NÁVRH AUTENTIZAČNÍHO SYSTÉMU POMOCÍ TELEFONNÍCH KARET

BAKALÁŘSKÁ PRÁCE

Petr Syrovátka

Jihočeská univerzita
Pedagogická fakulta
Katedra fyziky

České Budějovice 2006

Anotace

Tato bakalářská práce navrhuje a řeší autentifikační systém pro vstupní koridor ZŠ J. Š. Baara, pracoviště Nová ulice v Českých Budějovicích. Jako autentifikačního média bylo využito čipových karet. Práce obsahuje popis dostupných řešení, rozbor použitých technologií a v konečné fázi dokumentační projekt k realizovanému systému, který byl ve zmíněné škole uveden v činnost. K řešení bylo použito běžně dostupných prostředků, aby realizace nezatížila školní rozpočet. Všechny použité nástroje vycházely z modelu Open Source Licence, použita byla zejména platforma Linux.

Prohlášení

Prohlašuji, že jsem vypracoval bakalářskou práci samostatně a že jsem uvedl veškerou použitou literaturu, zdroje a citace v textu.

Petr Syrovátka

Poděkování

Děkuji za podporu při realizaci projektu Ing. Tomáši Šimkovi z firmy CCS international za podporu při programování ovládacího software a konfiguraci serveru a Mgr. Petře Mikové za jazykové korektury.

Obsah

Úvod

Záměr vybudování autentifikačního systému u dveří ve vstupním koridoru na ZŠ Nová ulice vznikl již před několika lety. Nezabezpečené vstupní dveře se staly postupem času velkou bezpečnostní hrozbou a vedly k nadměrnému pohybu cizích osob po budově školy a nárůstu krádeží, jejichž likvidaci následně odmítala pojišťovna.

V roce 1995 došlo k osazení vstupního koridoru zvonkem a interkomem, který měla k dispozici sekretářka a ředitelka školy. Z jejich kanceláří bylo následně možné odemknout elektromagnetický zámek a tím otevřít osobě u vstupu dveře do školy. Bohužel toto jednoduché řešení mělo několik zřejmých slabin. Jednak neexistovala vizuální kontrola nad počtem a skutečnou identitou vstupovaných osob a jednak kanceláře s koncovým zařízením interkomu jsou situovány až ve druhém patře budovy. Ke vstupu do budovy stačilo tedy uvést jakoukoliv záminku a po otevření zámku se osoba mohla pohybovat po celém areálu školy bez dalších omezení. Kontrola nad pohybem osob je dále vzhledem k rozlehlosti areálu prakticky nemožná.

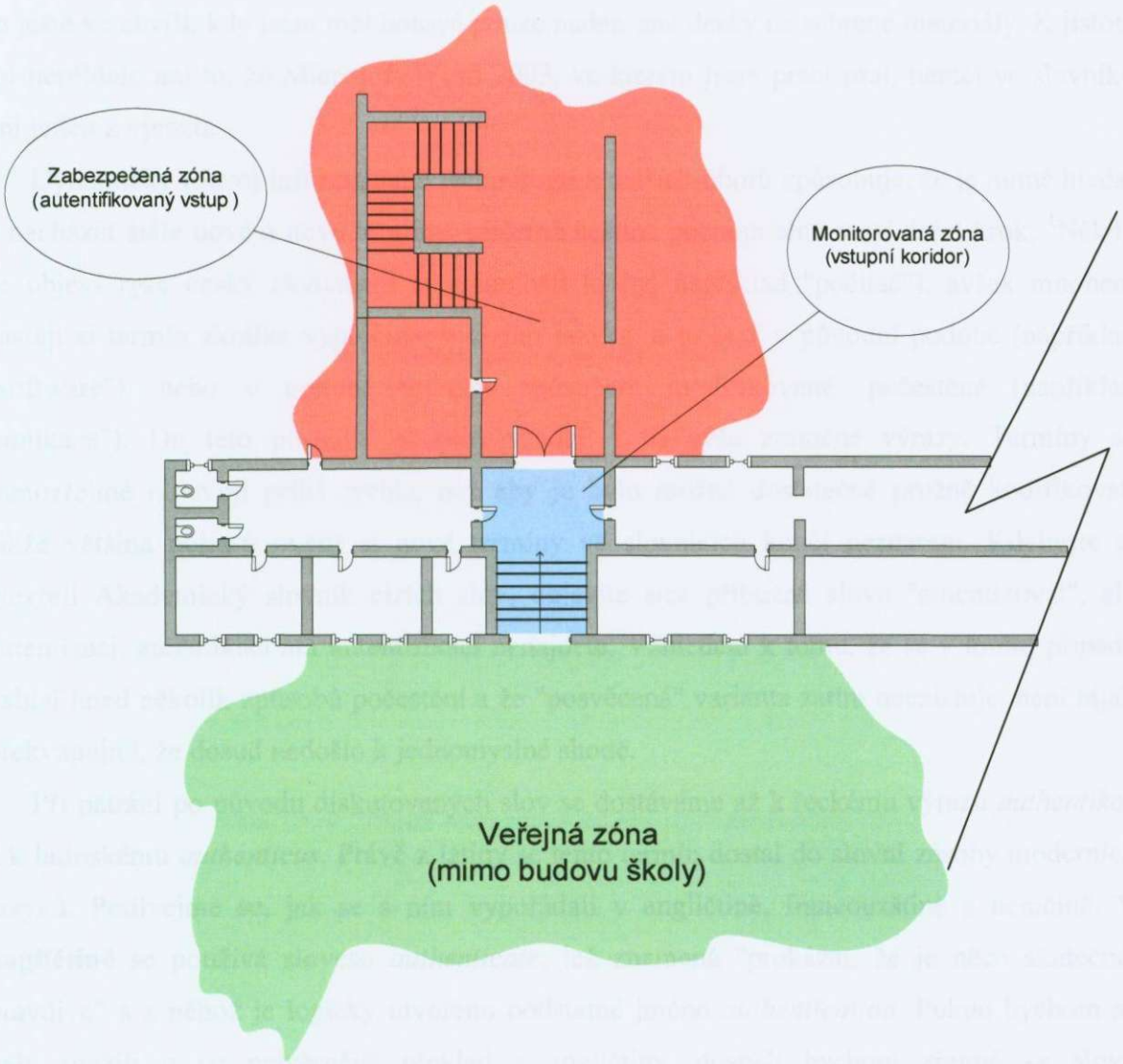
V roce 1999 se objevily na trhu první, cenově dostupné domácí videotelefony. Zdálo se, že řešení vizuální kontroly vstupujících osob je na dosah. Bohužel se zjistilo, že vzdálenost dveří vstupního koridoru a kanceláře školy (příp. kanceláře ředitele školy) je příliš velká na transport videosignálu běžným vedením. Cenová kalkulace na koaxiální vedení, případně zesílení signálu, následně oddálily realizaci projektu na neurčito. V následujících letech bylo učiněno ještě několik pokusů oslovit firmy se zabezpečovací a audiovizuální technikou s poptávkou montáže kamerového systému do prostoru vstupního koridoru, ale vždy skončily tyto snahy s poukazem na omezený rozpočet v plánu na následující rok.

V roce 2003 situaci velmi razantně změnilo několik faktorů. Škola snížila úvazek sekretářce, což mělo za následek, že od 14 hodin nebyla u již zmíněného interkomu žádná pravidelná obsluha. Škola navíc začala ve zvýšeném počtu organizovat mimoškolní aktivity formou odpoledních zájmových kroužků. Jedna z nově vybudovaných učeben výpočetní techniky byla otevřena na čtyři dny v týdnu v čase od 14 – 16:30 hodin pro všechny žáky školy, kteří mohli zcela zdarma a volně učebnu využívat. Některé prostory školní budovy byly pronajaty agentuře, která zde organizovala hudební školu.

Situace se stávala neudržitelnou. V první fázi se vstupní dveře po 14. hodině nechávaly jednoduše otevřené. To ústilo ve skutečnost, že po celé budově prakticky zmizely z chodeb všechny květiny a drobné předměty, po škole se volně pohybovaly celé skupiny osob s provozem školy vůbec nesouvisejících a bylo jen otázkou času, kdy dojde k pokusu o

vyloupení některé z uzamčených učeben a kanceláří. Ředitelství školy se pokusilo sestavit velice složitý systém otvírání vstupních dveří odpovědnými pracovníky, který trvá dodnes. Bohužel se žáci naučili vstupní dveře otevírat silou – přetlačením a povysazením elektromagnetického zámku. Ten je v současné době v dřevěných dveřích jen stěží udržován ve stavu, v jakém může představovat alespoň částečně překážku zabraňující vstupu do objektu. Chování žáků lze vysvětlit jednoduše tak, že pokud není na blízku někdo, kdo jim dveře otevře, není zároveň nablízku nikdo, kdo by je mohl postihnout za ničení vstupních dveří jejich násilným otvíráním. Vedoucí jednotlivých mimoškolních aktivit sice nadále své svěřence vpouští do prostoru školy a dveře za nimi zavírají, ale není vyřešen problém pozdních příchodů na odpolední vyučování a velkým problémem je také zpřístupnění učebny výpočetní techniky v odpoledních hodinách. Není zde totiž definováno kdy a jací žáci učebnu přijdou navštívit a není tedy možné zabezpečit někoho, kdo jim bude dveře otevírat a tím udrží školu zavřenou nežádoucím návštěvníkům.

Řešení problému vstupu do školy pouze vizuální kontrolou se tak stalo naprosto neúčinné právě vyvstalou nutností lidské obsluhy vstupního mechanizmu, která v nastalé situaci nebyla možná. Stávající systém otvírání dveří by měl být jednak v nové aplikaci doplněn o již zmíněnou vizuální kontrolu vstupních dveří a jednak o aplikaci autentifikačního systému, který na základě identifikačního média uživatele podle zadaného časového schématu vpustí do prostor školy, nebo jeho vstup zamítne, a to zcela automaticky, bez nutnosti systém dlouhodobě spravovat operátorem. Celé řešení musí pak spadat svou finanční náročností do neinvestičních nákladů školy a nezatížit operativní rozpočet školy více, než je nezbytně nutné. Po spuštění nového systému a rekonstrukci dnes již dosluhujících vstupních dveří vznikne celistvý systém řešící vstup do budovy. Celý systém byl zpracován jako bakalářská práce, jejíž nedílnou součástí je praktické provedení a uvedení aplikace do reálného provozu. V dalších částech tohoto dokumentu budou popsány jednotlivé části, jejich funkce, postup vývoje systému a v neposlední řadě problémy, na které jsem při řešení narazil, a jejich odstranění, stejně jako i možnosti rozšíření systému do budoucnosti a možností jeho dalšího využití.



Obr. 1- Orientační schéma budovy a rozdělení zón

1. Autentifikační systém

Ještě dříve, než se pokusím představit podstatu a metody autentifikačních systémů, bych se rád zastavil nad tímto termínem z hlediska etymologického. Již při hledání dostupných materiálů jsem narazil na patrné interpretační odchylky. V zásadě jsem narážel na termíny autentizační (autentizace), autentifikační (autentifikace) a autentikační (autentikace) systémy. Z kontextu jednotlivých statí pak jednoznačně vyplývalo, že se jedná vždy o „proces ověření identity uživatele". Který z termínů je správný a který je pouhým patvarem přejatého slova, se stalo jablkem sváru mezi několika pracovníky v IT, se kterými jsem svou práci konzultoval a

to ještě ve chvíli, kdy jsem měl hotové pouze nadepsané desky na sebrané materiály. K jistotě mi nepřidalo ani to, že Microsoft Word 2003, ve kterém jsem práci psal, neměl ve slovníků ani jeden z výrazů.

Dynamický rozvoj informačních technologií a dalších oborů způsobuje, že je nutné hledat a nacházet stále nové a nové termíny, přičemž čeština pochopitelně musí držet krok. [1]Někdy se objeví ryze český ekvivalent (v minulosti to byl například "počítač"), avšak mnohem častěji si termín zkrátka vypůjčíme z cizího jazyka, a to buď v původní podobě (například "software"), nebo v podobě určitým způsobem modifikované, počeštěné (například "aplikace"). Do této poslední skupiny spadají i tři výše zmíněné výrazy. Termíny se samozřejmě objevují příliš rychle, než aby je bylo možné dostatečně pružně kodifikovat, takže většina pokusů ověřit si nové termíny ve slovnících končí nezdarem. Kdybyste si otevřeli Akademický slovník cizích slov, objevíte sice příbuzné slovo "autentizovat", ale autentizaci, autentikaci ani autentifikaci nenajdete. Vzhledem k tomu, že se v tomto případě nabízí hned několik způsobů počeštění a že "posvěcená" varianta zatím neexistuje, není nijak překvapující, že dosud nedošlo k jednomyslné shodě.

Při pátrání po původu diskutovaných slov se dostáváme až k řeckému výrazu *authentikos* a k latinskému *authenticus*. Právě z latiny se tento termín dostal do slovní zásoby moderních jazyků. Podívejme se, jak se s ním vypořádali v angličtině, francouzštině a němčině. V **angličtině** se používá sloveso *authenticate*, jež znamená "prokázat, že je něco skutečné, pravdivé" a z něhož je logicky utvořeno podstatné jméno *authentication*. Pokud bychom se tedy snažili o co nejvěrnější překlad z angličtiny, dospěli bychom zřejmě ke slovu **autentikace**, přičemž bychom využili stejný mechanismus jako například u slova *communication* (komunikace). Ve **francouzštině** se zase důsledně používá slovo *authentification*, které je ekvivalentem anglického *authentication* a je utvořeno ze slovesa *authentifier*. Kdybychom tedy hledali cizokrajnou oporu pro slovo **autentifikace**, najdeme ho právě ve francouzštině. Zbývá nám ještě **němčina**. Zde najdeme dokonce dvě varianty - *die Authentifizierung* a *die Authentisierung*. Přestože první varianta má v počtu výskytů na německých webech navrch, běžně se používají obě dvě, přičemž právě termín *die Authentisierung* by mohl být inspirací pro český výraz **autentizace**.

Kořen všech výrazů je stejný. Není možné některý z nich vyloučit ani při posuzování jejich přípon, neboť u všech narážíme na přípony, které se běžně vyskytují i u jiných počeštěných výrazů (- **zace** - absolutizace, aklimatizace; **-fikace** - diskvalifikace, falzifikace; - **kace** - implikace, indikace). Slova jsou všechna bez problémů schopna přizpůsobení

[1] *Autentizace, autentikace nebo autentifikace?* [online]. 2004 [cit. 2005-06-20]. Dostupný z WWW: <http://interval.cz/clanek.asp?article=3680>.

specifikům českého jazyka (je možné je skloňovat podle určitého vzoru, můžeme ze slovesa vytvořit podstatné jméno a naopak...). Z tohoto pohledu bych si dovolil tvrdit, že se jedná o synonyma a mnou používaný termín autentifikační systém je naprosto platnou reprezentací procesu ověření identity uživatele.

