Význam informačních technologií v průmyslu komerční bezpečnosti

Importance of informative technology in industry of commercial security

Lenka Jelínková

Bakalářská práce
2006

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2006/2007

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lenka JELÍNKOVÁ**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Význam informačních technologií v průmyslu komerční bezpečnosti**

Zásady pro vypracování:

1. Vymezit pojem informační bezpečnost a stanovení jejich cílů. 2. Vyhodnotit možná bezpečnostní rizika, příp. hrozby spojené s ochranou informací a dat. 3. Stanovit možnosti ochrany prostřednictvím bezpečnostních mechanismů. 4. Vypracovat zásady pro zabezpečení dat a informací v průmyslu komerční bezpečnosti a následná aplikace na podnik v soukromém sektoru.

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

Danilák M., Svet počítačových vírusov, GRADA, 1992 Odehnal P., Zahradníček P., Praktická sebeobrana proti virům, GRADA, 1996 Ször P., Attack on Win 32, Data Fellows, 1998 Ször P., Attack on Win 32-PartII, Data Fellows, 1998 Nádeníček P., Přibyl T., Přikrylová O., Votruba T., Chip Special, Vogel Publishing, 2002 Luboš Dobda, Ochrana dat v informačních systémech, GRADA, 1998 Danuše Rodryčová, Pavel Staša, Bezpečnost informací jako podmínka prosperity firmy, GRADA, 2000 Gerald Kovacich, Průvodce bezpečnostního pracovníka informačních systémů, Unis Publishing, Brno 2000

Vedoucí bakalářské práce: **Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a statistiky

Datum zadání bakalářské práce: **4. září 2006**

Termín odevzdání bakalářské práce: **4. září 2006**

Ve Zlíně dne 4. září 2006

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že jsem na celé bakalářské práci pracovala samostatně a použitou literaturu jsem citovala.

Ve Zlíně, 05. 09. 2006 .....

jméno diplomanta

ABSTRAKT

Abstrakt česky

Současná společnost ve stále větší míře využívá informační systémy a technologie pro nejrůznější činnosti. Informace se proto staly klíčovými v každé společnosti a jejich ochrana je aktuální a stává se tak významným faktorem úspěchu či neúspěchu jakékoliv organizace. Proto jsem se v této bakalářské práci zaměřila jednak na možné pachatele útoků na informační systémy, ale především na nejrůznější možnosti ochrany proti nim.

Klíčová slova: bezpečnostní funkce, šifrování, identifikace, elektronický podpis, autentifikace, magnetická karta, čipová karta.

Abstrakt ve světovém jazyce

Our society is using intelligence systems as well as technology as for varions activities these times always in higher level. Information became as to be of great importance in every society and protection of this appears to be significant factor of being successful. Because of that I have drawn my attention in my bachelor work to possible attacks to intelligence systems as well as mainly on the posoibilitis how to protect against.

Key words: security function, encryption, identification, electronic signature, authenticity, chip card, magnetic card.

OBSAH

ÚVOD

Informace mají klíčovou roli v každé společnosti a jejich vlastnictví, zvláště v prostředí tržního hospodářství, představuje významnou výhodu pro soutěžící subjekty. V konkurenčním prostředí se stávají zbožím s vysokou tržní hodnotou. Ochrana informací před možnou ztrátou je proto, zejména v současné době, vysoce aktuální a stává se tak významným faktorem dlouhodobého úspěchu nebo naopak neúspěchu jakékoli organizace.

Ochrana informací se v každé organizaci řídí stupněm utajení, jejich konkrétní formou a podobou, místem kde se nalézají, vztahy k jiným organizacím apod. Management každé organizace proto vždy musí najít vlastní ochranný systém, vycházející z konkrétních a specifických podmínek své organizace. Současně to však také znamená výběr a určení kompetentních, spolehlivých zaměstnanců organizace, kteří budou oprávněni se seznamovat s určitým, konkrétním druhem informací, které se v organizaci nachází. Nejdůležitějším krokem při posuzování této problematiky však bude rozhodnutí o stanovení ochranných opatření ke každému druhu informací tak, aby byly chráněny nejen zájmy organizace, ale zároveň aby byly splněny i požadavky právních norem, které jednotlivé druhy informací upravují.

