VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÉ GRAFIKY A MULTIMÉDIÍ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER GRAPHICS AND MULTIMEDIA

PODPORA PRO AUTENTIZACI POMOCÍ OTISKŮ PRSTU

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE Bc. JAROSLAV BARTOŇ
AUTHOR

BRNO 2009

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÉ GRAFIKY A MULTIMÉDIÍ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER GRAPHICS AND MULTIMEDIA

PODPORA PRO AUTENTIZACI POMOCÍ OTISKŮ PRSTU

SUPPORT FOR FINGERPRINT AUTHENTICATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. JAROSLAV BARTOŇ
AUTHOR

VEDOUCÍ PRÁCE — Ing. JOZEF MLÍCH
SUPERVISOR

BRNO 2009

Abstrakt

Cílem diplomové práce je podpora pro autentizaci uživatele pomocí otisků prstů v pracovním prostředí KDE v operačním systému Linux. Popisuje základní pojmy z počítačové bezpečnosti a možnosti prokázání identity. Věnuje se biometrickým systémům a typům zpracovávaných charakteristik. Blíže popisuje autentizaci uživatele pomocí otisků prstů a komerčně dostupné snímače. Součástí řešení je aplikace pro správu otisků prstů a zásuvný modul grafického správce přihlášení KDM.

Klíčová slova

identita, identifikace, autentizace, verifikace, biometrický systém, FAR, FRR, geometrie ruky, otisky prstů, Linux, PAM, D-Bus, libfprint, fprintd

Abstract

The goal of the thesis is the finger-print authentication support within the Linux operating system and the K Desktop Environment (KDE). Theoretical part of the thesis firstly explains main IT security terms and ways to proof the identity. Secondly it describes biometric systems and types of processed biometric characteristics. Lastly the features of finger-prints, their markants as well as types of scanners used in scanning the finger-prints and ways to analyze the scanned material have been elaborated. Practical solution part of the thesis develops and establishes finger-print management application and plugin for KDM graphics login manager.

Keywords

identity, identification, authentication, verification, biometrics system, FAR, FRR, hand geometry, fingerprint, Linux, PAM, D-Bus, libfprint, fprintd

Citace

Jaroslav Bartoň: Podpora pro autentizaci pomocí otisků prstu, diplomová práce, Brno, FIT VUT v Brně, 2009

Podpora pro autentizaci pomocí otisků prstu

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana Ing. Jozefa Mlícha. Další informace mi poskytl Lukáš Tinkl ze společnosti Red Hat Czech. Uvedl jsem všechny literární prameny a publikace, z kterých jsem čerpal.

. . . . . .
Jaroslav Bartoň
20. května 2009

Poděkování

Chtěl bych poděkovat Ing. Jaroslavu Řezníkovi za pomoc při řešení problému s knihovnou `QtDBus` a Lukáši Tinklovi ze společnosti Red Hat Czech za možnost pracovat na tomto zajímavém projektu. Mé poděkování patří i Mgr. Petře Navrátilové, Ph.D. a Ing. Martinovi Navrátilovi za pomoc při závěrečných úpravách.

© Jaroslav Bartoň, 2009.
Tato práce vznikla jako školní dílo na Vysokém učení technickém v Brně, Fakultě informačních technologií. Práce je chráněna autorským zákonem a její užití bez udělení oprávnění autorem je nezákonné, s výjimkou zákonem definovaných případů.

Obsah

Obsah 2

Seznam obrázků 3

1 Úvod 4

2 Základní pojmy počítačové bezpečnosti 5
2.1 Možnosti ověření identity . . . 6

3 Biometrie a biometrické systémy 11
3.1 Kritéria pro biometrický systém . . . 13
3.2 Biometrický systém . . . 15
3.3 Výkonnost biometrických metod . . . 16

4 Identifikace a verifikace pomocí otisků prstů 19
4.1 Typy snímačů . . . 20
4.2 Funkce systému . . . 21

5 Identifikace a autentizace uživatelů v Unixových systémech 22
5.1 Soubor /etc/passwd . . . 22
5.2 Soubor /etc/shadow . . . 23
5.3 Zásuvné autentizační moduly . . . 24

6 Použité technologie 27
6.1 Komunikační sběrnice D-Bus . . . 27
6.2 Knihovna libfprint . . . 30
6.3 Fprintd . . . 30

7 KFingerManager 33
7.1 Zavedení otisku do systému . . . 34
7.2 Smazání otisků prstů . . . 34
7.3 Implementace . . . 35
7.4 Nastavení systému . . . 38
7.5 Známé problémy . . . 39

8 KDM 40
8.1 Architektura . . . 41
8.2 Zásuvné moduly . . . 41
8.3 Kgreet_fprintd . . . 42

8.4 KScreensaver 43
8.5 Známá omezení 43

9 Problémy systému PAM **45**
9.1 Podpora více autentizačních mechanizmů současně 45
9.2 Implementace PAM v grafických aplikacích 45
9.3 Možná řešení 46

10 Možné alternativní přístupy **47**
10.1 FingerprintGUI 47

11 Další vývoj **49**
11.1 Knihovny libfprint a libusb 49
11.2 Fprintd 49
11.3 KFingerManager 49
11.4 KDM 50
11.5 KScreensaver 50
11.6 PAM modul pro KWallet 50
11.7 Programy kdesu a kdesudo 50
11.8 Internetová prezentace 51
11.9 Bezpečnostní analýza 51

12 Závěr **52**

Použitá literatura **53**

Seznam příloh **57**

A Obsah přiloženého CD **58**

B Obraz disku pro virtuální počítač **59**

C Konfigurační soubory PAM **60**

D Konfigurační soubor kdmrc **61**

Seznam obrázků

2.1 Základní způsoby identifikace osoby 7
2.2 Občanský průkaz České republiky 9
2.3 Biočip 9
2.4 Identifikační karta 9

3.1 Bertillionáž 12
3.2 Zjednodušené schéma biometrického systému 16
3.3 Vztah mezi FRR a FAR – ideální biometrická aplikace 17
3.4 Vztah mezi FRR a FAR – reálná biometrická aplikace 17

4.1 Charakteristické znaky otisků prstu – daktyloskopické markanty 19
4.2 Funkce optického snímače otisků prstů 20
4.3 Termický snímač otisků prstů 20
4.4 Kapacitní snímač otisků prstů 20
4.5 Schéma zpracování otisku prstu 21

6.1 Diagram posílání zpráv systémem D-Bus 28

7.1 KFingerManager je součástí „*Nastavení systému*“ 33
7.2 Průběh zavádění otisku prstu 34
7.3 Chybová zpráva při pokusu smazat pouze jeden otisk prstu 35
7.4 Potvrzovací dialog před smazáním všech otisků prstů 35
7.5 Diagram komunikace mezi třídami a se službou `fprintd` 36

8.1 Správce přihlášení KDM 40
8.2 Výběr autentizačních modulů ve správci přihlášení KDM 41
8.3 Schéma komunikace při přihlašování 43
8.4 `Kgreet_plugin` použitý k odemčení spořiče obrazovky 44

10.1 Uživatelské rozhraní PAM modulu fingerprintPAM 47
10.2 Textové rozhraní PAM modulu fingerprintPAM 48

Kapitola 1

Úvod

Mnoho nově zakoupených notebooků je vybaveno snímačem otisků prstů. Výrobce notebooku ve většině případů podporuje pouze operační systémy Windows firmy Microsoft. Často jen v nejnovější verzi – Windows Vista. Předešlé verze, například XP a nižší, nejsou podporovány nebo jsou podporovány pouze omezeně. Uživatelé alternativních operačních systémů, kteří by rádi využili čtečku otisků prstů k přihlášení do systému, pro přístup k úschovně hesel či pro identifikaci uživatele v různých hrách (nejvyšší dosažené skóre, načtení herního profilu a jiné) mají smůlu – čtečka otisků prstů není v jejich systému podporována. Podpora pro autentizaci pomocí otisků prstů patří s 3717 hlasy od konce roku 2005 mezi nejvíce žádané vlastnosti pracovního prostředí KDE [8]. S větší dostupností snímačů otisků prstů se tlak na podporu biometrické autentizace zesiluje.

Diplomová práce navazuje na výzkum provedený v rámci semestrálního projektu. Jde o kapitoly 2 – 5. Semestrální projekt se zabýval problematikou ověřování identity (kapitola 2), popisoval funkci biometrického systému (kapitola 3) a identifikaci a verifikace pomocí otisků prstů (kapitola 4), zkoumal možnosti ověření identity v Unixových operačních systémech (kapitola 5).

Cílem této diplomové práce bylo implementovat aplikaci, která umožní autentizaci uživatele pomocí otisků prstů za využití služby `fprintd`. Kapitola 7 popisuje vytvořený program pro správu otisků prstů, kapitola 8 popisuje grafického správce přihlášení KDM, možňosti jeho rozšíření o nové autentzační moduly a vytvořený modul pro verifikaci uživatele pomocí otisků prstů.

Mezi použité technologie patří D-Bus, služba `fprintd` a knihovna `libfprint` (kapitola 6).

Diplomová práce dále diskutuje problémy návrhu autentizačního systému PAM a grafických aplikací (kapitola 9) a alternativní přístup použitý v FingerprintGUI (kapitola 10).

Kapitola 11 popisuje možnosti dalšího vývoje jednotlivých částí celého autentizačního řetězce a kapitola 12 zhodnocuje dosažené výsledky.

Kapitola 2

Základní pojmy počítačové bezpečnosti

Počítačová bezpečnost je velice obsáhlá oblast pro vědecké bádání. Obsahuje spoustu disciplín jako je kryptografie, kryptoanalýza, návrh a vývoj bezpečných systémů, bezpečné programování, automatická verifikace, zálohování a jiné. V poslední době se začíná prosazovat i biometrie a její využití pro identifikaci nebo verifikaci uživatele. Mezi základní pojmy patří identita, identifikace, verifikace a autentizace.

Pojem *identita* (latinsky *identitas*, odvozené od slova *idem – stejný*), neboli *totožnost*, se používá tehdy, když porovnáváme pojmy, objekty apod. Identitu chápeme jako totožnost něčeho s něčím případně se sebou samým [28].

Lidská identita je kombinace biologických i psychických, vrozených i získaných individuálních a specifických vlastností a schopnosti vnímat sám sebe. Další rozvoj naší osobnosti je závislý právě na schopnosti vnímání své vlastní identity [28]. Je to jednoznačná charakteristika každého z nás. Je ovšem nutné rozlišovat pojem fyzické a elektronické identity. *Fyzickou identitu* máme pouze jednu, *elektronických identit* můžeme mít kolik chceme (např. různé e-mailové účty, diskuzní fóra a další) (upraveno z [10]).

Slovo *identifikace* se zejména v poslední době stalo velice často používaným a moderním termínem, který v souvislosti s dalším věcným kontextem může nabývat nejrůznějších významových zabarvení. To je způsobeno zejména tím, že lidská společenství, státy, státní instituce, veřejné právní i privátní organizace a nakonec i jedinci mají stále větší zájem (nebo jsou dokonce nuceni) ve své praktické činnosti důsledně rozlišovat a zcela exaktně ztotožňovat nejrůznější jevy a jejich projevy (důsledky), akce a činnosti, zájmy a potřeby, osoby, zvířata, předměty, různé materiály apod. a podle toho korigovat své cíle, způsoby jejich optimálního dosažení, využití, udržení a zabezpečení jejich dalšího pozitivního rozvoje; tedy své vlastní chování. Mnohdy je to ochrana vlastních zájmů (státních, komerčních, soukromých či jiných) nebo dokonce otázka samotného existenčního přežití (konkurenční boj, vojenství a jiné).

V minulosti byl pojem *identifikace* spojován především s vojenskými a bezpečnostními aplikacemi. Vědecky orientovaná identifikace osob byla spojována hlavně s kriminalistickými a forenzními disciplínami.

Další, mnohem širší rozvoj zájmu o identifikaci samotnou, stejně jako o nejrůznější efektivní identifikační metody a postupy, byl zapříčiněn celkovým rozvojem lidstva, světové politiky, ekonomiky a moderních technologií, zejména pak informatiky a telekomunikací. Rozvoj počítačových a komunikačních technologií bouřlivě a masově probíhal teprve po-

slední dvě desetiletí dvacátého století.

Identifikace slouží ke zjištění identity osoby. Jedná se o situaci, kdy osoba zadá systému svoje „*tajemství*“, ale nesdělí mu svoji identitu. Systém pak má určit identitu na základě „*tajemství*“. Dojde k porovnání vzorku ze vstupu s celou databází vzorků, výstupem je „*identita nalezena*“ nebo „*identita nenalezena*“. Tento proces prohledávání databáze je časově velice náročný, zvláště pak u rozsáhlejších systémů obsahujících veliké množství registrovaných uživatelů. Pak je vhodné takovou databázi rozdělit na menší (upraveno z [10]).

Identifikace se též označuje jako porovnání 1:N nebo porovnání 1:MANY.

Autentizace je proces ověření (a tím i ustavení) identity (s požadovanou mírou záruky) uživatele nebo entity v systému, většinou s cílem řízení přístupu ke zdrojům v systému. Z uvedené definice vyplývá základní rozdělení autentizačních metod podle druhu zúčastněných subjektů. Rozeznáváme tedy autentizaci ve vztahu člověk – stroj, autentizaci ve vztahu stroj – stroj a autentizaci dat [9].

S pojmem *autentizace* se také často setkáváme u přístupových systémů. Při autentizaci systém potvrzuje autentičnost dané osoby. O autentizaci se může jednat jak při verifikaci tak při identifikaci. Rozhodnutí o hodnověrnosti uživatele proběhne na základě „*prahu*“. Pokud hodnota při porovnaní překročí tento práh, je uživatel hodnověrný jinak není. Práh pro porovnání například hesla je naprostá shoda, naopak u biometrických systémů je nastavení prahu složitým procesem (upraveno z [10]).

V případě verifikace uživatel zadá svoji elektronickou identitu a na základě ní dojde k ověření fyzické identity. Uživatel sdělil systému svoji identitu hned na počátku jejího ověřování a tak systém vyhledá jeho záznam. Při neexistujícím záznamu je uživatel okamžitě odmítnut. Pokud je záznam nalezen, dojde k porovnání „*tajemství*“ a v případě shody systém odpoví „*potvrzeno*“, jinak „*nepotvrzeno*“ (upraveno z [10]).

Verifikace bývá také označována jako porovnání 1:1, protože dojde k porovnání jedněch uložených dat s jedněmi vloženými daty.

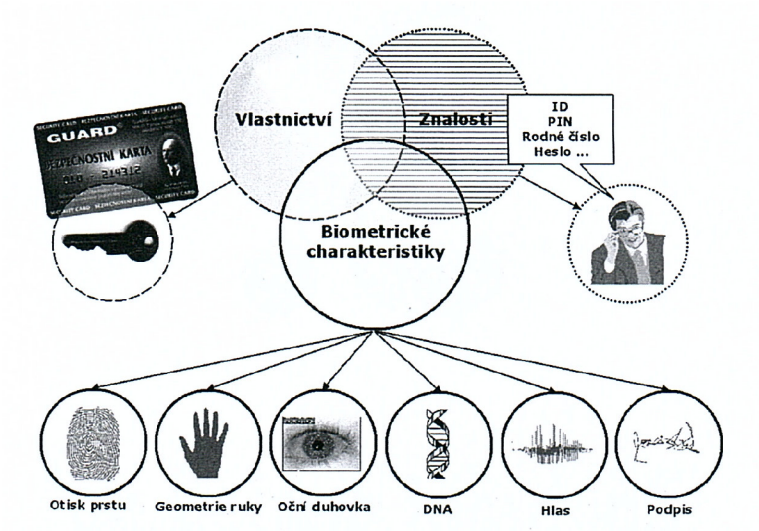
2.1 Možnosti ověření identity

Prokázání identity může být založena na několika různých možnostech. Každou možnost je možné pak dále specializovat, konkretizovat (viz obrázek 2.1):

- něco vím (heslo, pin, tajné tlačítko, ...),
- něco mám (klíč, RFID, kalkulátor, ...),
- něco jsem (otisky prstů, geometrie ruky, ...).

Něco vím

Historicky pravděpodobně nejstarší a ve své základní podobě nejméně kvalitní autentizační metodou je metoda založená na důkazu znalostí. Uživatel musí být vybaven znalostí hesla v dané podobě (numerického PIN, alfanumerického hesla – *password*, dlouhého alfanumerického hesla – *pass phrase*, atd.), kterou na výzvu systému prokáže zadáním z klávesnice. Hesla se dělí na statická (uživatel vždy zadává stejné heslo), hesla dynamická (zadávané heslo se mění podle předem známého algoritmu) a hesla jednorázová (heslo lze použít pouze jednou, uživatel má vytištěný aršík s jednorázovými hesly). Heslo bývá občas označováno jako sdílené tajemství.



Obrázek 2.1: Základní způsoby identifikace osoby (převzato z [28])

Problém nastane v okamžiku, kdy se uživatel zachová nezodpovědně a heslo úmyslně či neúmyslně kompromituje. Například volbou snadno uhodnutelného hesla, jeho prozrazením třetí osobě či zapsáním na místo přístupné třetím osobám. Druhá možnost aktivního útoku na autentizační protokol tohoto typu spočívá v odposlechu hesla. Ať už odpozorováním jeho zadání z klávesnice, skrytým programem typu trojský kůň, analýzou souborů s hesly uloženého na disku či získáním nezakódovaného hesla uloženého v operační paměti počítače (upraveno z [9, 28]).

Silná hesla by měla splňovat několik zásad (upraveno z [6]):

- **Délka hesla:** Minimální délka hesla by měla být 8 znaků.
- **Kombinace znaků:** Pro dosažení bezpečnosti hesla je nutné aby heslo bylo tvořeno kombinací čísel, speciálních symbolů, velkých a malých písmen. V ideálním případě alespoň 2 znaky z každé skupiny. Také je důležité se vyhnout speciálním znakům, které může být problém zadat na klávesnici s jiným rozložením (česká × anglická klávesová mapa).
- **Slovníkové výrazy:** Protože lámání hesel hrubou silou je časově velice náročná záležitost, kterou moderní operační systémy navíc znesnadňují zpomalováním reakce s rostoucím počtem pokusů, je velice často používanou metodou slovníkový útok. Při tomto útoku má útočník připravený slovník nejpoužívanějších slov, které bude zkoušet. Například některými administrátory oblíbené heslo *toor* nebo *god* pro uživatele root.
- **Osobní údaje:** Heslo by za žádných okolností nemělo obsahovat jméno, příjmení uživatele ani jeho blízkých, přátel, kočky, psa, ... Také by nemělo obsahovat žádná identifikační čísla (rodné číslo, číslo pasu, číslo občanského průkazu, a jiné) které mají nějakou spojitost s uživatelem.
- **Různá hesla:** Pro každý počítačový systém, je vhodné mít odlišné heslo. Při prozrazení hesla u jedné služby, poskytovatele, systému zůstanou ostatní systémy ne-

ohroženy. Pokud by se použila hesla stejná nebo podobná, hrozí, že kompromitací jednoho účtu uživatele budou otevřeny ke kompromitaci další účty téhož uživatele.

