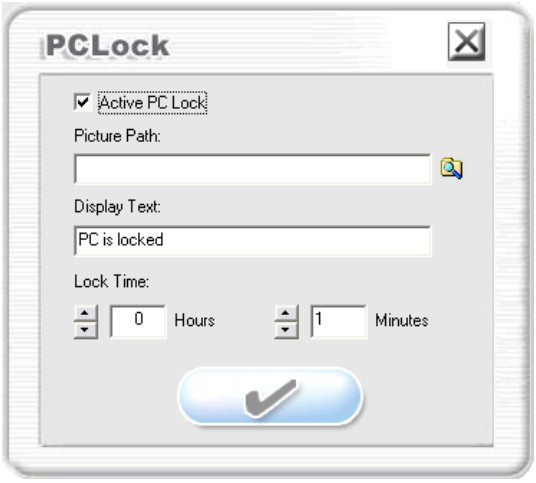
Obrázek 14: FingerPrinter 02

Po načtení otisků si můžeme vybrat způsob přihlašování. Jestli se chceme přihlašovat pouze otiskem, či kombinací otisku a hesla, či heslem nebo otiskem. Je dobré nespoléhat se na dokonalost čtečky a pro jistotu heslo zadat. Potvrdíme nastavení a můžeme začít flashdisk používat.



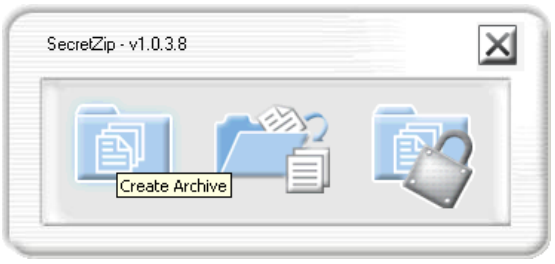
Obrázek 15: FingerPrinter 03

Základní funkcí flashdisku je, ochrana dat na disku samotném. Pokud nezadáme heslo nebo nenasnímáme otisk, obsah flashdisku se nám nezobrazí. Další možností využití je uzamykání pc.



Obrázek 16: FingerPrinter 04

Tento flash disk umožňuje i šifrování souborů. Zvolíme položku Menu SecretZIP:



Obrázek 17: FingerPrinter 05

Zvolíme vytvoření nového archivu a přidáme do něj soubory nebo složky, které chceme šifrovat. Potvrdíme vybrané a zobrazí se nám nabídka, zda chceme soubor šifrovaný, ZIP soubor, anebo šifrovaný ZIP.

Obrázek 18: FingerPrinter 06

Program nám vytvoří nový soubor s příponou *.ezc, který můžeme otevřít jen pomocí FingerPrinteru.

7.2.1 TESTOVÁNÍ PŘÍSTUPU

Pro uzamčení disku jsem zvolila prsteník pravé ruky. Při snímání kteréhokoli jiného prstu mi byl přístup odepřen.

Velmi pomalý průtah	Přístup povolen
Rychlý průtah	Přístup povolen
Velmi rychlý průtah	Přístup povolen
Malý tlak na snímač	Přístup povolen
Velký tlak na snímač	Přístup povolen
Vlhkost prstu - velká	Přístup odepřen
Vlhkost prstu - malá	Přístup povolen
Mírné sklony prstu	Přístup povolen
Velký sklon prstu	Přístup odepřen
Nasnímání pouze části prstu - vertikálně	Provedení čtečky to neumožňuje
Nasnímání pouze části prstu - horizontálně	Méně než ¾ prstu – Přístup odepřen
Znečištění: vrstva make-upu	Přístup povolen, otisk stejný jako při malém tlaku na snímač
Pouhé přiložení prstu	Čtečka neregistruje

Závěr: Neregistrovala jsem žádné odmítnutí způsobené chybou čtečky.