Informační bezpečnost však není důležitá jen pro organizace, představující podnikatelské subjekty, ale také pro stát. Každý stát proto chrání některé důležité informace, související s jeho bezpečností nebo ochranou jeho zájmů. Je poskytována zejména proto, že vyzrazení těchto informací nebo dokonce jejich pouhé ohrožení, by mohlo způsobit státu škodu nebo ohrožení jeho zájmů v nejrůznějších oblastech života společnosti. Většina států proto k ochraně svých nejdůležitějších informací (tj. utajovaných skutečností představující státní zájem), přijímá právní normy, které stanovují jaký druh informací bude chráněn a jakými způsoby bude ochrana těchto informací zabezpečována. Tento „speciální“ druh informací pak podléhá speciální ochraně, specifickým procedurám nakládání s nimi, při jejich ukládání a manipulaci s nimi.

1 BEZPEČNOST INFORMAČNÍCH TECHNOLOGIÍ

1.1 Pojem bezpečnost informačních technologií

Pod pojmem ***bezpečnost informačních technologií*** (dále jen IT) obvykle rozumíme ochranu odpovídajících IS a informací, které jsou v nich uchovávány, zpracovávány a přenášeny. Součástí takto obecně chápané bezpečnosti IT je i komunikační bezpečnost, tj. ochrana informace přenášené mezi počítači, fyzická bezpečnost, tj. ochrana před přírodními hrozbami a fyzickými útočníky a personální bezpečnost, tj. ochrana před vnitřními útočníky.

V soudobém chápání bezpečnosti IT je bezpečnost dána zajištěním:

- ***důvěrnost*** - k aktivům (k údajům) mají přístup pouze autorizované subjekty
- ***integrity*** **a** ***autenticity*** - aktiva (data, software, hardware) smí modifikovat jen autorizované subjekty a původ informací je ověřitelný
- ***dostupnosti-*** *a*ktiva (data nebo služby) jsou autorizovaným subjektům do určité doby dostupná, nedojde tedy k odmítnutí služby, kdy subjekt nedostane to na co má právo.

1.2 Základní principy bezpečnosti při použití IT

Pokud hovoříme v souvislosti s informačními technologiemi o ***zpracovávání informací***, *pak tím rozumíme použití těchto technologií k uchovávání, přenosu, vyhodnocování a prezentaci informací.*

Poněvadž se mnohdy jedná o informace s nezanedbatelnou hodnotou (např. zdravotní záznamy, daňová přiznání, bankovní účty, elektronické platební nástroje, výsledky vývoje nebo výzkumu, obchodní záměry), musí být chráněny tak:

- aby k nim měly přístup pouze oprávněné osoby;
- aby se zpracovávaly nefalšované informace;
- aby se dalo zjistit, kdo je vytvořil, změnil nebo odstranil;
- aby nebyly nekontrolovaným způsobem vyzrazeny;
- aby byly dostupné tehdy, když jsou potřebné.

1.3 Základní pojmy, vymezující oblast bezpečnosti IT

Model typů komponentů – složen ze 4 částí :

- ***hardware*** – procesor, paměti, terminály, telekomunikace atd.
- ***software*** – aplikační programy, operační systém atd.
- ***data*** – data uložená v databázi, výsledky, výstupní sestavy, vstupní data atd.
- ***lidé*** – uživatelé, personál-se ale zaměřujeme na bezpečnost IT a ne na obecnou bezpečnost, o lidské činitele se budeme zajímat jen do té míry, pokud se jejich činnosti a vlastnosti budou bezprostředně týkat bezpečnosti IT.