V unixových operačních systémech využívajících k autentizaci systém PAM lze vynutit požadavky na heslo pomocí parametrů modulů `pam_unix` a `pam_cracklib`. Více na straně 24. Silná hesla lze uživatelům vygenerovat – lze využít služeb programů jako je apg [21], pwgen [34], makepasswd [27] a jiných.

Něco mám

Poněkud dokonalejší metodou je využití bezpečnostních předmětů. Autentizace je v tomto případě provedena důkazem vlastnictví. Uživatel je vybaven vhodným bezpečnostním předmětem, který při autentizaci připojí (případně vloží, přiloží, atd.) k příslušnému čtecímu zařízení. Systém přečte předepsaným způsobem data uložená na bezpečnostním předmětu a využije je k autentizaci uživatele. V naprosté většině případů je bezpečnostní předmět určen pro pouhé (i když zabezpečené) uložení nějaké formy hesla. To umožňuje používat kvalitnější (tedy delší a nesnadno uhodnutelná, často dokonce náhodně generovaná) hesla a pravidelně je měnit bez jakýchkoliv nároků na zátěž paměti uživatelů. Pokud je zajištěn bezpečný komunikační protokol s bezpečnostním předmětem[1], chráněn proti zneužití při ztrátě předmětu[2], jedná se o bezpečnou metodu [9].

Pro autentizaci založenou na „*něco mám*“ lze použít (upraveno z [28]):

- **Osobní doklady:** Osobní doklady zpravidla obsahují fotografii držitele, datum a místo narození, národní příslušnost, národnost, osobní identifikační číslo (rodné číslo, číslo pojištění), identifikační číslo dokladu, datum vydání/platnosti dokladu, další osobnostní charakteristiky (výška, váha, barva očí, podpisový vzor, či jiné biometrické charakteristiky) (obrázek 2.2).

- **Plastové identifikační karty a čipy:** Historie karet začíná věrnostními kartami, ty později se začaly používat jako karty platební až se vyvinuly do dnešní podoby – ke kartám věrnostním a platebním přibyly karty identifikační. U identifikačních karet je důležité sledovat stupeň ochrany proti pozměnění a padělání, kompatibilita s mezinárodními normami, maximální funkční spolehlivost, vysoká odolnost proti vnějším vlivům. Pro účely identifikace a autentizace se v počítačových systémech používají identifikační karty s magnetickým záznamem nebo karty čipové (smart card) (obrázek 2.4).

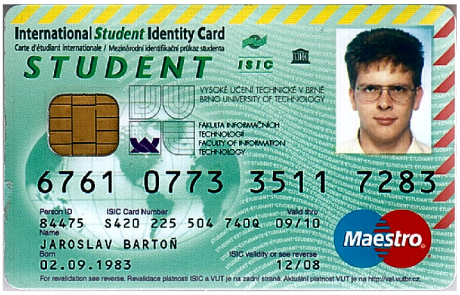
- **Biočip:** Počítačové čipy se postupně staly součástí různých zařízení, mezi nimi jsou také identifikační karty. Ale čipy lze použít i samostatně. Mnoho let se používají pro identifikaci zvířat, čip ve velikosti zrnka rýže je implantován pod kůži zvířete do oblasti lopatek. V čipu mohou být zaneseny údaje o majiteli, adresa a jiné. Poslední dobou se začíná objevovat myšlenka implantování čipu do lidského těla (obrázek 2.3).

[1] Předmět například nevydá heslo, pokud se systém vůči němu vhodně neautentizuje, což chrání předmět proti okopírování, klonování.

[2] Například přídavný PIN zadávaný uživatelem.

Obrázek 2.2: Občanský průkaz České republiky (převzato z [22])

Obrázek 2.3: Biočip (převzato z [43])



Obrázek 2.4: Plastová identifikační karta kombinovaná s čipovou platební kartou používaná na VUT

Něco jsem

Technologicky prozatím nejméně zvládnutá je technologie autentizace pomocí důkazu vlastností. Vychází z předpokladu, že každý člověk disponuje jistými unikátními a neměnnými tělesnými vlastnostmi (otisk prstu, obraz očního pozadí či duhovky, rytmus psaní na klávesnici, barva a tón hlasu, aj.), které má vždy k dispozici (odpadá nutnost nosit například čipovou kartu), aniž by si musel cokoliv pamatovat (odpadá nadměrná zátěž na paměť). Obecně lze říci, že řada biometrických zařízení zatím nedosáhla potřebného standardu [9]. Autentizaci pomocí „*něco jsem*“ lze nazvat biometrikou. Aby byly biometrické systémy bezpečné je třeba detekce živosti [30].

Biometrické metody používané v běžné praxi [28]:

- **Geometrie ruky:** Podstatou této metody je dvou nebo třírozměrné snímání délek nebo šířek jednotlivých prstů, kloubů nebo kostí.

- **Otisky prstů:** Otisky prstů jsou uznávány jako celosvětový standard policejně-soudní i bezpečnostně-komerční identifikace. Metoda je založena na unikátních obrazcích papilárních linií. Snímání otisků prstů neprobíhá jen pomocí klasického kriminalistického způsobu pomocí daktyloskopické černě, ale byly vyvinuty i speciální optickoelektronické čipy pro přímé snímání.

- **Krevní řečiště:** Biometrické technologie založené na snímání žil hřbetu/dlaně ruky (případně prstu) jsou jedny z nejmladších. Struktura žilního řečiště vytváří již před porodem a v dospělém věku se nemění, je velice výrazná a jedinečná. Snímání žilního řečiště je bezkontaktní metoda, na snímači nezůstávají latentní informace, zlepšuje hygienické podmínky. Při snímání jsou odmítnuty neživé předměty (není nutná detekce živosti). Hřbet/dlaň ruky je nasvícen infračerveným světlem a sejmut kamerou pracující v infračerveném spektru [4].

- **Rozpoznávání tváře, tvar ucha:** Tvář je pro každou osobu specifická. Výkonné počítačové technologie dokáží rozpoznávat tváře jednotlivých lidí podobným způsobem jako člověk. Lidská tvář obsahuje identifikační body, které jsou specifické a časově neměnné.

- **Ruční písmo a podpis:** Dochází ke zpracování nejen statických obrazů podpisu, ale i dynamických charakteristik při jeho psaní – rychlost pera, přítlak, směr podpisu, náklon pera a další relační charakteristiky.

- **Hlas a řeč:** Lidský hlas obsahuje mimo jiné i biometrické charakteristiky, které nelze zaměnit nebo zapomenout. Lidský hlas má charakteristiky fyziologické i behaviorální. Akustický signál hlasu je transformován do unikátního digitálního kódu.

- **Oční duhovka**: Barevný kruh kolem zorničky lidského oka obsahuje specifické unikátní identifikační body, pomocí kterých je možné s velkou přesností stanovit identitu osoby. Duhovka se skládá z náhodně rozmístěných, v čase neměnných barevných struktur, podobných sněžným vločkám. Žádné dvě duhovky oka nejsou stejné. Snímání probíhá za pomoci standardní video technologie [32].

- **Oční sítnice:** Obsahuje rovněž dostatek specifických anatomických bodů, které zajišťují vysokou identifikační přesnost. Snímání biometrického vzorku probíhá světelným paprskem. Bílá sítnice lidského oka část paprsku pohlcuje, část odráží. Takto je zmapováno řečiště drobných žilek a cévek sítnice, které zůstává během života jedince téměř neměnné.

- **DNA:** Má předpoklady stát se nejpřesnějším a nejspolehlivějším identifikátorem lidské bytosti. Obsahuje obrovské množství informací o každé osobě. Jen nepatrná část z nich je již dostačující pro identifikaci osoby. V 21. století bude hrát v kriminalistice i dalších oborech stejnou roli jako daktyloskopie ve století dvacátém.

Kapitola 3

Biometrie a biometrické systémy

Každá osoba je identická jen a pouze sama se sebou. Jestliže vědecky prokážeme a je prokázáno, že i naše fyzické (a psychické) charakteristiky jsou jedinečné, pak je lze úspěšně použít pro efektivní identifikaci osoby s velmi vysokým stupněm jedinečnosti a tedy i bezpečnosti a prokazatelnosti. Identitu osoby je pak téměř nemožné absolutně napodobit nebo pozměnit. Nelze ji ani odcizit, protože identifikační charakteristiky jsou bezprostředně spojené s identifikovanou osobou. Biometrická identita je navíc pro každého člověka přirozená – vlastní. Je s ním spojena již od narození [28].

Použití biometrických identifikačních metod se datuje až po faraonské dynastie Egypta, kde lidé byli měřeni, aby mohli býti identifikováni. Existuje mnoho písemných dokladů, popisujících biometrickou identifikaci osob v údolí Nilu, která zde byla „komerčně“ realizována již v době rozvoje prvního zemědělství. Pěstitelé obilí byli rozpoznáváni pomocí unikátních jizev a poranění, které v minulosti utrpěli, podle barvy a dalších charakteristik pleti, barvy očí, rozměrů a vah těla. Identifikace rolníků byla prováděna při výkupu obilí pro centrální sklady a sloužila k vyplácení mzdy a provize za vypěstované a prodané obilí do státních rezerv.

Zmínku o biometrické identifikaci nalezneme i ve Starém zákoně (12:5-6), ve kterém je popsáno vyvraždění 42000 osob, které v dnešním pojetí „neprošli biometrickou hlasovou verifikací“. Když Izraelité (konkrétně Efraimští) prchali z Egypta, byli pronásledováni faraonovým vojskem. Vojáci rozpoznávali uprchlíky od ostatních podle chybné výslovnosti slova „*shibboleth*“ (v českém překladu bible šibolet). Ti, kteří nesprávně vyslovovali toto slovo s písmenem „s“ na začátku, byli popravováni.

Identifikaci založenou na otiscích prstů (daktyloskopii) znali již staří Číňané. Babyloňané používali při potvrzování obchodních smluv otisk palce jako podpis na hliněných tabulkách. Obdobným způsobem byly ztvrzovány písemnosti v Persii.

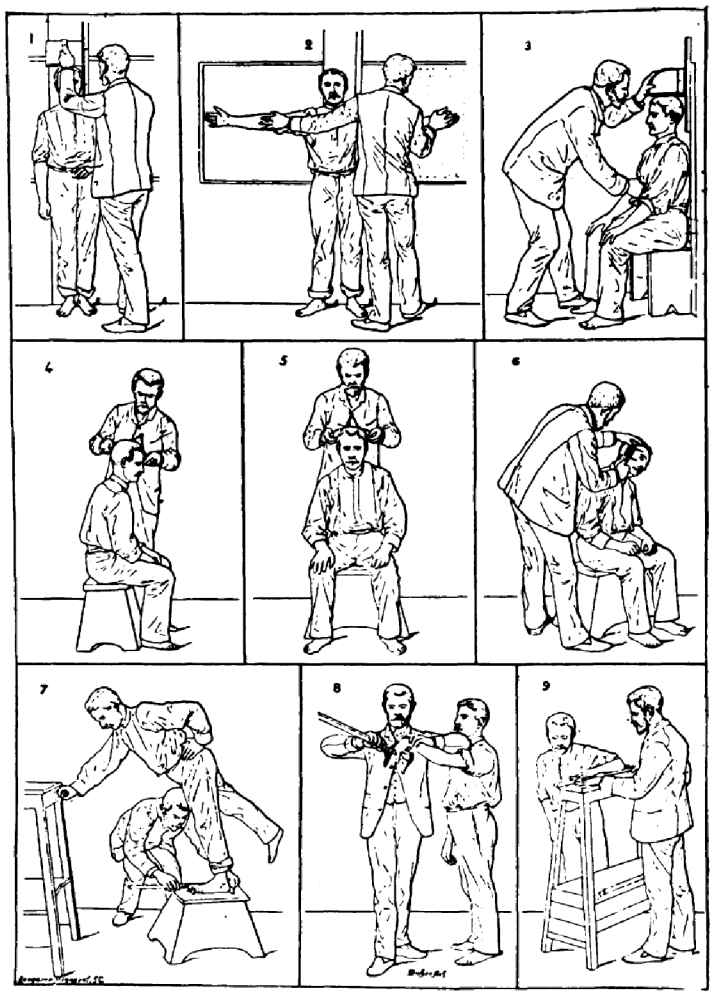
Na evropském kontinentu otisky prstů, tvořené „vrstevnicemi“, spirálami a smyčkami popsal v roce 1686 italský profesor anatomie *Marcello Malpighi*, aniž by si uvědomil jejich význam pro identifikaci.

Obrazci papilárních linií se hluboce vědecky zabýval (1832) až významný český přírodovědec a lékař *Jan Evangelista Purkyně*. Jeho zájem byl však přírodovědecký a lékařský, i když sám také navrhoval možnost dělení a třídění obrazců papilárních linií na základě vyskytujících se geometrických vlastností.

Na zavedení daktyloskopie do kriminalistické praktické činnosti se podílela celá řada vědců i praktiků, velmi často s lékařským vzděláním. Např. Sir *William J. Herschel* využíval v Indii otisky prstů jako potvrzení o převzetí finančních částek od roku 1856. *Dr. Henry Faulds* 1880 v Japonsku využíval nalezené daktyloskopické stopy k identifikaci předem vy-

tipovaných osob a uvažoval o zavedení daktyloskopických sbírek (evidencí). *Francis Gallton* 1880 a *Edward Henry* potom založili základy praktického využívání daktyloskopie kromě jiného i tím, že vytvořili třídící a registrační systémy využitelné v praxi.

Francouzský vědec, etnolog *Alphonse Bertillion* pro identifikaci osob zavedl do francouzské kriminalistické praxe metodu (tzv. *bertillionáž*) založenou na popisu a geometrickém měření rozměrů lidského těla a hlavy (obr. 3.1). Na základě těchto rozměrů rozčleňoval osoby do 243 kategorií. Znalost barvy očí a vlasů umožnila členění až do 1701 skupin. Metoda byla koncem 19. století postupně vytlačena daktyloskopií.



Obrázek 3.1: Bertillionáž (převzato z [42])

1) tělesná výška, 2) délka natažené paže, 3) výška v sedu, 4) délka hlavy, 5) šířka hlavy, 6) délka pravého ucha, 7) šířka pravého ucha, 8) délka levé nohy, 9) délka levého prostředníčku, 10) délka levého malíčku, 11) délka levého předloktí

Komerční využití biometrické identifikace bylo odstartováno v roce 1970 systémem nazvaným *Identimat*, který měřil *geometrii ruky* a byl využit pro přístup do investiční firmy *Shearson Hamill* na newyorské Wall Street. Tímto způsobem byla zároveň evidována docházka zaměstnanců. Stovky podobných zařízení byly následně instalovány v objektech společnosti *Western Electric*, americká námořní výzvědné služby a na ministerstvu energe-

tiky, stejně jako v dalších podobných objektech. Identimat sloužil až do roku 1980, kdy byl nahrazen zdokonalenými zařízeními.

V sedmdesátých letech 20. století bylo zpracování otisků prstů pro soudní praxi realizováno již na počítačích, které našly své místo na všech daktyloskopických pracovištích. Dnes se otisky prstů pro policejní a bezpečnostní účely na celém světě zpracovávají výhradně pomocí výpočetní techniky.

Technologie automatického rozpoznávání otisků prstů (*AFIS – Automated Fingerprint Identification System*) postupně pronikla i do civilního sektoru, kde se v průmyslově rozvinutých zemích stala základem pro kontrolu přístupu (do budov, technologických nebo počítačových zařízení, k bankomatům, ...).

Souběžně s vývojem identifikace pomocí otisků prstů probíhal vývoj i dalších biometrických metod. Například první metoda určená k identifikaci osob na základě struktury sítnice byla uvedena do provozu v roce 1980. Práce matematika *Dr. Johna Daughmana* z University of Cambridge položila základy pro průmyslově využitelnou identifikaci osoby pomocí *oční duhovky*.

Identifikace osoby pomocí počítačově zpracované *podoby lidské tváře* nebo podle podpisu jsou mladšího data. Na přelomu 20. a 21. století je intenzivně zpracováván lidský genom a technologie identifikace osoby pomocí deoxyribonukleové kyseliny (DNA) bude minimálně stejně převratná jako otisky prstů před více jak sto lety. Její využití je dnes převážně v kriminalisticko-policejní a soudně-znalecké praxi, ale postupně se prosadí i pro civilní účely.

Historie biometrické identifikace je převzata z [28].

3.1 Kritéria pro biometrický systém

Kritéria pro biometrický systém lze rozdělit do několika oblastí – operační, technická, metodologická, výrobní a finanční. Dále v textu se budu zabývat pouze kritérii *operačními* a *technickými*.

Operační kritéria

Mezi operační kritéria biometrických systémů patří následující [28] (přehled pro jednotlivé metody viz tabulka 3.1):

- **Jedinečnost:** Biometrické charakteristiky dané identifikační metody musí být dostatečně jedinečné (unikátní), aby bylo možné odlišit jednu osobu od druhé s vysokou přesností a spolehlivostí.

- **Neměnnost:** Prvky (markanty), na kterých je založena biometrická identifikace, musí být v čase neměnné. Je žádoucí, aby vlastnosti člověka, které se měří a dále technologicky zpracovávají, byly neměnné po celou dobu jeho života, nebo alespoň po dobu od produktivního do důchodového věku. Optimální je absolutní stálost identifikačních znaků.

- **Měřitelnost:** Charakteristiky, na nichž je založena identifikace musí být měřitelné a symbolicky vyjádřitelné. Musí být do předu známa teoretická i praktická chybovost měření, než je biometrická metoda zavedena do rutinní praxe.

