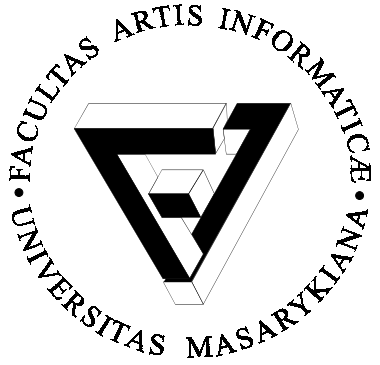
MASARYKOVA UNIVERZITA

FAKULTA INFORMATIKY

PROJEKT

Klient pro přihlášení uživatele do systému MS-Windows 9x



Pavel Minařík

Zadání projektu

Student ve své práci provede zhodnocení dosavadních možností operačních systémů řady MS-Windows 9x z hlediska monitorování aktivit přihlášených uživatelů. Dále v rámci své práce navrhne a prakticky zrealizuje programový systém zabraňující neoprávněnému použití počítače a umožňující sledování zvolených činností uživatele. Cílem práce je vytvořit program pro platformu MS-Windows s konfiguračním souborem, který určuje umístění centrální databáze v síti. Databáze bude obsahovat uživatelská jména a hesla. Dále pak tabulku formátu Paradox, která bude uchovávat záznamy o práci jednotlivých uživatelů. Administrátor bude vybaven speciálním programem, kterým bude moci z libovolného PC v síti měnit údaje o uživatelích.

Shrnutí

V této práci byl proveden podrobný rozbor všech operačních systémů MS-Windows z hlediska přihlašování uživatelů. Bylo zjištěno, že systémy řady MS-Windows 9x (ačkoliv jsou ještě hojně používány) nedosahují potřebné úrovně zabezpečení a nedisponují schopností sledovat informace o přihlašování jednotlivých uživatelů. Z výše uvedených důvodů byl navržen a implementován programový systém, který do prostředí operačních systémů řady MS-Windows 9x tuto požadovanou funkcionalitu doplňuje. Systém byl navrhován s ohledem na jednoduchost použití a nenáročnost na systémové zdroje. Součástí tohoto programového systému je také výkonný nástroj na konfiguraci možností systému a správu uživatelských identit, který však nevyžaduje zkušeného správce systému.

Klíčová slova

Operační systém, přihlášení uživatele, Klient pro přihlášení uživatele, Administrační aplikace, zotavení z havárie, centrální databáze, interval pro automatický zápis do centrální databáze, konfigurační soubor s údajem o umístění centrální databáze, BDE (Borland Database Engine), heslo pro plný přístup, uživatelské jméno, heslo, seznam oprávněných uživatelů, protokol o přihlašování uživatelů.

Obsah

Seznam obrázků v textu

1 Rozbor stávajících možností systémů Windows

1.1 MS-Windows řady 9x

Mezi tyto operační systémy společnosti Microsoft patří Windows 95, Windows 95 OSR2, Windows 98, Windows 98 SE (Second Edition) a Windows ME (Millenium Edition). Systémy řady Windows 95 již není třeba uvažovat, protože jejich architektura a podpora technického vybavení je značně omezená. Na v praxi reálně využitelném počítači lze provozovat systém Windows 98, proto je možné systém Windows 95 z tohoto rozboru vynechat. Operačnímu systému Windows ME bude věnována samostatná část. V dalším textu bude systémem řady MS-Windows 9x označen systém Windows 98 nebo Windows 98 SE. Tyto dva systémy se z hlediska tohoto rozboru v podstatě neliší. Hlavní rozdíly mezi těmito systémy spočívají v podpoře technického vybavení, preferovaném modelu ovladačů zařízení a podporou multimédií.

Operační systémy řady MS-Windows 9x jsou koncipovány jako jednouživatelské. Podpora více uživatelů se při bližším zkoumání jeví jako doplňkovou vlastností (přidanou později), ne jako vlastností jádra systému. Právě proto je zřejmé, že žádným dodatečným programovým vybavením není možné zajistit skutečnou podporu více uživatelů, tak jak ji známe z moderních operačních systémů společnosti Microsoft nebo ze systémů typu UNIX. Podpora více uživatelů, kteří využívají jeden počítač, musí být implementována především na úrovni jádra systému.

Dalším problémem je použitý souborový systém. Operační systémy MS-Windows řady 9x umožňují pracovat pouze s diskovými oddíly se systémem souborů FAT. Tento systém souborů nepodporuje uživatelská práva na úrovni jednotlivých uživatelů tak jako souborový systém NTFS, který je využíván operačními systémy s technologií NT. Přidělování práv na soubory a adresáře jednotlivým uživatelům je přitom nutná podmínka, kterou musí splňovat víceuživatelský systém.

Jiná situace je ovšem v oblasti autorizace přístupu k počítači. Opět platí, že podpora z hlediska operačních systémů řady MS-Windows 9x je zde velmi omezená a systém nedokáže přinutit uživatele autorizovat svůj přístup k počítači. Tuto situaci je ale možné řešit dodatečným programovým systémem. Cílem této práce je analyzovat požadované funkce tohoto systému, navrhnout vhodnou implementaci a tento systém vytvořit.

1.2 MS-Windows s technologií NT

Mezi operační systémy s technologií NT (oficiální termín společnosti Microsoft zní „built on NT technology“) patří Windows NT, Windows 2000 a Windows XP. Všechny budoucí operační systémy budou na této technologii také založeny. Tyto systémy jsou oproti starším MS-Windows řady 9x koncipovány jako víceuživatelské již na úrovni jádra, vyžadují autorizaci uživatele a umožňují monitorování aktivit uživatelů. Tyto systémy se používají v prostředí středních a větších firem, kde MS-Windows řady 9x neobstojí. Windows s technologií NT nabízejí také tzv. cestovní profily uživatelů. Tyto cestovní profily umožňují všem uživatelům v síti používat na libovolném počítači vlastní jednotná nastavení, která jsou uložena vzdáleně (většinou na primárním řadiči domény). Tuto vlastnost opět v systému MS-Windows řady 9x nenajdeme a bohužel ji ani nemáme možnost dodatečným programovým vybavením realizovat. Další výhodou systémů založených na technologii NT je možnost definovat tzv. skupinová oprávnění, která jsou přenášena transparentně na všechny členy takové skupiny. Výše uvedené vlastnosti jsou z hlediska tohoto rozboru klíčové a zároveň dostačující, i když samozřejmě nevyčerpávají všechny rozdíly.