2. Autentifikace vs. Identifikace

Pojmy identifikace a autentifikace jsou velice často v teoretických pramenech považovány za synonyma. Z hlediska praktického tomu tak ale není. Slovem identifikace označujeme prosté přiřazení určité, byť jen domnělé identity, zatímco autentifikací rozumíme bezpečné ověření jedinečného subjektu. Pro popis fází těchto postupů zavedu jednoduchý model terminálu, který je přístupný oprávněným osobám a každé z nich umožňuje přístup k osobní složce. Identifikace tak probíhá na základě prohlášení: „Já jsem Franta Horáček", což může prohlásit prakticky kdokoliv a význam tohoto kroku je čistě inženýrský. Proces autentifikace ovšem vyžaduje sofistikovanější přístup. Relace zasílání autentifikační komunikace mezi systémem (S) a uživatelem (U) bude reprezentovat obvyklá symbolika *zdroj → cíl: zpráva.*

Obecný scénář popisovaného schématu se tak odvíjí ve třech krocích:

1) U → S: iD_U
2) S → U: výzva
3) U → S: odpověď

Na základě identifikátoru iDU zaslaného v prvním kroku uživatelem vyhledá systém přihlašovací informace a rozhodne mimo jiné, jakým způsobem sestaví výzvu pro druhý krok. Na tuto výzvu uživatel reaguje zadáním příslušné odpovědi, kterou zašle systému k ověření. Pokud ověření dopadne kladně, je uživateli přiznána identita iDU, v opačném případě protokol končí chybovým stavem. Občas se ještě zavádí následná fáze autorizace, ve které se rozhodne o přidělení sady oprávnění v rámci systému. Autorizace může být závislá na dalších vstupních faktorech, například čas t, ve kterém uživatel o autentifikaci požádal, nebo výstup z databáze služeb a směn, případně rozvrhu kompetencí v čase proměnlivých. Je třeba zdůraznit, že v případě autentifikace pomocí nějakého média, například čipové karty, se nejedná o autentifikaci (tedy bezpečné určení identity subjektu) osoby tímto médiem se

prokazující, ale o autentifikaci použitého média. Vzhledem k tomu, že je v těchto případech dost náročné vytvořit duplikát identifikačního média, je třeba zabezpečit ještě bezpečnostní mezeru vznikající v případě jeho ztráty. Přes výše popisovaná rizika je autentifikace pomocí nejrůznějších médií rozšířená a pro většinu aplikací dostatečná.

3. Autentifikační metody

Masivní a všeobecně rozšířená autentifikace pomocí elektronického média dala vzniknout celému odvětví elektrotechnického průmyslu, které se touto problematikou zabývá. Každý člověk dnes u sebe nosí i několik různých autentifikačních médií, která mu slouží ke zpřístupnění služeb tak běžných, jako je výdej oběda nebo výběr peněžní hotovosti. V této kapitole se pokusím nastínit princip funkce nejrozšířenějších autentifikačních médií naší doby.

3.1. Čipové karty

Objevují se v našem životě stále častěji a mnoho lidských činností je s čipovými kartami nerozlučně spjato (například použití telefonních automatů, bankomatů atd.). Nepochybně pro jejich využití hovoří i cenová dostupnost těchto médií. [2]Čipové karty jsou plastové destičky o velikosti 85.6 x 54.0 x 0.76 mm, do nichž jsou zaintegrovány čipy. Tyto karty vynalezl v roce 1974 Rolland Moreno a od té doby se rozšířily po celém světě a úspěšně tak nahrazují méně bezpečné magnetické karty. Nejvíce se jich používá v mobilních telefonech, dále se čipové karty používají při placení za telefonní služby, v bankovnictví, pro dekodéry videosignálu a v řadě dalších aplikací. Čipové karty lze dělit podle několika různých hledisek.

- podle funkce, respektive použití karty, na paměťové (kde převažuje funkce uchovaní informace) a ostatní (většinou "chytřejší"). U tohoto hlediska je pozice pomyslné dělící čáry nejméně jednoznačná, protože většina moderních paměťových karet používá nějaký autentifikační protokol.
- podle způsobu komunikace s kartou na synchronní (např. stará česká telefonní karta) a asynchronní (většina "chytřejších" karet, například už zmíněné SIM karty).

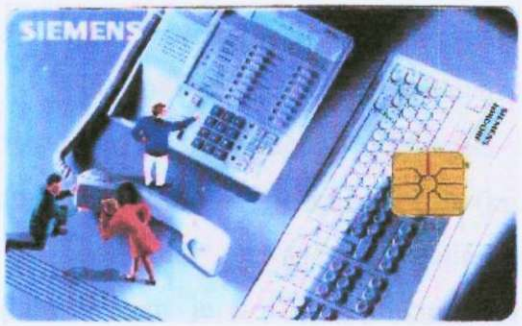
[2] *Přístupový identifikační systém* [online]. 1998 [cit. 2005-03-22]. Dostupný z WWW: <http://www.mujweb.cz/www/frenky/projekt.htm>.

- podle konkrétního komunikačního protokolu. Zvláště u čistě paměťových karet můžeme nalézt komunikaci pomocí "sběrnic" známých z oblasti jednočipových mikropočítačů. Takto je lze rozdělit na I2C (tato sběrnice je někdy též označována 2 wire), SPI, MicroWire (někdy též značené 3 wire) a dále různé proprietární sběrnice.

- podle toho, zda odpovídají normě ISO 7816 - jednotlivým jejím částem. K tomu je třeba poznamenat, že všechny karty odpovídají ISO 7816-1, téměř všechny (asi 99%) ISO 7816-2 části rozmístění kontaktů a významu napájecích kontaktů, většina (kromě telefonních karet a karet do různých prodejních automatů snad všechny) zcela odpovídá ISO 7816-2 a mnohé z nich "umějí" alespoň reset a ATR podle normy ISO 7816-3. Karty plně odpovídající i normě ISO 7816-3 patří v dnešní době mezi ty "chytřejší" a používají se například jako předplatitelské karty pro dekodéry "placených" satelitních kanálů a jako už několikrát zmíněné SIM karty.

Dále můžeme čipové karty rozdělit na :

- Paměťové karty s jednoduchou zadrátovanou logikou
- Chytré karty
- Superchytré karty



Obr. 2- Ukázky čipových karet.

3.1.1. Paměťové karty s jednoduchou zadrátovanou logikou

Do této kategorie patří i karty, kde čip slouží pouze jako paměťové médium (paměťové karty - Memory Cards, karty s uloženou hodnotou - Stored-Value Memory Cards, předplatitelské karty - Prepaid Cards). Pro přístup do paměti typu EPROM nebo EEPROM se používá jednoduchá zadrátovaná logika, která je dána už při výrobě. Typickými představiteli těchto karet jsou telefonní karty. Například telefonní čipová karta SPT Telecom obsahuje 32 bytovou paměť, kde je prvních 12 B určeno pro identifikaci karty a následujících 18 B pro záznam jednotek. Vzhledem k významu telefonní karty pro realizaci projektu bakalářské práce bude její detailní popis následovat v kapitole 4.2. Výrobní cena těchto karet se pohybuje od 50 centů do 5 dolarů.

3.1.2. Chytré karty

Tímto názvem se označují převážně karty, které obsahují mikroprocesor (Microprocessor Cards) a jsou schopny provádět různé operace s daty uloženými v paměti čipové karty. Základní operační systém je v paměti typu ROM, aplikace v paměti typu EEPROM Electrically Erasable Programmable ROM; více než 1 000 000 cyklů čtení/zápis a až 10 000 možných přeprogramování). Data mohou byt uložena v pamětech typu EPROM (Electrically Programable ROM) a EEPROM, zatímco paměť typu RAM je používána pouze pro uchování mezivýsledků při výpočtech. Navíc se na kartě nachází ještě sériový I/O port, vlastní CPU a na některých kartách ještě kryptografická jednotka na ochranu dat. Vlastní CPU je 8-bitový a většinou vychází z mikroprocesorů typu 8051 a 6805. Časté je použití těchto karet jako nositelů kódovacího klíče. Pro kódování informací je výhodné, že i v případě, kdy se používá tzv. "public-key security systém" (tzn. existuji dva klíče: jeden pro zakódování - ten je

veřejný, a druhý pro rozkódování - ten zná pouze příjemce), je klíč i celý kódovací algoritmus uložen uvnitř čipu karty, takže je velice obtížně přístupný. Pro tyto účely je do klasické struktury přidán aritmetický koprocesor, který podporuje šifrovací instrukce. Typickým příkladem tohoto typu karet je čip MC68HC5SC49 firmy Motorola (krátce SC49), který má odpovídající výkon a HW podporu pro provádění "public-key" a "private-key" kryptografických operací. Za tímto účelem je do čipu přidán koprocesor zvaný MAP (Modular Arithmetic Processor). MAP obsahuje knihovny pro "secret-key" a "public-key" algoritmy, jako DES, RSA, DSS a SHA, jakož i množství matematických funkcí. SC49 obsahuje kód velikosti 13,3 KB v ROM a má k dispozici 512 B RAM. Pro uchování dat se na čipu nachází 4 KB EEPROM. U těchto karet bývají data uložena v paměti také šifrována. Výrobní cena těchto karet se pohybuje od 3 do 15 dolarů.

3.1.3. Superchytré karty

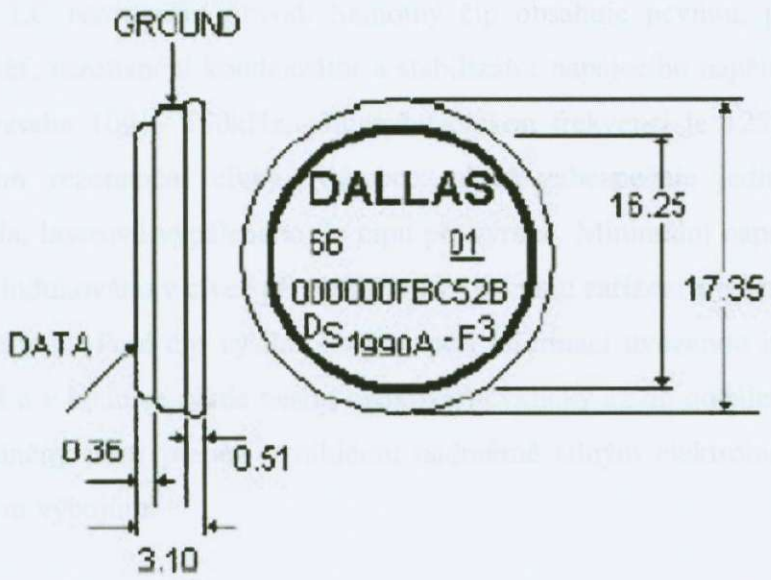
Tyto karty se poprvé objevily v roce 1988, kdy obsahovaly kromě mikroprocesoru navíc klávesnici a display. Bohužel kvůli skutečnosti, že tyto karty musely obsahovat navíc baterie, jejich tloušťka přesáhla rozměr udaný v normě ISO 7810.

3.2. Kontaktní čipy

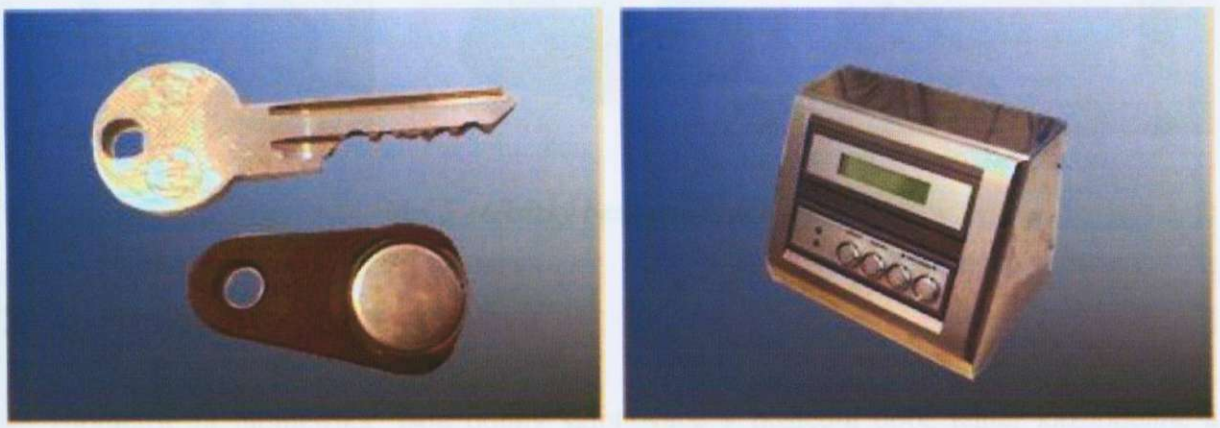
Tuto kategorii již několik let v praxi reprezentuje produktová řada iButton – unikátní čipové sady vyráběné firmou Dallas. [3]V principu se jedná, stejně jako v případě výše popsaných čipových karet, o paměti ROM (EPROM, EEPROM, ...), přičemž jsou dostupné jen s unikátním sériovým číslem. V některých verzích je paměť doplňována částí pro uživatelský zápis například pro osobní údaje majitele. V řadě výrobků iButton se nacházejí čipy s hloubkou 3 a 5 milimetrů. Produktová řada bez uživatelské paměti má 64 a 128 bitů, verze s uživatelskou pamětí disponují 128b až 64kb pro uživatelský zápis. Každý čip obsahuje originální sériové číslo, dále tak zvaný „family" kód a nezbytnou část CRC (část kontrolního součtu). Na přenos dat postačuje jeden datový vodič a jeden vodič zemnící. Pro vyhodnocení a řízení přenosu dat se používá většinou mikrokontroléru (I8051, PIC16C51...). Přenos dat nastává po úvodní inicializační sekvenci. Kontrolér po přiložení čipu ke čtecímu zařízení vyšle resetovací impulz, na který čip odpoví presentačním impulzem. Po této inicializační fázi vyšle kontrolér některý z příkazů:

[3] *Dallas iButton* [online]. 2004 [cit. 2005-09-09]. Dostupný z WWW: <http://www.maxim-ic.com/products/ibutton/>.

- **Read ROM** (přečtení celého obsahu paměti)
- **Search ROM** (Hledání informace v paměti – využívá se pro čipy s možností uložení uživatelských dat)



Obr 3 - Konstrukční schéma čipu Dallas – iButton



Obr. 4 - Kontaktní čip Dallas a čtečka docházkového systému iButton

3.3. Bezkontaktní čipy

Typickým a nejrozšířenějším reprezentantem této řady je jednoznačně výrobek firmy EM Microelectronic – čipová řada H4XXX. [4]Tyto čipy umožňují odeslání informace z jimi vybavených karet při přiblížení ke čtečce přibližně na 8 – 10 centimetrů. Jako vysílač informace se používá LC rezonanční obvod. Samotný čip obsahuje pevnou, popřípadě i programovatelnou paměť, rezonanční kondenzátor a stabilizátor napájecího napětí. Obvod je schopný operovat v rozsahu 100 – 150kHz, přičemž typickou frekvencí je 125kHz. Ta je zabezpečena připojením rezonanční cívky. Výrobce taktéž zabezpečuje jedinečnost 48 bitového sériového čísla, laserově vypáleného do čipu při výrobě. Minimální napájecí napětí je 1,5V. Toto napětí je indukováno v cívce při přiblížení ke čtecímu zařízení a je stabilizováno integrovaným stabilizátorem. Poté čip vysílá obsahovanou informaci uvozenou inicializační hlavičkou (je jedinečná a v kódu se nikde nesmí opakovat) cyklicky až do oddálení cívky od čtečky. Čipy jsou chráněny proti přepětí vzniklému nadměrně silným elektromagnetickým polem a elektrostatickým výbojům.