- **Uchovatelnost:** Naměřené identifikační charakteristiky musí být možné uchovávat s přijatelnými náklady, aniž by došlo ke ztrátě jejich kvality.
- **Spolehlivost:** Proces měření, zpracování, ukládání a vyhodnocování biometrických charakteristik musí být dostatečně spolehlivý a kdykoliv zopakovatelný se stejnými výsledky.
- **Exkluzivita:** Identifikační metoda by měla být dostatečná takovým způsobem, aby nebyla nutná další podpůrná identifikační činnost.
- **Praktičnost:** Metoda musí být po všech směrech praktická. Uživatel by měl být v minimálním kontaktu s technologickým zařízením a během procesu identifikace ztratit co nejméně času, měl by vykonat minimální množství požadovaných úkonů. Měření by mělo být co nejjednodušší, obsahovat co nejméně měřených a ukládaných charakteristik a vyžadovat minimum tréninku uživatele.
- **Přijatelnost:** Snímání, stejně jako další zpracování, uchování a vyhodnocovaní biometrických údajů by mělo být přijatelné pro vysoké procento lidí. Metody, které zasahují do integrity lidského těla nebo ho poškozují, oslabují nemohou být použity. Stejně tak není vhodné používat biometrické metody, které by mohly vystavit uživatele nepříjemné zvědavosti okolí. Jednotlivec i společnost musí být přesvědčeni, že zařízení je odolné proti podvodům a padělkům nejrůznějšího typu a je spolehlivé. Musí být zajištěna ochrana všech získaných údajů před neoprávněným přístupem či zneužití.
- **Uživatelská přívětivost:** Proces snímání a vyhodnocovaní nesmí být nikterak vtíravý, ale naopak nerušivý. Osoba by neměla mít žádné nepříjemné pocity diskriminace v souvislosti například s barvou pleti, věkem, profesí, fyzickým či psychickým stavem. Daná metoda identifikace a z ní vyplývající periferní snímací zařízení by měly být vhodně zvolené, aby nerušily.

Biometrická metoda	Snímání	Neměnnost	Jednoznačnost	Přijatelnost
Geometrie ruky	Optické – infračervené	Dobrá	1:10 000	Velmi dobrá
Otisk prstu	Optické, elektronické	Velmi dobrá	1:1 000 000	Dobrá
Žilní řečiště	Optické – infračervené	Dobrá	Neznámá	Velmi dobrá
Tvář	Optické, infračervené	Dobrá	Neznámá	Dobrá
Hlas	Elektroakustické	Proměnlivá	1:10 000	Dobrá
Podpis	Statický obraz, dynamické	Proměnlivá	1:10 000	Velmi dobrá
Oční duhovka	Optické	Velmi dobrá	1:6 000 000	Nedobrá
Oční sítnice	Optické – laser	Velmi dobrá	1:1 000 000	Nedobrá

Tabulka 3.1: Základní biometrické metody a jejich charakteristiky (upraveno z [10, 28])

Technická kritéria

Mezi nejčastěji vyhodnocovaná kritéria v oblasti technického řešení biometrické identifikace obvykle patří následující charakteristiky (upraveno z [28]):

- **Čas zpracování a vyhodnocení:** Čas nutný pro zpracování a vyhodnocení identifikačních charakteristik by měl být co nejkratší (maximálně jednotky vteřin) – uživatel pak nemá pocit promrhaného času a systém lépe akceptuje.

- **Přijatelná chybovost:** Chyba snímání (kvantizační šum, šum prostředí, šum přenosového kanálu, šum snímače), chyba zpracování (předzpracování dat, extrakce rysů, klasifikace), chyba vyhodnocení (chybné odmítnutí – FRR, chybné přijetí – FAR).

- **Nezávislost na vnějším prostředí:** Zařízení nesmí být ovlivňováno vnějšími vlivy prostředí – elektromagnetický šum, protisvětlo, hluk, teplota (zmrzlé × upocené ruce), vlhkost, kouř, prach.

- **Požadovaný prostor na uložení a zpracování charakteristik, velikost šablony:** I přes relativně malou velikost šablony na jednoho uživatele je důležité sledovat požadavky na požadovaný prostor na uložení a zpracování charakteristik. S rostoucím počtem zavedených uživatelů rostou nároky na požadovaný prostor a u zařízení s vnitřní pamětí (nevyžadujících stálé připojení k centrální databázi) lze snadno narazit na limit počtu uživatelů a také roste čas potřebný k identifikaci uživatele (prozkoumání celé databáze).

3.2 Biometrický systém

Biometrické zpracovaní probíhá v pěti základních etapách [28] (obrázek 3.2) – sběr dat, přenost dat, zpracování signálu, proces rozhodování a uložení dat.

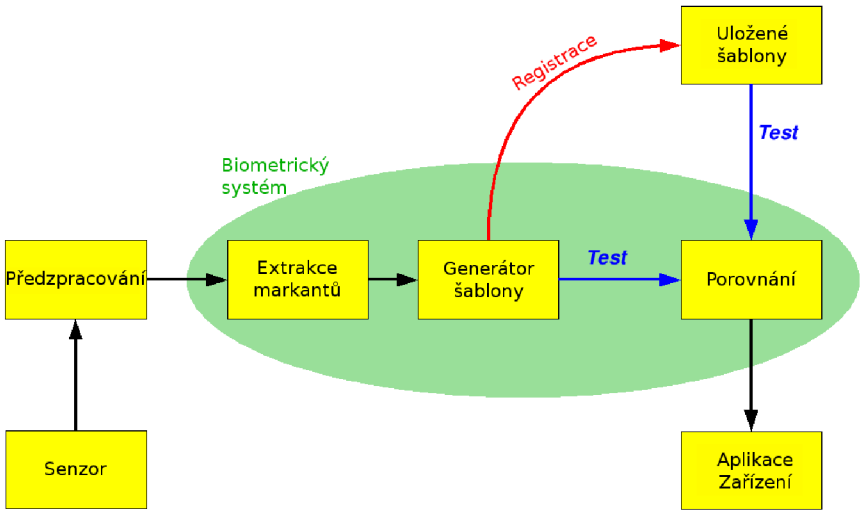
Biometrické zpracování začíná měřením anatomicko-fyziologických nebo behaviorálních charakteristik člověka – snímání biometrických dat senzory (sběr dat). Měření musí být opakovatelná záležitost, naměřené hodnoty musí být vždy stejné nebo s předem známou a vyhovující přesností.

Mezi jednotlivými moduly biometrického systému mezi sebou komunikují (přenos dat). Pokud systém zpracovává nebo skladuje data na jiném místě než je umístěn je třeba zabezpečit přenos dat. Biometrické aplikace pracují obecně s velkými objemy dat. Aby byl přenos a jejich uložení bylo efektivní (rychlé, minimálně zatěžovalo přenosové kanály, kladlo nízké požadavky na skladovací prostor, a pod.), před přenosem a dalším zpracováním se data komprimují.

Zpracování signálu se může dále dělit na více kroků – *předzpracování signálu* a *generování šablony* (pro uložení nebo porovnání). *Předzpracování signálu* je proces úpravy signálu do formy vhodné pro další zpracování (filtrování, zesílení a další). *Generování šablony* provede extrakci unikátních biometrických charakteristik, kontrolu kvality a vyhledání v databázi porovnáním s dalšími vzorky markantů.

Během rozhodování je získána šablona z databáze uložených šablon a šablony vzniklé z právě nasnímané biometrické vlastnosti. Probíhá porovnání uložené šablony se šablonou právě nasnímaného vzorku. První ukládání tzv. referenční šablony se nazývá registrace (enrollment) šablony (template). Cílem porovnání je ztotožnit nasnímanou šablonu se šablonou (šablonami) uloženou v databázovém systému (porovnání 1:1, 1:N – verifikace, identifikace).

Rozlišujeme uložení dat v kriminalisticko-soudním a komerčně-obchodním prostředí. V kriminalisticko-soudním prostředí se budou ukládat jak výchozí nasnímané data, tak šablony které z nich vznikly. Je to proto, že pouze původní, nasnímaná data lze předložit jako důkaz. Naopak v komerčně-obchodním prostředí se ukládají spíše šablony. V praxi se mohou také oba principy kombinovat. Pokud nějaký dodavatel biometrického systému vylepší algoritmy, lze původní nasnímané vzorky použít k tvorbě nových šablon poskytujících vyšší stupeň zabezpečení.



Obrázek 3.2: Zjednodušené schéma biometrického systému (přeloženo z [40])

3.3 Výkonnost biometrických metod

V okamžiku uvedení do praxe vzniká u zákazníků otázka: Jak je zařízení výkonné a spolehlivé? Jaká je spolehlivost metody na základě které bylo zkonstruováno? Pomocí jakých charakteristik lze porovnávat dvě zařízení, pracujících na stejných principech, vyrobené odlišnými výrobci [28]?

V průběhu let byly zavedeny dva základní pojmy [28, 10]:

1. **Pravděpodobnost chybného odmítnutí** autorizované osoby biometrickým zařízením (v anglické literatuře nazývané **False Rejection Rate, FRR**).

2. **Pravděpodobnost chybného přijetí** neautorizované osoby (v anglické literatuře **False Acceptance Rate, FAR**) (vztah FAR a FRR viz obrázek 3.3, 3.4).

Pravděpodobnost chybného přijetí nebo odmítnutí nelze teoreticky vypočítat. Biometrické metody identifikace/verifikace jsou založeny na statistickém vyhodnocování podobnosti biometrického vzoru a biometrické šablony. Při každém snímání biometrického vzoru nejsou zaznamenávány absolutně stejné hodnoty, stejné markanty pořizovaných charakteristik. V důsledku se pak i obě porovnávané šablony nepatrně liší. *Míra ztotožnění* (někdy nazývaná *výsledek porovnání*, *skóre*) je pak pokaždé odlišná a závisí především na každé biometrické aplikaci a jejím řešením [28].

Pravděpodobnost chybného odmítnutí – FRR

FRR je pravděpodobnost, že biometrický systém klasifikuje chybně dva biometrické vzory od stejné osoby jako odlišné a tím selže při přijetí oprávněného uživatele [10].

Pravděpodobnost chybného odmítnutí je definována jako [28]:

$$FRR = \frac{N_{FR}}{N_{EIA}} \tag{3.1}$$

nebo

$$FRR = \frac{N_{FR}}{N_{EVA}}. \tag{3.2}$$

N_{FR} je počet chybných odmítnutí, N_{EIA} je počet pokusů oprávněných osob o identifikaci a N_{EVA} je počet pokusů oprávněných osob o verifikaci.

Pravděpodobnost chybného přijetí – FAR

FAR je pravděpodobnost, že biometrický systém klasifikuje chybně dva biometrické vzory pocházejících od různých osob jako stejné a tím selže při odmítnutí neoprávněného uživatele (útočníka) [10].

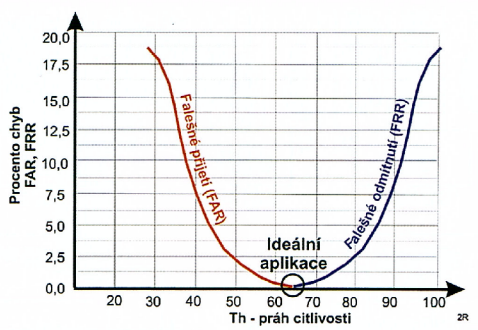
Pravděpodobnost chybného přijetí je definována jako [28]:

$$FAR = \frac{N_{FA}}{N_{IIA}} \tag{3.3}$$

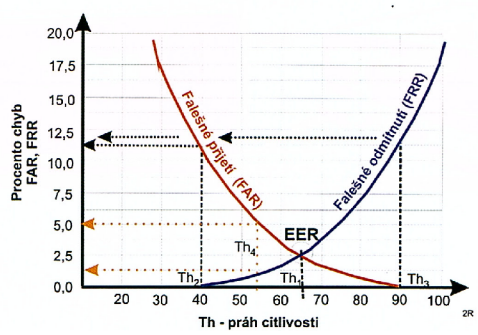
nebo

$$FAR = \frac{N_{FA}}{N_{IVA}}. \tag{3.4}$$

N_{FR} je počet chybných přijetí, N_{IIA} je počet pokusů neoprávněných osob o identifikaci a N_{IVA} je počet pokusů neoprávněných osob o verifikaci.



Obrázek 3.3: Vztah mezi FRR a FAR – ideální biometrická aplikace (převzato z [28])



Obrázek 3.4: Vztah mezi FRR a FAR – reálná biometrická aplikace (převzato z [28])

Další charakteristiky

Můžeme sledovat také následující charakteristiky [10]:

- **Míra neschopnosti nasnímat, FTA:** Udává podíl chybných záznamů v automatickém módu záznamu daného senzoru. Tj. zaznamenání biometrické charakteristiky je odmítnuto, ačkoliv je biometrická charakteristika přítomna. S rostoucí hodnotou FTA klesá vhodnost senzoru pro záznam biometrické charakteristiky. Slouží k hodnocení kvality senzorů.

- **Míra neschopnosti zaregistrovat, FTE:** Udává procentuální podíl uživatelů, které není schopen se systém naučit. Míry FTE se často vyskytují u systémů, které mají kontrolu kvality biometrické charakteristiky. Biometrické charakteristiky s nedostatečnou kvalitou nejsou systémem naučeny. Údaj FTE ohodnocuje schopnost algoritmu pracovat i s nekvalitními biometrickými charakteristikami.
- **Míra chybné shody, FMR:** Udává podíl chybně akceptovaných osob. Na rozdíl od FAR nejsou do celkových součtů brány v potaz pokusy, které byly neúspěšné ještě před samotným porovnáním (to je FTA, FTE).
- **Míra chybné neshody, FNMR:** Udává podíl chybně neakceptovaných osob. Na rozdíl od FRR nejsou do celkových součtů brány v potaz pokusy, které byly neúspěšné ještě před samotným porovnáním (to je FTA, FTE).

Kapitola 4

Identifikace a verifikace pomocí otisků prstů

Identifikace pomocí otisků prstů je jedna z nejznámějších a propagovaných biometrických metod. Otisky prstů jsou používány více jak století pro jejich unikátnost a neměnnost v čase. Identifikace pomocí otisků prstů je populární kvůli snadnému pořízení, velkému počtu zdrojů otisků (10 prstů) a jejich zavedenému použití v kriminalistice a kontrole imigrantů [23]. Informace uvedené v této kapitole a obrázky jsou převzaté z [10].

Otisk prstu normálně vypadá jako série tmavých linek, které reprezentují vystouplé *papilární linie* a světlých míst reprezentujících níže položené místo mezi dvěma papilárními liniemi (obrázek 4.1).

Obrázek 4.1: Charakteristické znaky otisků prstu – daktyloskopické markanty

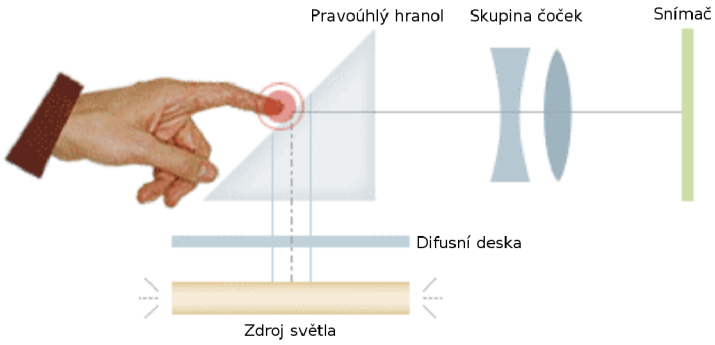
Dílčím úkolem automatizovaného zpracování daktyloskopických otisků je nalezení markantů, na základě kterých se dále provádí porovnání s jinými otisky. Vyhledávání daktyloskopických markanků probíhá na skeletizované[1] kresbě papilárních linií. Většina současných řešení využívá pouze nejjednodušší daktyloskopické markanty – začátek a ukončení papilární linie a dvojitou vidlici.

[1]Skeletizace – papilární linie jsou převedeny na tenké čáry o tloušťce jednoho pixelu.

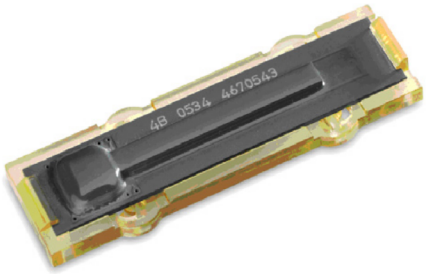
4.1 Typy snímačů

Existuje několik různých typů snímačů. Mezi nejčastěji používané se řadí:

- **Optický:** Jedná se o relativně jednoduchý optický princip. Zdroj světla osvětlí plochu prstu, který je přiložen na skleněnou plochu senzoru (existují bezkontaktní i 3D optické senzory) a kamera nasnímá (CCD) obraz (obrázek 4.2) [1].
- **Kapacitní:** Senzor je složen z matice malých vodivých plošek, na nichž je napařená vrstva nevodivého oxidu křemičitého. Jemnost těchto vodivých plošek je vyšší než jemnost papilárních linií. Přiložením prstu vzniknou nad plochami těchto plošek kondenzátory, jejichž výstupem je hodnota odpovídající překryvu plochy plošky [1, 37] (obrázek 4.4).
- **Tlakové:** Senzor je složen ze tří vrstev, přičemž mezi elektrovodivé vrstvy je vložen nevodivý gel. Přiložením prstu na plochu senzoru dojde ke stisku nevodivého gelu tak, že se elektrovodivé vrstvy dotknou.
- **Termické:** Princip je založen na tepelném záření – papilární linie mají vyšší vyzařování tepla jak prohlubně mezi nimi. Prst je protažen přes pyroelektrickou buňku, která snímá tepelné vyzařování (obrázek 4.3) [2].



Obrázek 4.2: Funkce optického snímače otisků prstů [1]



Obrázek 4.3: Termický snímač otisků prstů [2]

Obrázek 4.4: Kapacitní snímač otisků prstů [37]

4.2 Funkce systému

Funkce systému je znázorněna na obrázku 4.5, skládá se z následujících kroků:

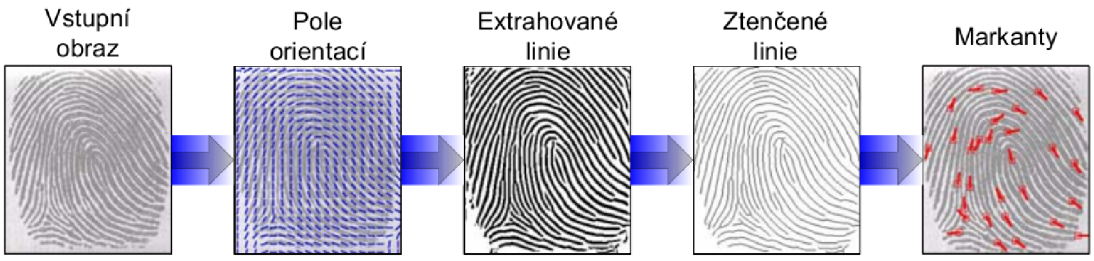
- **Vstupní obraz:** Získání obrazu otisku prstu ze senzoru či z jiné předlohy → digitální otisk prstu. Ve vstupním obrazu je velké množství šumu, což vyžaduje následnou úpravu ve třetím kroku zpracování. Také je nutné dbát na vlivy jako např. znečištění povrchu otisku prstu, poranění apod. Nezbytné je kontrolovat živost prstu, resp, zda není na prstu nalepen falešný otisk.