1.3 MS-Windows ME

Tento operační systém nelze jednoznačně zařadit ani do jedné z výše uvedených kategorií. I když se nejedná o systém založený na technologii NT, podporuje některé moderní technologie, které v systémech MS-Windows řady 9x nenajdeme. Proto také patří svými nároky na technické vybavení mezi moderní systémy jako např. Windows 2000 nebo XP. Tento systém není z hlediska této analýzy podstatný, protože platí, že tam, kde lze provozovat Windows ME, lze bez problémů provozovat i Windows 2000. Dalším argumentem je pak skutečnost, že tento systém se téměř nepoužívá. Microsoft tento systém uvedl jako mezistupeň mezi Windows 98 SE a Windows 2000.

1.4 Použití systémů s technologií NT místo MS-Windows řady 9x

Z výše uvedeného rozboru vlastností vyplývá, že migrací na systémy s technologií NT lze vyřešit všechny problémy, které se vyskytují u systémů řady MS-Windows 9x. Bohužel, takto jednoduché řešení není vždy proveditelné. Nejsou to pouze nároky na technické vybavení, které použití těchto moderních systémů limitují. Následující přehled si klade za cíl vyčerpat všechna fakta, která mohou omezit možnost použití moderních systémů založených na technologii NT.

- Technické vybavení nesplňuje požadavky na provoz nového systému, výměna technického vybavení je příliš nákladná, hlavně v případě, že plně dostačuje práci při použití systému MS-Windows řady 9x.
- V počítači je využíváno speciální technické vybavení, které pod novým systémem nepracuje, např. z důvodu absence ovladačů.
- V počítači je používáno programové vybavení, které korektně nepracuje pod novým systémem, 100% kompatibilita není vždy zaručena.
- Společnost vlastní licence na systémy řady MS-Windows 9x, které by se pak staly bezcennými, zvláště pak při vlastnictví tzv. OEM licencí, které jsou vázány na konkrétní počítače.

Uvedené problémy lze vždy řešit jen za cenu nákladů, které mohou být v některých případech neúměrně vysoké. Zvláště menší společnosti nebo neziskové organizace si nemohou dovolit vynaložit vysoké prostředky, které jsou schopny použít účelněji, ačkoliv mají zájem využívat alespoň některé z těchto moderních funkcí a vlastností. Minimálně by ocenili možnost získat přehled využití počítačů svými zaměstnanci. S ohledem na tento požadavek je třeba analyzovat funkce a navrhovat tento programový systém.

2 Analýza funkcí navrhovaného programového systému

2.1 Reálné požadavky malých společností a organizací

Velmi často se objevuje jednoduchý a jasný požadavek ze strany majitelů malých firem nebo neziskových organizací. „Chceme vědět, kdy se kdo k počítači přihlásil, jak dlouho pracoval a kdy se odhlásil.“ Tento požadavek přesně odpovídá modelu směnného provozu u počítačů a legitimnímu zájmu zaměstnavatele, aby jeho zaměstnanci dodržovali předepsanou pracovní dobu, za kterou jsou placeni. Takový směnný provoz může mít například technická podpora nebo firma provozující chat na internetu. Místem typického nasazení navrhovaného programového systému je právě menší společnost s výše uvedenými požadavky. Dalším požadavkem je realizovat takový systém s minimálními náklady a nároky na znalosti a schopnosti uživatele.

2.2 Vlastnosti a funkce navrhovaného programového systému

Základní rysy, které musí programový systém „Klient pro přihlášení uživatele do systému MS-Windows 9x“ splňovat, lze shrnout do několika bodů. Jedná se pouze o návrh vlastností, který zatím ponechává otázku implementace otevřenou.

- Blokovat možnost pracovat s počítačem, vyžadovat autorizaci,
- udržovat centrálně seznam oprávněných uživatelů,
- možnost měnit seznam oprávněných uživatelů z libovolného počítače v síti,
- zajistit ochranu seznamu oprávněných uživatelů,
- využívat minimum systémových zdrojů, pracovat transparentně,
- centrálně protokolovat přihlášení a odhlášení uživatelů k počítačům,
- jednoduše konfigurovat vlastnosti programového systému.

Programový systém musí splňovat všechny výše uvedené požadavky, aby byl schopen zajistit požadovanou bezpečnost, transparentnost vůči uživatelům a jednoduchost správy i konfigurace. Systém nepředpokládá zkušeného administrátora. Následující kapitola se zabývá podrobným rozborem jednotlivých bodů výše uvedeného seznamu.

3 Návrh implementace programového systému

3.1 Seskupení vlastností a funkcí

Z výše uvedeného seznamu vlastností a funkcí systému jsou patrné tři základní oblasti, které lze řešit odděleně. Skupina požadavků na centrální uložení vede k nutnosti nasazení databáze. Seznam oprávněných uživatelů lze řešit jen jako běžný konfigurační soubor, avšak protokolování si použití databáze vynutí z důvodu čitelnosti protokolů. Proto celá tato část bude implementována jako relační databáze.