Obr.5 - Ukázky bezkontaktních čipů

3.4. Biometrické systémy

Biometrie či biometrika[5] jsou pojmy skloňované v poslední době téměř každodenně a snad ve všech možných i nemožných pádech. Nejčastěji tomu je zejména v souvislosti s identifikací osob při zajištění vnitřní bezpečnosti a ochrany osob, majetku či různých objektů. Biometrie je založena jak na evidentní, tak na vědecky prokázané realitě, že lidé se jeden od druhého navzájem odlišují svým vzhledem a svými projevy (jednáním a chováním). Veškeré dříve i nyní existující biometrické systémy jsou založeny na principu, že lidské

[4] *Identifikácia pomocou čipových kariet* [online]. 2001 [cit. 2005-09-15]. Dostupný z WWW: <fel.utc.sk/~nagy/BS/PDF/ID_Karty_Weber.pdf>.
[5] plk. JUDr. VANČO, Emil . *Biometrie, biometrika - geneze, vývoj a současné pojetí* [online]. [2001] [cit. 2005-09-09]. Dostupný z WWW: <www.mvcr.cz/casopisy/kriminalistika/2005/01/vanco_info.html>.

vlastnosti jsou zpravidla u každého jedinečné, a také na tom, že určité znaky člověka, jako jsou otisky prstů, hlas, tvar tváře a další, jsou po celou dobu lidské existence relativně neměnné (blíže srov. např. základní zákony daktyloskopie nebo DNA) . Na základě měřitelnosti těchto charakteristik je proto možné osoby od sebe navzájem rozeznat. Platí však také jiné pravidlo, a to že člověk se v průběhu svého života mění, a proto i zdánlivě neměnné fyziologické znaky podléhají tomuto procesu. Oblast zabývající se jedinečnými a měřitelnými charakteristikami a vlastnostmi pro rozpoznávání nebo verifikaci identity lidské bytosti je obecně nazývána biometrií. Současná biometrie se zabývá měřením a zachycením fyziologických vlastností živých bytostí. Zpravidla jde přitom o spojení nezaměnitelných znaků určitého člověka s jeho osobními daty. Nezaměnitelným znakem může být, kromě nejvíce využívaného otisku prstu, také např. oční duhovka, hlas, rozměry ruky či obličeje, podpis apod. Kontrola oprávnění přístupu na základě těchto údajů přináší podstatně vyšší úroveň bezpečnosti než doposud obvyklé prostředky, jako jsou např. různé magnetické karty, hesla nebo PIN. Časem přibyly i geometrie ruky, analýza hlasu, geometrie obličeje, sítnice, duhovky, vlastnoruční podpis, DNA, žíly na zápěstí, ale může k nim přibýt např. identifikace podle pachu, podle rýhování nehtu či otisků rtů nebo uší. Tyto systémy v různé kombinaci zvyšují bezpečnost vstupní, pohybovou, hlídací, rozhodovací atd. Tam, kde se donedávna spoléhalo na různé jiné kombinace bezpečnostních systémů, nejčastěji elektronických, založených na různých číselných kombinacích - kódech, přechází se nyní na více bezpečné a prokazatelnější prvky. Převažují-li teď systémy založené na jedné či kombinaci dvou biometrických charakteristik, je cílem vytvořit postupně komplexní systém založený na kombinaci více charakteristik. Velký problém současné biometrie je především to, že biometrické znaky nemusejí být natolik jedinečné, aby je nebylo možné obejít. To je hlavní příčina bránící jejich četnějšímu rozšíření. Podstatou všech biometrických systémů je automatizované snímání biometrických charakteristik - znaků a následně jejich porovnávání s údaji o charakteristikách osob obsažených v předem vytvořené databázi. Současné biometrické systémy využívají nejrůznější snadno rozlišitelné znaky odlišující jednoho člověka od ostatních. Biometrické technologie jsou nyní prostředkem k dosažení rychlé a uživatelsky pohodlné autentizace s poměrně vysokým stupněm přesnosti. Jejich předností je skutečnost, že ověření identity osoby nelze přenést na nikoho jiného, ukrást nebo oklamat. Všem biometrickým systémům je však společné to, že v současné době ještě neumožňují stoprocentní rozpoznání. Člověk se v průběhu života mění, a tomuto procesu podléhají i zdánlivě neměnné znaky. Při poměrně nízké hladině tolerance systému stačí i malá změna

k tomu, aby systém hlásil chybu. Z některých zkoušek současných biometrických systémů vyplývá, že míra jejich chybovosti může dosahovat až dvouciferného procentuálního podílu.

3.4.1. Verifikace otisků prstů

Je nejstarší, nejznámější a nejrozšířenější biometrický systém a dokonalý biometrický identifikační prostředek. Otisky prstů jsou nejvyužívanější způsob identifikace v kriminalistice, ale i v běžném životě, a to zejména v různých bezpečnostních systémech, bankách, bezpečnostních službách a podobně. Podstatou je především optické snímání otisků prstů.

Obr. 6 - Ukázka daktyloskopické čtečky

Tyto biometrické systémy poměrně rychle „identifikují" oprávněnou osobu na základě předem vytvořeného referenčního vzorku v databázi a umožňují jí vstup do objektu, přístup do určitých systémů nebo přístup k určitým službám. Jsou ale také poměrně zranitelné. Byly zaznamenány a publikovány úspěšné pokusy s obelstěním systému např. pomocí zvýraznění původního otisku oprávněné osoby. Mezi nevýhody těchto systémů patří také to, že drobné poranění prstu může být důvodem odmítnutí akceptace, a naopak, existuje možnost akceptace kopie prstu zhotovené ze silikonu anebo dokonce z potravinářské želatiny. Tyto nevýhody odstraňují čtečky snímající infračervený obraz daktyly. To zaručuje vyloučení neorganických napodobenin a dokonce odstraňuje rizika spojená s poraněním nebo nečistotou snímaného otisku. Infračervený obraz totiž vychází z hlubší podkožní vrstvy prstu, který těmito vlivy nebývá zasažen.

3.4.2. Geometrie obličeje

Verifikace obličeje je dnes jednou z nejvíce zkoumaných biometrických metod. Veškeré technologie vycházejí ze zjištění, že lidský obličej obsahuje cca 80 typických rysů. Ke zjištění totožnosti osoby údajně stačí rozpoznat 14 - 20 z nich. Vlastní rozpoznávání je založeno na srovnávání obrazu sejmutého kamerou s obrazem, který je uložen v centrální databázi. K „jednoznačné identifikaci" slouží většinou tvar obličeje a poloha opticky významných míst na tváři, jako jsou oči, nos, ústa či obočí. V databázi se neuchovává přesná poloha očí, nosu a rtů, ale ukládá se jen vzdálenost očí, vzdálenost rtů od nosu, úhel mezi špičkou nosu a jedním okem atd. Obličej a jeho individuální znaky jsou v podstatě jako otisky prstů. Na přesnost rozpoznávacího procesu údajně nemají vliv vousy, bradka nebo paruka, ale naopak existuje například vliv emočních stavů, morfologických změn v důsledku stárnutí nebo plastických operací. Nevýhodami verifikace obličeje jsou zatím zejména nedokonalé kamerové systémy a vliv různých faktorů na verifikaci. Z některých informací vyplývá, že k nebývalému obchodnímu boomu řady firem zabývajících se biometrickou detekcí prostřednictvím elektronických zařízení došlo na základě jejich prohlášení, že jejich software dokáže rozpoznat hledané osoby v davu snímaném kamerami. Skutečnost je však taková, že schopnost porovnat jakýkoliv sejmutý obličej s předpřipravenou databází je úžasně nízká. Tento fakt mohou u nás potvrdit i někteří pracovníci Policie ČR, pro jejichž útvary byly podobné systémy v minulosti již zakoupeny.

3.4.3. Geometrie ruky

Podstatou této starší metody je snímání ruky speciálním scannerem produkujícím 3D foto s redukcí dat do 9bytové hodnoty. Původní systémy byly založeny na jednoduchém měření délky jednotlivých prstů. Později se zdokonalilo i měření snímající tvar ruky, což znamená, že se zkoumá délka a šířka dlaně a jednotlivých prstů, boční profil ruky apod. Postupně se tato metoda vyvinula do automatizovaného snímání geometrie ruky. Současná zařízení pro „jednoznačnou identifikaci" pomocí ruky jsou založena na měření fyzikálních charakteristik ruky a prstů z hlediska třídimenzionální perspektivy. Výhodou je jednoduché použití systémů a vhodnost pro aplikace s omezenou pamětí pro ukládání dat. K nevýhodám patří např. vliv změny velikosti ruky v důsledku přibrání nebo zhubnutí nebo nevhodnost pro osoby s revmatickýma rukama.

3.4.4. Verifikace hlasu

Podstatou této biometrické metody je elektronická identifikace osoby pomocí rozšířené analýzy digitálního „otisku hlasu". Tvar hlasivek, ústní dutiny, jazyka a zubů způsobují, že rezonance vokálního traktu je u různých osob dostatečně odlišná. Některé ověřovací technologie zakládají svá autentizační rozhodnutí na analýze vět. Věta má více akustických informací než jednotlivá slova. Ta bývají krátká a neobsahují dostatečnou akustickou informaci, která by spolehlivě odlišila mluvčího. Používané věty zná pouze autentický mluvčí a mohou jimi být i množiny slov, které je mluvčí schopen vyslovit opakovaně. K nejúspěšnějším z technik pro ověřování hlasu patří porovnávání vzorků pomocí analýzy signálů řeči - spektrum. Používá se především ke vzdálenému přístupu do informačních systémů (např. prostřednictvím telefonu) . Jiným, většině lidí známým jednoduchým příkladem používání hlasové analýzy, může být takzvané vytáčení volaných hlasem u některých typů mobilních telefonů. Významnost ověřování hlasu mezi biometrickými technikami spočívá v její rychlosti, spolehlivosti a jednoduchosti použití. Nevýhodou může být za určitých okolností (nastydnutí, šum okolí, atd.) mnohem komplikovanější ověření než u jiných biometrických systémů.

3.4.5. Verifikace sítnice

Sítnice je na světlo citlivý povrch zadní strany oka. Skládá se z velkého počtu nervových buněk, které převádějí světelné paprsky na nervové signály. Jsou to tyčinky a čípky. Čípky poskytují barevné vidění, tyčinky pouze černobílé vidění. Každá tyčinka a čípek jsou spojeny s nervy, jejichž signály vystupují z oka pomocí očního nervu. Oční nerv společně s artérií sítnice vystupuje z oka v bodě, kde nejsou žádné čípky ani tyčinky; jedná se o tzv. slepou skvrnu. Pro ověření sítnice se používá obraz struktury sítnice v okolí slepé skvrny získávaný pomocí zdroje světla s nízkou intenzitou a optoelektronického systému. Tento obraz je digitalizován a převeden na vzorek délky přibližně 40 bytů. Obrazy sítnice mají stejné charakterizační vlastnosti jako např. otisky prstů. Verifikace sítnice je velice přesná biometrická metoda, ale vyžaduje, aby se uživatel díval do přesně vymezeného prostoru a měl zaostřeno na daný bod. Tento požadavek není vhodný v případě, že uživatel nosí brýle, nebo je mu nepříjemný kontakt se snímacím zařízením. Kladem ověřování pomocí sítnice je značná spolehlivost a velmi obtížná napodobitelnost.

3.4.6. Verifikace duhovky

Neexistuje jiná biometrická charakteristika člověka, která by poskytovala více rozlišovacích možností než právě duhovka. Nalezení dvou identických duhovek náhodným výběrem je mnohonásobně méně pravděpodobné než nalezení dvou identických otisků prstů. Podstata metody je založena na zákonitosti, že stejně jako např. otisky prstů nebo obraz sítnice, i duhovku oka má každý člověk jedinečnou. Verifikace duhovky se vyznačuje velmi vysokou přesností. Na rozdíl od DNA jsou duhovky dvou identických dvojčat samozřejmě rozdílné a jedinečné. I obě duhovky jednoho člověka jsou jedinečné a naprosto rozdílné.

Obr. 7 - Kamera BM-ET330 (Panasonic) pro snímání duhovky

3.4.7. Otisk DNA

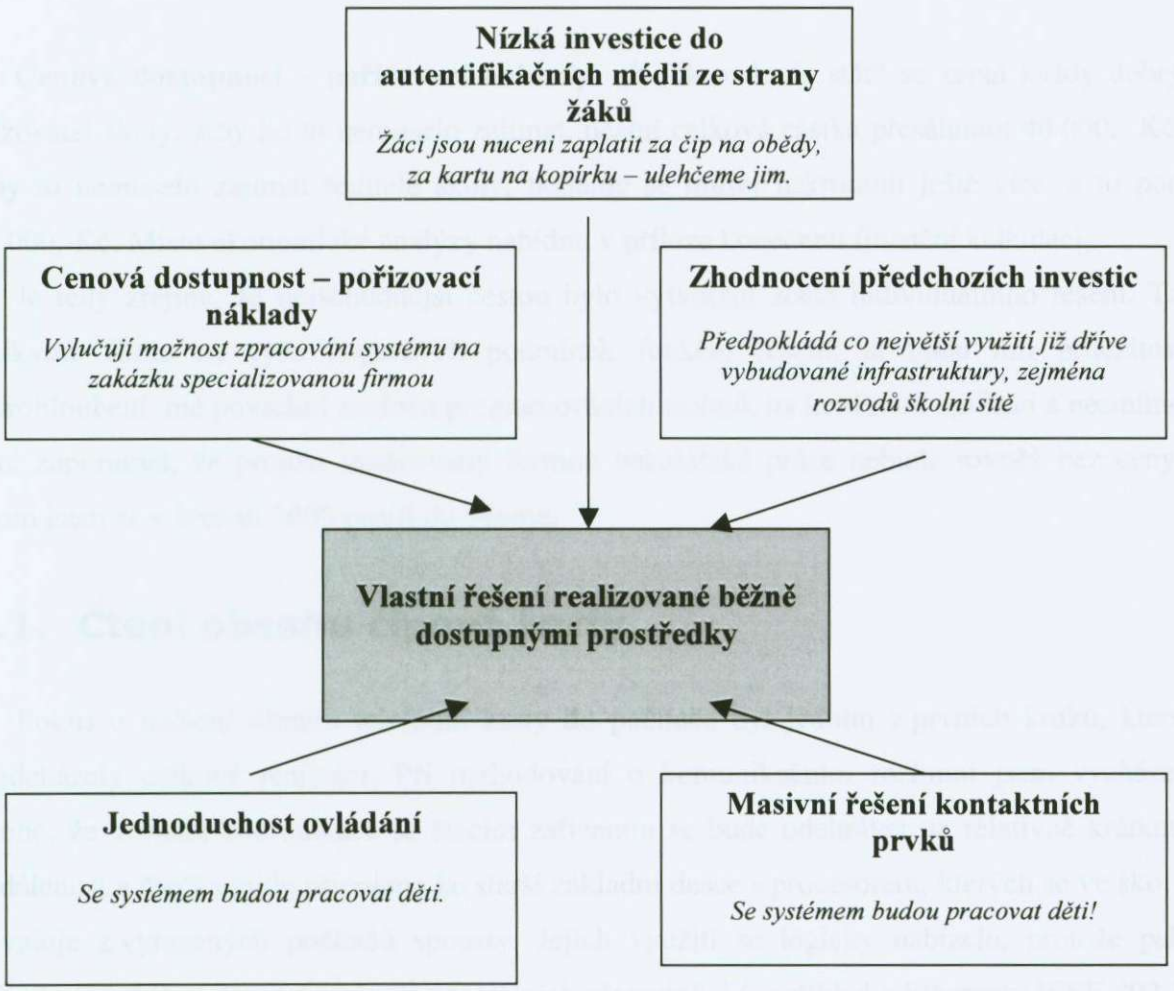
Vychází se z principu, že stejně jako má každý člověk jedinečné otisky prstů, má i jedinečný DNA otisk - přesněji řečeno genetický profil. Možnosti jeho získání jsou však mnohem širší než u otisků prstů. DNA profil se vyskytuje a je stejný v podstatě v každé buňce, tkáni a podobně. Obecně platí, že genetický profil nemůže být změněn žádnou dosud známou úpravou. Platí také to, že žádní jedinci nemají, s výjimkou geneticky identických dvojčat, shodné genetické profily. DNA metoda získává stále významnější místo v oblasti identifikace v kriminalistice a v oblasti znaleckého dokazování. Z technického hlediska je však pro masové rozšíření nedostupná.