- **Pole orientací:** V každém bodu obrazu se spočte směr papilární linie z okolí (dle tónů šedé barvy). Nachází-li se bod přímo na papilární linii, určuje s maximální pravděpodobností její směr. Nejprve se vypočte pole orientací pro každý bod obrazu. Ve druhém kroku dojde k transformaci na blokové pole orientací. Blokové pole orientací je následně namapováno na původní obrázek otisku prstu.

- **Extrahované linie:** Úprava obrazu + černobílé linie. Také sem patří úpravy histogramu – například škálování histogramu. S tím je spjatá kontrola kvality výstupního obrazu. Pro filtrování se používá 2D Gaborova funkce. Pro prahování obrazu se využívá takzvané **schéma RAT** (*Regional Average Thresholding*), které nejprve rozdělí obrázek na bloky 8×8, potom spočte průměrnou úroveň šedé v této oblasti, dále nastaví hodnotu levé části 8×4 na tuto hodnotu a posune operační okno o 4 body vpravo. Je-li dosažen pravý okraj, posune se okno o 8 bodů dolů a začne se opět zleva.

- **Ztenčené linie:** Ztenčování papilárních linií na 1 pixel. Pro ztenčování se používá relativně jednoduchý algoritmus, jehož účelem je zredukovat počet pixelů na obrazu papilární linie tak, že její tloušťka je pouze 1 pixel.

- **Markanty:** Detekce a extrakce markantů. Zde se pro detekci papilárních linií používá takzvaná **Hongova metoda**. Ke každému markantu se ukládá pozice, typ (ukončení, vidlička) a gradient (orientace pokračování papilární linie). Extrahované markanty jsou porovnané se šablonou.



Obrázek 4.5: Schéma zpracování otisku prstu

Existují i metody založené na 2D korelaci mezi vstupem a šablonou (výpočetně náročné) a metody založené na vlastnostech papilárních linií – orientace a frekvence papilárních linií, tvar linie, texturní informace atd.

Kapitola 5

Identifikace a autentizace uživatelů v Unixových systémech

UNIX je víceuživatelský, víceúlohový systém. *Víceuživatelský* znamená, že operační systém umožňuje, aby stejný počítač používalo současně mnoho různých lidí. *Víceúlohový* znamená, že každý uživatel může současně spouštět mnoho různých programů.

Jedna ze základních vlastností takového operačního systému spočívá v tom, že zabrání různým lidem (nebo programům) aby se vzájemně ovlivňovali. Bez této ochrany by nevypočitatelný program (vytvořený nějakým studentem v úvodním kurzu programování) mohl ovlivnit ostatní programy a uživatele, mohl by náhodou vymazat nějaké soubory, nebo by dokonce mohl zastavit celý počítač. Aby k takovýmto nehodám nemohlo docházet, byla jakási forma počítačové bezpečnosti zahrnuta do základní filosofie UNIXu.

Unixová bezpečnost ovšem zajišťuje daleko více, než jen paměťovou ochranu. UNIX má promyšlený bezpečnostní systém, který ovládá způsob, jímž uživatelé přistupují k souborům, modifikují systémové databáze a používají systémové prostředky. Tyto mechanizmy bohužel nejsou příliš platné pokud je systém špatně nakonfigurován, neopatrně používán nebo obsahuje vadný software. Prakticky většina bezpečnostních problémů, které byly v UNIXu za celou dobu nalezena byla způsobena některou z těchto příčin a nikoliv nedostatky v samotném návrhu systému [6].

5.1 Soubor /etc/passwd

V souboru `etc/passwd` si UNIX ukládá údaje o všech uživatelích. Soubor `/etc/passwd` obsahuje uživatelské jméno, skutečné jméno, identifikační údaje a další základní údaje o účtu. Každý řádek v souboru popisuje jeden záznam databáze, položky záznamu se od sebe oddělují dvojtečkou [6].

Ukázka souboru `/etc/passwd`:

```
haldaemon:x:107:116:Hardware abstraction layer,,,:/home/haldaemon:/bin/false
gdm:x:108:118:Gnome Display Manager:/var/lib/gdm:/bin/false
djaara:x:1000:1000:Jaroslav Barton,,,:/home/djaara:/bin/bash
```

Položka	Obsah
djaara	Uživatelské jméno

Položka	Obsah
x	Heslo je uloženo v souboru `/etc/shadow`[1]
1000	Identifikační číslo uživatele (UID)
1000	Identifikační číslo skupiny (GID)
Jaroslav Barton,,,	Plné jméno uživatele
`/home/djaara`	Domácí adresář uživatele
`/bin/bash`	Uživatelův výchozí shell

Tabulka 5.1: Příklad údajů v souboru `/etc/passwd`

5.2 Soubor /etc/shadow

V souboru /etc/shadow si UNIX ukládá údaje o heslech uživatelů, počet dnů, kdy bylo heslo naposledy změněno, počet dnů, po jejichž uplynutí může být změněno, kolik dnů předem má být uživatel informován o vypršení hesla, po kolikati dnech od vypršení platnosti hesla je účet zablokován. Položky jsou od sebe odděleny dvojtečkou, na každý řádek popisuje jeden záznam databáze.

Ukázka souboru `/etc/shadow`:

```
haldaemon:!:13801:0:99999:7:::
gdm:!:13801:0:99999:7:::
djaara:$1$j7p/vBce$OzD6kVsoK9wkOnJxW5Hrp/:13915:0:99999:7:::
```

Položka	Obsah
djaara	Uživatelské jméno.
1j7p/vBce$OzD6kVsoK9wkOnJxW5Hrp/	Zašifrované heslo[2].
13915	Heslo bylo změněno 13915 dnů po 1. 1. 1970.
0	Heslo může být kdykoliv změněno.
99999	Po kolikati dnech musí být heslo změněno.
7	Kolik dnů před vypršením hesla má být uživatel informován.
	Po kolikati dnech po vypršení hesla je účet zablokován.
	Počet dnů od 1. 1. 1970, kdy byl účet zablokován.
	Rezervované pole.

Tabulka 5.2: Příklad údajů v souboru `/etc/shadow` [18]

[1] Hesla byla dřív součástí souboru `/etc/passwd`. Tento soubor je veřejně čitelný pro všechny uživatele, což představuje bezpečnostní riziko (usnadnění uhodnutí hesla). Proto byla hesla přesunuta do souboru `/etc/shadow`, který je čitelný pouze správcem systému a skupinou shadow.

[2] K heslu je přidána „sůl“ (uložena mezi druhým a třetím výskytem znaku $) a je zašifrováno hešovací funkcí.

5.3 Zásuvné autentizační moduly (Pluggable Authentication Modules, PAM)

PAM může dělat spoustu věcí, ale jeho primární zaměření je autentizovat vaše uživatele. PAM navíc umožňuje nastavit prostředí, ve kterém budou uživatelé pracovat. Jakmile se uživatel odhlásí, PAM se postará o ukončení pracovního prostředí kontrolovanou cestou [17].

Autentizace v UNIXu je prováděna porovnáním zašifrovaného hesla uživatele s heslem v souboru (dnes v `/etc/shadow`, dříve v `/etc/passwd`). Každý program, který vyžadoval autentizaci si musel autentizační mechanizmus implementovat sám. Tento chaotický přístup k autentizaci více vynikne pokud se přidá více aplikací provádějící nějaký druh autentizace (přihlášení do grafického uživatelského rozhraní, služby jako FTP, SSH, IMAP, POP, webové a jiné aplikace). S počtem aplikací rostou nároky na administrátora, který kromě `/etc/passwd` musí spravovat i mnoho dalších databází uživatelů. Noční můrou pak pro každého administrátora byla ztráta konzistence těchto databází. Také uživatelé si musí pamatovat více uživatelských jmen a hesel, což není příjemné.

PAM a kompatibilní aplikace redukují komplexnost autentizace. S PAM může administrátor použít jednu databázi pro každý autentizační proces v systému, pokud o to stojí. Také je možné použít několik rozdílných autentizačních mechanizmů – práci odvede PAM a pro uživatele je vše transparentní.

Další dobrou zprávou je, že znalost PAM na jednom Unixovém operačním systému lze snadno využít i na dalších Unixových systémech.

Systém PAM umožňuje snadnou změnu databáze a tak přechod k řešením, které škálují znatelně lépe než běžný textový soubor, nebo umožňují uložit i další údaje. Například LDAP nebo relační databáze. Aplikace používající PAM si nevšimnou žádné změny, vše bude bez problémů fungovat [17].

PAM a slabá hesla

Jelikož možnosti a schopnosti PAM lze rozšiřovat pomocí zásuvných modulů, vznikly i moduly, který umožňuje vynutit požadavky na hesla. Například tradiční modul `pam_unix` nebo modul `pam_cracklib`.

Modul `pam_unix` je tradiční Unixový autentizační modul PAM. Je určen pro autentizaci pomocí hesla, získání a nastavení informací o uživatelském účtu, které nejčastěji získává ze souborů `/etc/passwd` a `/etc/shadow`. Modul se skládá ze 2 komponent: *komponenty hesla* (password component) a *komponenty sezení* (session component). *Komponenta hesla* se stará o aktualizaci uživatelských hesel. *Komponenta sezení* pak ukládá informace o tom kdy se uživatel přihlásil a odhlásil ze systému. Informace o modulu `pam_unix` naleznete v manuálové stránce [38].

`Pam_cracklib` je modul určený pro doplňkovou kontrolu síly hesla. Při změně hesla je modulu předáno heslo, které je zkontrolováno proti slovníku a také pomocí několika pravidel tak, aby byly identifikovány slabá hesla. Detailní informace o možnostech modulu `pam_cracklib` naleznete v manuálové stránce [16].

PAM a otisky prstů

Pro autentizaci pomocí otisků prstů existují PAM moduly `pam_thinkfinger`, `pam_fprint` a `pam_fprintd`.

Modul `pam_thinkfinger` spolupracuje se čtečkou otisků prstů od firmy UPEK/SGS Thomson Microelectronics. Tato čtečka je nejčastěji umístěna v noteboocích firem Dell, IBM/Lenovo a Toshiba. `Pam_thinkfinger` je zodpovědný za autentizaci pomocí otisků prstů za využití knihovny `libthinkfinger`. Modul se spouští pouze pro uživatele, kteří mají nasnímán otisk prstu v systému [20].

`Pam_fprint` je jednoduchý modul, který využívá služeb knihovny `libfprint` pro zpracovaní, vyhodnocení a autentizaci pomocí otisků prstů. Uživatel je místo výzvy k zadání hesla požádán o nasnímání jeho otisku prstu. Knihovna `libfprint` podporuje větší počet snímačů otisků prstů než knihovna `libthinkfinger`. Vývoj `pam_fprint` je teprve v počátku [13], přesto se většina pozornosti soustředí na modul `pam_fprintd`.

`Pam_fprintd` je nástupce `pam_fprint`. Stejně jako `pam_fprint` pro práci se čtečkou otisků prstů a jejich vyhodnocení používá knihovnu `libfprint`. S touto knihovnou ale nekomunikuje přímo, ale za pomoci služby `fprintd` dostupné přes komunikačního rozhraní D-Bus (viz kapitola 6.1). Služba je spouštěna automaticky v případě potřeby. Více v kapitole 6.3.

Podpora pro autentizaci pomocí otisků prstů v GUI[3]

I když jsou některé typy čteček otisků prstů podporovány, stav stále není uspokojivý. Je problém s jejich použitím při přihlašování do grafického uživatelského rozhraní. V GNU/Linuxu jsou nejčastěji používaní správci přihlášení GDM a KDM. GDM dokáže spolupracovat s `pam_thinkfinger` bez problémů, KDM má problémy [29].

Před nedávnem vznikl projekt Fingerprint GUI [35], který má usnadnit a umožnit identifikaci a verifikaci v grafickém uživatelském rozhraní. S výše popsanými zásuvnými moduly PAM není identifikace možná, lze je použít pouze v režimu verifikace (uživatel nejdříve zadá svoje uživatelské jméno a poté je ověřen pomocí otisku prstu). Ani tento projekt zatím není plně kompatibilní se všemi používanými správci přihlášení.

Konfigurační soubory PAM

Konfigurační soubory systému pam jsou uloženy v adresáři `/etc/pam.d/`. Umožňují specifická nastavení pro jednotlivé služby. Služby spojené s lokálním přihlášením mohou mít nastaveno využití biometrických metod, ostatní mohou být chráněny jen heslem.

Zkrácená ukázka obsahu souborů common-auth, common-password a common-session ze systému Ubuntu 8.04.2:

```
auth        sufficient  pam_thinkfinger.so
auth        requisite   pam_unix.so nullok_secure use_first_pass
password    requisite   pam_unix.so nullok obscure md5
session     required    pam_unix.so
```

PAM se angažuje ve čtyřech funkčních oblastech. Jde o autentizaci uživatele, kontrolu účtu, správu relace a změnu hesla. V těchto oblastech pak různé moduly provádí kontrolní nebo výkonné funkce.

Během autentizace (`auth`) se ověřuje identita uživatele. Může proběhnout kontrola hesla, připojení k serveru Kerberos, nebo jiná kontrolní činnost.

[3] GUI – grafické uživatelské rozhraní.

Kontrola účtu (`account`) provádí další ověřování, které nemá přímou souvislost s identitou uživatele. Příkladem je povolení přístupu jen během určité doby nebo omezení počtu současně přihlášených uživatelů.

Správa relace (`session`) se aktivuje před a po provedení služby. Obvykle nastavuje proměnné prostředí (*environment*) a omezuje systémové prostředky. Mezi další možnosti patří „*uvěznění*“ procesu pomocí chroot, připojení dalších souborových systémů nebo protokolování.

Konečně změna hesla (`password`) je oblast, jejíž moduly se starají o aktualizaci hesel a podobných uživatelských informací. Obvykle zde najdeme kontrolu délky a kvality hesla (např. pomocí knihovny `pam_cracklib`), nebo například zápis hesla do databáze.

Dalším prvkem ve schématu zabezpečení je kontrolní příznak. Ten určuje, jak s modulem zacházet. Možné hodnoty jsou `required` (povinný), `requisite` (bezpodmínečný), `sufficient` (postačující) a `optional` (nepovinný).

Modul, který je povinný a při kontrole neuspěje, sice způsobí zamítnutí přístupu, ale až po provedení ostatních modulů ze stejné oblasti. Bezpodmínečný modul se liší okamžitým oznámením neúspěchu. Můžeme si představit, že takový modul zjistí pokus o přihlášení přes nějaké nespolehlivé médium (třeba nezašifrované spojení). Díky včasnému odmítnutí přístupu zabrání, aby uživatel poslal přes toto médium heslo, které by mohl zachytit každý nadanější hacker.

Modul s příznakem postačující může okamžitě ukončit kontroly s výsledkem „*úspěch*“, ale jedině za předpokladu, že tento modul uspěl a žádný z předchozích modulů nezamítnul přístup. Jinak je modul ignorován a přechází se na další kontrolu. Obvyklým využitím je přeskočení všech zdlouhavých kontrol, pokud aplikaci spouští superuživatel.

Úspěch či neúspěch nepovinných modulů se nezahrnuje do celkového výsledku. Jistě bychom nechtěli, aby byl uživatelům zakázán přístup jen proto, že dočasně není možné připojit souborový systém (např. CDROM) [5].

Kapitola 6

Použité technologie

V současné době existuje několik technologií umožňující komunikaci se snímačem otisků prstů, autentizace uživatele, zobrazení uživatelského rozhraní. Tato kapitola se zabývá jednotlivými technologiemi, které byly použity v rámci této diplomové práce a popisuje jejich vzájemnou komunikaci.

6.1 Komunikační sběrnice D-Bus

D-Bus je systém pro posílání zpráv přes sběrnici, což umožňuje snadnou komunikaci mezi aplikacemi. Mimo meziprocesové komunikace podporuje také správu životního cyklu aplikace. Lze jednoduše napsat kód, který umožní spustit jen jednu instanci aplikace nebo služby. Také umožní spouštět aplikace a služby na požádání.

D-Bus podporuje jak systémové služby (reakce na události typu „Nalezeno nové zařízení“ nebo „Změna v tiskové frontě“), tak služby spojené s přihlášeným uživatelem (nejčastěji meziprocesová komunikace uživatelem spuštěných programů). Diagram průběhu komunikace můžete vidět na obrázku 6.1.

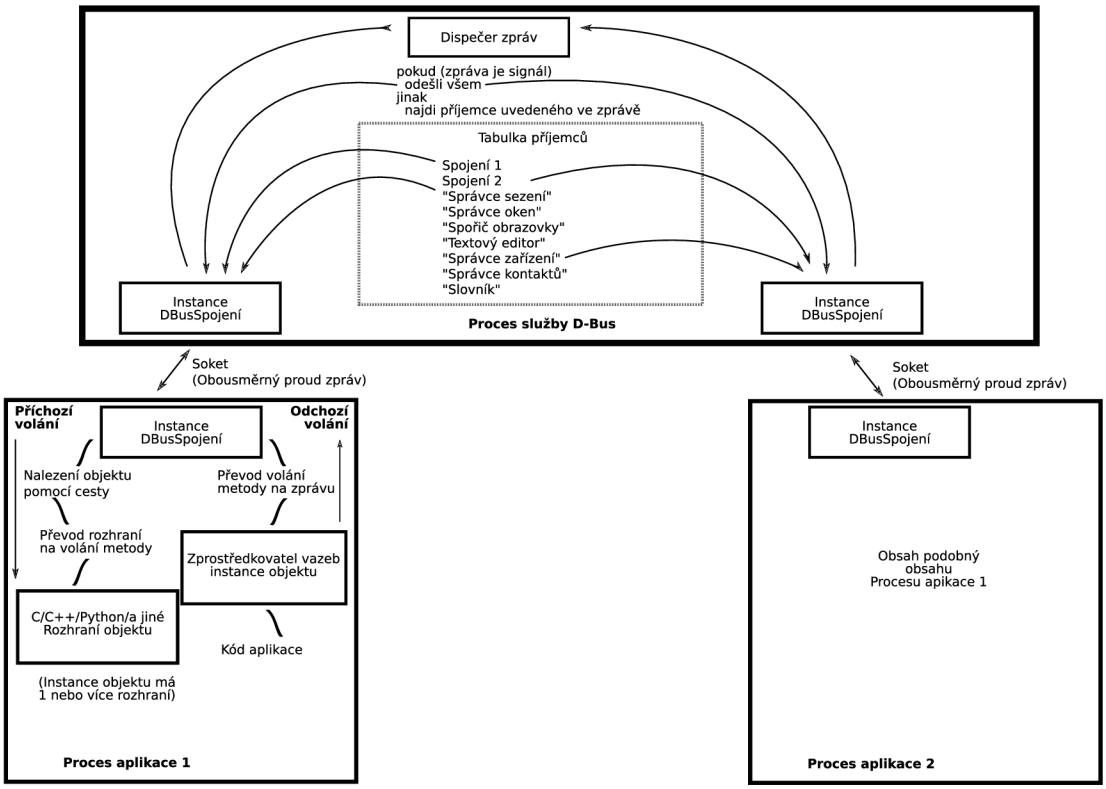
Sběrnice zpráv je postavena na obecném rozhraní předávání zpráv pro komunikaci jednoho programu s jiným programem[1]. Toto rozhraní lze využít k přímé komunikaci programů bez nutnosti využívat D-Bus. V současnosti mohou být aplikace umístěny na jednom počítači, mohou komunikovat přes nezabezpečené TCP/IP spojení, což je vhodné pouze pro bezpečné lokální sítě s domovskými adresáři připojenými přes síťový souborový systém NFS. Podpora pro lépe zabezpečené síťové přenosy je plánována [39].