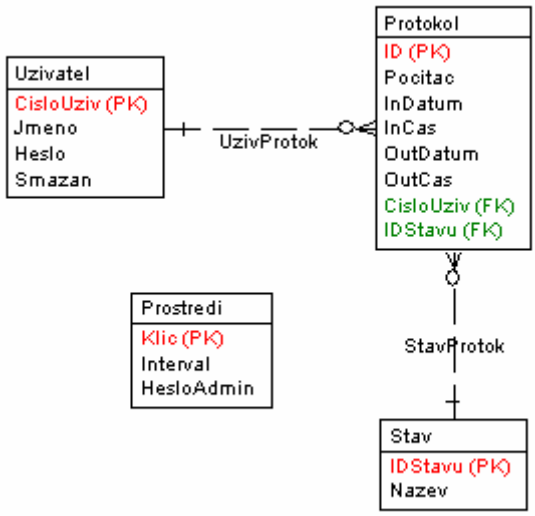
Skupina požadavků týkající se samotného klienta vyžaduje vytvoření aplikace pro platformu MS-Windows řady 9x, která bude používat pouze jediný lokální konfigurační soubor informující klienta o umístění centrální databáze v síti. Všechna ostatní relevantní data získá klient z této centrální databáze. Klient bude implementován s velkým ohledem na spotřebovávané systémové zdroje v moderním vývojovém prostředí Borland Delphi verze 6.0, které používá rozšířenou verzi programovacího jazyka Pascal (tzv. Object Pascal).

Skupina požadavků, které se týkají správy seznamu uživatelů a konfigurace, vede na vytvoření speciální aplikace, která bude dostupná pouze administrátorovi systému. Pomocí této aplikace bude administrátor schopen měnit seznam uživatelů a případná další nastavení (jako např. konfigurační soubor určující uložení centrální databáze v síti). Přístup do této aplikace bude chráněn heslem. Konfigurační aplikace bude také implementována ve vývojovém prostředí Borland Delphi verze 6.0.

Jak klient, tak konfigurační aplikace bude používat systém generování dotazů jazyka SQL. Tyto dotazy bude následně zasílat relační databázi, která bude odpovídat relevantními daty. Jako vhodná technologie pro implementaci databáze se jeví platforma Paradox, pro přístup k databázi lze využít Microsoft ADO nebo Borland Database Engine, který používá Paradox jako svou nativní platformu. Lze říci, že oba dva přístupy jsou rovnocenné a měly by poskytovat stejné služby pro aplikační programy. Výhodou systému Borland Database Engine je vyšší rychlost zpracování, která plyne z úzké provázanosti s platformou Paradox. Oba zmíněné přístupy umožňují pouze základní manipulace s daty (implementují pouze část jazyka SQL – tzv. data manipulation language), které však pro potřeby navrhovaného systému plně dostačují.

3.2 Návrh relační databáze

V centrální databázi programového systému je třeba uchovávat seznam uživatelů s jejich hesly. Dále je třeba protokolovat přihlášení a odhlášení jednotlivých uživatelů. Důležitá je především informace a datu a času přihlášení i odhlášení. V síti je zapojeno více počítačů, proto je třeba zachytit i informaci ke kterému počítači se uživatel přihlásil. Systém musí také rozlišovat mezi různými stavy přihlášení konkrétního uživatele. Dále je třeba zaznamenat heslo plného přístupu ke všem funkcím a interval automatického zápisu do databáze (klient bude v těchto intervalech provádět záznam o aktivitě uživatele).



Obr. 1: Model relační databáze využívané programovým systémem

Přílohou tohoto návrhu je podrobná elektronická dokumentace navrhované relační databáze, která popisuje fyzickou strukturu databázových tabulek, význam jednotlivých polí a smysl vazeb. Použití indexů je v uvažované databázi zbytečné. Data o uživatelích nejsou takového rozsahu, aby indexy vyžadovala, v případě potřeby lze indexy doplnit. Do protokolu bude klient jen zapisovat, pouze při přihlášení bude provedena operace čtení.

3.3 Návrh klienta

Požadavek, aby klient blokoval práci s počítačem až do přihlášení uživatele, lze zajistit vyřazením standardních mechanizmů operačních systémů řady MS–Windows 9x pro přepínání programů, ukončování programů a vyvolání nabídky start. Proto klient musí při svém spuštění provést následující kroky:

- přepnutí do režimu aplikace přes celou obrazovku a vždy navrchu (always on top),
- registraci jako systémová služba (využití volání Win32API, které zaregistruje proces jako systémovou službu, kterou nemůže uživatel ukončit, protože není zobrazována správci úloh),
- zákaz použití kombinací kláves Ctrl+Esc, Alt+Tab, Alt+F4, Ctrl+Alt+Del (využití volání Win32API, které umožňuje zakázat a zpětně povolit možnost využít tyto kombinace kláves).

Z výše uvedeného je zřejmé, že pokud bude klient spuštěn a žádný uživatel nebude přihlášen, tak funkce vypnout počítač, která se nachází v nabídce dostupné přes tlačítko „Start“, nebude k dispozici. Proto musí klient umožnit vypnout počítač (opět lze využít volání příslušné funkce Win32API).

Jakmile je uživatel (po kontrole jména a hesla) přihlášen do systému, je třeba provést minimalizaci klienta na lištu spuštěných programů a do práce uživateli nezasahovat. Zároveň musí klient opět povolit použití kombinací kláves Crtl+Esc, Alt+Tab, Ctrl+Alt+Del, apod. Pokud se uživatel chce odhlásit, obnoví klienta na plnou velikost a provede odhlášení. Klient musí umožnit také opětovnou minimalizaci na lištu spuštěných programů (pokud si uživatel odhlášení rozmyslí nebo klienta obnoví na plnou velikost omylem). Po odhlášení klient opět zabrání práci s počítačem a zablokuje zmíněné kombinace kláves.

Z důvodu bezpečnosti bude u uživatelských hesel použit mechanismus jednosměrného šifrování, tzn. ze zašifrovaného hesla není možné zpětně vygenerovat heslo v čitelné podobě. Jiný postup bude použit v případě konfiguračního souboru, který určuje umístění databáze v síti. Tento zašifrovaný soubor bude třeba dešifrovat a získat tak síťovou cestu pro přístup k databázi. Pro zabránění přístupu uživatelů k souborům databáze je vhodné využít vlastnosti všech operačních systémů MS-Windows 95 nebo novějších, které umožňují vytvořit tzv. skrytou sdílenou složku. Na tuto složku se vztahují všechna platná pravidla jako na běžnou sdílenou složku, avšak tato složka se v systému nezobrazuje. To znamená, že uživatel musí znát její název, aby mohl přistupovat k jejímu obsahu. Skrytou sdílenou složku lze vytvořit připojením znaku „$“ za název pod kterým je složka sdílena. Tento znak se stává součástí jejího názvu.