4. Praktická realizace projektu

Vytvoření jednoduchého autentifikačního systému pro vstupní koridor základní školy v žádném případě nebylo sledováno jako pokus o převratnou novinku v oblasti autentifikační a monitorovací techniky. Z výše zpracované teoretické části vyplývá, že trh je zaplněn podobnými systémy v nejrůznějších cenových kategoriích a bylo by jistě možné využít některý z osvědčených výrobků renomovaných firem. Rovněž by pravděpodobně nebylo složité nakoupit příslušné komponenty a svépomocí z nich sestavit systém, který by víceméně odpovídal našim požadavkům. Při návrhu jsem vycházel z několika požadavků:

Nízká investice do autentifikačních médií ze strany žáků prakticky vylučuje hromadný nákup kontaktních čipů, nebo speciálních čipových karet. Jak již název bakalářské práce napovídá, zvolil jsem nakonec běžnou, všude dostupnou a levnou telefonní kartu. Vzhledem k tomu, že na škole funguje kopírka, s autentifikací na tato média (jednoduché proprietární řešení s omezenou kapacitou) mnozí žáci již takovou kartu mají a její duplicitní využití není vyloučeno.

Zhodnocení předchozích investic počítá v neposlední řadě s počítačovou sítí ve škole zbudovanou v letech 2003 – 2005, která se stále rozrůstá. Hostování vlastního webového serveru, konektivita se statickou IP adresou, server s OS Linux – Debian, to vše jsou nezanedbatelné hodnoty, které je možné efektivně využít při budování autentifikačního systému. Specializované firma by pravděpodobně prosazovala zařízení v rámci vlastní dodávky, včetně montáže vlastního instalačního rozvodu. Ta by znamenalo další, tak pracně vymýcené plastové elektroinstalační lišty po školních chodbách a samozřejmě zvýšené pořizovací náklady.



Jednoduchost ovládání není v žádném případě narážka na schopnost provozního personálu školy obsluhovat složitější systémy. Jejich pracovní náplní však není jen kontrola vstupu osob do objektu, a tak by složitost celkového systému neměla přesáhnout složitost ovládání běžné webové stránky. Zjednodušené a intuitivní ovládání nemusí nutně znamenat méněcennou aplikaci.

Masivní řešení kontaktních prvků je podmínkou k trvalé funkčnosti zařízení. Z dlouholeté zkušenosti z práce v základním školství musím konstatovat, že zařízení, ke kterému budou žáci přistupovat a přímo s ním přicházet do styku, bude vystaveno extrémní zátěži. S jakoukoliv tolerancí se nedá počítat. Očekávat se dají pokusy o fyzické poškození (škrábání, pálení, vsouvání cizích předmětů), ale i nejrůznější nápady spojené s pokusy o neautorizovaný vstup. Je třeba ovšem podotknout, že většina takových excesů je vedena spíše zvědavostí „co se s tím dá udělat a co to vydrží", než vyloženou snahou něco zničit. Každopádně bude nezbytné ke všem těmto poznatkům přihlédnout při konstrukci snímače autentifikačního média.

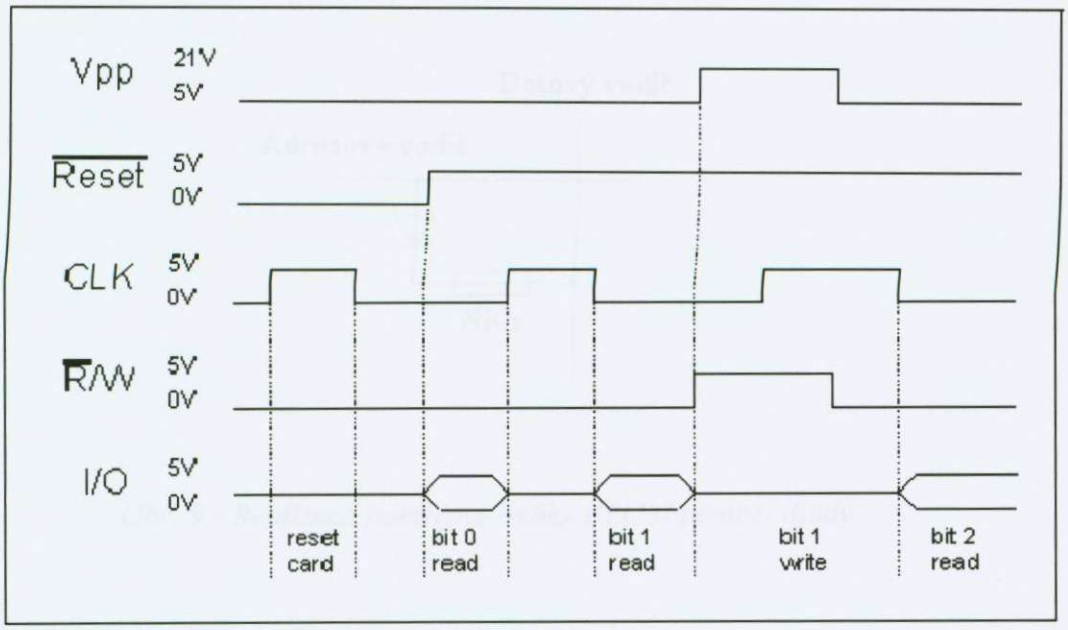
Cenová dostupnost – pořizovací náklady: „Kolik to bude stát" se zeptá každý dobrý zřizovatel školy. Aby ho to nemuselo zajímat, nesmí celková částka přesáhnout 40 000,- Kč. Aby to nemuselo zajímat ředitele školy, budeme se muset uskromnit ještě více, a to pod 10 000,-Kč. Místo ekonomické analýzy nabídnu v příloze konečnou finanční kalkulaci.

Je tedy zřejmé, že nejschůdnější cestou bylo vytvoření zcela individuálního řešení. To poskytne škole za výše popsaných podmínek funkční řešení, já budu mít příležitost k prohloubení mé povrchní znalosti programovacích technik na konkrétní aplikaci a nesmíme také zapomínat, že projekt zpracovaný formou bakalářské práce nebude rovněž bez ceny. Proto jsem se v březnu 2005 pustil do vývoje.

4.1. Čtení obsahu čipové karty

Pokus o načtení obsahu telefonní karty do počítače byl jedním z prvních kroků, které předcházely celkové realizaci. Při rozhodování o komunikačním rozhraní jsem vycházel z toho, že veškerá komunikace se čtecím zařízením se bude odehrávat na relativně krátkou vzdálenost a čtečka bude připojena ke starší základní desce s procesorem, kterých se ve škole povaluje z vyřazených počítačů spousty. Jejich využití se logicky nabízelo, protože pak nebude nutné investovat do vývoje speciálních převodníků (například z Ethernetu IEEE 802.3 na sériový protokol RS232 a podobně). V tomto případě je použití torza klasického stolního počítače nejjednodušší, nejrychlejší a pravděpodobně i nejlevnější variantou. Pro komunikaci se čtečkou jsem vybral paralelní port. Jednak se vzhledem ke struktuře komunikačních dat přímo nabízel a jednak jej (jak se záhy ukázalo) bylo možné přes čtečku připojit přímo k čipové kartě a nebylo nutné upravovat velikost napětí v logické jedničce (u IEEE 802.3 definované příjemně v 5V) a dodávaný výkon stačil na potřebnou komunikaci. Zároveň bylo možné k jednomu paralelnímu portu připojit nejen čtečku, ale i relé na přímé ovládání elektromagnetického zámku ve dveřích.

Na první pokusy jsem používal stařičký notebook 386/SX, na jehož LPT port jsem připojil konektor s telefonní kartou. Ta měla v první fázi jednotlivé vodiče napevno připojené na jednotlivé kontakty. Do notebooku jsem nainstaloval programovací jazyk Pascal 7.0, který byl pro první pokusy zcela dostatečný. Z materiálů dostupných na internetu jsem čerpal informace o průbězích komunikačního signálu na jednotlivých kontaktech telefonní karty:



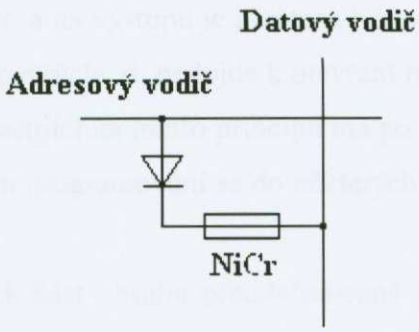
Obr. 8 - Průběh resetu, čtení a zápisu na telefonní kartě

Na základě tohoto schématu jsem byl schopen realizovat první pokusný program v jazyku Pascal, který měl ověřit možnost načtení celého obsahu karty a jeho vypsání na obrazovku. Z uvedeného schématu je patrné, že zajímavý je pro účely autentifikace karty pouze úsek resetu a čtení, který se pak bude opakovat, aniž by následoval jakýkoliv zápis na kartu. Schéma nezachycuje ještě napájecí kontakt, který je stále v logické 1, takže je paměť napájena 5V.

4.2. Popis čipové telefonní karty

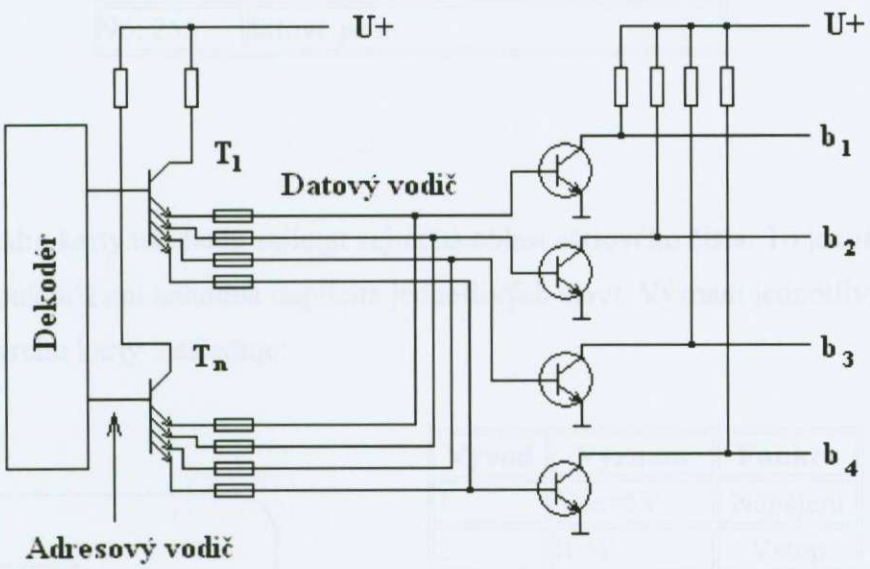
Telefonní karta je v podstatě paměť typu PROM[6] (Programable Read Only Memory). Zápis do ní samozřejmě neprobíhá v celé části, ale jen v části s počtem předplacených jednotek. Obyčejná paměť PROM neobsahuje po vyrobení žádnou pevnou informaci a je až na uživateli, aby provedl příslušný zápis informace. Tento zápis je možné provést pouze jednou a poté již paměť slouží stejně jako paměť ROM (Read Only Memory). Paměti PROM představují statické a energeticky nezávislé paměti. Buňku paměti je možné realizovat podobně jako u paměti ROM. Při výrobě je vyrobena matice obsahující spojené adresové vodiče s datovými vodiči přes polovodičovou diodu a tavnou pojistku z niklu a chromu (NiCr). Takto vyrobená paměť obsahuje na začátku samé hodnoty 1.

[6] *Vnitřní paměti* [online]. 2002 [cit. 2005-07-23]. Dostupný z WWW: <http://www.fi.muni.cz/usr/pelikan/ARCHIT/TEXTY/INTPAM.HTML>.



Obr. 9 - Realizace paměťové buňky PROM pomocí diody

Zápis informace se provádí vyšší hodnotou elektrického proudu (cca 10 mA), která způsobí přepálení tavné pojistky a tím i definitivně zápis hodnoty 0 do příslušné paměťové buňky. Paměti typu PROM se také realizují pomocí bipolárních multiemitorových tranzistorů, jak je uvedeno na následujícím obrázku.



Obr. 10 - Realizace paměťové pomocí bipolárních muliemitorových tranzistorů

Takto realizovaná paměť PROM obsahuje pro každý adresový vodič jeden multiemitorový tranzistor. Každý z těchto tranzistorů obsahuje tolik emitorů, kolik je datových vodičů. Při čtení z paměti je opět na příslušný adresový vodič přivedena hodnota logická 1, která způsobí, že tranzistor se otevře a ve směru kolektor emitor začne procházet

elektrický proud. Jestliže je tavná pojistka průchozí, procházející proud otevře tranzistor, který je zapojen jako invertor, a na výstupu je přečtena hodnota 0. Jestliže tavná pojistka byla při zápisu přepálena, tzn. je neprůchozí, nedojde k otevření tranzistoru a na výstupu je řečtena hodnota 1. Paměť PROM pracující na tomto principu má po svém vyrobení ve všech buňkách zapsánu hodnotu 0 a při jejím programování se do některých buněk přepálením tavné pojistky zapíše hodnota 1.

U telefonní karty je však část obsahu předdefinovaná již z výroby: jedná se o údaje a kódy, podle kterých je karta identifikována automatem a je s ní umožněna manipulace. Karta má informační kapacitu 256b :

Bity	Význam
0..7	kontrolní součet
8..19	831h pro telefonní karty
20..31	počet jednotek na nové kartě
32..40	kód výrobce
41..79	sériové číslo
80..87	11h
88..95	kód země (55h-Česká Republika)
96..255	bitové pole

Při načítání obsahu karty nás bude zajímat zejména oblast sériového čísla. To je totiž unikátní, a tak se nepředpokládá ani náhodná duplicita jednotlivých karet. Význam jednotlivých kontaktů na povrchu karty následuje:

Vývod	Význam	Funkce
1	Vcc=5V	Napájení
2	R/W	Vstup
3	CLK	Vstup
4	Reset	Vstup
5	Gnd=0V	Zem
6	Vpp	Vstup
7	I/O	Výstup
8	Fuse	

4.3. Program čtení obsahu karty

Jak již bylo zmíněno, první program byl napsán v jazyce Pascal 7.0 a měl pouze ověřit možnost načtení obsahu karty a jeho porovnání s deklarovanými hodnotami. Rovněž jsem měl obavu, zda nebude nutné zaváděním přesných časových konstant řídit časování výstupních a vstupních komunikačních impulzů. Tento jednoduchý pokus prokázal, že moje obavy byly zbytečné. U takto pomalého PC je komunikace bez problémů. Pozdější aplikace na rychlých počítačích však dále prokázaly, že čipové telefonní karty nepotřebují v této kategorii žádné zvláštní ohledy a zvládají bez nejmenších problémů i vyšší rychlosti komunikace.

```
Program cteckar;

uses    crt;

const   PrinterPort = $3BC;                    {Základní adresa LPT portu a deklarace
        OutPort = PrinterPort + 0;              jejích vstupních a výstupních segmentů}
        InPort = PrinterPort + 1;
        sgReset = $01;                         {Deklarace částí komunikace
        sgClock = $02;                          odpovídající konkrétnímu významu v
        sgRW    = $03;                          celkové sadě hodnot současně
        sgDefault = sgReset;                    odesílaných na výstup}
        Napajeni = $10;
        s8 = $08;

var     pocet:byte;
        vstup:byte;
        getz:byte;

procedure Send (B: byte);                      {Resetovací signál}
        begin Port[OutPort] := B end;


begin                                          {Čtení prvního bitu}
pocet := 0;

Send(sgDefault xor sgReset + Napajeni + s8);
Send(sgDefault xor sgReset xor sgClock + Napajeni + s8);

Send(sgDefault xor sgReset + Napajeni + s8);
Send(sgDefault + Napajeni + s8);


                                               {Cyklické čtení dalších bitů}
repeat

getz:= Port[Inport];


                Send(sgDefault xor sgClock + Napajeni +
s8);
                Send(sgDefault + Napajeni + s8);
```

```
write (getz);
pocet := pocet +1;

until pocet=255;

repeat

until keypressed;
end.
```

K výše popsanému kódu jsem následně - spíše ze setrvačnosti - připsal modul pro separaci sériového čísla karty (41 – 79bit), po vložení „Master" karty modul pro administraci datového souboru, do kterého bylo možné přidávat a odebírat další karty, a modul pro čtení karty a následnou autentifikaci, tedy zjištění, zda je karta přítomna v datovém souboru. V případě pozitivní autentifikace byla na volný pin výstupního portu zavedena logická 1, která následně přes tranzistor sepnula relé ovládající elektromagnetickou kotvu v zámku.