Popis protokolu

D-Bus je protokol s nízkou latencí a režií, jednoduchý pro použití v meziprocesové komunikaci. Byl navržen tak, aby zabraňoval vícenásobným oběhům zpráv a také podporuje asynchronní zprávy. Nízká režie je zajištěna použitím binárního formátu zpráv a neprovádí konverzi z a do textového formátu jako je například XML[2] [26], protože D-Bus je primárně zaměřen na lokální meziprocesovou komunikaci, nikoliv síťovou.

[1] Jeden s jedním, one-to-one.

[2] eXtended Markup Language – značkovací jazyk vycházející ze SGML.



Obrázek 6.1: Diagram posílání zpráv systémem D-Bus (přeloženo z [39])

Protokol zpráv

Zpráva se skládá z *hlavičky* a *těla*. Pokud přirovnáme zprávu k balíčku, *hlavička* je adresa a *tělo* zahrnuje obsah balíčku. Systém doručení zpráv používá informace z *hlavičky* k nalezení adresáta a jak ji interpretovat. Příjemce zpracovává *tělo* zprávy.

Tělo zprávy se skládá z žádného nebo více argumentů, ty mají typové hodnoty. Například `integer` nebo pole `bytů`.

Hlavička i tělo zprávy používají stejný typový systém a formát pro převod dat. Každý typ hodnoty má formát pro přenos. Převod hodnoty na přenosový formát dat se nazývá *marshalling*, převod zpět z přenosového formátu se nazývá *unmarshalling*.

Typové značky

Protokol D-Bus nezahrnuje informaci o typu dat v převedených datech. Blok přenášených hodnot musí mít známou typovou značku. Tato značka je tvořena z typových kódů. Typový kód je ASCII[3] znak reprezentující typ hodnoty. Díky použití ASCII znaků je typová značka vždy platný ASCII řetězec. Jednoduchým porovnáním řetězců zjistíme zda jsou typové značky ekvivalentní. Popis typových značek naleznete v [26].

[3] American Standard Code for Information Interchange – kódová tabulka která definuje znaky anglické abecedy, a jiné znaky používané v informatice.

Platná jména

Různá jména v systému zpráv D-Bus mají nějaké omezení. Omezení na maximální délku jména je 255 znaků a platí jak pro jména sběrnic, rozhraní a členů [26]. Jména jsou typu STRING a musí být platný řetězec v kódování UTF-8[4]. Kompletní seznam omezení naleznete v [26].

Základní omezení všech jmen je:

- Smí obsahovat pouze ASCII znaky "[A-Z][a-z][0-9]_"
- Nesmí překročit maximální délku.
- Nesmí začínat tečkou.

Sběrnice zpráv

Sběrnice zpráv přijímá připojení od jedné nebo více aplikací. Připojená aplikace si může vyměňovat zprávy s kteroukoliv další připojenou aplikací.

Sběrnice zpráv zachovává mapování mezi jménem a spojením aby bylo možné směrovat zprávy mezi více připojeními. Každé spojení má jedno unikátní jméno po celou dobu připojení ke sběrnici. Unikátní jméno je automaticky přiřazováno. Aplikace si může vyžádat další jména. Jako další jména se většinou používají *známá* jména jako je „`org.freedesktop.TextEditor`“. O takto získaných jménech říkáme, že jej spojení vlastní.

Sběrnice samotná vlastní speciální jméno – `org.freedesktop.DBus`. Přes toto jméno lze sběrnici posílat zprávy. To aplikacím umožňuje provádět administrativní požadavky. Aplikace může například požádat o přiřazení jména ke spojení [26].

Přidělování jména

Každé spojení má minimálně jedno jméno přidělené při připojení. Toto jméno je vráceno jako odpověď na volání metody `org.freedesktop.DBus.Hello`. Toto automaticky přidělené jméno se nazývá *unikátní jméno*. Unikátní jména nejsou nikdy použita znovu pro dvě rozdílná připojení na stejné sběrnici.

Vlastnictví unikátního jména je prerekvizita pro interakci se sběrnicí zpráv. Je to logické, protože unikátní jméno je vždy první jméno, které aplikace vlastní a poslední o které aplikace přichází (při odpojení, ukončení aplikace).

Pro získání dalšího jména lze použít zprávu `org.freedesktop.DBus.RequestName`, uvolnění takto získaného jména se provede zprávou `org.freedesktop.DBus.ReleaseName` [26].

Spouštění služeb

Sběrnice zpráv může spustit aplikaci na požádání od jiné připojené aplikace. Aplikace, která může být spuštěna touto cestou se nazývá služba. V systému D-Bus je spuštění služby provedeno na základě jména. Aplikace požádá sběrnici zpráv o spuštění programu se známým jménem jako je například `org.freedesktop.TextEditor`. Pro nalezení spustitelného souboru odpovídajícího jménu používá služba D-Bus soubory popisující službu. Tyto soubory definují mapování mezi spustitelnými soubory a jmény.

[4] UTF je zkratka UCS Transformation Format. Je to způsob kódování řetězců znaků Unicode/UCS do sekvencí bajtů.

Ukázka souboru popisujícího službu:

```
[D-BUS Service]
Names=org.freedesktop.ConfigurationDatabase;org.gnome.GConf;
Exec=/usr/libexec/gconfd-2
```

Když aplikace požádá o spuštění služby pomocí jména, služba D-Bus se pokusí nalézt službu, která vlastní toto jméno a spustí odpovídající spustitelný soubor. Pokud selže, reportuje chybu.

Systémová sběrnice zpráv

Počítač může mít systémovou sběrnici zpráv dostupnou pro všechny aplikace v systému. Tato sběrnice zpráv může být použita pro posílání systémových událostí (změna konfigurace počítače, ...).

6.2 Knihovna libfprint

Knihovna `libfprint` je knihovna určená pro snadnou tvorbu aplikací podporujících dostupné snímače otisků prstů. Je vytvořena v programovacím jazyce C. Je primárně určena pro počítačové systémy s operačním systémem GNU/Linux, ale je snadno přenositelná na další systémy. Poskytuje jednotné rozhraní pro přístup k množství rozdílných typů snímačů. Seznam podporovaných snímačů naleznete v [14].

`Libfprint` umožňuje získat obrázky otisků prstů, zahrnuje kód pro zpracování a porovnání obrázků. Přímo podporuje zavedení uživatele pro pozdější porovnání uložené šablony a otisku získaného ze snímače [12]. Knihovna `libfprint` podporuje i identifikaci uživatele.

6.3 Fprintd

`Fprintd` je služba systému D-Bus (kapitola 6.1), která nabízí funkcionalitu knihovny `libfprint` přes meziprocesovou komunikační sběrnici. Přidání této vrstvy nad knihovnu `libfprint` umožnilo vyřešit některé problémy spojené se současným přístupem a soupeřením více aplikací o přístup ke snímači otisků.

Není pěkné si myslet, že je služba `fprintd` nezbytná. Proto je spouštěna přes D-Bus pomocí aktivačního mechanizmu (strana 29). To znamená, že je spuštěn pouze když je potřeba a navíc se automaticky ukončí při nečinnosti [11].

Pro komunikaci se službou `fprintd` se používá systémová sběrnice správ.

Služba `fprintd` je rozdělena na dvě části:

- Správce zařízení.
- Zařízení.

Součástí zdrojových kódů služby `fprintd` je také zásuvný modul PAM (kapitola 5.3) `pam_fprintd` (strana 32).

Správce zařízení

Pro komunikaci se správcem zařízení je třeba použít následující jména:

- Jméno služby `org.reactivated.Fprint`,
- cestu `/net/reactivated/Fprint/Manager`,
- jméno rozhraní `org.reactivated.Fprint.Manager`

Pomocí správce zařízení můžeme získat seznam instalovaných čteček otisků prstů voláním metody `GetDevices`. Výchozí čtečku otisků prstů získáme voláním metody `GetDefaultDevice`.

Kompletní popis rozhraní najdete v souboru `src/manager.xml` ve zdrojových kódech služby.

Zařízení

Pro komunikaci se zařízením je třeba použít následující jména:

- Jméno služby `org.reactivated.Fprint`,
- cestu `/net/reactivated/Fprint/Device/`**X**,
- jméno rozhraní `org.reactivated.Fprint.Device`

V cestě k objektu zařízení pak číslo **X** určuje o které zařízení se jedná. To nám umožňuje pracovat s konkrétním zařízením v případě, že je jich k počítači připojeno několik.

Objekt zařízení má následující vlastnosti:

- `name:` Název snímače.
- `scan-type:` Typ snímače (průtahový, plošný).
- `num-enroll-stages:` Počet kroků potřebných k zavedení otisku.

Pro práci se zařízením lze použít následující metody a signály:

- `ListEnrolledFingers:` Pomocí této metody získáme seznam otisků prstů zavedených pro uživatele na daném zařízení.
- `DeleteEnrolledFingers:` Smaže všechny zavedené otisky prstů pro uživatele na daném zařízení. Služba `fprintd` neumí smazat pouze zvolený otisk prstu, vždy se musí smazat všechny [24].
- `Claim:` Metoda pro zažádání o přístup k zařízení před zahájením práce. Zavedení uživatele, verifikace i identifikace vyžadují přidělené zařízení.
- `Release:` Metoda pro uvolnění zařízení po ukončení práce.
- `VerifyStart:` Metoda pro zahájení verifikace uživatele.
- `VerifyStop:` Ukončí probíhající verifikaci uživatele.

- Signál `VerifyFingerSelected:` Informuje aplikaci o tom, který prst bude použit pro verifikaci.
- Signál `VerifyStatus:` Informuje aplikaci o průběhu verifikace.
- `EnrollStart:` Zahájí zavádění zvoleného otisku prstu.
- `EnrollStop:` Ukončí probíhající zavádění otisku prstu.
- Signál `EnrollStatus:` Informuje aplikaci o průběhu zavádění otisku.

V kompletním popisu rozhraní zařízení najdete dále zadefinovaná jména prstů používaná při komunikaci se službou `fprintd`, jména a popis jednotlivých stavů posílaných signály `VerifyFingerSelected`, `VerifyStatus`, `EnrolStatus`, jména a popis možných chyb a také specifikované parametry, které jednotlivé metody vyžadují. Kompletní popis rozhraní zařízení najdete v souboru `src/device.xml` ve zdrojových kódech služby.

Pam_fprintd

Tento zásuvný modul PAM používá pro komunikaci se čtečkou otisků prstů službu `fprintd` se kterou komunikuje přes sběrnici zpráv D-Bus (kapitola 6.1).

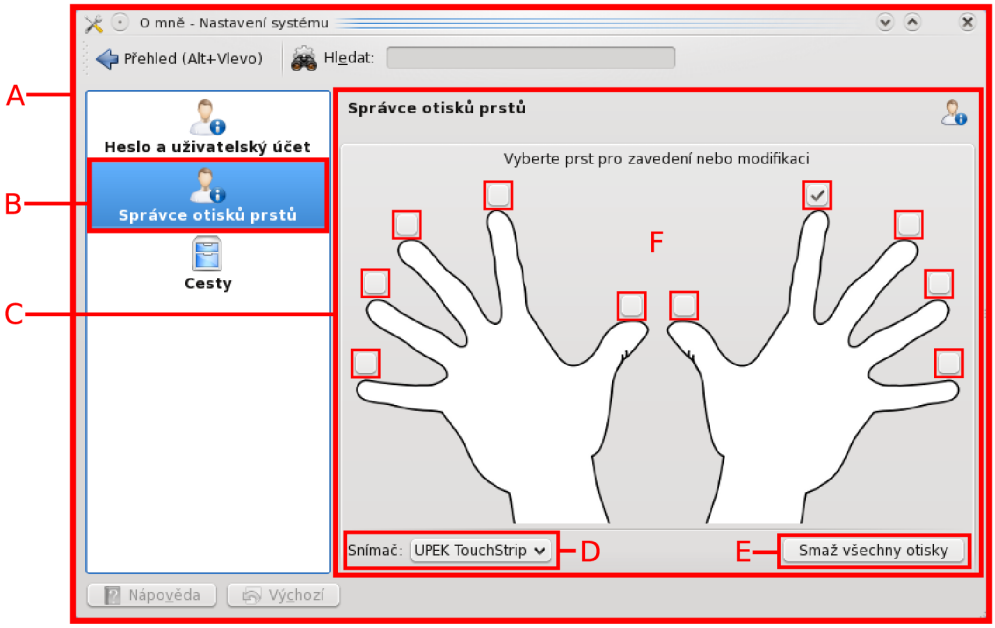
`Pam_fprintd` na rozdíl od modulu `pam_thinkfinger` nepodporuje zadání hesla v průběhu verifikace uživatele pomocí otisku prstu. V případě potřeby zadat heslo je tedy nutno počkat až vyprší časový limit verifikace. To je velice nepříjemné. Pokusil jsem se tuto funkcionalitu doprogramovat, ale kód byl odmítnut kvůli použití mechanizmu `uinput` (viz strana 46) [19].

Ukázku konfigurace systému PAM pro použití modulu `pam_fprintd` naleznete v kapitole popisující grafického správce přihlášení KDM (kapitola 8.3).

Kapitola 7

KFingerManager

KFingerManager je modul určený pro správu otisků prstů. Je integrovaný do „*Nastavení systému*“ pracovního prostředí KDE, kde tak doplňuje modul určený pro správu osobních informací a změnu hesla. Tato integrace je velice příjemná, uživatel má všechny informace o uživatelském účtě pohromadě.



Obrázek 7.1: KFingerManager je součástí „*Nastavení systému*“

A Okno „*Nastavení systému*“, položka „*O mně*“.

B Vybrán „*Správce otisků prstů*“.

C Uživatelské rozhraní *Správce otisků prstů*.

D Volba snímače otisků prstů.

E Tlačítko pro smazání všech otisků prstů.

F Zaškrtávací pole. Zaškrtnutí jednoho z polí spustí proces zavedení nového otisku prstu pro prst v jehož blízkosti je umístěno (obrázek 7.2). Zaškrtnutá pole indikují již zavedené otisky prstu (v tomto případě pravý ukazováček).

Program využívá službu `fprintd` (kapitola 6.3) dostupnou přes sběrnici D-Bus (kapitola 6.1). Možnosti programu pro správu otisků prstů závisí na možnostech této služby. KFingerManager umožňuje zavést zvolené otisky prstu do systému a dříve zavedené otisky smazat.

7.1 Zavedení otisku do systému

Při zavádění otisku prstu do systému je uživatel přehledně informován o počtu kroků potřebných k zavedení otisku a aktuální stav zavádění otisku (obrázek 7.2). V každém kroku je zobrazena zpráva popisující uživateli jakou akci má provést. Pokud nastane chyba, je uživateli srozumitelným způsobem vysvětlena. Pokud se lze z chyby zotavit, je popsáno uživateli jak má postupovat.

Obrázek 7.2: Průběh zavádění otisku prstu

A Okno zobrazené při zavádění otisku prstu.

B Textová informace o průběhu zavádění otisku prstu.

C Obrázky otisku prstu znázorňují počet kroků potřebných k zavedení otisku do systému. Stav aktuálního kroku je zobrazen stavovou ikonou zobrazenou vpravo dole vedle obrázku otisku prstu.

D Tlačítko *Zrušit* je zobrazeno dokud není úspěšně dokončeno zavádění otisku prstu. Poté se změní na tlačítko *OK*.

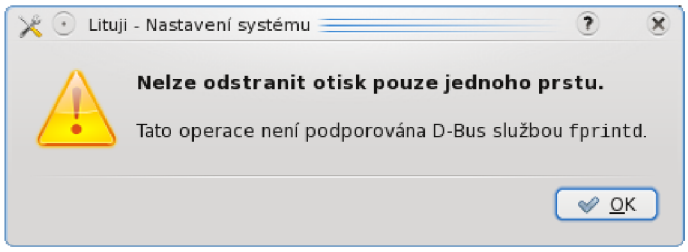
E Animace nasnímání otisku prstu.

7.2 Smazání otisků prstů

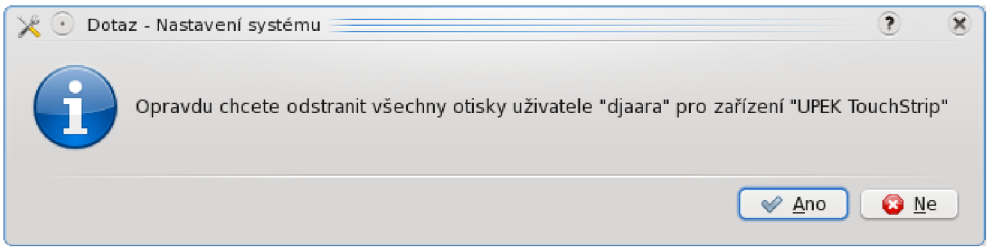
Při pokusu smazat pouze zvolený otisk prstu je uživatel informován že to není možné (obrázek 7.3). Služba `fprintd` dostupná přes komunikační sběrnici D-Bus tuto vlastnost nepodporuje [24]. Autor této služby nenašel žádný případ použití při kterém by se mohlo hodit smazat pouze jeden otisk prstu.