Klient zapisuje do databáze informaci o tom, že uživatel je stále přihlášen do systému v pravidelných intervalech. Velikost tohoto intervalu zadává administrátor a je uložena v centrální databázi. Při spuštění klient provede zjištění hodnoty tohoto intervalu a konfiguraci svého časovače. Tuto funkci si vynucuje skutečnost, že ne vždy je možné spolehnout se na stabilitu systému. K havárii systému může dojít např. závažnou chybou systému, selháním zařízení, chybou programového vybavení nebo výpadkem napájení. Pokud by v pravidelných intervalech nebyla informace o posledním známém okamžiku práce zapisována, nebylo by možné určit dobu, po kterou uživatel se systémem pracoval, kdyby systém havaroval a uživatel se nestihl odhlásit ručně. Tato funkce zajistí, že se údaj zapsaný v protokolu po havárii systému nebude od skutečnosti lišit o více než o velikost zadaného intervalu. Pro běžný provoz stačí délka intervalu cca 5 minut (interval bude zadán s přesností na sekundy, proto uložená hodnota bude 300), zároveň systém nepovolí zadání kratšího intervalu než 15 sekund. Klient by generoval zbytečné zatížení sítě.

V některých případech může administrátor vyžadovat ukončení klienta. Tuto funkci systém zpřístupní po zadání hesla pro plný přístup přes tlačítko určené k vypnutí počítače. Funkce tlačítka se tedy změní z vypnutí počítače na ukončení klienta.

Klient musí být spuštěn při každém startu počítače. Jako nejvhodnější umístění se jeví příslušná část registru systému Windows. Volba umístění však plně závisí na uvážení administrátora a může být v podstatě libovolná.

Závěrem je třeba říci, že navrhovaný klient si neklade za cíl 100% zabránění přístupu k počítači. Jedná se o aplikační program, ne o součást systému, proto nemůže poskytnout takto vysokou úroveň zabezpečení. Hlavním cílem je monitorování dodržování předepsané pracovní doby, proto jeho vyřazením z provozu by uživatel nic nezískal.

3.4 Návrh konfigurační aplikace

Nejprve je třeba provést napojení na centrální databázi a kontrolu hesla pro plný přístup. Při prvním spuštění konfigurační aplikace ještě nemůže být vygenerován šifrovaný konfigurační soubor, který určuje umístění centrální databáze v síti. Proto bude nejprve uživatel dotázán na toto umístění. Po úspěšné autorizaci nabídne konfigurační aplikace uživateli následující funkce, které může využít pro přizpůsobení si aplikačního systému vlastním požadavkům.

- Změna hesla pro plný přístup,
- změna intervalu automatického zápisu do centrální databáze,
- úprava seznamu uživatelů,
- výpis přihlašovacího protokolu,
- vygenerování šifrovaného konfiguračního souboru s údajem o umístění centrální databáze v síti.

Při změně hesla pro plný přístup systém kontroluje délku, která musí být minimálně šest znaků, jinak změnu neprovede. Toto omezení se netýká hesel jednotlivých uživatelů, kteří mohou mít přiděleno heslo libovolné délky. Implicitní heslo pro plný přístup je slovo „password“, toto heslo by mělo být administrátorem okamžitě změněno. Zároveň z bezpečnostních důvodů je vhodné uschovat aplikaci pro konfiguraci na bezpečném místě mimo dosah běžných uživatelů.

Interval automatického zápisu do centrální databáze je implicitně nastaven na 300 sekund, systém vyžaduje zadání této hodnoty z rozmezí 15 až 900 sekund. Význam intervalu automatického zápisu do centrální databáze je popsán v kapitole 3.3.

Konfigurační program nabízí v rámci úpravy seznamu uživatelů možnost přidat uživatele, smazat uživatele, změnit uživatelské jméno a změnit heslo. Hesla jednotlivým uživatelům přiděluje administrátor, nemají možnost je sami měnit. Toto chování systému je z hlediska cílové skupiny uživatelů bezpečnějším a jednodušším řešením zároveň. Při odstraňování uživatele systém kontroluje jeho výskyt v některém z protokolovaných záznamů. Pokud je v protokolu uživatel nalezen, nemůže být ze seznamu fyzicky odstraněn. U takového uživatele systém pouze nastaví atribut smazán a uživatel se již není schopen přihlásit. Smazaného uživatele je možné opět převést do aktivního stavu pomocí funkce „obnovit smazaného uživatele“.

Funkce výpis slouží administrátorovi systému pro kontrolu práce jednotlivých uživatelů na počítačích. Umožňuje omezit výpis na informace pouze o zadaném uživateli nebo zadaném počítači, případně zobrazovat pouze informace od/do zadaného data.

Konfigurační program dále umožní vygenerovat šifrovaný konfigurační soubor s údaji o umístění centrální databáze v síti. Tento konfigurační soubor se musí nacházet ve stejné složce jako samotný klient.

3.5 Pokročilé zotavení z havárie

Důležitým aspektem je schopnost klienta zotavit se z pádu systému a opravit data zapsaná v centrální databázi. Z tohoto důvodu systém rozlišuje čtyři možné stavy přihlášení uživatele. V následujícím přehledu jsou uvedeny včetně popisu.

- **In** (uživatel se právě přihlásil do systému, od jeho přihlášení neuplynulo ani tolik sekund, kolik je zadáno v parametru „Interval automatického zápisu do centrální databáze“).
- **Working** (uživatel pracuje se systémem, klient v pravidelných intervalech zapisuje do databáze údaj o aktuálním datu a čase).
- **Out** (uživatel se manuálně odhlásil, datum a čas odhlášení obsahuje přesnou informaci o tom, kdy tak učinil).
- **Auto out** (systém odhlásil uživatele automaticky; jak může k této situaci dojít vysvětluje následující text).