8 ZÁVĚR

Autentizace pomocí otisků prstů měla ze všech biometrik největší šanci se masově rozšířit mezi běžné uživatele osobních počítačů, především díky velikosti snímačů, možnosti jejich miniaturizace, a díky pohodlnosti snímání otisku. Jako u každé nové technologie, i kvalita snímacích zařízení byla z počátku vykoupena cenou. Dnes již ale jejich nevětší boom ustoupil a každý si na trhu může najít čtečku v potřebné cenové relaci. Někteří výrobci ale vrhají stín na tuto metodu autentizace. Poměrně často se setkávají s kritikou zařízení s integrovanou čtečkou otisků, jako jsou notebooky, u kterých je cena zvýšena díky čtečce, která je spíše ozdobou, než skutečně funkčním zabezpečovacím prvkem. Při výběru správné čtečky bychom si nejprve měli promyslet, k čemu čtečku budeme chtít využívat, jaká data chceme chránit a kolik do ní chceme investovat.

Cílem této práce bylo především představit používané technologie a principy z oblasti snímání otisků prstů, ale také porovnání s ostatními používanými biometrikami a přístupy k počítači a datům. Dále si tato práce kladla za cíl nahlédnout do problematiky otisky prstů vs. ochrana osobních údajů, představení na trhu dostupných zařízení se čtečkou a možností softwaru.

Na závěr práce jsem zařadila testování půjčeného zařízení a také vyhodnocení dotazníku. Cílem dotazníku bylo zjistit rozšíření čteček a důvěru v ně. Ze 72 respondentů čtečku otisků vlastnilo pouhých 13, proto ze získaných dat nemohu vyvozovat nějaké závěry. Myslím si, že lidé zatím tuto metodu chápou jako zbytečný nadstandard (pro přístup k osobním počítačům a datům) a proto si čtečky otisků prstů pořizují především lidé zajímající se o nové technologie.

9 SEZNAM OBRÁZKŮ

10 SEZNAM LITERATURY

[1] RAK, Roman, Václav MATYÁŠ, Zdeněk ŘÍHA a kolektiv. *Biometrie a identita člověka*: *ve forenzních a komerčních aplikacích*. Praha: Grada Publishing, a.s., 2008. ISBN 978-80-247-2365-5.

[2] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi*. 2008. Dostupné z: http://www.fbi.vsb.cz/export/sites-root/fbi/040/cs/sys/resource/PDF/biometricke_metody.pdf

[3] KAŠNÝ, Pavel. *Reálné hodnocení parametrů snímačů otisku prstu na základě praktických měření*. Zlín, 2011. Dostupné z: http://dspace.k.utb.cz/handle/10563/15471. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně.

[4] MALTONI, Davide a kolektiv. *Handbook of Fingerprint Recognition*. 2. vydání.

London: Springer, 2009. ISBN 978-1-84882-253-5.

[5] *Comfis* [online]. ©2008 [cit. 2012-06-21]. Dostupné z: http://www.comfis.cz/biometrie

[6] BOUŠKA, Petr. *Biometrické systémy: zpracování otisku prstu včetně možnosti rekonstrukce otisku z biometrické šablony*. Brno, 2007. Dostupné z: http://is.muni.cz/th/50818/fi_m/diplomova_prace.pdf?lang=en. Diplomová práce. Masarykova univerzita.

[7] *Bez klíčů* [online]. ©2007 [cit. 2012-06-21]. Dostupné z: http://www.bezklicu.cz/

[8] *Suprema* [online]. ©2011 [cit. 2012-06-21]. Dostupné z: http://www.supremainc.com/eng/product/pc_14.php?mark=35

[9] *Jet Flash* [online]. ©2011 [cit. 2012-06-21]. Dostupné z: http://www.jetflash.cz/

[10] *Alza* [online]. ©2012 [cit. 2012-06-21]. Dostupné z: http://www.alza.cz/

[11] *Extra notebook.cz*. [online]. 11. 6. 2010 [cit. 2012-06-21]. Dostupné z: http://extranotebook.cnews.cz/thinkpad-zdedeny-poklad-%E2%80%93-druha-cast-video

[12] *AuthenTec* [online]. ©2012 [cit. 2012-06-21]. Dostupné z: http://authentec.com/