Tento systém - zcela materiálově nenáročný a jednoduchý - ale nikdy nebyl přímo realizován ve zcela funkční praxi a zůstal pouze zkušebním zařízením. V rámci školní infrastruktury by představoval autonomní zařízení bez možnosti síťové administrace, náročný na obsluhu (při prvotní autorizaci vyžadoval fyzickou přítomnost pověřené osoby s administrátorskými právy u zámku) a v neposlední řadě nesplňoval standard, který jsem si naplánoval v prvotní fázi předrealizační přípravy.

4.4. Čtečka telefonních karet

Samotné zařízení čtečky čipových telefonních karet bylo spíše záležitostí konstrukční. Samotné kontaktní zařízení neobsahuje žádnou elektroniku. Jedná se pouze o normalizovanou sadu kontaktů, ke kterým se po vsunutí přitlačí čipová karta a o ostatní se postará ovládací software. Zcela šťastnou náhodou se mi dostala do rukou nefunkční čtečka SIM karet do mobilních telefonů. SIM karty se vkládaly do šablony stejné tloušťky a velikosti, jako má naše telefonní karta. I když kontakty na SIM kartě jsou tvarově odlišné, jejich hlavní plošky naprosto přesně korespondují s kontakty na klasické telefonní kartě. Po rekonstrukci kontaktního pole, které bylo prasklé, a vyřazení obvodu, který měl význam pouze u původního účelu použití čtečky, jsem získal plastovou krabičku, která obsahovala vodící a přítlačný mechanizmus. Ten vsunutou kartu přesně navede na kontaktní pole a umožní čtení.

Bohužel již od samého začátku bylo jasné, že tato miniaturní plastová krabička, určená původně pro citlivé ruce technika, nemůže obstát v náporu několika desítek dětských uživatelů, kteří budou pravidelně zkoušet její odolnost. Při shánění vhodného kontaktního

rámce pro opravu původní čtečky jsem zjistil, že toto pole lze nahradit libovolným typem odebraným například ze starého a nefunkčního mobilu. Kontakty konektorů určených pro povrchovou montáž - například konektorů používaných v mobilních telefonech, u kterých se nepočítá s častou manipulací s kartami - jsou ale zpravidla postříbřené, narozdíl od konektorů používaných v aplikacích, které jsou mnohem náročnější na manipulaci s kartami, jako například náš autentifikační systém, tam jsou všechny kontakty zpravidla pozlacené a vývody jsou v provedení pro běžnou montáž.

Musel jsem tedy navrhnout řešení, které by křehké plastové jádro obrnilo. Zároveň jsem musel počítat se skutečností, že někdy dojde k poškození vnitřních kontaktů a ochranná konstrukce bude muset být přístupná a rozebíratelná. Ze všech pokusů, jak vestavit plastový mechanizmus s kontaktním polem do odolnějšího obalu, případně ochranné konstrukce, vyšla nejlépe myšlenka vytvoření jakéhosi brnění vysoustruženého z kovu, do kterého jsou citlivé části zavřeny. Z konstrukční oceli jsou zároveň i přední část vodící lišty, takže bude čtečka ochráněna i před pokusy o kroucení kartou ve štěrbině. Celé tělo čtečky je zasekáno do zdi a z čelní strany překryto plechovým štítkem přišroubovaným ke zdi. Celé zařízení se tak stává celkem nedobytným a bytelným řešením. V případě potřeby výměny kontaktů se odšroubuje štítek a vysune se celé jádro, které je pouze takto přístupné.

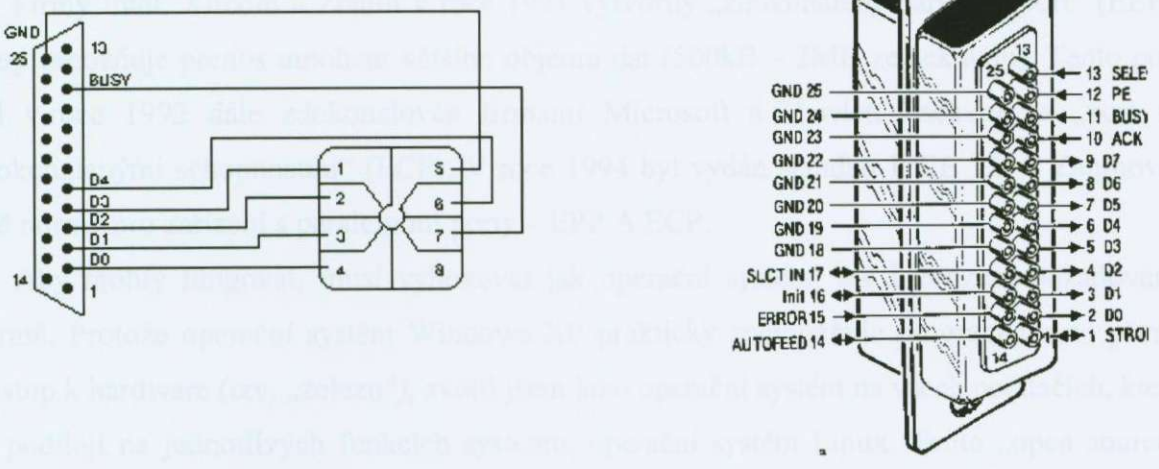
Obr.11 - Otevřené pouzdro z konstrukční oceli – uvnitř samotná čtečka

4.5. Komunikační rozhranní

Paralelní port[7] se v hojné míře používá k propojení různých periferií s počítačem (tiskárny, skenery, externí pevné disky, vyjímatelné disketové jednotky...). Využívá se zejména proto, že dokáže relativně rychle přenášet data. V dnešní době je ale nahrazován porty USB, které jsou mnohonásobně rychlejší.

sériové porty	až 115kB/sekundu
USB 1.1	až 6MB/sekundu
paralelní porty	8MB/sekundu
karta Ethernet	10MB/sekundu
rychlý Ethernet FireWire	100MB/sekundu
USB 2.0 480/sekundu	až 400MB/sekundu
propojení IDE	500MB/sekundu
grafická sběrnice AGP	až 8GB/sekundu

Paralelní porty zprvu začala vyrábět firma IBM pro propojení tiskáren od firmy Centronics, což byla nejlepší značka tiskáren té doby. Centronics v té době používala skutečně „zvláštní" kabel. Firmy IBM ho poupravila a vznikl klasický 25 pinový konektor, jak ho známe v dnešní době. Ostatní firmy ho záhy převzaly, a tak se stal hojně používaný. Když počítač posílá data do tiskárny nebo do jakéhokoliv jiného zařízení, odesílá je po 8 bitech (1 byte). Těchto 8 bitů odesílá paralelně (odtud paralelní port), narozdíl od sériového.



Obr. 12 - Popis připojení kontaktů telefonní karty k paralelnímu rozhraní (popis kontaktů telefonní karty viz. str. 25)

[7] *Paralelní port* [online]. 2002 [cit. 2005-09-10]. Dostupný z WWW: <www.soom.cz/index.php?name=usertexts/show&aid=70>.

Klasický paralelní port je schopný přenášet 50-150kilobytů za sekundu. Zde je popis každého pinu:

1. pin
   - „synchronizační signál"
   - napětí 5V, nebo 0V
   - zařízení rozpoznává, že jsou posílána data
2.-9. pin
   - 8 datových bitů
   - 5V=1
   - 0V=0
10. pin
   - potvrzení příjmu dat
11. pin
   - zařízení je zaneprázdněno (5V), klesá na 0V, počítač může vysílat další data
12. pin
   - pomocí něj tiskárna signalizuje, že došel papír (5V)
13. pin
   - jestliže zařízení vysílá 5V, je online
14. pin
   - počítač vysláním 5V vyšle signál „auto feed"
15. pin
   - - sníží-li se napětí na 0V, vyskytla se chyba
16. pin
   - - klesá-li napětí na 0V, tiskárna může tisknout
17. pin
   - - dálkové odpojení tiskárny (ofline)
18.-25. pin
   - zemnící piny

Firmy Intel, Xircom a Zenith v roce 1991 vytvořily „zdokonalený paralelní port" (EEP), který umožňuje přenos mnohem většího objemu dat (500kB – 2MB ze sekundu). Tento port byl v roce 1992 dále zdokonalován firmami Microsoft a Hewlett Packard na „port se zdokonalenými schopnostmi" (ECP). V roce 1994 byl vydán standart IEEE 1284. Zahrnoval dvě normy pro zařízení s paralelními porty – EPP A ECP.

Aby mohly fungovat, musí vyhovovat jak operační systém, tak i zařízení požadované normě. Protože operační systém Windows XP prakticky znemožňuje programátorovi přímý přístup k hardware (tzv. „železu"), zvolil jsem jako operační systém na všech počítačích, které se podílejí na jednotlivých funkcích systému, operační systém Linux. Tento „open source" operační systém již delší dobu bezchybně běží na našich školních serverech a jeho otevřená struktura přímo vybízela k použití. Vzhledem k tomu, že konečné uživatelské rozhraní a ovládací aplikace budou dostupné jako webová stránka, nebude toto řešení klást nároky na operační systém koncového uživatele a bude přístupné z libovolného operačního systému a prohlížeče.

5. Programové řešení

Back End autentifikačního systému, jak již bylo výše popsáno, převážně využívá jednoho staršího PC s nainstalovaným operačním systémem Linux Debian propojeným sítí se serverem. Na serveru je rovněž nainstalován operační systém Linux Debian. Pro řešení autentifikačního systému je podstatná instalace MySQL serveru a PHP serveru. Tyto programové balíky tvoří základní platformu, kterou je celý systém podporován a následně ovládán.

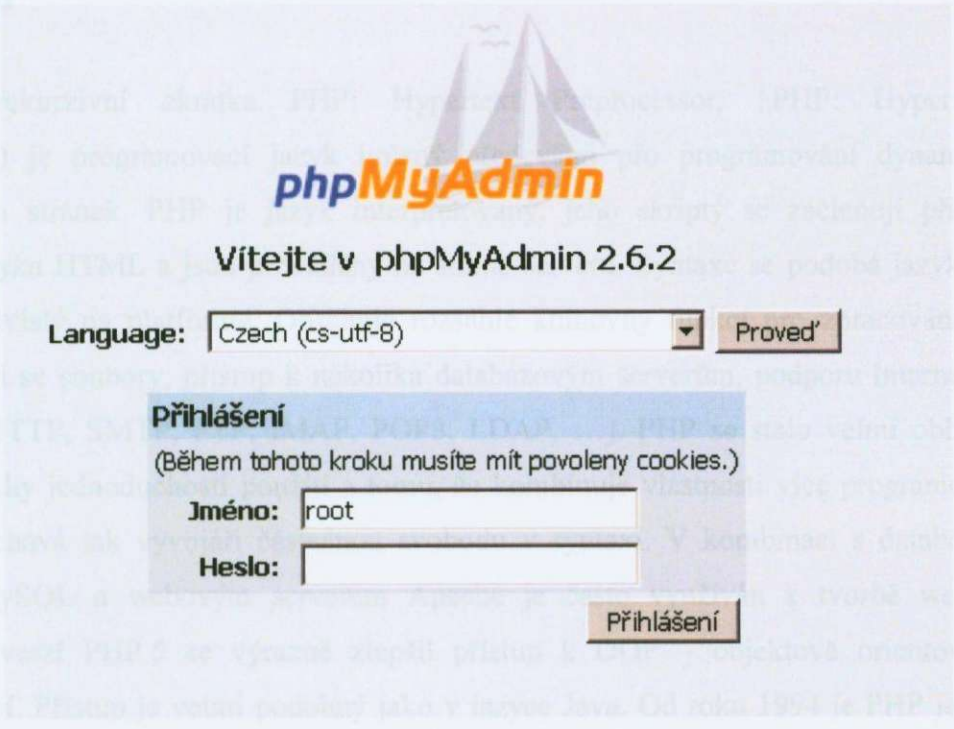
5.1. MySQL server

SQL (Structured Query Language) je jazyk pro práci s databázemi[8]. SQL je standardem pro komunikaci s databázemi typu MS Access, MySQL, Oracle atd. SQL se skládá z mnoha příkazů, které se velmi podobají klasickému jazyku - angličtině. V 70. letech 20. století probíhal ve firmě IBM výzkum relačních databází (databázový systém, který je založen na relačním modelu dat a relační algebře. Data jsou uspořádána do tabulek (relací), nad kterými jsou definovány přípustné operace). Bylo nutné vytvořit sadu příkazů pro ovládání těchto databází. Vznikl tak jazyk SEQUEL (Structured English Query Language). Cílem bylo vytvořit jazyk, ve kterém by se příkazy tvořily syntakticky co nejblíže přirozenému jazyku (angličtině). K vývoji jazyka se přidaly další firmy. V r. 1979 uvedla na trh firma Relational Software, Inc. (dnešní Oracle Corporation) svůj relační databázový systém Oracle. IBM uvedla v roce 1981 nový systém SQL/DS a v roce 1983 systém DB2. Dalšími systémy byly např. Progress, Informix a SyBase. Ve všech těchto systémech se používala varianta jazyka SEQUEL, který byl přejmenován na SQL. Relační databáze byly stále významnější a bylo nutné jejich jazyk standardizovat. Americký institut ANSI (American National Standards Institute) původně chtěl vydat jako standard zcela nový jazyk RDL. SQL se však prosadil jako de facto standard a ANSI založil nový standard na tomto jazyku. Tento standard bývá označován jako SQL-86 podle roku, kdy byl přijat. V dalších letech se ukázalo, že SQL-86 obsahuje některé nedostatky a naopak v něm nejsou obsaženy některé důležité prvky týkající se hlavně integrity databáze. V roce 1992 byl proto přijat nový standard SQL-92 (někdy se uvádí jen SQL2). Zatím nejnovějším standardem je SQL3, který reaguje na potřeby nejmodernějších databází s objektovými prvky. Standardy podporuje prakticky každá relační databáze, ale obykle nejsou implementovány vždy všechny požadavky normy. A naopak,

[8] *SQL* [online]. 2004 [cit. 2005-09-15]. Dostupný z WWW: <cs.wikipedia.org/wiki/SQL>.