Podle výše uvedených informací je po havárii systému stav posledního přihlášení uživatele k danému počítači buď „Working“ s uvedeným posledním známým časem práce nebo „In“, který má uveden pouze čas přihlášení. Systém tuto informaci rozpozná a změní

stav přihlášení na „Auto out“, tedy uživatel odhlášen systémem automaticky. Zároveň je patrné, že údaj zapsaný v centrální databázi se od skutečnosti neliší o více než velikost intervalu pro automatický zápis do centrální databáze. Toto zotavení z havárie zabraňuje možným problémům, které mohou vzniknout jako důsledek nestability systému. Navrhovaný způsob je dostatečně robustní, aby se vyrovnal s havárií operačního systému počítače a zabránil zmatečným údajům v centrální databázi.

4 Implementace programového systému

4.1 Centrální databáze

Tabulky centrální databáze je třeba před použitím vytvořit a uvést do implicitního stavu. Přílohou tohoto návrhu systému je SQL skript, který generuje všechny tabulky centrální databáze a zadává do nich potřebná data. Následující tabulky ukazují přehlednou formou obsah centrální databáze při nasazení programového systému do provozu. Centrální databáze se tedy skládá ze 4 níže uvedených tabulek.

Uzivatel			
CisloUziv	**Jmeno**	**Heslo**	**Smazan**
1	Admin	šifra(password)	

Stav	
IDStavu	**Nazev**
I	In
O	Out
W	Working
A	Auto out

Prostredi		
Klic	**HesloAdmin**	**Interval**
1	šifra(password)	300

Protokol
tabulka je prázdná

Obr. 2: Stav databáze při nasazení systému do provozu

Centrální databáze je implementována na platformě Paradox 7 s použitím české znakové sady Paradox Czech 852, která je potřebná pro správné abecední řazení a korektní zobrazování znaků s diakritikou. Před uvedením programového systému do provozu je doporučeno použít tyto vygenerované tabulky, které jsou součástí tohoto návrhu systému. Nabízí se zde i možnost využít skriptu, zde však hrozí nebezpeční nesprávné interpretace databázovým strojem. Jako databázový stroj byl použit Borland Database Engine ve verzi 5.01, který se z pohledu nároků na provoz systému jeví jako vhodnější než Microsoft ADO.

4.2 Klient, konfigurační aplikace

Součástí návrhu jsou zdrojové kódy vlastní realizace navrhnutého systému obou součástí programového systému stejně jako spustitelné soubory. Obě součásti, tedy „Klient pro přihlášení uživatele do systému MS-Windows 9x“ a „Konfigurační aplikace klienta a centrální databáze“ byly vytvořeny přesně podle navrhnuté specifikace ve vývojovém prostředí Borland Delphi 6. Požadované funkce pracují spolehlivě na počítači s operačním systémem Windows 98 nebo Windows 98 SE. Následující kapitola již představuje vytvořený programový systém z pohledu uživatele a z pohledu administrátora.

5 Programový systém z pohledu uživatele

Uživatelé tohoto programového systému se setkají pouze s jediným aplikačním oknem, které zahrnuje všechny jim dostupné funkce. Toto aplikační rozhraní vyžaduje zadání uživatelského jména a hesla, po přihlášení uživatele se aplikační okno skryje a umožní uživateli pracovat s počítačem. Na pokyn uživatele se okno obnoví, informuje uživatele o času přihlášení a celkové době jeho práce, nabídne mu možnost se odhlásit, případně vypnout počítač (pokud je uživatel přihlášen, systém jej automaticky odhlásí a poté vypne počítač). Zde se bohužel setkáváme s aplikačním omezením daným operačním systémem. Uživatelé by měli vypínat počítač pouze pomocí rozhraní programového systému a přestat používat standardní vypnutí přes nabídku „Start“. Zakázat zobrazování této funkce v nabídce „Start“ pravděpodobně není možné. Následující obrázek ukazuje aplikační rozhraní klienta pro přihlášení uživatele do MS-Windows 9x v situaci, kdy uživatel není přihlášen.

Obr. 3: Aplikační okno klienta pro přihlášení v situaci kdy čeká na přihlášení uživatele

Pokud není žádný uživatel přihlášen, jsou k dispozici pouze dvě funkce: „Přihlásit“ a „Vypnout PC“. Pokud uživatel zvolí přihlásit, provede systém ověření jeho identity, pokud zadaná dvojice „Uživatelské jméno“, „Heslo“ není platná, uživatele o této skutečnosti informuje a přihlášení odmítne. V opačném případě aktualizuje informace o přihlášeném uživateli, provede záznam do centrální databáze a minimalizuje se. Funkce „Vypnout PC“, která je k dispozici vždy provede okamžité vypnutí počítače. Při vyvolání této funkce klient ověřuje, zda v poli „Heslo“ není zadáno platné heslo pro plný přístup. Pokud ano, provede místo vypnutí počítače ukončení sebe sama. Tuto funkci může využít administrátor systému. Následující obrázek aplikačního okna zachycuje situaci, kdy je uživatel přihlášen.

Obr. 4: Aplikační okno klienta pro přihlášení v situaci kdy je uživatel přihlášen

Systém zobrazuje jméno aktuálně přihlášeného uživatele, dále pak datum a čas kdy se k počítači přihlásil (jméno počítače je zobrazeno v titulku okna) a počítá jak dlouho již přihlášený uživatel se systémem pracuje (celkový počet hodin, minut a sekund). Pokud by uživatel změnil datum nebo čas v počítači, tato hodnota nebude ovlivněna, protože systém si udržuje informaci o datu a čase sám, na operační systém nespoléhá. Funkce „Přihlásit“ v tuto chvíli není k dispozici, což je logické, uživatel je již přihlášen. Funkce „Odhlásit“ uvede klienta do původního stavu (čeká na přihlášení), zapíše informaci o odhlášení do centrální databáze a zablokuje možnost počítač používat. Funkce „Minimalizovat“ provede skrytí (minimalizaci) klienta na lištu spuštěných programů, funkce „Úplně skrýt“ provede skrytí klienta do oznamovací oblasti (vedle zobrazeného času na liště spuštěných programů). Obě tyto funkce jsou přístupné pouze v situaci, kdy je nějaký uživatel přihlášen.