[13] *Dell* [online]. 31. 1. 2012 [cit. 2012-06-21]. Dostupné z: http://support.dell.com/support/topics/global.aspx/support/kcs/document?docid=464604&doclang=cs

[14] *Ochrana osobních údajů* [online]. ©2010 [cit. 2012-06-21]. Dostupné z: http://oou.cz/

[15] *Fingera*: *evidenční docházkový systém* [online]. ©2006-2009 [cit. 2012-06-21]. Dostupné z: http://fingera.cz/

[16] *Zákony ČR* [online]. © 2004 - 2011 [cit. 2012-06-21]. Dostupné z: http://zakonycr.cz/

[17] MATYÁŠ, Václav a Jan KRHOVJÁK a kolektiv. *Autorizace elektronických transakcí a autentizace dat i uživatelů*. Brno: Masarykova univerzita/Nakladatelství, 2008. ISBN 978-80-210-4556-9.

[18] *Aktion*: *Elektronická identita* [online]. ©2012 [cit. 2012-06-22]. Dostupné z: http://www.aktion.cz/cs/download/katalogove_listy/kl_elektronicka_identita.pdf

[19] HANÁČEK, Petr a Václav MATYÁŠ. *Čipová karta v informačních systémech*. ©2008. Dostupné z: http://www.datakon.cz/datakon08/d03_tut_hanacek.pdf

[20] SATRAPA, Pavel. Autentizace uživatelů. *Ústav Nových technologií a aplikované informatiky* [online]. 2012 [cit. 2012-06-22]. Dostupné z: http://www.nti.tul.cz/~satrapa/vyuka/site/cv/hesla-sifry.pdf

11 RESUMÉ

Out of all biometric identifiers, the authentication by means of taking fingerprints had the biggest chance to expand on a mass scale among common users of personal computers, mainly thanks to the size of the sensors, the possibility of their miniaturization and thanks to the comfortable way of taking fingerprints. As it is common in cases of all new technologies also the quality of fingerprint readers used to be related to their price. However, the boom of fingerprint readers decreased and everyone can find a reader of suitable price today. Nevertheless, some producers cast a shadow upon this method of authentication. They often face the criticism of devices with integrated fingerprint reader, e.g. laptops whose prices increase thanks to the integrated reader which serves as a decoration rather than as a real functional security component. When choosing suitable fingerprint reader it is convenient to know for which purposes we are going to use it, what kind of data are we going to protect and how much money we are going to spend on it.

The main aim of the thesis was a presentation of technologies and principles used in the area of fingerprint scanning, but also a comparison of the fingerprint readers and other biometric methods and of various kinds of access to computers and data. Another aim of the thesis was to depict the issue of fingerprints versus privacy policy, the introduction of devices with fingerprint readers and the possibility of software available in the market.

The conclusion of the thesis includes the test of borrowed fingerprint reader and also a questionnaire appraisal. The target of the questionnaire was to ascertain how much are the fingerprint readers used and to what extent people trust in them. Out of 72 respondents only 13 persons own fingerprint reader and so it is impossible to draw a conclusion from the research. I believe that people perceive this method as a needles anachronism (when speaking about access to computers and personal data) and the fingerprint readers are being bought mainly by people who are interested in new technologies.