Bylo mu poskytnuto několik případů použití [25, 15], ale žádný nebyl dostatečně pádný aby stál za doplnění této funkcionality do služby `fprintd`.

Program umožňuje smazat všechny otisky prstů, což je v současnosti jediná možnost jak uživateli umožnit zavést novou sadu otisků prstů do systému. Smazání všech otisků prsů musí uživatel potvrdit (obrázek 7.4).



Obrázek 7.3: Chybová zpráva při pokusu smazat pouze jeden otisk prstu



Obrázek 7.4: Potvrzovací dialog před smazáním všech otisků prstů

7.3 Implementace

KFingerManager je naprogramován v jazyce C++ s využitím knihovny Qt na které je postaveno i pracovní prostředí KDE. Pro komunikaci se službou `fprintd` se používá implementace rozhraní D-Bus z knihovny QtDBus.

Knihovna QtDBus zapouzdřuje objekty dostupné přes sběrnici D-Bus (kapitola 6.1) a umožňuje převádět signály D-Bus na signály knihovny Qt, přistupovat k vlastnostem objektů a volat metody objektu.

Jelikož je pro překlad zdrojových souborů pracovního prostředí KDE použit systém CMake rozhodl jsem se ho použit i ve správci otisků prstů KFingerManager. To usnadní budoucí integraci zdrojových kódů KFingerManager se zdrojovými kódy KDE a jejich společný překlad. KFingerManager se tak stane nedílnou součástí pracovního prostředí KDE.

Pro správu zdrojových souborů je použít systém správy verzí Git.

V diplomové práci se vyskytl problém při komunikaci přes sběrnici D-Bus, kdy autoři různých implementací rozhraní sběrnice D-Bus různě pochopili omezení na jména vlastností. To znemožnilo přímý přístup k vlastnosti `num-enroll-stages` a `scan-type`.

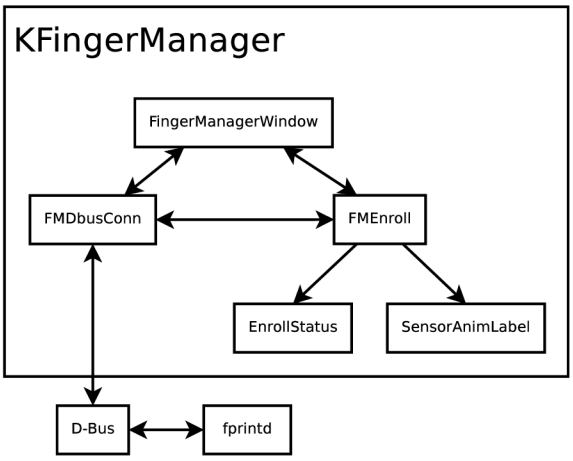
Implementace rozhraní D-Bus v knihovně QtDBus totiž nepovoluje pomlčku v názvu vlastnosti [3] a tím je znemožněn přímý přístup. Vlastnosti s pomlčkou v názvu lze přečíst jinou cestou a tím je k nim zajištěn alespoň nepřímý přístup.

V programu je použito několik ikonek z konkurenčního projektu FingerprintGUI (kapitola 10.1). Před zařazením ikonek jsem si vyžádal svolení původního autora.

Program je rozdělen do několika tříd:

- **FingerManagerWindow**: Výchozí třída programu, zajišťuje integraci do „*Nastavení systému*“, načtení konfiguračního souboru a poskytuje uživatelské rozhraní pro volbu senzoru otisků prstů, smazání všech otisků a spouští zavedení otisku (obrázek 7.1).
- **FMDbusConn**: Třída pro komunikaci se službou `fprintd` (kapitola 6.3), kompletně zastřešuje komunikaci přes sběrnici D-Bus (kapitola 6.1). Ostatní třídy využívají jejích služeb pro komunikaci se službou `fprintd`. Na obrázku 7.5 naleznete znázornění komunikace mezi třídami a se službou `fprintd`.
- **FMEnroll**: Třída dialogového okna pro zavedení nového otisku prstu do systému. Obsahuje informace o průběhu zavádění a animaci nasnímání otisku prstu. V závislosti na průběhu zavádění otisku prstu je zobrazeno buď tlačítko pro potvrzení zavedení otisku prstu nebo tlačítko pro zrušení zavádění (zavedení otisku prstu nebylo dokončeno nebo se nezdařilo). Zobrazení dialogu je na obrázku 7.2.
- Dále bych zmínil třídu `EnrollStatus` a `SensorAnimLabel`. Třída `EnrollStatus` zobrazuje obrázek otisku prstu a vedle něj zobrazuje stavovou ikonu. Ta se mění v závislosti na výsledku nasnímání otisku v daném kroku. Zobrazuje potvrzovací ikonu, pokud se podaří nasnímat otisk prstu, jinak zobrazuje chybovou ikonu. Chybová ikona je zobrazena pouze po dobu zobrazení informace o chybě zavádění. `SensorAnimLabel` zobrazuje animaci nasnímání otisku prstu. Typ snímače je zadán při vytváření instance objektu, výchozí je průtahový snímač.

Komunikace mezi třídami



Obrázek 7.5: Diagram komunikace mezi třídami a se službou `fprintd`

FMDbusConn

`FMDbusConn` poskytuje metody, pomocí kterých lze získat informace od služby `fprintd` dostupné přes sběrnici D-Bus. Při spuštění programu se postará o start služby `fprintd` (pokud neběží).

Pro třídu `FingerManagerWindow` na požádání zjišťuje seznam instalovaných snímačů otisků prstů a také výchozí snímač, seznam zavedených otisků prstů uživatele, smazání všech otisků uživatele.

Také umožňuje zahájit a ukončit zavedení nového otisku prstu uživatele a informuje o průběhu zavádění.

FingerManagerWindow

`FingerManagerWindow` využívá třídu `FMDbusConn` pro komunikaci se službou `fprintd`.

Třídu `FMEnroll` spouští při zavádění nového otisku prstu uživatele do systému a předává ji informaci o prstu zvoleném k zavedení do systému a zvolený snímač. Návratová hodnota pak třídu `FingerManagerWindow` informuje o úspěchu zavádění.

FMEnroll

Pro zobrazení aktuálního stavu využívá třídy `EnrollStatus` a `SensorAnimLabel`. Stejně jako třída `FingerManagerWindow` používá třídu `FMDbusConn` a využívá jejich služeb týkajících se zavádění otisků prstů a přijímá informace o průběhu zavádění.

Konfigurační soubor

Různí vydavatelé distribucí založených na systému GNU/Linux rádi upravují vzhled aplikací. Vzhled aplikace KFingerManager je specifikován v konfiguračním souboru `kfingerrc`. Tento konfigurační soubor specifikuje použitý obrázek rukou a umístění jednotlivých zaškrtávacích polí.

Tento konfigurační soubor se jmenuje `kfingerrc` a v po instalaci je společný pro všechny uživatele systému (`/usr/share/kde4/apps/kfingermanager/kfingerrc`).

Díky tomu, že pracovní prostředí KDE vyhledává nejdříve uživatelské konfigurační soubory a až poté systémové si může uživatel vytvořit uživatelskou kopii tohoto konfiguračního souboru a upravit ho (`~/.kde/share/config/kfingerrc`).

Konfigurační soubor `kfingerrc` se skládá ze dvou částí. V části `[fingers]` jsou specifikovány pozice středů jednotlivých zatrhávacích polí. Souřadnice je zadána ve tvaru A/x a A/y, kde A je číslo prstu ke kterému se zatrhávací pole vztahuje. Prsty jsou číslovány od jedné do deseti od levého malíčku po levý palec a od pravého palce po pravý malíček.

V části `[image]` je parametrem `base` specifikována posun obrázku směrem dolů vůči počátku souřadnic. To je kvůli možnosti umístit zatrhávací pole nad obrázek. Parametr `filename` pak obsahuje cestu k obrázku rukou.

```
[fingers]
1/x=14
1/y=136
10/x=510
10/y=136
2/x=22
2/y=68
3/x=49
3/y=18
4/x=127
4/y=-7
```

```
5/x=240
5/y=87
6/x=285
6/y=87
7/x=398
7/y=-7
8/x=476
8/y=18
9/x=502
9/y=68

[image]
base=20
filename=/usr/share/kde4/apps/kfingermanager/hands.png
```

7.4 Nastavení systému

„*Nastavení systému*“ je program zastřešující různé moduly pro správu systému. Jednotlivé moduly jsou rozděleny do čtyř sekcí.

- **Vzhled a chování:** V této sekci se nachází moduly pro nastavení vzhledu systému, vizuálních efektů, systémových hlášení a reakce oken na různé události.
- **Osobní:** Moduly pro nastavení a změnu informací o uživatelském účtu, volba výchozích aplikací, regionální a jazyková nastavení a konfigurace zpřístupnění pro hendikepované uživatele.
- **Síť a připojení:** Zde umístěné moduly umožňují změnit nastavení sítě, uživatelské jméno a heslo ke sdílením MS Windows.
- **Správa počítače:** Správa instalovaných programů, změna a nastavení data, času a časového pásma, instalace nových řezů písma, změna klávesových zkratek, konfigurace multimédií, připojených obrazovek a jiné.

Kvůli integraci do systémových nastavení je hlavní okno odvozeno od třídy `KCModule`. Také je třeba provést registraci nového modulu. Registrace vyžaduje soubor popisující jméno aplikace, jméno spustitelného souboru nebo knihovny, ikonu a zařazení modulu.

Konfigurační soubor `kfingermanager.desktop`:

```
[Desktop Entry]
Exec=kcmshell4 kfingermanager
Icon=preferences-desktop-user
Type=Service
X-KDE-ServiceTypes=KCModule
X-DocPath=kcontrol/kfingermanager/index.html

X-KDE-Library=kcm_kfingermanager
X-KDE-ParentApp=kcontrol
```

```
X-KDE-System-Settings-Parent-Category=about-me
X-KDE-Weight=50

Name=Fingerprint Manager
Name[cs]=Správce otisků prstů
```

Při instalaci se tento soubor nakopíruje do adresáře `/usr/share/kde4/services/`. Tento soubor je také nutné zaregistrovat, jinak o něm pracovní prostředí KDE nebude vědět. Registrace může být automatická (reakce na změnu souboru, periodická kontrola) případně manuální, vynucená. Manuální registrace se provede příkazem `kded4 --check`.

KFingerManager se integruje pod osobní nastavení, konkrétně informace o uživatelském účtu (obrázek 7.1), případně lze spustit samostatně

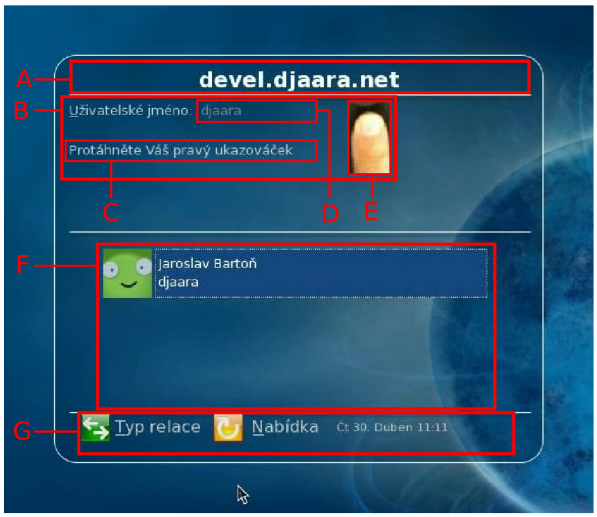
7.5 Známé problémy

V některých kombinacích jádra operačního systému, verze knihovny `libusb` a `libfprint` může dojít k občasné částečné či plné nefunkčnosti programu. Tato nefunkčnost postihuje i PAM modul `pam_fprintd`. Je způsobena nedostupností snímače otisků prstů knihovně `libusb` případně chybami v komunikaci se snímačem.

Kapitola 8

KDM

KDM (obrázek 8.1) je grafický správce přihlášení pro počítače používající operační systém unixového typu. Je součástí pracovního prostředí KDE a nahrazuje XDM, výchozího správce přihlášení systému X Window. KDM každému uživateli umožňuje volbu vlastního pracovního prostředí. Stejně jako pracovní prostředí KDE používá grafickou knihovnu Qt a lze konfigurovat v „*Nastavení systému*“ (kapitola 7.4).



Obrázek 8.1: Správce přihlášení KDM, použit zásuvný modul pro verifikaci pomocí otisku prstu

A Jméno počítače, ke kterému se uživatel přihlašuje.

B Uživatelské rozhraní zásuvného modulu `kgreet_fprintd`.

C Textová zpráva o průběhu přihlášení pomocí otisku prstu.

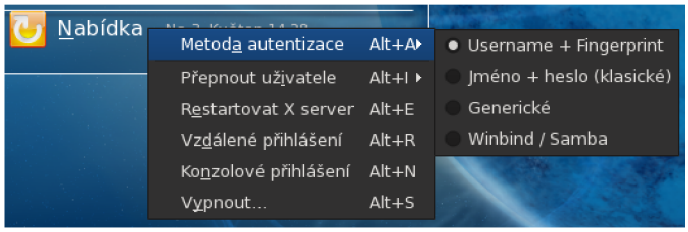
D Vstupní pole pro zadání uživatelského jména. V průběhu verifikace je neaktivní.

E Animace nasnímání otisku prstu.

F Seznam uživatelů systému. Při zvolení uživatele z tomto seznamu se automaticky nastaví uživatelské jméno ve vstupním poli pro zadání uživatelského jména (**D**).

G Umožňuje změnit typ sezení (výběr pracovního prostředí), volbu zásuvného modulu pro autentizaci, vypnout počítač, zobrazuje aktuální čas.

Také umožňuje zobrazení seznamu uživatelů systému obsahující uživatelské jméno, „reálné jméno“ a volitelně také malý obrázek, který si může uživatel změnit. Pro přihlášení lze zvolit z několika zásuvných modulů pro různé autentizační mechanizmy [41] (obrázek 8.2). Vzhled uživatelského rozhraní lze změnit pomocí motivů vzhledu. Motivy vzhledu popisují použité pozadí, vzhled, rozměry a pozadí ovládacích prvků.



Obrázek 8.2: Výběr autentizačních modulů ve správci přihlášení KDM

8.1 Architektura

Správce přihlášení je rozdělen do 2 částí. Jedna z částí se stará o uživatelské rozhraní (*frontend*), ta je naprogramována v jazyce C++. Druhá část má na starosti různé funkční záležitosti (*backend*) a je naprogramována v jazyce C. *Frontend* a *backend* spolu komunikují pomocí mechanizmu zasílání zpráv. Tento komunikační systém umí přenášet celočíselné hodnoty, pole, řetězce, parametry příkazové řádky a jiné.

Veškerá komunikace s autentizačním systémem PAM je prováděna v *backendu*. Kromě systému PAM spolupracuje i se systémem Kerberos. Jednotlivé autentizační zásuvné moduly využívají služeb *backendu*. KDM neumožňuje vícenásobný přístup k systému PAM.

Zásuvné moduly správce přihlášení KDM ovlivňují zobrazené ovládací prvky. Jsou odvozeny od třídy `KGreeterPlugin` a implementují jeho rozhraní. Jednotlivé zásuvné moduly mohou ovlivnit použitou konfiguraci PAM (kapitola 5.3).

8.2 Zásuvné moduly

V základní instalaci správce přihlášení jsou dostupné následující zásuvné moduly (obrázek 8.2):

- `kgreet_classic`: Přihlášení pomocí uživatelského jména a hesla. Tento zásuvný modul je výchozí.
- `kgreet_generic`: Zásuvný modul jehož zdrojový kód je vhodný jako základ pro tvorbu dalších zásuvných modulů.
- `kgreet_winbind`: Přihlášení uživatele pomocí uživatelského jména a hesla. Ověření proběhne proti zvolené doméně Windows Server.

Zásuvné moduly nemohou nijak aktivně ovlivnit verifikaci uživatele, slouží pouze pro interakci s uživatelem. Zásuvný modul umožní zvolit pouze použitý konfigurační soubor PAM.

Také nelze načíst více autentizačních zásuvných modulů najednou. Uživatel si musí před verifikací zvolit konkrétní autentizační modul, ten pak bude používán po celou dobu sezení (lze změnit úpravou systémové proměnné). Tyto zásuvné autentizační moduly používá například i `kscreensaver`.

8.3 Kgreet_fprintd

Pro podporu autentizace pomocí otisků prstů jsem vytvořil zásuvný modul pojmenovaný `kgreet_fprintd`. Vychází ze zdrojového kódu `kgreet_classic`. Používá konfigurační soubory systému PAM `kdm-fprintd`. `system-auth-fprintd` a `kscreensaver-fprintd`.

Zásuvný modul obsahuje jedno vstupní pole pro zadání uživatelského jména, pole pro zobrazení informace o průběhu verifikace a animaci zobrazující nasnímání otisku. Animace a informace o průběhu je zobrazena pouze v okamžiku aktivního snímače otisků prstů (obrázek 8.1).

Při implementaci tohoto modulu se vyskytl problém s překreslováním uživatelského rozhraní. Funkce `handleVerify` z *frontendu* zablokuje vlákno překreslující uživatelské rozhraní čekáním na výsledek verifikace. Oprava umístěná na přiloženém DVD v adresáři se zdrojovými kódy zásuvného modulu správce přihlášení zajistí spuštění funkce `handleVerify` v samostatném vlákně.

Modul je naprogramován v programovacím jazyce C++, pro práci s grafickým rozhraním využívá knihovny Qt pro sestavení je použit systém CMake. Pro správu zdrojových souborů je použít systém správy verzí Git.

Průběh přihlášení pomocí modulu kgreet_fprintd

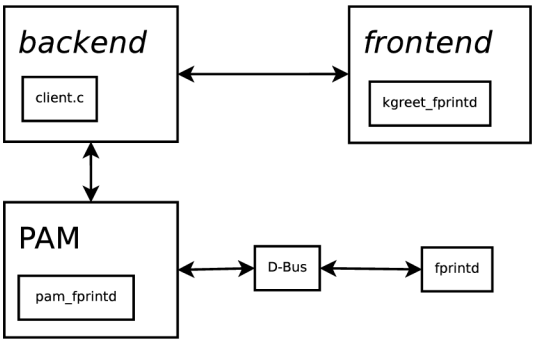
Při přihlašování pomocí modulu `kgreet_fprintd` uživatel zadá a potvrdí uživatelské jméno ve vstupním poli. Modul pak zahájí verifikaci uživatele odesláním zprávy *backendu*. *Backend* aktivuje systém PAM se správným názvem služby (ovlivňuje použité konfigurační soubory) a zaregistruje sadu zpětných volání aby mohl reagovat na zprávy od systému PAM. Modul `kgreet_fprintd` následně odešle uživatelské jméno a čeká na zprávu od systému PAM.