6 Programový systém z pohledu administrátora

6.1 Instalace systému na klientské počítače

Instalace programového systému na počítače se systémem MS-Windows 9x, kde je vyžadována autorizace uživatele probíhá ve dvou krocích. Nejprve je třeba nainstalovat přiložený BDE (Borland Database Engine). Instalace BDE proběhne automaticky na systémový disk do složky „Program Files\Commnon Files“. Žádná konfigurace BDE není třeba, prostou instalací je vše hotovo. Druhý krok zahrnuje nakopírování spustitelného souboru přihlašovací aplikace a konfiguračního souboru s údajem o umístění centrální databáze. Pokud nebude konfigurační soubor k dispozici nebo v zadaném umístění nebude uložena platná centrální databáze, bude klient práci s počítačem blokovat. Jako poslední krok je třeba zajistit spuštění klienta ihned po zavedení operačního systému. Složka „Po spuštění“ není vhodná, uživatelé s ní mohou snadno manipulovat. Jako vhodné se jeví umístění záznamu do registru systému, které spuštění po zavedení operačního systému zajistí.

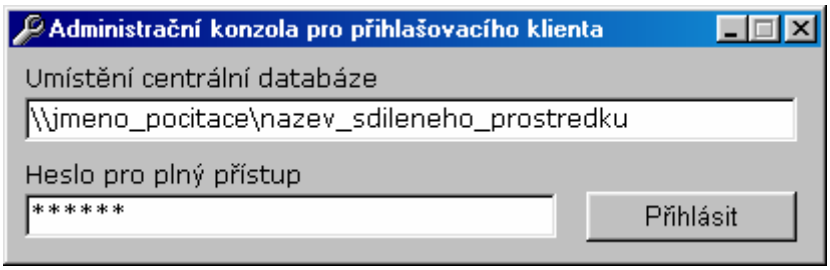
6.2 Instalace administrační aplikace

Administrační aplikaci lze používat na libovolné počítači, který je zapojen do sítě a zároveň má k dispozici BDE. Jak nainstalovat databázové jádro BDE na počítač je popsáno v bodě 6.1. Postup i databázové jádro je stejné. Administrační aplikace se skládá z jediného spustitelného souboru a konfiguračního souboru s údajem o umístění centrální databáze. Tento konfigurační soubor je stejný jako ten, používaný na klientských počítačích. Pokud tento konfigurační soubor není k dispozici, nabídne administrační aplikace možnost zadat umístění centrální databáze ručně. Taková situace nastane právě při zavádění tohoto programového systému do provozu. Administrační aplikace poté umožní vygenerovat příslušní konfigurační soubor k dalšímu použití.

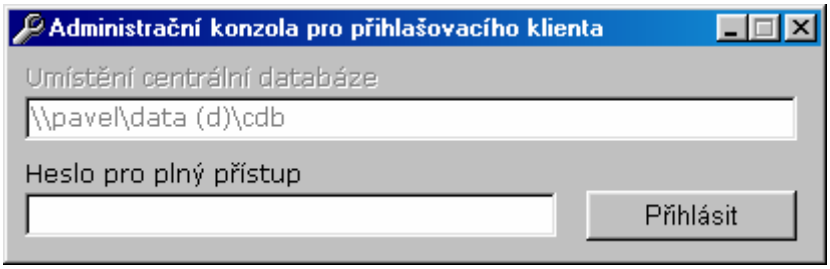
Administrátor systému by měl dbát na bezpečnost a dodržovat všechny zásady uvedené v kapitole 3. Především je třeba upozornit na nutnost použití skryté sdílené složky a uschování administrační aplikace. Dále je třeba dbát na volbu přidělovaných hesel. Hesla by měla být dlouhá alespoň 6 znaků (u hesla pro plný přístup je 6 znaků striktně vyžadováno jako minimum) a měla by obsahovat i jiné znaky než písmena abecedy. S výhodou lze využít oddělovačů a jiných nestandardních znaků, systém neklade na použité znaky žádná omezení. V další části této kapitoly jsou podrobně rozebrány všechny funkce, které administrační aplikace nabízí. Zároveň tato část upřesněná a doplněná pravidla, která byla formulována v rámci návrhu programového systému v kapitole 3. Znalost těchto pravidel je nutnou podmínkou zvládnutí nasazení programového systému „Klient pro přihlášení uživatele do MS-Windows 9x“.

6.3 Popis administrační aplikace

Po spuštění administrační aplikace je uživatel dotázán na umístění centrální databáze (v případě, že ještě není vytvořen konfigurační soubor) a heslo pro plný přístup. Jakmile je konfigurační soubor s údajem o umístění centrální databáze administrační aplikaci k dispozici, načte jej z tohoto konfiguračního souboru a nedovolí uživateli tento údaj zadat (toto chování lze změnit spuštěním administrační aplikace s parametrem „-zadej“, pak bude existence konfiguračního souboru ignorována). Následující dvojice obrázků ukazuje přihlášení do konfigurační aplikace v případě kdy konfigurační soubor neexistuje a v případě kdy je již vytvořen.



Obr. 5: Přihlášení do administrační aplikace, když není k dispozici konfigurační soubor

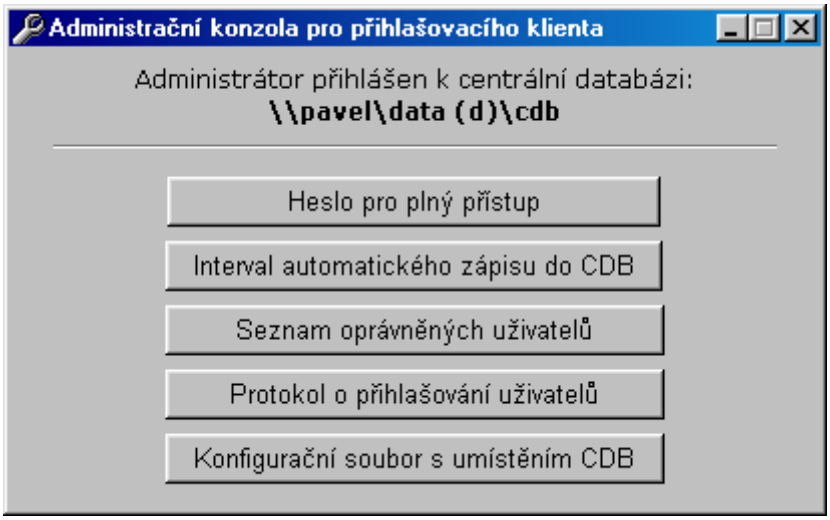


Obr. 6: Přihlášení do administrační aplikace, pokud je k dispozici konfigurační soubor

První obrázek také ukazuje jakým způsobem zadat informaci o centrální databázi. Jedná se o standardní síťovou cestu v operačních systémem Microsoft Windows. Pokus o přihlášení může skončit třemi způsoby.