12 PŘÍLOHY

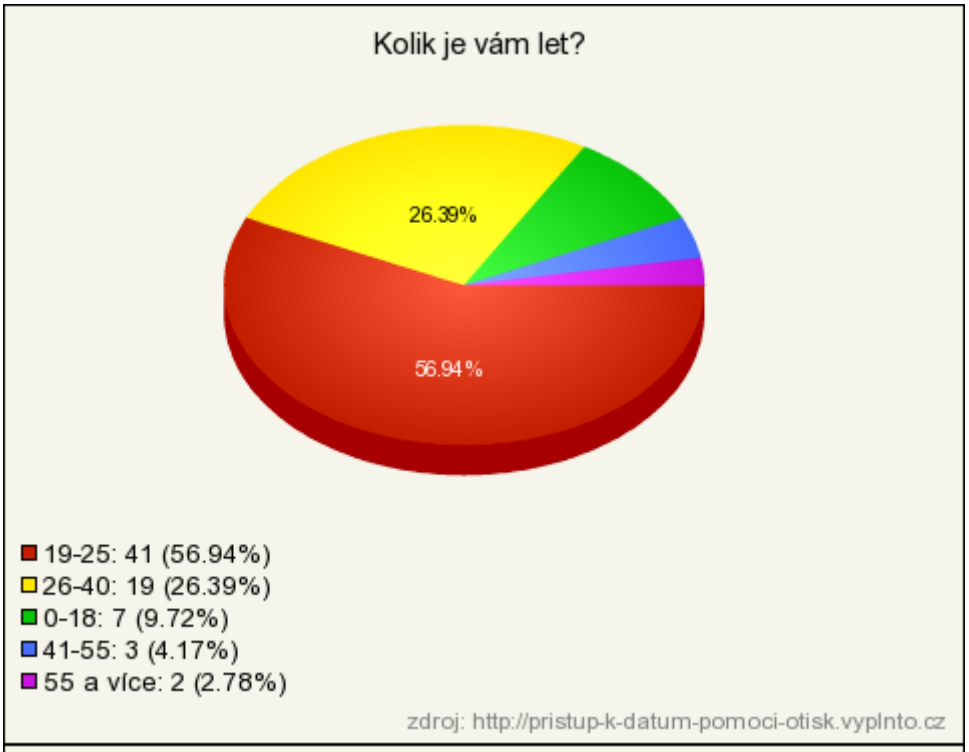
PŘÍLOHA Č. 1 - Dotazník: Přístup k datům pomocí otisků prstů

1. Kolik je vám let?
   Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.
   a. 0 - 18
   b. 19 - 25
   c. 26 - 40
   d. 41 - 55
   e. 55 a více
2. Setkali už jste se někdy se čtečkou otisků prstů?
   Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Ano → otázka č. 3, Ne → otázka č. 11, Nevím, co to je → konec dotazníku].
   a. Ano
   b. Ne
   c. Nevím, co to je
3. Vlastníte nějaké zařízení se čtečkou otisků prstů?
   Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Ano → otázka č. 6, Ne → otázka č. 4, Já osobně ne, ale někdo z mých blízkých takové zařízení vlastní → otázka č. 11].
   a. Ano
   b. Ne
   c. Já osobně ne, ale někdo z mých blízkých takové zařízení vlastní
4. Uvažujete o koupi zařízení se čtečkou otisků prstů?
   Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Ano → otázka č. 5, Ne → otázka č. 11].
   a. Ano
   b. Ne
5. O jaké zařízení by se jednalo?
   Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.
   a. Notebook
   b. USB čtečka otisků prstů
   c. Flashdisk
   d. Tablet
   e. Jiné
6. Jaké zařízení vlastníte?
   Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí nebo napsat odpověď vlastními slovy.
   a. Notebook
   b. USB čtečka otisků prstů

   c. Flashdisk
   d. Tablet
   e. Jiná odpověď …

7. Jste s tímto zařízením spokojeni?
   Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.
   a. Ano
   b. Ne
8. Ohodnoťte vámi používané zařízení:
   Povinná otázka, respondent se musel u každé podotázky rozhodnout mezi odpověďmi „1", „2", „3", „4" a „5", respondent se musel u každé podotázky rozhodnout mezi odpověďmi na dané škále.
   a. Vzhled: 1 2 3 4 5
   b. Rychlost: 1 2 3 4 5
   c. Funkčnost: 1 2 3 4 5
9. Funguje vaše zařízení dokonale, nebo jste se již setkali s nějakou chybou?
   Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí a podle toho se mu zobrazily další otázky [Zatím bez problémů → otázka č. 11, Občas chybuje → otázka č. 10, Často chybuje → otázka č. 10].
   a. Zatím bez problémů
   b. Občas chybuje
   c. Často chybuje
10. S jakými chybami jste se setkali:
    Nepovinná otázka, respondent mohl napsat odpověď vlastními slovy.
11. Myslíte si, že jsou tato zařízení důvěryhodná?
    Povinná otázka, respondent se musel rozhodnout mezi odpověďmi „souhlasím", „spíše souhlasím", „nevím", „spíše nesouhlasím" a „nesouhlasím".
12. Dokázali byste si představit, že jsou otisky prstů nahrazena veškerá hesla a piny?
    Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.
    a. Ano
    b. Ne
13. Dokázali byste si představit nahrazení PINu u platebních karet otisky prstů?
    Povinná otázka, respondent musel zvolit jednu z nabízených odpovědí.
    a. Ano
    b. Ne
    c. Líbila by se mi kombinace otisků a pinu