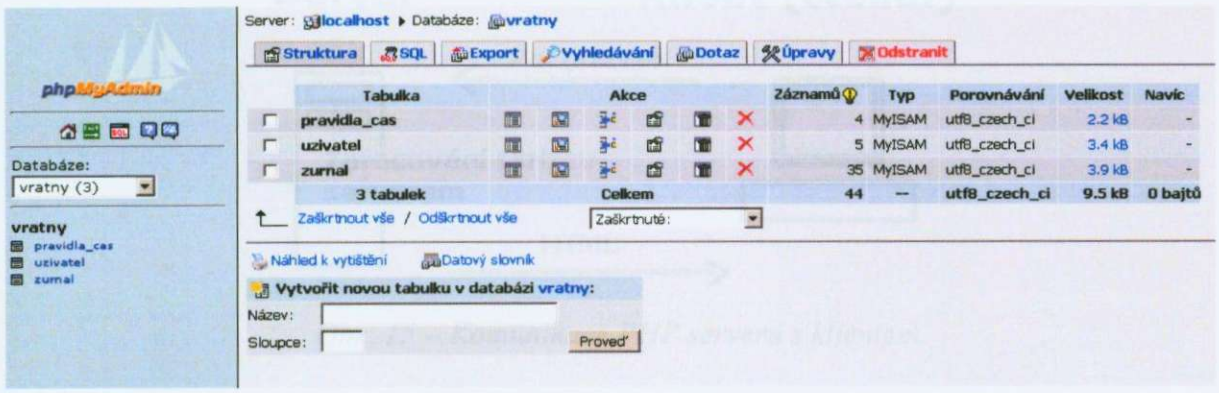
každá z nich obsahuje prvky a konstrukce, které nejsou ve standardech obsaženy. Přenositelnost SQL dotazů mezi jednotlivými databázemi je proto omezená.

MySQL je databázový systém, která vznikl ve švédské firmě MYSQL AB. MySQL je multiplatformní databáze. Komunikace s ní probíhá – jak už název napovídá – pomocí jazyka SQL. Podobně jako ostatní SQL databáze se jedná o dialekt tohoto jazyka s některými rozšířeními. Pro svou snadnou implementovatelnost (lze jej instalovat na Linux, MS Windows, ale i další operační systémy), výkon a především díky tomu, že se jedná o volně šiřitelný software, má vysoký podíl na databázových systémech v současné době používaných. Velmi oblíbená a často nasazovaná je kombinace MySQL, PHP a Apache jako základní software webového serveru. Proti komerčním databázím má MySQL ale také několik slabých míst: má jen jednoduché způsoby zálohování a až donedávna nepodporovalo pohledy, triggery a vložené procedury. Tyto vlastnosti jsou doplňovány teprve v posledních letech, kdy začaly nejčastějším uživatelům produktu – programátorům webových stránek – již poněkud scházet. Databáze MySQL je asi nejpoužívanější databázový systém pro malé webové projekty. Ovšem chybí jí nějaké příjemné uživatelské prostředí pro ladění a správu dat. Naštěstí existují řešení třetích stran, které tento nedostatek řeší. Webová aplikace phpMyAdmin je jednou z nich. Při instalaci jsem volil mezi provedením phpMyAdmin administrovatelné přes klasický http protokol, nebo phpMyAdmin SSL – přístup pomocí bezpečného SSL protokolu. Objektivně byl přístup přes SSL velmi zpomalen zdlouhavým načítáním, proto jsem dal přednost klasické verzi phpMyAdmin.



Obr. 13 - Login přímo z webového prohlížeče

Jeho instalací jsem získal všeobecně dynamický přístup k MySQL databázím, jejich tvorbě a správě. Prostředí umožňuje velice jednoduše zakládat databáze, jednotlivé tabulky a jejich struktury.



Obr. 14 - Výpis tabulek MySQL databáze použitých v projektu autentifikačního systému

V průběhu zkušebního provozu a ladění systému mi bylo toto prostředí velice užitečné. Vhodnými vizualizačními prvky, interaktivním prostředím a v neposlední řadě českou lokalizací mi byl phpMyAdmi jako ne příliš zkušenému programátorovi oporou.

5.2. PHP

PHP[9] (rekurzivní zkratka PHP: Hypertext Preprocessor, „PHP: Hypertextový preprocesor“) je programovací jazyk určený především pro programování dynamických internetových stránek. PHP je jazyk interpretovaný, jeho skripty se začleňují přímo do struktury jazyka HTML a jsou prováděny na straně serveru. Syntaxe se podobá jazyku Perl. PHP je nezávislý na platformě. Obsahuje rozsáhlé knihovny funkcí pro zpracování textu, grafiky, práci se soubory, přístup k několika databázovým serverům, podporu internetových protokolů (HTTP, SMTP, FTP, IMAP, POP3, LDAP, ...). PHP se stalo velmi oblíbeným především díky jednoduchosti použití a tomu, že kombinuje vlastnosti více programovacích jazyků a nechává tak vývojáři částečnou svobodu v syntaxi. V kombinaci s databázovým serverem MySQL a webovým serverem Apache je často využíván k tvorbě webových aplikací. S verzí PHP 5 se výrazně zlepšil přístup k OOP – objektově orientovanému programování. Přístup je velmi podobný jako v jazyce Java. Od roku 1994 je PHP jedním z

[9] *PHP* [online]. 2004 [cit. 2005-09-15]. Dostupný z WWW: <cs.wikipedia.org/wiki/PHP>.

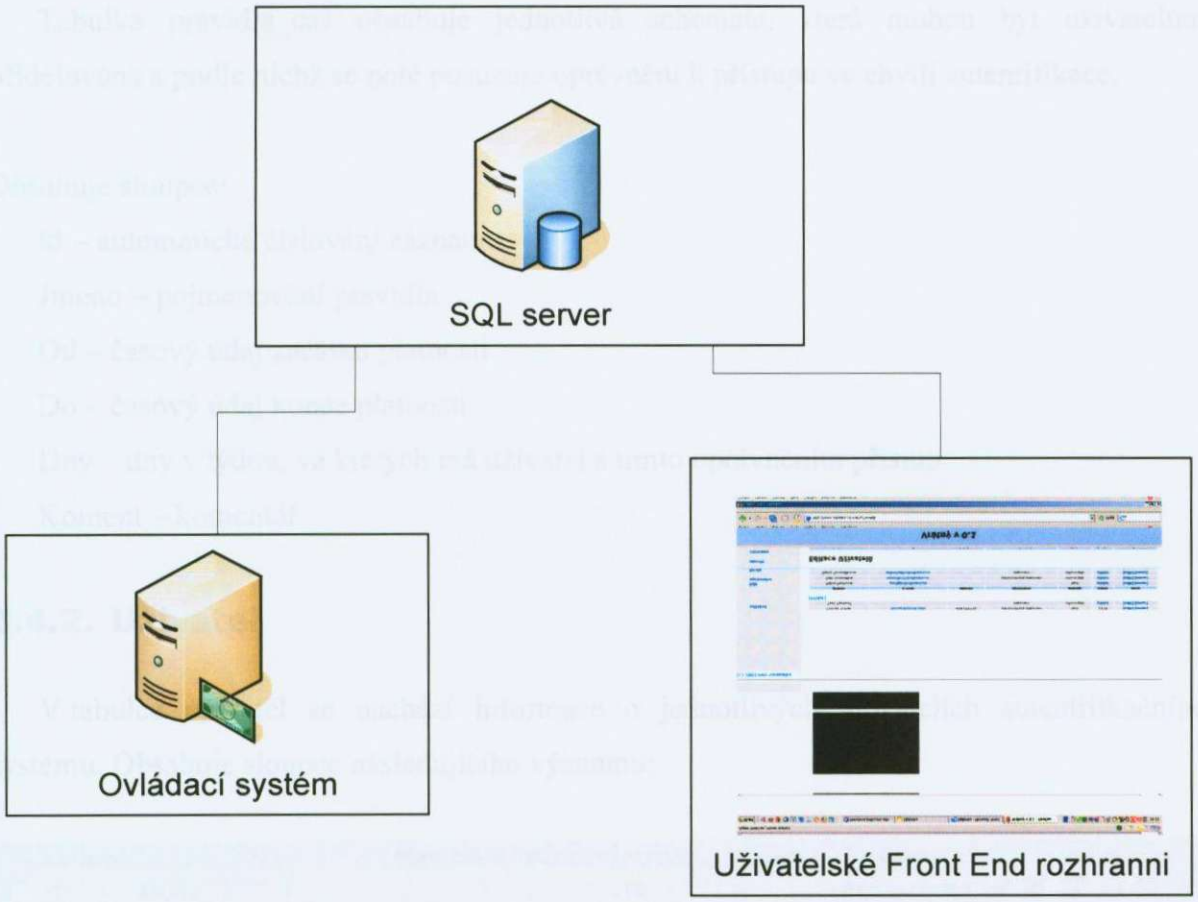
nejpoužívanějších způsobů tvorby dynamicky generovaných WWW stránek. Jeho tvůrce (Rasmus Lerdorf) jej vytvořil pro svou osobní potřebu přepsáním z Perlu do jazyka C.

Obr. 15 – Komunikace PHP serveru s klientem

Vzhledem k možnostem PHP byly všechny démony pro komunikaci s MySQL serverem, pro komunikaci s uživatelem i práci se získanými daty zpracovány právě v PHP. Jedinou výjimku reprezentuje skript v jazyku C, který je spouštěn na ovládacím počítači a načítá obsah karty na standardní výstup a případně spíná elektromagnetickou závoru.

5.3. Koncepce Software

Celý autentifikační systém je v podstatě SQL databáze napojená na uživatelské Front End řešení, kterým lze celý systém ovládat, přidávat a odebírat uživatele, přidělovat jim přístupová oprávnění, případně přímo otevírat zámek vstupních dveří. Back End rozhraní poté přímo získává autentifikační informaci z čipové karty a na základě údajů v databázi řídí přímo vstup do objektu prostřednictvím elektromagnetického zámku. Jak už bylo zmíněno výše, komunikaci s databází jsem přenechal skriptům napsaným v jazyce PHP. Toto řešení je v daných podmínkách dostatečně robustní a ve vnitřní síti neskýtá žádná bezpečnostní rizika.



Obr. 16 - Schématické znázornění koncepce autentifikačního systému

Jak bude patrné z popisu jednotlivých částí, byl systém navrhován zcela otevřeně pro přidávání dalších zámků pro ostatní zóny, případně i připojení jiných technologií. Vytvoření uzavřeného systému by bylo v tomto specifickém prostředí zcela nekoncepční.

5.4. SQL databáze

Pro systém byly navrženy celkem tři tabulky, jejichž popis následuje:

5.4.1. Pravidla_čas

Sloupec	Typ	Porovnávání	Vlastnosti	Nulový	Výchozí	Extra	Akce
id	int(11)			Ne		auto_increment	
jmeno	varchar(10)	utf8_czech_ci		Ne	nové		
od	time			Ne	00:00:00		
do	time			Ne	00:00:00		
dny	set('pondělí', 'úterý', 'středa', 'čtvrtek', 'pátek', 'sobota', 'neděle')	utf8_czech_ci		Ne			
koment	varchar(100)	utf8_czech_ci		Ne	Nové pravidlo		

Tabulka pravidla_cas obsahuje jednotlivá schémata, která mohou být uživatelům přidělována a podle nichž se poté posuzuje oprávnění k přístupu ve chvíli autentifikace.

Obsahuje sloupce:

Id – automatické číslování záznamu

Jmeno – pojmenování pravidla

Od – časový údaj začátku platnosti

Do – časový údaj konce platnosti

Dny – dny v týdnu, ve kterých má uživatel s tímto oprávněním přístup

Koment – komentář

5.4.2. Uživatel

V tabulce uživatel se nachází informace o jednotlivých uživatelích autentifikačního systému. Obsahuje sloupce následujícího významu:

Sloupec	Typ	Porovnávání	Vlastnosti	Nulový	Výchozí	Extra	Akce
id	int(11)			Ne		auto_increment	
login	varchar(15)	utf8_czech_ci		Ano	NULL		
heslo	varchar(20)	utf8_czech_ci		Ne			
karta	varchar(20)	utf8_czech_ci		Ano	NULL		
prava	set('administrace', 'otevirani')	utf8_czech_ci		Ano	NULL		
aid	varchar(10)	utf8_czech_ci		Ano	NULL		
jmeno	varchar(40)	utf8_czech_ci		Ano	nepojmenovaný		
prijmeni	varchar(40)	utf8_czech_ci		Ano	uživatel		
trida	varchar(40)	utf8_czech_ci		Ano	NULL		
email	varchar(40)	utf8_czech_ci		Ano	NULL		
komentar	varchar(200)	utf8_czech_ci		Ano	NULL		
telefon	varchar(15)	utf8_czech_ci		Ano	NULL		

Id – automatické číslování záznamu

Login – přihlašovací jméno (má význam pro uživatele s právem otevírání a administrace)

Heslo – heslo pro přihlášení do webové aplikace

Karta – sériové číslo karty

Prava – možno nastavit na otevírání, nebo administrace, nebo nic (význam viz. dále)

Aid – jméno sady přístupových práv odpovídající záznamu v tabulce pravidla_cas

Jmeno – jméno uživatele

Prijmeni – příjmení uživatele

Trida – třída, kterou uživatel navštěvuje

Email – elektronický kontakt na uživatele

Komentar – komentář

Telefon – telefonní kontakt na uživatele

5.4.3. Žurnál

Komunikačním uzlem, log Filem, a pomocnou tabulkou je tabulka žurnál. Význam jednotlivých sloupců je následující:

	Sloupec	Typ	Porovnávání	Vlastnosti	Nulový	Výchozí	Extra	Akce
☐	id	int(11)			Ne		auto_increment	
☐	vznik	datetime			Ne	0000-00-00 00:00:00		
☐	typ	enum('info', 'warning', 'error', 'command')	utf8_czech_ci		Ne	info		
☐	stav	enum('request', 'progress', 'done')	utf8_czech_ci		Ne	done		
☐	puvod	varchar(100)	utf8_czech_ci		Ano	*NULL*		
☐	data	varchar(200)	utf8_czech_ci		Ano	*NULL*		
☐	uid	int(11)			Ne	0		
☐	ttl	int(11)			Ne	10		

ID – automatické číslování záznamu

Vznik – čas a datum vzniku záznamu v žurnálu

Typ – v současné verzi démon, který záznam zakládá, nastavuje na hodnotu „command“

Stav – v průběhu zpracování nabývá hodnot „request“, „progress“ a „done“

Původ – název démona, který záznam založil

Data – kód příkazu

Uid – kterého uživatele se záznam týká

Ttl – „Time to live“. Při každé akci se hodnota dekrementuje a pokud na záznam žádný démon nereaguje, je po čase smazán.

5.5. Programová část PHP

V této části se pokusím popsat na základě rozboru některých podstatných částí výkonných démonů proces zpracovávání událostí v systému. Z kódů uvádím jen podstatné části, které mají vliv na přímou koncepci autentifikacního systému.