1.3.1 Objekt IS

Pasivní entita, která obsahuje/přijímá informace a je přístupná autorizovaným subjektům IS

1.3.2 Subjekt IS

Aktivní entita (osoba, proces nebo zařízení činné na základě příkazu uživatele) autorizovatelná pro získání informace z objektu, vydávání příkazů ovlivňujících udělení práv přístupu k objektu, změnu stavu objektu apod.

1.3.3 Zranitelné místo

Je slabinou IS využitelnou ke způsobení škod nebo ztrát útokem na IS.

Existence zranitelných míst je důsledek chyb, selhání v analýze, v návrhu a/nebo v implementaci IS, důsledek vysoké hustoty uložených informací, složitosti softwaru, existence *skrytých kanálů* pro přenos informace jinou než zamýšlenou cestou. Podstata zranitelného místa může být fyzická, přírodní, fyzikální, v lidském faktoru.Zranitelná místa vznikají jako důsledek selhání (opomenutí, zanedbání) v návrhu..

1.3.4 Hrozba

Možnost využitkovat zranitelné místo IS k útoku na něj – ke způsobení škody na aktivech.

Hrozby lze kategorizovat na:

- ***objektivní***
    - *přírodní* (požár, povodeň, výpadek napětí, poruchy...), u kterých je prevence obtížná a u kterých je třeba řešit spíše minimalizaci dopadů vhodným plánem obnovy; v tomto případě je třeba vypracovat havarijní plán;
    - *fyzikáln*í- např. elektromagnetické vyzařování;
    - *technické nebo logické*- porucha paměti, softwarová „zadní vrátka“, špatné propojení jinak bezpečných komponent, krádež, resp. zničení paměťového média, nebo nedokonalé zrušení informace na něm
- ***subjektivní***, tj. hrozby plynoucí z lidského faktoru
    - *neúmyslné* - např. působení neškoleného uživatele / správce
    - *úmyslné* - představované potenciální existencí *vnějších útočníků* (špioni, teroristi, kriminální živly, konkurenti, hackeři) i *vnitřních útočníků*

1.3.5 Útok

Buďto *úmyslné využitkování zranitelného místa*, tj. využití zranitelného místa ke způsobení škod/ztrát na aktivech IS, nebo *neúmyslné uskutečnění akce*, jejímž výsledkem je škoda na aktivech.

Při analýze možných forem útoků na IT je třeba typicky řešit problémy typu - jak se projevuje počítačová kriminalita, jaké jsou možné formy útoků, kdo útočí, kdo může páchat počítačový zločin, jaká rizika souvisí s používáním informačních technologií, jak se chránit před útoky apod. Následně řešenými problémy jsou pak rozhodnutí typu - jak detekovat útok, jak zjistit bezpečnostní incident, jak reagovat na útok, co dělat, když dojde k bezpečnostnímu incidentu. Útok může být *úmyslný* nebo *neúmyslný*, resp. *náhodný*.

Rozpoznáváme:

- ***útoky na hardware, které lze vést –***
  - *přerušením* – přírodní havárie, neúmyslné útoky způsobené kouřením, údery, úmyslné útoky krádeží, destrukcí odposlechem – krádež času procesoru, místa v paměti;
  - *přidáním hodnoty* – změnou režimu činnosti.
- ***útoky na software, které lze vést –***
  - *přerušením* – mezi neúmyslné útoky může patřit vymazání softwaru způsobené špatným konfiguračním systémem nebo archivačním systémem, použití neotestovaných programů, chyby operátora; mezi úmyslné útoky patří např. úmyslné vymazání programu;
  - *odposlechem* – provedení neoprávněné kopie programu, pirátství;
  - změnou – např. využitím „zadních vrátek“ (neveřejných spouštěcích postupů z doby tvorby softwaru);
  - *přidáním hodnoty* – zabudováváním virů, atd.
- ***útoky na data, které lze vést –***

  - *přerušením* – mezi neúmyslné útoky lze zařazovat jejich neúmyslné vymazání, mezi úmyslné útoky pak úmyslné vymazání, sabotáž

  - *odposlechem* – porušení důvěrnosti, krádež kopií

  - *změnou* – porušení integrity, neautorizované modifikace dat

  - *přidáním hodnoty* – opakovanými neautorizovanými dílčími odběry peněžního konta (salámový útok), generování transakcí atd.