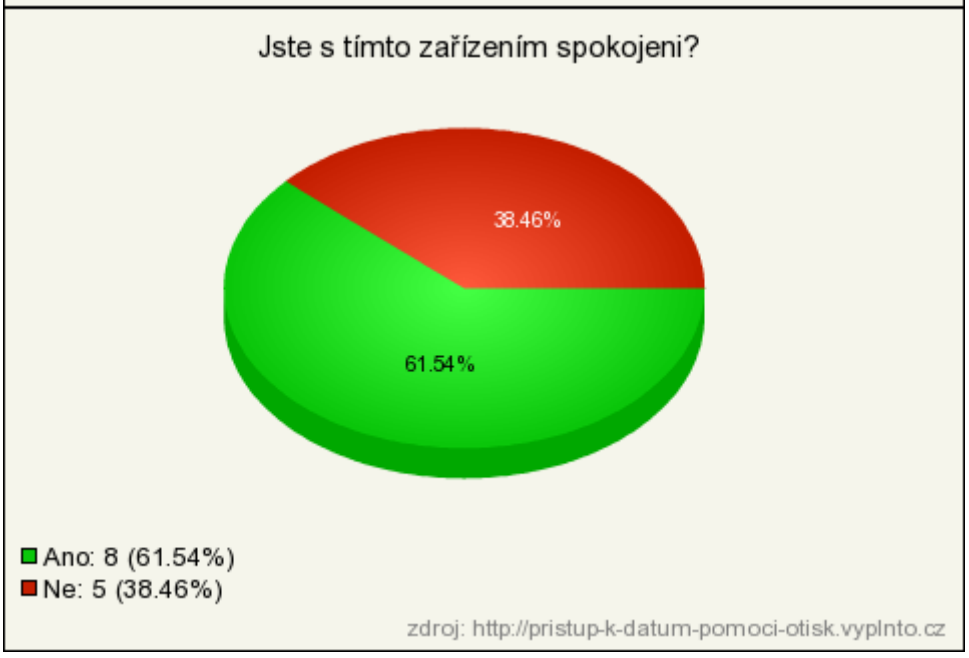
Příloha č. 2 – Grafy dotazníku

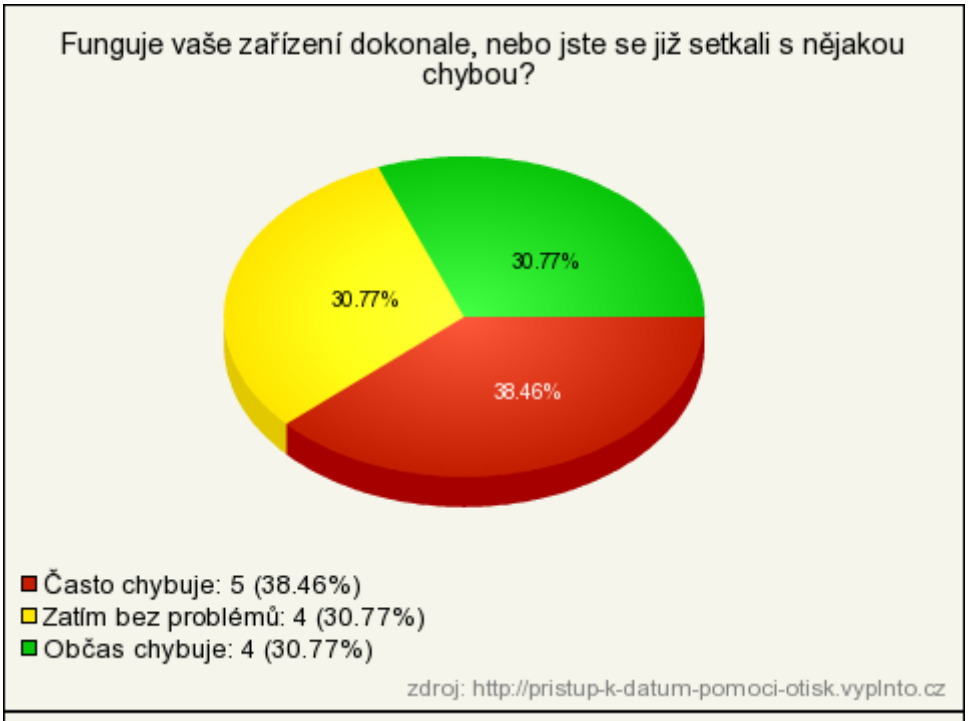


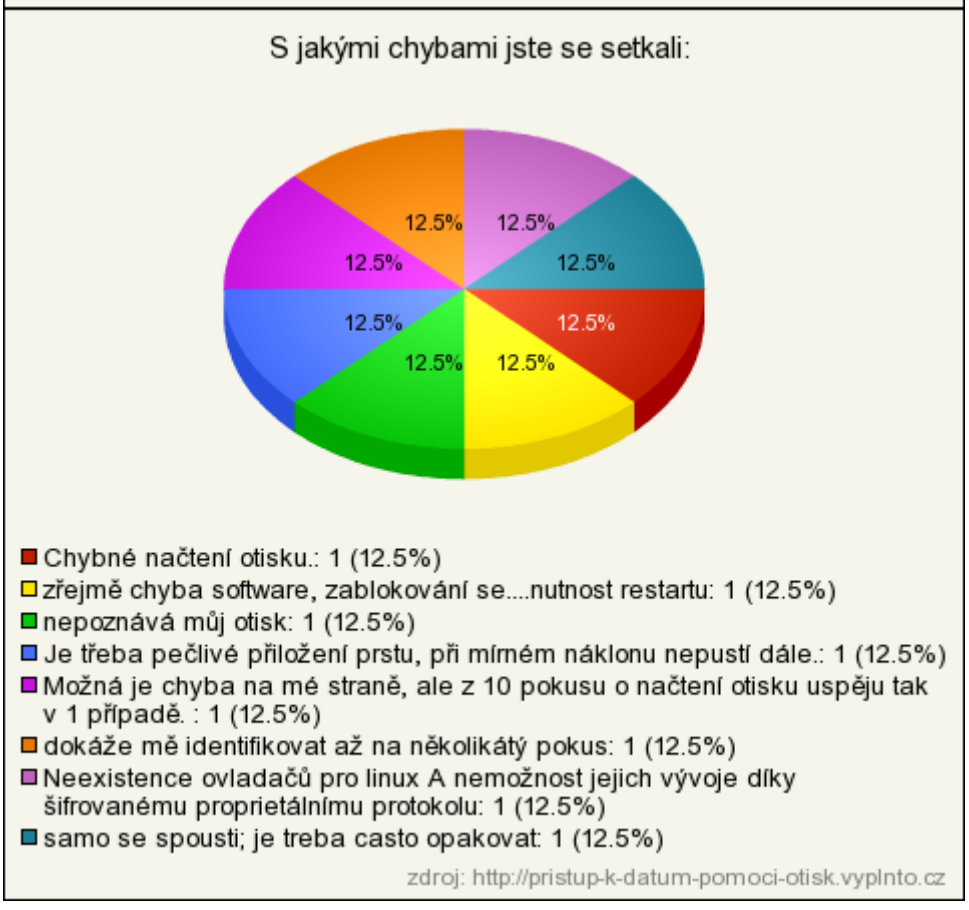

Vlastníte nějaké zařízení se čtečkou otisků prstů?
28.89%
17.78%
53.33%
Ne: 24 (53.33%)
Ano: 13 (28.89%)
Já osobně ne, ale někdo z mých blízkých takové zařízení vlastní: 8 (17.78%)
zdroj: http://pristup-k-datum-pomoci-otisk.vyplnto.cz