Systém PAM načte konfigurační soubory (v příloze C) a zjistí, že pro verifikaci uživatele má použít zásuvný modul `pam_fprintd` (strana 32). `Pam_fprintd` se spojí přes sběrnici D-Bus (kapitola 6.1) se službou `fprintd` (kapitola 6.3) a zjistí typ snímače a jméno snímače. Poté zahájí samotnou verifikaci. `Pam_fprintd` vytvoří zprávu pro uživatele popisující co má provést.

Systém PAM poté zprávu odešle do *backendu*, který ji předá *frontendu*. *Frontend* zprávu zpracuje a nastaví textovou zprávu o průběhu verifikace a spustí animaci.

Služba `fprintd` posílá přes sběrnici D-Bus zprávy o výsledcích verifikace a případných problémech. Tyto zprávy přijímá `pam_fprintd`, zpracuje je a případně je předá *backendu* a ten je předává *frontendu*. Pokud `frontend` zprávě nerozumí, zůstává její zpracování na *backendu*. Ten vytvoří dialogové okno zobrazující zprávu.

Jakmile služba `fprintd` dospěje ke konečnému rozhodnutí posílá zprávu modulu `pam_fprintd`. Ten podle výsledku verifikace buď ukončí zpracování (v případě neúspěchu) a informuje o tom *backend*, ten pošle zprávu *frontendu*, který zobrazí informaci o neúspěchu a po prodlevě lze pokus o přihlášení zopakovat. V opačném případě informuje *backend* a ten pokračuje v přihlášení uživatele, na konci je uživatel přihlášen ve vybraném pracovním prostředí.



Obrázek 8.3: Zjednodušené schéma komunikace při přihlašování pomocí modulu `kgreet_fprintd`

Povolení modulu kgreet_fprintd

Aby bylo možné tento modul využívat, je ho třeba povolit v konfiguračním souboru KDM a spořiče obrazovky. Konfigurační soubor KDM je uložen v souboru `/etc/kde/kdm/kdmrc`. Povolení zásuvného modulu pro verifikaci pomocí otisků prstů se provede pomocí konfigurační volby `PluginsLogin` v sekci `X-*-Greeter`.

Ukázka konfiguračního souboru `kdmrc`, kompletní konfigurační soubor naleznete v příloze D:

```
[X-*-Greeter]
PluginsLogin = fprintd, classic, generic, winbind
```

8.4 KScreensaver

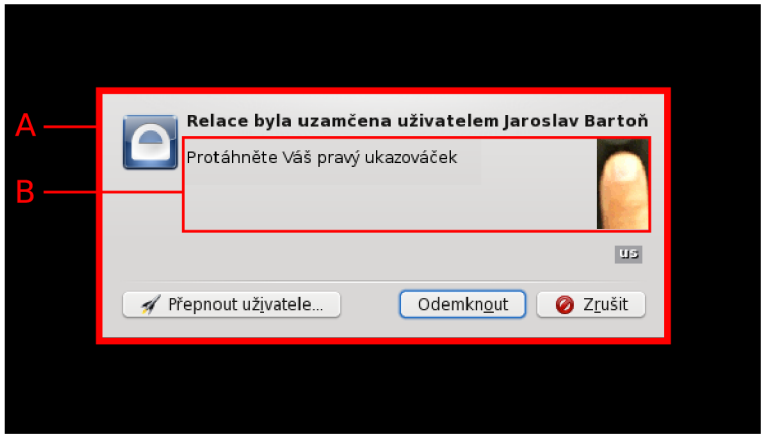
Spořič obrazovky používá stejné zásuvné moduly jako správce přihlášení. Aby bylo možné použít plugin pro verifikaci uživatele pomocí otisku prstu, je třeba ho povolit v konfiguračním souboru spořiče obrazovky `kscreensaverrc`. Tento konfigurační soubor může být buď globální a umístěn v adresáři `/usr/share/config`, případně uživatelský v adresáři `~/.kde/share/config/kscreensaverrc`.

Ukázka konfiguračního souboru `kscreensaverrc`:

```
[ScreenSaver]
PluginsUnlock=classic,generic,fprintd
```

8.5 Známá omezení

Zásuvný modul `kgreet_fprintd` podporuje verifikaci uživatele pouze pomocí otisků prstů. Pokud je tento modul použit, lze i spořič obrazovky odemknout pouze pomocí otisku prstu. To je v některých případech velice omezující. Ne vždy se musí verifikace pomocí otisku prstu podařit – například zmrzlé ruce, zvrásněná kůže po pobytu ve vlhku a jiné.



Obrázek 8.4: `Kgreet_plugin` použitý k odemčení spořiče obrazovky

A Dialog zobrazený při odemykání uzamčeného spořiče obrazovky.

B Modul `kgreet_fprintd` spuštěný v režimu odemykání – neobsahuje vstupní pole pro zadání uživatelského jména, pouze textovou informaci o průběhu verifikace uživatele a animaci nasnímání otisku prstu.

Kapitola 9

Problémy systému PAM

Při implementaci PAM modulů, které pro verifikaci uživatele využívají i jiné mechanizmy než je nejběžnější uživatelské jméno a heslo se dospělo k několika problémům. Mezi tyto problémy patří:

- Podpora více autentizačních mechanizmů současně.
- Implementace PAM v grafických aplikacích.

Tyto problémy jsou popsány dále v textu.

9.1 Podpora více autentizačních mechanizmů současně

Původní návrh systému PAM umožňuje zřetězení autentizačních mechanizmů. Toto zřetězení je vhodné pro moduly využívající uživatelské jméno a znalost kódu, hesla. Uživatel zadá kód/heslo pouze prvnímu modulu a to je postupně zkoušeno ve všech modulech v řetězci, první modul kterému se verifikace podaří zpracování ukončí (záleží na nastavení systému PAM).

Více současně spuštěných autentizačních mechanizmů je potřeba například pro umožnění biometrické verifikace uživatele současně s možností verifikace pomocí jiných mechanizmů. Pokud modul založený na znalosti předchází modulu biometrickému dochází například k problémům s nutností zadat znalost předtím, než je uživateli umožněno nasnímat biometrickou vlastnost. K nasnímání biometrické vlastnosti dojde pouze pokud předchozí modul selže. Tím je uživatel nucen zadat chybně kód/heslo, pokud chce využít biometrickou verifikaci. Při opačném pořadí modulů v řetězci není uživateli umožněno zadat heslo dříve než vyprší časový limit biometrické verifikace. Tato vlastnost je uživatelsky nepříjemná. Použití více autentizačních mechanizmů současně není v systému PAM přímo podporováno.

9.2 Implementace PAM v grafických aplikacích

Uživatelé unixových systémů se nejčastěji setkávají se systémem PAM v grafickém správci přihlášení (KDM [7], GDM [33]), uzamčeném spořiči obrazovky, aplikaci pro změnu identity (kdesu, gksu). Implementace komunikace se systémem PAM je většinou v rámci pracovního prostředí jednotná – v KDE je stejný kód použit v KDM i `kscreensaver`, v GNOME je pak stejný kód v GDM a `gnome-screensaver`.

Tyto implementace původně nepočítaly s možností verifikace pomocí biometrických vlastností nebo čipovou kartou. Problém nastává v okamžiku, kdy nejde předat veškeré

informace potřebné k verifikaci najednou. Například v okamžiku, kdy uživatel musí přiložit nebo protáhnout prst na snímači. Stejný problém nastává i u dalších biometrických metod. Systém PAM pak nemůže provést verifikaci v krátkém čase a uživatelské rozhraní není překreslováno. Kvůli tomu nelze v průběhu verifikace zobrazit animaci, nejsou překreslovány informativní zprávy a jiné. To je uživatelsky nepříjemné.

9.3 Možná řešení

Načtení hesla biometrickým modulem

PAM modul `pam_thikfinger` načítá heslo a ukládá jej pro další autentizační moduly. Pokud uživatel zadá heslo, je zpracování modulem `pam_thinkfinger` ukončeno a následující moduly vyzkouší uložené heslo. Jinak se pokusí o biometrickou verifikaci. Načítání hesla probíhá v samostatném vlákně. Pro ukončení tohoto vlákna je využito emulace stisknutí klávesy Enter.

Emulace stisku klávesy je provedeno zápisem do souboru `uinput`. Tento soubor je uložen v souborovém systému zařízení `/dev/`. Soubory zařízení slouží pro komunikaci mezi zařízeními, jádrem a uživatelským prostorem. Po otevření tohoto souboru `pam_thinkfinger` vytvoří virtuální klávesnici a v okamžiku ukončení biometrické verifikace se provede zápis klávesy.

Bohužel toto řešení není považováno za nejvhodnější a není akceptováno. Doporučení zní použít vícenásobný přístup k systému PAM [19]. Každý autentizační mechanizmus je pak zpracováván samostatně, není nutné zřetězení.

Vícenásobný přístup k systému PAM

Nový a do budoucna vhodný přístup je použít vícenásobný přístup k systému PAM. Vícenásobný přístup k systému PAM je založen na tom, že pro každou možnost verifikace se spustí samostatné vlákno. Vlákno uživatelského rozhraní tak není blokováno a uživatel přitom může využít možností všech autentizačních mechanizmů.

Lze tak vytvořit modul pro verifikaci pomocí hesla, moduly pro biometrickou verifikaci a další. Řízení těchto modulů má na starosti správce modulů. Ten zahajuje verifikaci a také ukončuje ostatní moduly, pokud některý z nich uspěje. Verifikace selže pouze pokud selžou všechny moduly. Nejdále je v implementaci tohoto přístupu správce přihlášení GDM. Tyto úpravy jsou obsaženy ve větvi `multistack` [31] systému správy verzí Git.

Kapitola 10

Možné alternativní přístupy

10.1 FingerprintGUI

FingerprintGUI je kompletní systém pro verifikaci a identifikaci uživatele pomocí otisků prstů [35]. Skládá se z modulu PAM a programu pro správu otisků prstů. Využívá služby knihovny `libfprint` a podporuje i uzavřenou knihovnu `libbsapi` pro čtečky od výrobce UPEK.

PAM modul využívá mechanizmu `uinput` a obsahuje i grafické uživatelské rozhraní. To je spuštěno pokud nalezne spuštěný systém X Window (obrázek 10.1), jinak s uživatelem komunikuje pomocí textových zpráv (obrázek 10.2).

Obrázek 10.1: Uživatelské rozhraní PAM modulu fingerprintPAM (převzato z [36])

Na rozdíl od ostatních PAM modulů podporuje fingerprintPAM i identifikaci uživatele pomocí otisku prstu. Plně podporuje správce přihlášení GDM, se správcem přihlášení KDM nespolupracuje.

Problémy FingerprintGUI

Návrh FingerprintGUI není zcela bezchybný:

- Grafické uživatelské rozhraní pro komunikaci s uživatelem implementuje přímo PAM modul. Aby mohl zobrazovat něco na displayi, tak musí:

```
root@test:~# logout

Ubuntu 8.04.1 test tty1

test login: root
Fingerprint Login 0.4
Authenticating root
Swipe your finger or type ENTER to give password...
```

Obrázek 10.2: Textové rozhraní PAM modulu fingerprintPAM (převzato z [36])

  - Získat identifikátor displaye (ze systémové proměnné, z identifikace konzole předané systémem PAM).
  - Získat číslo procesu systému X Window běžícího na daném displayi (ze souboru `/tmp/.X0-lock`, 0 reprezentuje identifikátor displaye).
  - Získat umístění souboru s autentizačním kódem pro systém X Window, jinak by nemohl spustit grafickou aplikaci (ze souboru umístěném v adresáři `/proc`[1]).

- Generuje pseudonáhodný řetězec, který používá k potvrzení identity uživatele od procesu uživatelského rozhraní.

- Pro časovou synchronizaci používá uspání procesu.

Grafické uživatelské rozhraní FingerprintGUI nezapadá do uživatelského rozhraní žádného dostupného grafického správce přihlášení (překryje jej). Samotné spuštění grafického uživatelského rozhraní je komplikovaná akce závislá na několika podmínkách. Neočekávané chování v krajních situacích může vést až k nemožnosti se přihlásit.

[1] /proc – Virtuální souborový systém obsahující adresáře odpovídající číslům procesů v systému. Každý adresář obsahuje informace o odpovídajícím procesu. Adresáře vznikají při spuštění procesu a zanikají při jeho ukončení.

Kapitola 11

Další vývoj

11.1 Knihovny libfprint a libusb

Knihovna `libfprint` využívá pro přístup ke snímačům otisků prstů knihovnu `libusb` v nejnovější verzi 1.0, která zatím není plně stabilizovaná. Proto může v některých kombinacích jádra operačního systému, verze knihovny `libusb` a `libfprint` dochází k občasným problémům (strana 39). Je tedy potřeba stabilizovat tento řetězec, aby docházelo co k nejmenšímu množství chyb při komunikaci. Tyto chyby totiž znemožňují bezproblémové využití autentizace uživatele pomocí otisků prstů.

11.2 Fprintd

Služba `fprintd` nepodporuje smazání pouze jednoho zavedeného otisku prstu uživatele. Již zavedený otisk prstu je možné nahradit jiným, což ale neřeší problém. Pokud bude uživatel chtít obměnit sadu zavedených otisků prstů, musí je všechny smazat a znovu zavést. To je uživatelsky velice nepříjemné. Autor služby `fprintd` tuto funkcionalitu odmítá [24].

Další možné rozšíření služby `fprintd` je podpora identifikace uživatele. To pak umožní přihlášení uživatele pouhým nasnímáním otisku prstu stejně jako to dnes funguje s většinou čteček v systému Microsoft Windows XP/Vista. Identifikace uživatele je podporována knihovnou `libfprint`.

Seznam instalovaných snímačů otisků prstů je vytvořen při spuštění služby `fprintd`. Služba tak nereaguje na snímače připojené po jejím spuštění a také nereflektuje odpojení snímače. Aby byl tento problém odstraněn je potřeba generovat seznam instalovaných zařízení periodicky nebo při každém dotazu na seznam dostupných zařízení.

11.3 KFingerManager

Program pro správu otisků prstů zatím obsahuje animaci pouze pro průtahové snímače otisků prstů. Bylo by vhodné vytvořit i animaci pro plošné snímače.

Dále kompletně chybí uživatelská dokumentace. Dokumentaci lze jednoduše integrovat do „*Nastavení systému*“ a tak ji má uživatel snadno dostupnou.

KFingerManager v současnosti obsahuje pouze českou a anglickou lokalizaci. Jestli se má stát standardní součástí pracovního prostředí KDE a jeho „*Nastavení systému*“, je třeba jej lokalizovat do dalších jazyků.

11.4 KDM

Ve správci přihlášení KDM je třeba zprovoznit verifikaci uživatele v samostatném vlákně, aby bylo možné v jejím průběhu zobrazovat animaci nasnímání otisku prstu a vypisovat informace o průběhu. V současnosti je ověření uživatele prováděno ve vlákně které vykresluje i uživatelské rozhraní a to se po celou dobu verifikace vykresluje pouze pokud je to vynuceno z jiného vlákna.

Tato změna společně s úpravou mechanizmu modulů pro komunikaci se systémem PAM by mohla umožnit použití několika autentizačních mechanizmů najednou. Následující řešení by mohlo být použito než budou vyřešeny všechny problémy.

Motivy vzhledu správce přihlášení KDM nepočítají s vytvořeným modulem a uživatelské rozhraní není úplně dokonalé. Bude potřeba upravit alespoň výchozí motiv vzhledu používaný v dané distribuci Linuxu.

Kgreet_fprintd

Částečným řešením pro „souběžnou“ verifikaci pomocí otisku prstu nebo pomocí hesla by mohlo být rozšíření modulu `kgreet_fprintd` o vstupní pole pro zadání hesla. PAM modul pro verifikaci hesla by předcházel PAM modulu pro verifikaci pomocí otisku prstu. Pokud by uživatel chtěl verifikaci pomocí hesla, zadal by heslo. `Kgreet_fprintd` by pak selhání verifikace pomocí hesla identifikoval tak, že by dostal zprávu žádající protažení otisku prstu. V ten okamžik by ukončil další zpracování. Naopak pokud by uživatel nechal vstupní pole pro heslo prázdné, PAM moduly ověřující uživatele podle hesla by skončily chybou a bylo by možné přejít k verifikaci pomocí otisku prstu.

Zásuvný modul `kgreet_fprintd` v současnosti obsahuje pouze českou a anglickou lokalizaci. Jestli se má stát standardní součástí KDM, je třeba jej lokalizovat do dalších jazyků.

11.5 KScreensaver

Spořič obrazovky použitý v pracovním prostředí KDE používá stejné moduly pro komunikaci se systémem PAM jako správce přihlášení KDM. A také trpí stejným problémem jako KDM. V případě použití verifikace pomocí otisku prstu se uživatelské rozhraní nepřekresluje po dobu práce systému PAM. Je proto potřeba nalézt řešení, které umožní verifikaci spouštět v samostatném vlákně jak v KDM, tak i ve spořiči obrazovky.

11.6 PAM modul pro KWallet

KWallet je úschovna hesel pro pracovní prostředí KDE. Její odemčení je možné pouze pomocí hesla. Některé distribuce GNU/Linuxu poskytovaly PAM modul `pam_kwallet`, který umožňoval odemčení úschovny v návaznosti na přihlášení uživatele do systému či odemčení spořiče obrazovky. Po úpravě KWallet by mohl dát na výběr zadání hesla úschovny nebo ověření uživatele pomocí systému PAM. Tím by šlo zajistit odemčení úschovny pomocí otisku prstu.

11.7 Programy kdesu a kdesudo

Program kdesu umožňuje spouštět programy s oprávněními jiného uživatele. Kdesu nepoužívá stejné moduly jako KDM či KScreensaver. Bylo by vhodné i kdesu vybavit pod-

porou pro verifikaci pomocí otisku prstu.

11.8 Internetová prezentace

Bylo by vhodné vytvořit internetovou prezentaci programu KFingerManager a zásuvného modulu `kgreet_fprintd`. Tato prezentace by popisovala způsob instalace a nastavení jednotlivých komponent tak, aby spolu vzájemně spolupracovaly. Prezentace by měla být v angličtině, případně i v dalších jazycích, aby byla dostupná co největšímu počtu uživatelů.