Obecně by bylo možné říci, že pokud některý z démonů vygeneruje příkaz, který chce od systému zpracovat, zapíše jej do již zmíněné tabulky žurnál, označí se za původce a nastaví stav záznamu na „request“. Naopak pokud se v tabulce objeví záznam se stavem „request“, jednotliví démoni tomuto záznamu věnují pozornost a zkoumají, zda není adresován právě

jim. Na následujících příkladech budu demonstrovat chování systému v případě, že se uživatel pokusí získat přístup do vnitřní zóny zasunutím čipové karty do čtečky:

```
<?PHP
require_once 'conn.inc';
echo "server bezi (zamek)\n";
function nastav_zpracovani($id, $kam) {
  mysql_query("UPDATE zurnal SET stav='$kam' WHERE id='$id' limit 1");
}
function udalost_otevri($id, $cislo) {
  nastav_zpracovani($id, 'done');
  echo "oteviram dvere\n";
  exec ("/usr/local/bin/daemon-hardware otevri");
  echo "dokonceno\n";
}
function zpracuj_udalost($cm) {
  echo "zachycena udalost, vyvolal $cm->puvod, ttl=$cm->ttl, data $cm->data\n";
  list($cmd, $arg1)=explode(' ', $cm->data);
  switch ($cmd) {
  case 'otevri':
    udalost_otevri($cm->id, $arg1);
    break;
  default:
    echo "udalost nebyla timto daemonem podchycena\n";
  }
}
$old_karta=0;
function cti_kartu() {
  global $old_karta;
  exec ("/usr/local/bin/daemon-hardware cti", $ret);
  $karta=$ret[0];
  if (($karta!=$old_karta) && $karta) {
    $old_karta=$karta;
    echo "prectena unikatni karta, zapisuji do zurnalu";
    mysql_query("INSERT INTO zurnal SET typ='command', stav='request', puvod='daemon-
zamek', data='karta $cislo', vznik=NOW()");
  }
}
while (1) {
  cti_kartu();
  usleep (500000);
  $res=mysql_query("SELECT * from zurnal WHERE typ='command' AND stav='request' AND
ttl>0");
  if ($cm=mysql_fetch_object($res)) zpracuj_udalost($cm);
  cti_kartu();
}
?>
```

Tento kód reprezentuje démona běžícího na straně zámku a majícího za úkol načíst od pomocného programu číslo karty (v případě načtení relevantní hodnoty založit záznam v žurnálu) a zpracovat záznam ze žurnálu, pokud je ve stavu „request" a sloupec data odpovídá hodnotě „otevři". Démon běží ve smyčce z řádků 36 – 42. Každou 0,5 vteřiny nahlédne do žurnálu a hledá řádky typu „command", ve stavu „request", u kterých hodnota Time to Live je větší než 0. Pokud takový záznam nalezne, pokračuje program funkcí *zpracuj_udalost* z řádky 13 až 21. Ta určí, zda byl záznam určen pro tohoto démona, a pokud byl, spustí funkci *událost_otevři*.

Hlavní smyčka rovněž každým průchodem spouští funkci *čti_kartu*, která spouští externí program pro čtení sériového čísla karty, ošetřuje případ dlouhodobého zasunutí karty do čtečky (řádek 28 - 30) a v případě načtení platné hodnoty zakládá záznam v žurnálu. Záznam bude čekat na zpracování démonem na straně serveru.

```
1  echo "server bezi\n";
2
3  function nastav_zpracovani($id, $kam) {
4    mysql_query("UPDATE zurnal SET stav='$kam' WHERE id='$id' limit 1");
5  }
6
7  function udalost_karta($id, $cislo) {
8    nastav_zpracovani($id, 'done');
9    echo "kontroluji pristup pro kartu $cislo\n";
10   $res=mysql_query("SELECT * FROM uzivatel WHERE karta='$cislo'");
11   if (!$us=mysql_fetch_object($res)) {
12     echo "karta neznama, loguji pro pozdejsi pouziti\n";
13     mysql_query("INSERT INTO zurnal SET typ='command', stav='done', puvod='karta',
14 data='neznama $cislo', vznik=NOW()");
15     return;
16     }
17   $den=date('%w')-1;
18   if ($den<0) $den=6;
19   $den=pow(2,$den);
20   $cas=date('%G:%i:%s');
21   // overeni v jednom SQL dotazu
22   $res=mysql_query("SELECT uzivatel.login, uzivatel.aid, pravidla_cas.dny+0 FROM
23 uzivatel,pravidla_cas WHERE uzivatel.aid=pravidla_cas.jmeno AND uzivatel.karta='$cislo'
24 AND (pravidla_cas.dny+0 & $den) AND pravidla_cas.od<='$cas' AND
25 pravidla_cas.do>='$cas'");
26   if ($ac=mysql_fetch_object($res)) {
27     echo "pristup povolen $ac->login";
28     mysql_query("INSERT INTO zurnal SET typ='command', stav='request', puvod='daemon-
29 server', uid='$ac->id', data='otevri', VZNIK=NOW()");
30     echo mysql_error();
31     return;
32     }
33   mysql_query("INSERT INTO zurnal SET typ='command', stav='done', puvod='karta',
34 data='nepovoleno', vznik=NOW(), uid='$us->id'");
```

```
35    echo mysql_error();
36    echo "pristup byl zamitnut\n";
37  }
38
39  function zpracuj_udalost($cm) {
40    echo "zachycena udalost, vyvolal $cm->puvod, ttl=$cm->ttl, data $cm->data\n";
41    list($cmd, $arg1)=explode(' ', $cm->data);
42    switch ($cmd) {
43    case 'karta':
44      udalost_karta($cm->id, $arg1);
45      break;
46    default:
47      echo "udalost nebyla timto daemonem podchycena\n";
48    }
49    mysql_query("UPDATE zurnal SET ttl=ttl-1 WHERE id='$cm->id' limit 1");
50  }
51
52  while (1) {
53    usleep (300000);
54    $res=mysql_query("SELECT * from zurnal WHERE typ='command' AND stav='request'
55  AND ttl>0");
56    if ($cm=mysql_fetch_object($res)) zpracuj_udalost($cm);
57  }
58
59  ?>
```

Také ve skriptu na straně serveru běží démon ve smyčce z řádek 52 – 57. Ze žurnálu se vybírají záznamy odpovídající typu „command", stavu „request" a Time to live větším než nula. Pokud je takový záznam nalezen, spouští se funkce *zpracuj_událost*. Pokud tato funkce určí pozitivní relevantnost pro tohoto démona a data odpovídají hodnotě karta, spouští se funkce pojmenovaná *událost_karta*(řádky 7 - 36). Číslo karty je nejprve vyhledáváno v tabulce uživatelů. Pokud zde číslo karty není nalezeno, v tabulce žurnál je založen záznam s tímto číslem. Později je možné tento záznam použít při zakládání nového uživatele a tuto anonymní kartu přiřadit novému živiteli. Pokud je číslo karty nalezeno, je spuštěn proces, který zjišťuje oprávněnost přístupu v porovnání s tabulkou Pravidla_cas.

Určení, zda má uživatel právo na přístup v aktuální den, probíhá pomocí skriptu z řádek 17 – 22. Do proměnné $den se přiřadí hodnota aktuálního dne v týdnu, bohužel v anglosaském pořadí dnů v týdnu, kdy 0 odpovídá neděli, 1 pondělku a tak dále. Proto je hodnota číselného údaje hned na začátku snížena o 1 a následujícím příkazem je dni s hodnotou menší než 0 přiřazeno číslo 6. Příkazem z řádku 19 vytvořím pro jednotlivé dny tzv. bitovou masku:

Den v týdnu	Po	Út	St	Čt	Pá	So	Ne
Číslo dne po úpravě	0	1	2	3	4	5	6
Bitová maska	1	2	4	8	16	32	64

Tento postup má význam v tom, že součtem jednotlivých povolených dní vzniká nezaměnitelná hodnota, ze které lze logickým součinem určit, zda se v množině povolených dní nachází právě aktuální den. Porovnání časového údaje je již banální záležitostí.
V případě, že je zjištěno, že karta je autentifikována jako registrovaná a v aktuálním čase má povolen přístup, je do žurnálu vložen záznam typu „command", ve stavu „request" a daty „otevři". Jak již bylo popsáno dříve, na tento záznam zareaguje démon zámku, který jej načte a určí jako příkaz, na který zareaguje otevřením.

Oba popsaní démoni, respektive jejich výkonné funkce, nastavují okamžitě, jak se ujmou zpracování některého ze záznamů, jejich hodnotu stavu na stav „done". Stav „progress", který je rovněž přípustný, je zdokumentován v systému pro případ implementace jiných, déle trvajících procedur, které mohou být do autentifikačního systému později přidávány. Při dobách trvání vyhodnocení čísel karty nebo vyřízení požadavku na otevření zámku nemá tento stav smysl.

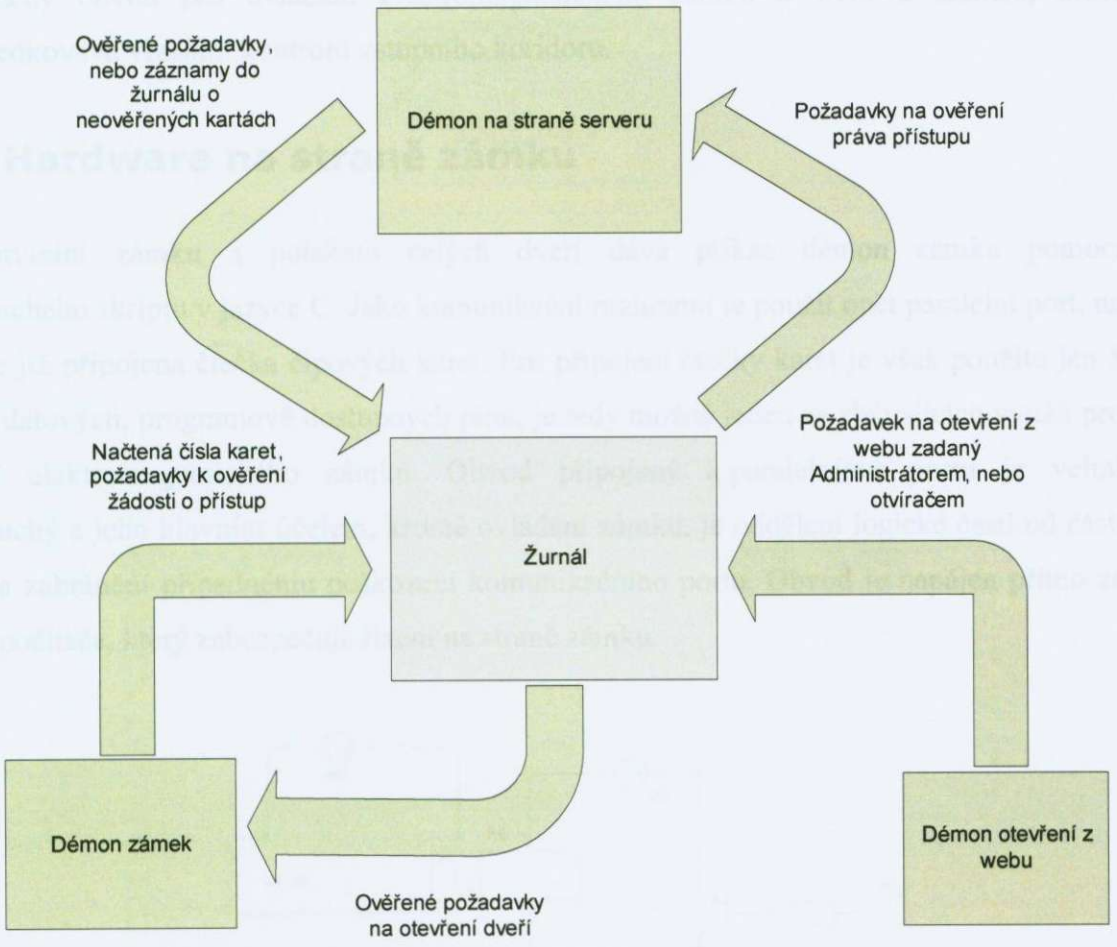
Příkaz k otevření dveří může ještě generovat démon, kterého může z webového rozhraní spustit uživatel, který má oprávnění k otvírání dveří z webu, nebo k administraci systému. Toto oprávnění je zakotveno v tabulce uživatel ve sloupci práva. Výsledkem tohoto členění jsou tři kategorie uživatelů registrovaných v systému:

- standardní uživatel
- otvírač dveří
- administrátor

Standardní uživatel si může v závislosti na přidělené sadě oprávnění otevřít dveře čipovou kartou. Nemá možnost se přihlásit pomocí webového rozhranní k ovládací aplikaci, ani do ní jakýmkoliv způsobem zasahovat.

Otvírač dveří má stejné možnosti jako standardní uživatel, navíc ale po přihlášení k systému může pomocí démonu otvírat dveře z webu. Do ostatních administračních položek nemá možnost přistupovat.

Administrátor může kromě výše zmíněných funkcí navíc přidávat a odebírat uživatele, zakládat a editovat sady oprávnění ke vstupu a manipulovat se záznamy v žurnálu, které může kontrolovat a analyzovat.



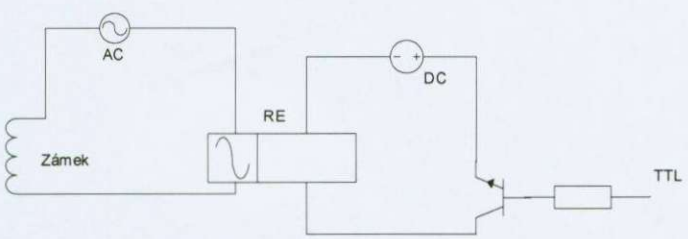
Obr. 17 - Procesní schéma komunikace démonů v systému.

6. Realizace hardware

Veškerým hardware použitým v systému je již výše popsaná čtečka čipových karet, dále jednoduchý obvod pro ovládání elektromagnetického zámku a webová kamera, která zprostředkovává vizuální kontrolu vstupního koridoru.

6.1. Hardware na straně zámku

K otvírání zámku a potažmo celých dveří dává příkaz démon zámku pomocí jednoduchého skriptu v jazyce C. Jako komunikační rozhranní je použit opět paralelní port, na který je již připojena čtečka čipových karet. Pro připojení čtečky karet je však použito jen 5 z osmi datových, programově dostupných pinů, je tedy možné jeden ze zbývajících využít pro spínání elektromagnetického zámku. Obvod připojený k paralelnímu portu je velmi jednoduchý a jeho hlavním účelem, kromě ovládání zámku, je oddělení logické časti od části silové a zabránění případnému poškození komunikačního portu. Obvod je napájen přímo ze zdroje počítače, který zabezpečuje řízení na straně zámku.



Obr. 18 - Schéma ovládací časti na straně zámku.

6.2. Webová kamera

V úvodu jsem naznačoval, že jednou z výchozích podmínek byla i vizuální kontrola vstupního koridoru. Původně měla být připojena k ovládacímu počítači USB kamera, která by přenášela obraz do nainstalovaného Broadcastingového systému a obraz by byl šířen dále počítačovou sítí. Zde ale došlo na problémy s kompatibilitou běžně dostupných USB webových kamer s operačním systémem Linux. Podporovaných modelů je poskromnu, a proto jsem nakonec zvolil východisko, ve kterém jsem do monitorovaného prostoru umístil web kameru s Fast Ethernet rozhraním. IP kamera umožňuje přímé připojení k síti a Upload

jednotlivých snímků přímo na FTP server. Některé druhy těchto webových kamer umožňují i Broadcast plynulého video streemu v MPEGu, ale jejich cena převyšuje hranici přijatelných cenových nákladů. Zvláště pak proto, že 1 – 3 snímky za sekundu bez patrného zpoždění je zobrazovací rychlost pro tyto účely více jak dostatečná.