Uvažujete o koupi zařízení se čtečkou otisků prstů?
100%
Ne: 24 (100%)
zdroj: http://pristup-k-datum-pomoci-otisk.vyplnto.cz

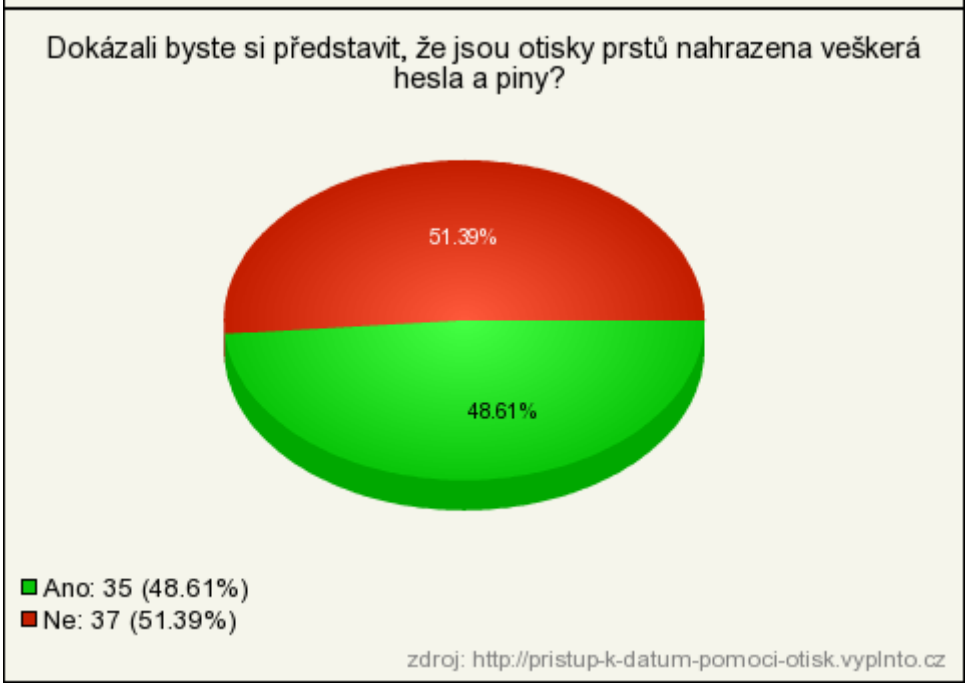

Jaké zařízení vlastníte?
76.92%
Notebook: 10 (76.92%)
Flashdisk: 1 (7.69%)
otvírač dveří: 1 (7.69%)
USB čtečku otisků prstů: 1 (7.69%)
zdroj: http://pristup-k-datum-pomoci-otisk.vyplnto.cz