1.3.6 Útočník

může být ***vnější***, ale v organizaci se často vyskytuje i ***vnitřní*** útočník.

Podle znalosti a vybavenosti rozeznáváme:

- ***útočníky slabé síly*** - amatéři, náhodní útočníci, využívající náhodně objevená zranitelná místa při běžné práci; jedná se o náhodné, často neúmyslné útoky, útočníci mají omezené znalosti, příležitosti i prostředky, pro ochranu před nimi stačí přijmout relativně *slabá bezpečnostní opatření*, která jsou levná
- ***útočníky střední síly*** - hackeři, jejichž častým krédem je dostat se k tomu, k čemu nejsou autorizovaní; jedná se o *běžné útoky*, útočníci mají mnohdy hodně znalostí, obvykle ale nemají zjevné příležitosti k útokům a mívají omezené prostředky; jako ochrana proti nim se přijímají *bezpečnostní opatření střední síly*
- ***útočníky velké síly*** - profesionální zločinci, kteří mají původ obvykle mezi počítačovými profesionály, je pro ně typická vysoká úroveň znalostí, mají obvykle dostatek prostředků (peněz) a mnohdy i dost času k provedení útoku, provádějí *útoky vymykající se běžné praxi*, pro ochranu před nimi je nutno přijímat *silná bezpečnostní opatření*.

1.3.7 Riziko

Představuje existenci hrozby. *Rizikem* rozumíme pravděpodobnost využitkování zranitelného místa IS. Říkáme, že se hrozba uplatní s takovou a takovou pravděpodobností. Rizika lze terizovat vedle pravděpodobnosti výskytu bezpečnostního incidentu i potenciálně způsobenou škodou.

Obr.1.Vzájemné vztahy ve správě rizik

2 BEZPEČNOSTNÍ FUNKCE

Zabezpečujeme-li IS, je třeba nejprve stanovit ***bezpečnostní cíle*** a způsob jejich dosažení. Bezpečnostní cíle jsou dílčí přínosy k bezpečnosti, kterou dosahuje IS z hlediska udržení důvěrnosti, integrity a dostupnosti. Pro jejich dosažení se aplikuje používání *funkcí prosazujících bezpečnost*, nazývaných rovněž *bezpečnostní funkce* nebo *bezpečnostní opatření.*

Bezpečnostní funkce přispívá buďto ke splnění jednoho bezpečnostního cíle, nebo ke splnění několika bezpečnostních cílů. Abychom mohli bezpečnostní cíle stanovit, je potřeba znát zranitelná místa, jak lze tato zranitelná místa využitkovávat, možné formy útoků, kdo může zranitelná místa využitkovat nebo jejich prostřednictvím způsobit neúmyslnou škodu, kdo jsou potenciální útočníci, s jakou pravděpodobností dochází k útoku, jak se lze proti útokům bránit a jaké škody mohou útoky způsobit.

Prostředkem použitým pro dosažení stanovených bezpečnostních cílů IS jsou bezpečnostní funkce IS (bezpečnostní opatření), které mohou být administrativního, fyzického nebo logického typu, tj. mohou být implementovány takovými *mechanismy*, jakými jsou administrativní akce, hardwarová zařízení, procedury, programy.