- Uživatel korektně je přihlášen,
- zobrazení chybového hlášení „Zadané umístění neobsahuje platnou centrální databázi“ (v zadané síťové cestě nebyly nalezeny příslušné databázové tabulky),
- zobrazení chybového hlášení „Heslo pro plný přístup není platné“ (v zadané síťové cestě se nachází platná centrální databáze, ale zadané heslo není správné).

Jakmile je uživatel přihlášen, má k dispozici všechny požadované funkce zmiňované v kapitole 3, která se zabývá rozborem požadavků a návrhem tohoto programového systému. Jedná se o změnu hesla pro plný přístup, změnu intervalu automatického zápisu do centrální databáze, úpravu seznamu uživatelů, kteří mají právo se přihlašovat k počítačům a možnost vygenerování šifrovaného konfiguračního souboru s údajem o umístění centrální databáze. Uživatel má dále k dispozici možnost prohlížet záznamy v protokolu o přihlašování uživatelů k jednotlivým počítačům. Následující obrázek ukazuje uspořádání výše zmiňovaných funkcí v okně administrační aplikace. Funkce úprava seznamu uživatelů je realizována prostřednictvím samotného okna stejně jako výpis protokolu o přihlašování.



Obr. 7: Dostupné funkce v okně administrační aplikace

Funkce „Heslo pro plný přístup“ umožní administrátorovi změnit heslo pro plný přístup. Systém kontroluje minimální požadovanou délku (6 znaků), pokud je zadané heslo kratší, změna není povolena.

Funkce „Interval automatického zápisu do CDB“ umožní uživateli změnit velikost intervalu kdy klient zapisuje do centrální databáze informaci o práci přihlášeného uživatele. Po vyvolání této funkce je administrátorovi k dispozici informace o aktuální velikosti tohoto intervalu. Systém kontroluje zadanou velikost (minimálně 15 sekund, maximálně 900 sekund) a pokud zadaná hodnota nesplňuje podmínky, změna není povolena.

Funkce „Konfigurační soubor s umístěním CDB“ vygeneruje nový konfigurační soubor s údajem o umístění centrální databáze (název tohoto souboru je „cdblogin.dat“). Pokud již soubor existuje, systém na tuto skutečnost upozorní, a nabídne možnost jej přepsat.

Funkcím „Seznam oprávněných uživatelů“ a „Protokol o přihlašování uživatelů“ jsou věnovány dvě následující samostatné části této kapitoly.

6.4 Úprava seznamu oprávněných uživatelů

Po vyvolání funkce „Seznam oprávněných uživatelů“ je otevřeno okno se seznamem všech uživatelů a s funkcemi pro úpravy tohoto seznamu.

Obr. 8: Okno funkce „Seznam oprávněných uživatelů“

Uživatelé v seznamu jsou seřazeni abecedně, neaktivní (smazaní) uživatelé jsou na konci tohoto seznamu a mají nastaven atribut „Smazán“ na „A“. Uživatelé, kteří již figurují v protokolu o přihlašování uživatelů nemohou být z tabulky odstraněni, proto jsou funkcí „Smaž uživatele“ pouze označeni jako neaktivní a nemohou se přihlásit. Pomocí funkce „Obnov uživatele“ je možné neaktivního uživatele opět obnovit do stavu kdy se bude moci přihlásit (atribut smazán bude nastaven na prázdnou hodnotu).

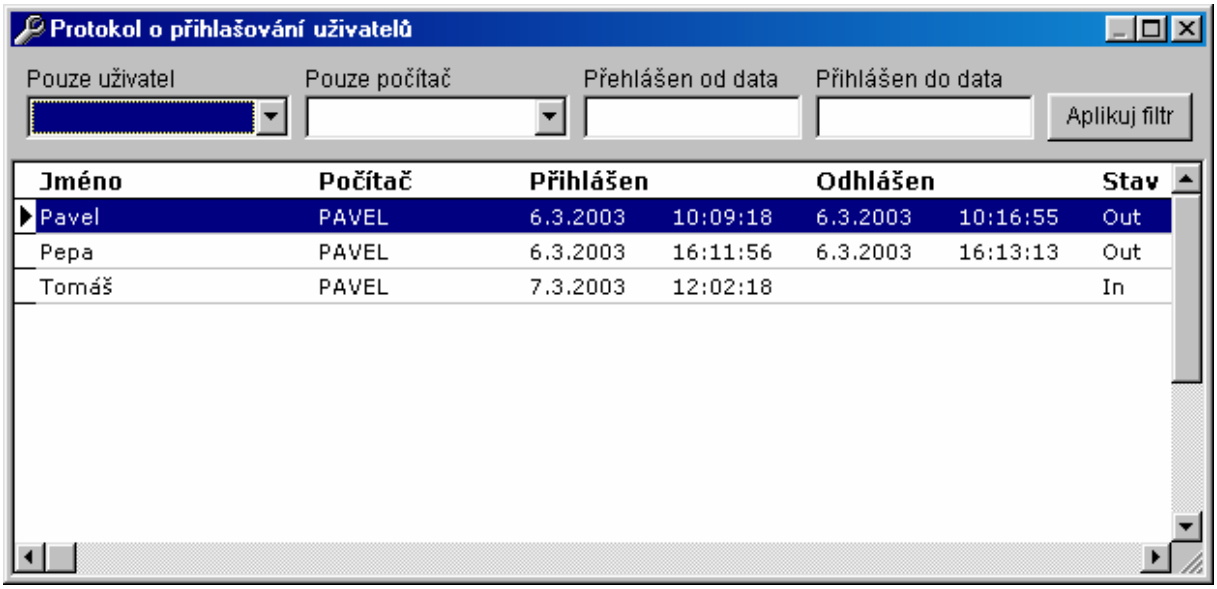
Funkce „Přidej uživatele“ se dotáže po řadě na uživatelské jméno a heslo. Pokud je některý z těchto atributů prázdný, nebude uživatel do systému přidán. Dále systém kontroluje možnou duplicitu a pokud již uživatel se zadaným jménem existuje, rovněž nebude do systému přidán (systém na tuto skutečnost upozorní hlášením). Systém rozlišuje velká a malá písmena u jmen uživatelů.