Dále by internetová prezentace mohla přinést fórum pro dotazy uživatelů a systém pro hlášení a správu chyb.

11.9 Bezpečnostní analýza

PAM modul `pam_fpritnd` komunikuje se službou `fprintd` přes sběrnici D-Bus. Na tu se může připojit kdokoliv a zažádat si i o známé jméno. Proto je nutné prozkoumat jak složité je vytvořit falešný program, který se za službu `fprintd` pouze vydává. Ověření identity služby založené na kryptografii tvorbu falešné služby znesnadní.

Kapitola 12

Závěr

Práce pojednává o vývoji vybavení notebooků pro biometrické metody. Mezi ně patří snímače otisků prstů. Vysvětluje i základní pojmy z počítačové bezpečnosti a ukazuje základní možnosti prokázání identity (kapitola 2).

Popisuje základní komerčně dostupné biometrické systémy, zabývá se biometrickými systémy obecně. Věnuje se sledovaným parametrům biometrických systémů a také jak se měří výkonnost těchto systémů (kapitola 3).

Protože cílem diplomové práce je podpora pro autentizace uživatelů pomocí otisků prstu, zabývá se biometrií otisků prstů podrobněji, popisuji markanty, komerčně dostupné typy snímačů, průběh zpracování otisků prstů od nasnímání po jejich zpracování a vyhodnocení (kapitola 4).

Práce také zkoumá jaké jsou možnosti autentizace uživatelů v systémech UNIX. Popisuje původní princip a z něj vycházející systém zásuvných autentizačních modulů systému PAM. Vysvětluje nevýhody při používání autentizačních čipů, karet a hesel. U hesel se navíc věnuje obraně proti slabým heslům pomocí modulů systému PAM a programy určené ke generování hesel (kapitola 5).

Veškerá práce na podpoře autentizace uživatele pomocí otisků prstů je věnována pracovnímu prostředí KDE, kde zatím nebyly žádné pokusy o implementaci verifikace pomocí otisků prstů. V pracovním prostředí GNOME je autentizace pomocí otisků prstů vyvíjena již delší dobu a je tedy lépe podporována.

Samotná implementace je diskutována v kapitolách 6 – 8, přičemž v šesté kapitole jsou popisovány technologie použité při implementaci, kapitola 7 popisuje správu otisků prstů a další kapitola se zabývá jednotlivými případy autentizace. Konkrétně se zde píše o přihlášení k počítači a odemčení uzamčeného spořiče obrazovky. Možnosti dalšího vývoje a rozšíření výsledků diplomové práce jsou diskutovány v kapitole 11.

Implementací správce otisků prstů a autentizačního zásuvného modulu pro správce přihlášení bylo splněno zadání práce. K bezchybné funkčnosti je třeba vyřešit problém zablokování uživatelského rozhraní v průběhu autentizace. Jako dočasné řešení lze využít opravu umístěnou na přiloženém DVD.

Práce dále diskutuje problémy návrhu systému PAM a grafických aplikací, které jej využívají. Popisuje také možná řešení těchto problémů (kapitola 9).

Věnuje se také alternativním přístupům k řešení problému identifikace a verifikace uživatele pomocí otisků prstu (kapitola 10).

Literatura

[1] AKME LOCK LLC: The Biometrics Fingerprint Sensor. [on-line], 2008 [cit. 2008-12-29]. Dostupný z WWW <http://www.akmelock.com/biometric/doc/bftech.pdf>.

[2] ATMEL: FingerChip Thermal Fingerprint Sweeping Sensor, Hardware Based, Navigation and Click Function, SPI Interface. [on-line], [cit. 2008-12-29]. Dostupný z WWW <http://www.atmel.com/dyn/resources/prod_documents/doc5347.pdf>.

[3] Bartoň, J.: GObject property names vs D-Bus property names. [on-line], 2009-03-30 [cit. 2009-04-26]. Dostupný z WWW <https://bugs.freedesktop.org/show_bug.cgi?id=20948>.

[4] Bartoň, J.: *Technologie žil hřbetu/dlaně ruky.* 2007, 15 s., Rešerše.

[5] Bobčík, B.: PAM - správa autentizačních mechanismů. [on-line], 19. 9. 2000 [cit. 2009-04-24]. Dostupný z WWW <http://www.root.cz/clanky/pam-sprava-autentizacnich-mechanismu/>.

[6] Borland, R.: *Bezpečnost v UNIXu a Internetu v praxi.* Computer Press, 1998, ISBN 80-7226-082-0.

[7] Buddenhagen, O.: The kdm Handbook. [on-line], 2007-12-07 [cit. 2009-01-06]. Dostupný z WWW <http://docs.kde.org/stable/en/kdebase-workspace/kdm/index.html>.

[8] Charles: Support fingerprint reader login in kdm. [on-line], 2005-11-19 [cit. 2009-05-08]. Dostupný z WWW <http://bugs.kde.org/show_bug.cgi?id=116682>.

[9] Doseděl, T.: *Analýza autentizačních schémat.* (Soutěžní práce pro konferenci Student EEICT 2002), 2002.

[10] Drahanský, M.: *Biometrické systémy BIO: Studijní opora.* 2006, reg. č. CZ.04.1.03./3.2.15.1/0003.

[11] Drake, D.: Fprintd. [on-line], 3 March 2008 [cit. 2008-04-24]. Dostupný z WWW <http://reactivated.net/fprint/wiki/Fprintd>.

[12] Drake, D.: Libfprint. [on-line], 23 November 2008 [cit. 2009-05-01]. Dostupný z WWW <http://reactivated.net/fprint/wiki/Libfprint>.

[13] Drake, D.: Main page – fprint project. [on-line], 10 August 2008 [cit. 2008-10-02]. Dostupný z WWW <http://reactivated.net/fprint/wiki/Main_page>.

[14] Drake, D.: Supported devices. [on-line], 20 November 2008 [cit. 2009-05-01]. Dostupný z WWW <http://reactivated.net/fprint/wiki/Libfprint:Supported_devices>.

[15] Egorkine, A.: [fprint] [fprintd] Delete only one finger. [on-line], tue Apr 14 04:26:17 BST 2009 [cit. 2009-05-03]. Dostupný z WWW <http://lists.reactivated.net/pipermail/fprint/2009-April/001150.html>.

[16] Gafton, C.: *pam_cracklib – PAM module to check the password against dictionary words*. 2006.

[17] Geisshirt, K.: *Pluggable Authentication Modules: The Definitive Guide to PAM for Linux SysAdmins and C Developers*. 32 Lincoln Road, Olton, Birmingham, B27 6PA, UK: Packt Publishing, 2007, 119 s., ISBN 978-1-904811-32-9.

[18] Haugh, J. F.: *shadow - soubor se zašifrovanými hesly*.

[19] Hoenig, T.: [fprint] [PATCH] Support for password prompt while finger scanning. [on-line], sat Feb 14 19:37:58 GMT 2009 [cit 2009-04-24]. Dostupný z WWW <http://lists.reactivated.net/pipermail/fprint/2009-February/001089.html>.

[20] Hoenig, T.; Machek, P.; Capello, L.; aj.: *pam_thinkfinger - PAM module for fingerprint authentication through libthinkfinger*. 2007.

[21] Mirzazhanov, A. I.: APG (Automated Password Generator). [on-line], Saturday, 13-Sep-2003 14:29:18 ALMST [cit. 2008-12-25]. Dostupný z WWW <http://www.adel.nursat.kz/apg/>.

[22] MVČR: Platné typy občanských průkazů. [on-line], 6.8.2008 [cit. 2008-12-25]. Dostupný z WWW <http://www.mvcr.cz/clanek/rady-a-sluzby-dokumenty-platne-typy-obcanskych-prukazu.aspx>.

[23] National Science and Technology Council: *Fingerprint Recognition*. NSTC, 2006.

[24] Nocera, B.: [fprint] [fprintd] Delete only one finger. [on-line], Tue Mar 24 17:03:17 GMT 2009 [cit. 2009-04-26]. Dostupný z WWW <http://lists.reactivated.net/pipermail/fprint/2009-March/001132.html>.

[25] Nocera, B.: [fprint] [fprintd] Delete only one finger. [on-line], sat Apr 11 00:24:53 BST 2009 [cit. 2009-05-03]. Dostupný z WWW <http://lists.reactivated.net/pipermail/fprint/2009-April/001147.html>.

[26] Pennington, H.: D-Bus Specification. [on-line], november 8, 2006 [cit. 2009-04-25]. Dostupný z WWW <http://dbus.freedesktop.org/doc/dbus-specification.html>.

[27] Pronchery, P.: Random password and cypher generator (DES, MD5, ...). [on-line], Nov 28th 2007 16:30 UTC [cit. 2008-12-25]. Dostupný z WWW <http://people.defora.org/~khorben/projects/makepasswd/>.

[28] Rak, R.; Matyáš, V.; Říha, Z.; aj.: *Biometrie a indentita člověka ve forenzních a komerčních aplikacích.* U Průhonu 22, Praha 7: GRADA, 2008, 664 s., ISBN 978-80-247-2365-5.

[29] Roberge, D.: kdm crashes with pam_thinkfinger. [on-line], 2008-04-13 [cit. 2008-12-29]. Dostupný z WWW <https://bugs.launchpad.net/ubuntu/+source/kdebase-workspace/+bug/216697>.

[30] Schuckers, S.; Hornak, L.; Norman, T.; aj.: Issues for Liveness Detection in Biometrics. WEST VIRGINIA UNIVERSITY – Center for Identification Technology Research.

[31] Strode, R.: GDM git repository. [on-line], 18-Feb-2009 [cit. 2009-04-24]. Dostupný z WWW <http://www.gnome.org/~halfline/gdm/>.

[32] Sun, Z.; Dong, W.; Tan, T.: Technology Roadmap for Smart Iris Recognition. P.O. Box 2728, Beijing, 100190, P.R. China: Center for Biometrics and Security Research & National Laboratory of Pattern Recognition Institute of Automation, Chinese Academy of Sciences, June 2008, s. 1–7.

[33] The GNOME Project: GDM - The GNOME Display Manager. [on-line], 2005 [cit. 2009-01-06]. Dostupný z WWW <http://projects.gnome.org/gdm/>.

[34] Ts'o, T.: Password Generator. [on-line], july 4, 2007 [cit. 2008-12-25]. Dostupný z WWW <http://pwgen.sourceforge.net/>.

[35] Ullrich, W.: Fingerprint GUI: Use Fingerprint Devices with Linux. [on-line], 27.10.2008 [cit. 2008-12-29]. Dostupný z WWW <http://www.pdfserver.net/fingerprint/index.php>.

[36] Ullrich, W.: Screenshots. [on-line], 2009 [cit. 2009-04-30]. Dostupný z WWW <http://darkblue.homeip.net/fingerprint/screenshots.php>.

[37] UPEK: UPEK FIPS 201 Compliant Silicon Fingerprint Sensor. [on-line], [cit. 2008-12-29]. Dostupný z WWW <www.upek.com/pdf/UPEK_flyer_FIPS201.pdf>.

[38] Various people: *pam_unix – Module for traditional password authentication.* 2007.

[39] Walters, C.: What is D-Bus? [on-line], 2009-01-07 [cit. 2009-04-24]. Dostupný z WWW <http://www.freedesktop.org/wiki/Software/dbus>.

[40] Wikipedia: Biometrics — Wikipedia, The Free Encyclopedia. [on-line], 22 December 2008 [cit. 2008-12-29]. Dostupný z WWW <http://en.wikipedia.org/w/index.php?title=Biometrics&oldid=259489552>.

[41] Wikipedia: KDE Display Manager — Wikipedia, The Free Encyclopedia. [on-line], 26 March 2009 [cit. 2009-04-27]. Dostupný z WWW <http://en.wikipedia.org/w/index.php?title=KDE_Display_Manager&oldid=279777051>.

[42] WWW stránky: File:Bertillon - Signalement Anthropometrique.png. [on-line], 11 April 2006 [cit. 2008-12-27]. Dostupný z WWW <http://en.wikipedia.org/wiki/File:Bertillon_-_Signalement_Anthropometrique.png>.

[43] WWW stránky: Worldwide concern about biochip implant... [on-line], november 22, 2008 [cit. 2008-12-25]. Dostupný z WWW <http://www.tldm.org/News4/MarkoftheBeast2.htm>.

Seznam příloh

A Obsah přiloženého CD **58**

B Obraz disku pro virtuální počítač **59**

C Konfigurační soubory PAM **60**

D Konfigurační soubor kdmrc **61**

Dodatek A

Obsah přiloženého CD

```
.
|-- dp                       - zdrojové soubory textu diplomové práce
|-- rpm                      - instalační balíčky
|   |-- srpm                 -    zdrojové balíčky
|   `-- x86_64               -    balíčky pro architekturu x86_64
|-- src                      - zdrojové soubory programů
|   |-- KFingerManager       - správce otisků prstů
|   |   |-- img              -    použité obrázky
|   |   |-- pot              -    soubory pro lokalizaci
|   |   `-- src              -    zdrojové soubory
|   `-- kgreet_fprintd       - zásuvný modul správce přihlášení
|       |-- img              -     použité obrázky
|       |-- pot              -     soubory pro lokalizaci
|       `-- src              -     zdrojové soubory
|-- vbox                     - obraz disku systému Fedora 10
|------ xbarto42-dp-cb.pdf  - diplomová práce s jednobarevným textem
`------ xbarto42-dp-brv.pdf - diplomová práce s barevnými odkazy
```

Dodatek B

Obraz disku pro virtuální počítač

Na přiloženém DVD naleznete v adresáři `vbox` obraz disku systému Fedora 10 s nainstalovanými a nakonfigurovanými balíčky vytvořenými v rámci diplomové práce. Tento obraz lze použít ve virtuálním počítači VirtualBox. Systém Fedora je nainstalován v jeho 64 bitové verzi, pro zprovoznění je tedy potřeba 64 bitový procesor a 64 bitová verze VirtualBoxu. Vývoj probíhal na 64 bitové verzi systému a proto byl zvolen také pro ukázkovou verzi. Systém je nainstalován v anglické lokalizaci, stejný obraz disku bude vystaven i na internetové prezentaci.

Zprovoznění virtuálního systému

Pro zprovoznění systému je třeba podniknout několik kroků:

- Nainstalovat program VirtualBox.
- Vytvořit nový virtuální počítač.
- Nastavit název počítače a typ operačního systému: xbarto42, systém Linux, verze Fedora (64-bit).
- Nastavit velikost operační paměti na 512MB.
- Zvolíme použít existující disk a ve správci virtálních médií přidáme existující soubor s obrazem disku.
- Potvrdit vytvoření nového virtuálního počítače.
- Povolit sběrnici USB a přístup ke snímači otisků prstů v nastavení virtuálního pčítače.

Použití virtuálního systému

Vytvořený virtuální počítač lze spustit. Po chvíli naběhne správce přihlášení KDM v němž lze vybrat uživatele **test** s heslem **test4test**. Po přihlášení lze v „*System settings*“ zavést otisky prstůa při dalším přihlášení zvolit autentizaci pomocí otisků prstů. Heslo uživatele **root** je **root4test**.

Dodatek C

Konfigurační soubory PAM

Konfigurační soubor kdm-fprintd

```
#%PAM-1.0
auth     [success=done ignore=ignore default=bad] pam_selinux_permit.so
auth       required    pam_env.so
auth       substack    system-auth-fprint
auth       optional    pam_gnome_keyring.so
account    required    pam_nologin.so
account    include     system-auth
session    required    pam_selinux.so close
session    required    pam_loginuid.so
session    optional    pam_console.so
session    required    pam_selinux.so open
session    optional    pam_keyinit.so force revoke
session    required    pam_namespace.so
session    optional    pam_gnome_keyring.so auto_start
session    include     system-auth
```

Konfigurační soubor system-auth-fprintd

```
#%PAM-1.0
auth        required      pam_env.so
auth        sufficient    pam_fprintd.so
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so
```

Konfigurační soubor kscreensaver-fprintd

```
#%PAM-1.0
auth       include system-auth-fprintd
account    include system-auth
password   include system-auth
session    include system-auth
```

Dodatek D

Konfigurační soubor kdmrc

```
[General]
ConfigVersion=2.3
ConsoleTTYs=tty2,tty3,tty4,tty5,tty6
PidFile=/var/run/kdm.pid
ReserveServers=:1,:2,:3
ServerVTs=1
StaticServers=:0

[Shutdown]
BootManager=None
HaltCmd=/sbin/poweroff
RebootCmd=/sbin/reboot

[X-*-Core]
AllowShutdown=Root
AutoReLogin=false
ClientLogFile=.xsession-errors-%d
Resources=/etc/X11/xdm/Xresources
Session=/etc/kde/kdm/Xsession
SessionsDirs=/usr/share/xsessions,/usr/share/apps/kdm/sessions,/etc/X11/dm/sessions
Setup=/etc/X11/xdm/Xsetup_0

[X-*-Greeter]
AntiAliasing=true
BackgroundCfg=/etc/kde/kdm/backgroundrc
ColorScheme=ObsidianCoast
EchoPasswd=true
FaceSource=PreferUser
FailFont=Abyssinica SIL,12,-1,5,50,0,0,0,0,0
FocusPasswd=true
ForgingSeed=1108476160
GUIStyle=
GreetFont=Abyssinica SIL,16,-1,5,50,0,0,0,0,0
GreetString=Fedora 9 (Sulphur)
GreeterPos=50,50
```

```
HiddenUsers=root
Language=cs
LogoArea=Logo
LogoPixmap=/usr/share/icons/hicolor/96x96/apps/fedora-logo-icon.png
MaxShowUID=65530
MinShowUID=500
SelectedUsers=
ShowUsers=NotHidden
SortUsers=true
StdFont=Abyssinica SIL,10,-1,5,50,0,0,0,0,0
Theme=/usr/share/kde4/apps/kdm/themes/SolarMania
UseBackground=true
UseTheme=true
UserCompletion=false
UserList=true
PluginsLogin = fprintd, classic, generic, winbind

[X-:*-Core]
AllowShutdown=All
NoPassEnable=false
NoPassUsers=
ServerArgsLocal=-br -nolisten tcp
ServerTimeout=30
TerminateServer=true

[X-:*-Greeter]
DefaultUser=djaara
FocusPasswd=true
LoginMode=DefaultLocal
PreselectUser=Previous

[X-:0-Core]
AutoLoginEnable=false
AutoLoginLocked=false
AutoLoginUser=

[Xdmcp]
Enable=false
Willing=/etc/X11/xdm/Xwilling
Xaccess=/etc/X11/xdm/Xaccess
```