Podle způsobu implementace rozeznáváme bezpečnostní funkce:

- ***softwarového charakteru*** (mnohdy označované jako *logické bezpečnostní funkce*)

  např. softwarové řízení přístupu, funkce založené na použití kryptografie, digitální podepisování, antivirové prostředky, zřizování účtů, standardy pro návrh, kódování, testování, údržbu programů, ochranné nástroje v operačních systémech (ochrana paměti, ochrana souborů řízením přístupu, přístupové matice, přístupové seznamy, hesla, autentizace přístupu k terminálu), ochranné nástroje v aplikačních systémech pro autentizaci přístupu, pro autentizaci zpráv atd.

- ***hardwarového charakteru*** (mnohdy označované jako *technické bezpečnostní funkce*)

  autentizace na bázi identifikačních karet, šifrovače, autentizační kalkulátory, firewally, archivní pásky – záložní kopie dat a programů

- ***administrativního a správního charakteru*** **-** ochrana proti hrozbám souvisejícím s nedokonalostí odpovědnosti a řízení systému IT; výběr a školení důvěryhodných

osob, hesla, autorizační postupy, přijímací a výpovědní postupy, právní normy, zákony, vyhlášky, předpisy, etické normy, licenční politika, nástroje provozního řízení, zpravodajství o událostech a stavech významných z hlediska bezpečnosti, sběru a analýzy statistik, konfigurace systému apod.

- ***fyzického charakteru*** **-** stínění, trezory, zámky, strážní, jmenovky, protipožární ochrana, záložní generátory energie.

2.1 Bezpečnostní mechanismy

Pro implementaci funkcí prosazujících bezpečnost se používají bezpečnostní mechanismy. ***Bezpečnostní mechanismus*** je logika nebo algoritmus, který hardwarově (technicky), softwarově (logicky), fyzicky nebo administrativně implementuje bezpečnostní funkci.

Mohou být při implementaci bezpečnostních funkcí spolu různými způsoby kombinovány tak, aby implementace bezpečnostní funkce byla přesná, účinná a ekonomická. Většina bezpečnostních funkcí bývá implementovatelná několika způsoby, tj. různými typy bezpečnostních mechanismů. Například bezpečnostní funkci identifikace a autentizace můžeme implementovat -

- ***ověřováním znalosti nějaké tajné nepadělatelné informace*** (heslo nebo osobní identifikační číslo – PIN, Personal Identification Number);
- ***ověřováním vlastnění nějakého předmětu*** (klíč, magnetická nebo čipová karta);
- ***ověřováním nějakých fyzických charakteristik*** (otisk prstu, vzorek oční duhovky).

3 KRYPTOGRAFIE V IS

Šifrování, neboli kryptografie je *transformace dat do nečitelné podoby*. Důvodem k šifrování je ochránit důvěrné a osobní informace znemožněním jejich čitelnosti pro všechny, komu nejsou určeny, dokonce i pro osoby, které mají přístup k těmto šifrovaným datům. Opačný postup k šifrování se nazývá ***dešifrování*** – tedy transformace šifrovaných dat do jejich původní srozumitelné podoby.

Dešifrování i šifrování vyžaduje užití nějaké tajné informace, obvykle označované jako klíč. Tento klíč nepovolí vstup neoprávněným osobám. Obsahuje data, obvykle řetězec alfanumerickým znaků. Jakmile jsou data šifrována, mohou být uložena na nedostatečně chráněných médiích nebo přenášena po nechráněných sítích- jako je Internet.

V bezpečných algoritmech, šifrováním zprávy pomocí různých klíčů dostaneme kompletně různé šifry a také dešifrování nesprávným klíčem dá náhodně vypadající text (nicméně existují také kryptosystémy, kde dešifrování různými klíči může dát různé rozumně vypadající zprávy).

3.1 Základní pojmy:

Kryptografie – zabývá se navrhováním kryptografických algoritmů a způsoby jejich využívání.