Funkce „Změň jméno“ a „Změň heslo“ umožní úpravu uživatelského jména (hesla) vybraného uživatele. Opět platí, že systém kontroluje platnost zadaných údajů a pokud dojde k rozporu s výše uvedenými pravidly, nebude změna provedena.

Funkce „Zavřít“ ukončí práci se seznamem uživatelů a vrátí se do hlavního okna administrační aplikace systému.

6.6 Výpis protokolu o přihlašování uživatelů

Administrační aplikace umožňuje správci systému prohledávat protokol o přihlašování uživatelů. Přehlednou formou vypisuje všechny údaje zapsané v databázi a nabízí možnost filtrování vypisovaných dat. Jak vypadá výpis protokolu a jaké filtrovací možnosti tento výpis nabízí je ukázáno na následujícím obrázku.



Obr. 9: Výpis protokolu o přihlašování uživatelů a nabízené možnosti filtrování

V protokolu jsou zobrazeny popořadě následující údaje: jméno uživatele, jméno počítače (na který se uživatel přihlásil), datum a čas přihlášení, datum a čas odhlášení nebo posledního známého okamžiku, kdy uživatel ještě s počítačem pracoval a stav tohoto přihlášení. Význam všech stavů je důkladně vysvětlen v části 3.5 (Pokročilé zotavení z havárie). Datum a čas není vyplněn, pokud od přihlášení uživatele k počítači, neuplynulo ani tolik sekund jaká je velikost intervalu pro automatický zápis do centrální databáze.

Požadovaný výpis lze filtrovat čtyřmi různými způsoby, které lze libovolně kombinovat, požadovaný filtr je proveden po provedení funkce „Aplikuj filtr“. Filtr „Pouze uživatel“ umožňuje omezit výpis protokolu pouze na údaje o přihlašování vybraného

uživatele. Pokud je nastavena hodnota „jakýkoliv“, nebude tento filtr aktivní a budou vypsány informace o přihlašování všech uživatelů. Filtr „Počítač“ obsahuje seznam všech známých počítačů na které se lze přihlásit. Tento seznam se doplňuje dynamicky vlastním chodem systému (obsahuje všechny počítače, na které se již nějaký uživatel přihlásil). Opět nabízí možnost nastavit hodnotu na „jakýkoliv“, tedy tento filtr nepoužít. Jinak omezí výpis protokolu pouze na vybraný počítač. Filtr „Přihlášen od data“ a „Přihlášen do data“ omezí výpis na všechny záznamy, kde je datum přihlášení větší rovno (mešní rovno), zadanému datu. Zkombinováním všech filtrů lze například vypsat všechny záznamy o přihlašování uživatele „Tomáš“ k počítači „PAVEL“ za měsíc březen (mezi „1.3.2003“ a „31.3.2003“).

7 Závěr

7.1 Zhodnocení výsledků

Všechny formulované požadavky na systém „Klient pro přihlášení do MS-Windows 9x“ se podařilo splnit bez jakýchkoliv implementačních omezení. Systém vyhovuje všem formulovaným požadavkům, které byly definovány v kapitole 2 (Analýza funkcí navrhovaného programového systému) a dává k dispozici menším organizacím s počítači s MS-Windows 9x technologii umožňující sledovat využívání svých počítačů a dodržování pracovní doby. Systém nevyžaduje „odborníka“ v roli správce systému, této úlohy se může zhostit každý středně zkušený uživatel systémů MS-Windows. Dosažená úroveň zabezpečení a nároky na systémové zdroje plně dostačují zvažovaném účelu programového systému.

7.2 Možnosti modifikace a využití

Systém byl od počátku navrhován a budován jako jednoduchý, transparentní a přímočaře rozšiřitelný. Lze jej například modifikovat tak, aby při přihlášení uživatele byly provedeny libovolné operace, např. spuštění aplikací nebo skriptů. Pokud bude centrální databáze rozšířena o seznam počítačů, bude možné definovat, který uživatel se může přihlásit ke kterému počítači. Všechna tato rozšíření mohou být realizována v krátkém čase s minimálním úsilím a minimálními náklady. Teto programový systém je možné bez jakýchkoliv omezení používat na libovolné počítači s operačním systémem Microsoft Windows 98 nebo Windows 98 SE. Naproti tomu jej nelze používat na počítačích s operačním systémem s technologií NT (Windows 2000, XP), protože programový systém využívá součástí operačního systému, které nejsou na této platformě k dispozici.

Seznam použité literatury

Teixeira, S., Pacheco, X. Borland Delphi: průvodce vývojáře. Kniha IV, Win32 API, dynamicky linkované knihovny (DLL knihovny), tvorba aplikací s více thready, práce se soubory, získávání systémových informací, tvrdé jádro. 1. vyd. Brno: UNIS publishing, 1999. 288 s. ISBN80-86097-36-6.

Win 32 API - průvodce vývojáře: kompletní reference programátora pro Windows 95 a Windows NT. 1. vyd. Brno: UNIS publishing, 1997. ISBN80-86097-06-4.

Svoboda, L., Voneš, P., Konšal, T., Mareš, M. 1001 tipů a triků pro Delphi. 2. vyd. Praha: Computer Press, 2002. 309 s. ISBN80-7226-529-6.