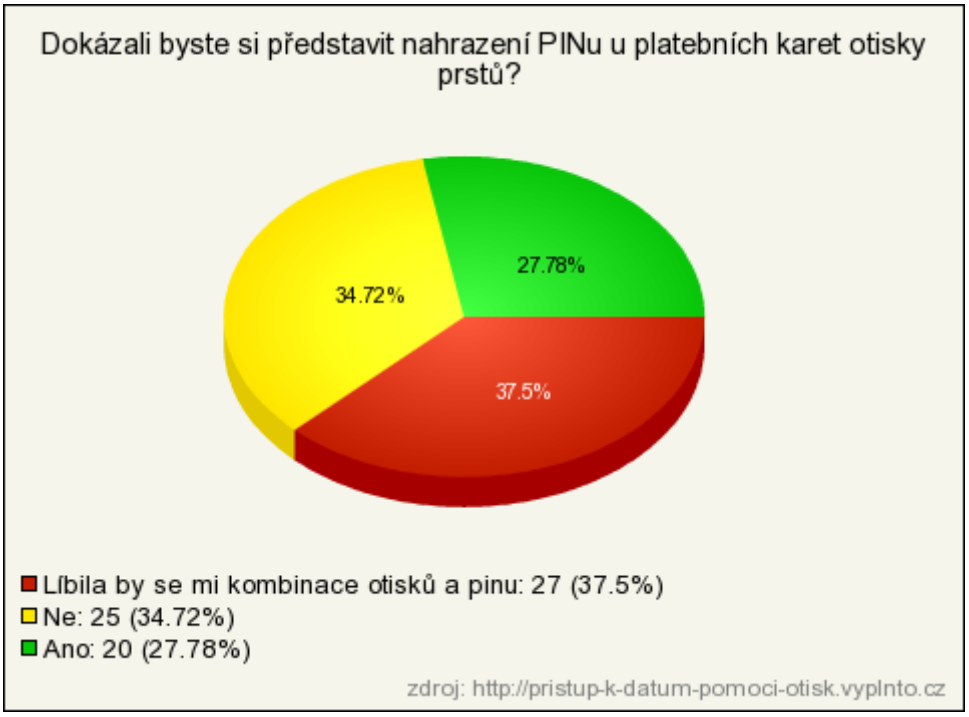

Jste s tímto zařízením spokojeni?
38.46%
61.54%
Ano: 8 (61.54%)
Ne: 5 (38.46%)
zdroj: http://pristup-k-datum-pomoci-otisk.vyplnto.cz


Funguje vaše zařízení dokonale, nebo jste se již setkali s nějakou chybou?
30.77%
30.77%
38.46%
Často chybuje: 5 (38.46%)
Zatím bez problémů: 4 (30.77%)
Občas chybuje: 4 (30.77%)
zdroj: http://pristup-k-datum-pomoci-otisk.vyplnto.cz


S jakými chybami jste se setkali:
12.5%
12.5%
12.5%
12.5%
12.5%
12.5%
12.5%
12.5%
Chybné načtení otisku.: 1 (12.5%)
zřejmě chyba software, zablokování se....nutnost restartu: 1 (12.5%)
nepoznává můj otisk: 1 (12.5%)
Je třeba pečlivé přiložení prstu, při mírném náklonu nepustí dále.: 1 (12.5%)
Možná je chyba na mé straně, ale z 10 pokusu o načtení otisku uspěju tak v 1 případě. : 1 (12.5%)
dokáže mě identifikovat až na několikátý pokus: 1 (12.5%)
Neexistence ovladačů pro linux A nemožnost jejich vývoje díky šifrovanému proprietálnímu protokolu: 1 (12.5%)
samo se spousti; je treba casto opakovat: 1 (12.5%)
zdroj: http://pristup-k-datum-pomoci-otisk.vyplnto.cz


Myslíte si, že jsou tato zařízení důvěryhodná?
11.11%
12.5%
45.83%
26.39%
souhlasím: 19 (26.39%)
spíše souhlasím: 33 (45.83%)
nevím: 8 (11.11%)
spíše nesouhlasím: 9 (12.5%)
nesouhlasím: 3 (4.17%)
zdroj: http://pristup-k-datum-pomoci-otisk.vyplnto.cz


Dokázali byste si představit, že jsou otisky prstů nahrazena veškerá hesla a piny?
51.39%
48.61%
Ano: 35 (48.61%)
Ne: 37 (51.39%)
zdroj: http://pristup-k-datum-pomoci-otisk.vyplnto.cz


Dokázali byste si představit nahrazení PINu u platebních karet otisky prstů?
27.78%
34.72%
37.5%
Líbila by se mi kombinace otisků a pinu: 27 (37.5%)
Ne: 25 (34.72%)
Ano: 20 (27.78%)
zdroj: http://pristup-k-datum-pomoci-otisk.vyplnto.cz