Obr. 19 - Použitá IP kamera NCS-230 SOHO

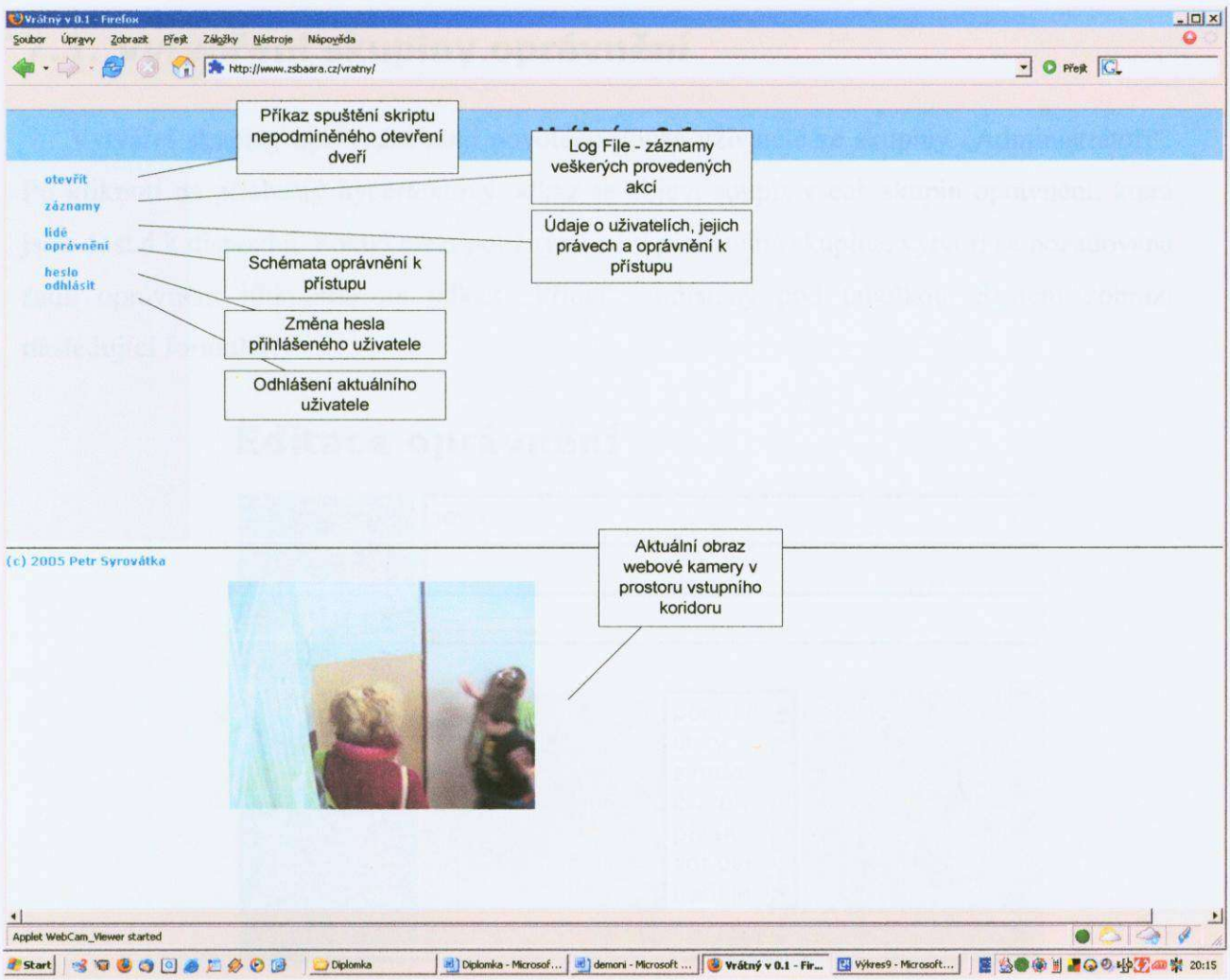
Obr. 20 – Situace vstupního koridoru – umístění kamery

7. Uživatelský manuál

7.1. Přihlášení do systému

Přihlásit se do systému mohou jen uživatelé s oprávněním otevírat pomocí webové aplikace vstupní dveře, nebo uživatelé s oprávněním administrátora. Ostatní uživatelé nemají možnost do systému jakýmkoliv systémem zasahovat.

Přihlašovací dialog otevřete zadáním adresy **www.zsbaara.cz/vratny** do webového prohlížeče. Poté budete vyzváni, abyste zadali vaše uživatelské jméno a heslo. Po korektním přihlášení se v okně prohlížeče zobrazí základní nabídka a náhled webové kamery snímající vstupní koridor.



Obr. 21 - Úvodní stránka webového rozhraní

7.2. Otevření dveří z webu

Otevřít dveře z Webové stránky příkazem „Otevřít" může pouze přihlášený uživatel ze skupiny „Otvírač dveří", nebo „Administrátor". Po kliknutí na příslušný hypertextový odkaz se v okně prohlížeče objeví hlášení, že se dveře otevírají. V případě poruchy zámku systém následně odpoví, že „Zámek nereaguje!". V takovém případě akci opakujte, případně kontaktujte administrátora systému.

POZOR! Každé otevření elektromagnetického zámku vygeneruje zápis do LogFile systému. Nikdy nenechávejte přihlášený systém bez dozoru a nenechte s ním manipulovat nepoučenou osobu!

7.3. Vytvoření skupiny oprávnění

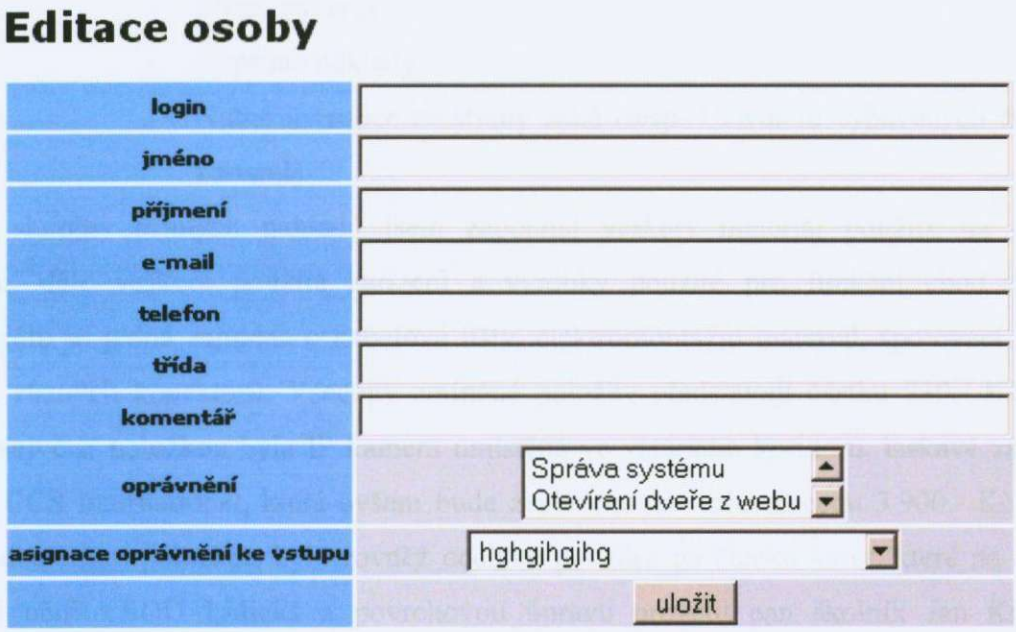
Vytvářet skupiny oprávnění mají povoleno pouze uživatelé ze skupiny „Administrátoři". Po kliknutí na příslušný hypertextový odkaz se objeví soupis všech skupin oprávnění, která jsou dosud k dispozici. Pokud mezi použitými není použitelná skupina, vytvoří se požadovaná sada oprávnění kliknutím na odkaz „Přidat", umístěný pod tabulkou. Systém zobrazí následující formulář:

Doporučuji volit výstižná jména skupin oprávnění a rovněž vyplňovat pečlivě řádku komentář, ve které by měl být popsán účel a skupina uživatelů, pro kterou bylo pravidlo vytvořeno. Po zadání počátečního a koncového času platnosti je možné provést výběr dne, ve

kterém bude oprávnění v tomto časovém rozsahu platné. Při stisknuté klávese CTRL je možné zvolit více dnů v tomto časovém rozsahu. Pokud je třeba jiných časových rozsahů v jiných dnech nebo dalšího časového limitu v již použitý den, je třeba rozpracované oprávnění uložit a v tabulce všech oprávnění zvolit volbu „Přidat" na zvýrazněné řádce se jménem editovaného oprávnění. Poté je možné pokrčovat dalším limitem ve stejném formuláři.

7.4. Přidání uživatele

Příkaz pod hypertextovým odkazem „Lidé" umožňuje uživateli ze skupiny „Administrátoři" přidávat nové uživatele a registrovat čipové karty. Výše zmíněný příkaz zobrazí tabulku všech doposud registrovaných uživatelů, včetně jejich personálií, oprávnění k otvírání dveří z Webu nebo správě systému a přiřazených sad oprávnění. Již založené uživatele je možné mazat, případně editovat tlačítkem na konci příslušného řádku tabulky. Pro přidání nového uživatele slouží odkaz „Přidat" na konci tabulky.



Po vyplnění všech položek je možné uživateli přiřadit již dříve zmíněné oprávnění. Pokud se jedná o uživatele, který nemá povoleno otvírat dveře z webového front endu, ani systém administrovat, nevybírá se žádná z možností v nabídce oprávnění. Výběr z roletového menu na konci tabulky přiřadí uživateli některou ze sad oprávnění ke vstupu pomocí čipové karty. Po uložení uživatele je možné přiřadit mu čipovou kartu. Je možné vybrat jednu z načtených, nepřiřazených karet, které se uchovávají v LogFile, respektive v tabulce žurnál. Pokud byl nově přidaný uživatel oprávněn k otvírání dveří, případně ke správě systému, jeho přístupové heslo bylo automaticky nastaveno na „heslo". Je tedy nutné aktuálního uživatele odhlásit,

přihlásit do systému nově založeného uživatele a příkazem „Heslo“ jeho přístupové heslo změnit. U běžných uživatelů není heslo podstatné.

7.5. Záznamy

Příkaz „Záznamy“ slouží uživatelům s oprávněním správce systému ke kontrole průchodů, záznamu neznámých karet, případně kontrole uživatelů, kteří otevírají dveře z webového prostředí. Zároveň může tato tabulka sloužit jako případný systém pro kontrolu docházky a podobně.

8. Finanční kalkulace

Jako jeden z hlavních ukazatelů pro realizaci projektu autentifikačního systému byla i cenová dostupnost. Z patrného důvodu jsem veškeré náklady rozdělil na tři oblasti:

- Přímé náklady
- Nepřímé náklady
- Nutné investice ze strany žáků (resp. Uživatelů vybavených čipovými kartami)

Do skupiny přímých nákladů jsem započítal veškerý materiál použitý na realizaci projektu, dále veškerá použitá zařízení a výrobky použité pro funkční chod systému. Z materiálu se jedná zejména o kabelové lišty, elektromontážní materiál, spojovací materiál několik různých konektorů. Všechny zmíněné položky představují částku 730,- Kč včetně DPH. Největší položkou byla IP kamera umístěná ve vstupním koridoru, laskavě zapůjčená firmou CCS International, která ovšem bude zaplacena za smluvní cenu 3 900,- Kč s DPH. Nezanedbatelnou položkou bylo rovněž ocelové pouzdro na čtečku karet, které na zakázku vyrobili učni z SOU Lidická a povrchovou úpravu provedl pan školník Jan Kropáček. Celková cena výrobku byla 400,-Kč včetně DPH.

Do kategorie nepřímých nákladů jsem započetl materiál a zařízení, která byla dříve v majetku organizace, ale protože již neplnila svůj původní účel, byla použita pro realizaci autentifikačního systému. Jednalo se zejména o nevyužitou část školní sítě, aktivní prvek pro připojení IP kamery a ovládacího PC, dále samotné PC, ke kterému je připojena čtečka karet a zámek dveří a rovněž samotná čtečka, která dříve sloužila jako bezpečnostní prvek u PC na program, který již není využíván a rovněž zmíněné PC je již vyřazeno z inventáře.

Nutné investice ze strany žáků jsou v podstatě symbolické. Jednak existuje možnost, že si žák sám opatří telefonní kartu. Nezáleží na tom, zda je karta používána pro jiné účely, nebo zda jsou na ní nějaké jednotky. Tyto skutečnosti nejsou podstatné pro funkci systému. V případě většího zájmu, je možné karty nakoupit komerčně, protože jejih cena je mimořádně příznivá. Jedná se o cca 10,- Kč za kartu.

9.Závěr

Celá realizace projektu byla neobyčejným přínosem. Musel jsem se seznámit s celou řadou postupů a technik z nejrůznějších oborů, o které jsme měl zájem, ale časová vytíženost mi nedovolovala se jim věnovat na konkrétní aplikaci, která by měla smysl a reálné uplatnění. Za pomoci přátel – živých i elektronických – jsem se důkladně seznámil se základy databázových aplikací a rozšířil si znalosti v oblasti programování webových aplikací. Měl jsem možnost poznat blíže prostředí komunikačních rozhraní a získat do budoucnosti představu o ovládání elektroniky přes PC. Vybudoval jsem systém, který bude mít do budoucnosti další využití a možná se stane jádrem autentifikačních procesů i pro jiné využití, než řízení přístupu do budovy.

Projekt byl nepochybně přínosem i pro ZŠ J. Š. Baara, kde podobný se stal funkční systém řešením situace popsané v úvodu práce. Pokud bude vůle ze strany vedení, je možné pracovat na jeho dalším rozšiřování a zvyšování jeho kvalit.

Jak jsem již několikrát v této práci uvedl, v porovnání s profesionálním řešením by se mohl mnou navržený autentifikační systém jevit jako hračka. Pravdou je, že podle kritérií, která jsem si v úvodu stanovil, by ve specifickém prostředí základní školy představovalo takovéto řešení zátěž, jejíž význam a přínos by byl sporný. Účelem nebylo vyvinout robustní komplet, který by obstál v komerčním prostředí, ale jednoduché a účelné řešení, použitelné v konkrétním případě. Tento záměr se podařil.

Seznam použité literatury

- Autentizace, autentikace nebo autentifikace? [online]. 2004 [cit. 2005-06-20]. Dostupný z WWW: http://interval.cz/clanek.asp?article=3680>.

- Přístupový identifikační systém [online]. 1998 [cit. 2005-03-22]. Dostupný z WWW: http://www.mujweb.cz/www/frenky/projekt.htm>.

- Dallas iButton [online]. 2004 [cit. 2005-09-09]. Dostupný z WWW: <http://www.maxim-ic.com/products/ibutton/>.

- plk. JUDr. VANČO, Emil . Biometrie, biometrika - geneze, vývoj a současné pojetí [online]. [2001] [cit. 2005-09-09]. Dostupný z WWW: www.mvcr.cz/casopisy/kriminalistika/2005/01/vanco_info.html>.

- Vnitřní paměti [online]. 2002 [cit. 2005-07-23]. Dostupný z WWW: <http://www.fi.muni.cz/usr/pelikan/ARCHIT/TEXTY/INTPAM.HTML>.

- Paralelní port [online]. 2002 [cit. 2005-09-10]. Dostupný z WWW: <www.soom.cz/index.php?name=usertexts/show&aid=70>.

- SQL [online]. 2004 [cit. 2005-09-15]. Dostupný z WWW: <cs.wikipedia.org/wiki/SQL>.

- PHP [online]. 2004 [cit. 2005-09-15]. Dostupný z WWW: <cs.wikipedia.org/wiki/PHP>.

- Linux - Dokumentační projekt. [s.l.] : Computer Press, 2001. 989 s. Operační systémy.

- GUTMANS, Andi, BAKKEN, Stig Saether, RETHANS, Derick. Mistrovství v PHP. Brno : Computer Press, 2005. 650 s.