Kryptoanalýza – zabývá se metodami umožnující získat ze šifrovaného textu text otevřený – bez znalosti klíče, zkoumá odolnost a naopak zranitelnost jednotlivých kryptosystémů.

Kryptologie – vědní disciplína zahrnující kryptografii i kryptoanalýzu.

Kryptografický algoritmus – vyjadřuje matematický postup, který přetváří otevřený text do takové podoby, kdy se původní informace stává nečitelnou a obráceně, postup, který přetváří šifrový text do podoby otevřeného textu.

Klíč – parametr kryptografického algoritmu.

Heslo – řetězec znaků sloužící k ověření uživatelovy identity.

Šifrování – proces, během kterého byl použit šifrovací algoritmus.

Dešifrování – proces, kdy získáme otevřený text šifrovaného textu pomocí šifrovacího algoritmu klíče.

Symetrická šifra – algoritmus používající pro šifrování i dešifrování tentýž klíč.

Asymetrická šifra – algoritmus používající 2 odlišné klíče- jeden pro šifrování, druhý pro dešifrování.

Hash algoritmus – slouží pouze k šifrování informace, bez možnosti dešifrování.

Veřejný klíč – jeden z dvojice klíčů asymetrického šifrovacího algoritmu. Obvykle se používá k šifrování a nemusí být utajován.

Kryptografii dělíme:

- Symetrická kryptografie
- Asymetrická kryptografie

3.2 Symetrická kryptografie

Kryptografické algoritmy, které používají ten samý klíč pro šifrování i dešifrování . Tyto šifry se používají k zabezpečení rychlého utajovaného přenosu většího objemu. Jsou představovány širokou třídou tzn. Blokových šifer – zpracovávají otevřený text po větších blocích, obvykle 64 bitech. Symetrické šifry se v praxi využívají především pro zašifrování zálohovaných dat.

Mezi nejznámější symetrické šifry patří:

- Rozlomení šifry DES (Data Encryption Standard)
- Současný kryptografický standard AES (Advanced Encryption Standard)

3.2.1 Šifrovací algoritmus DES

Šifrovací norma DES (Data Encryption Standard) je mezinárodním standardem, který se obecně označuje normovací zkratkou DEA-1 (Data Encryption Algorithm) a byl oficiálně zaveden v roce 1976. Od té doby DES úspěšně odolává většině pokusů o vyluštění. Je sice faktem, že pro lepší bezpečnost bylo nutné zvětšit délku klíče, ale přesto základní princip šifrování zůstal zachován.

Díky tomu nám vznikne 56-bitový klíč. Jelikož několik klíčů se považuje za tzv. slabé klíče (weak keys), doporučuje se je během výběru vyloučit, protože veškerá bezpečnost šifry DES je založena na síle klíče.

DES je typickým příkladem propastného rozdílu mezi softwarovou a hardwarovou implementací, neboť při šifrování hardwarových čipem je několiksetkrát rychlejší.

- ***BezpečnostDESu***

  DES byl navržen firmou IBM (konkrétně kryptografy Tauchmanem a Mayerem), ale jeho implementaci jako amerického standardu důsledně kontrolovala a korigovala americká NSA, což vedlo k domněnce, že do něj zabudovali skrytý vstup (trap door), kterým se dá snáze zašifrované zprávy dešifrovat. I přesto, že veškeré informace k tomuto tématu jsou pečlivě střeženy, objevují se zprávy, které tuto domněnku potvrzují. Vedle nich však bylo řečeno i to, že NSA možná záměrně upravila detaily algoritmu tak, aby nemohl být skrytý vstup implementován samotných tvůrcem, tj. firmou IBM. Vedle (ne)existence skrytého vstupu do algoritmu, je bezpečnost algoritmu zásadně ovlivněna klíčem, neboť při symetrickém šifrování je na něm plně závislá. Původní návrh IBM počítal s 112-bitovým klíčem, přesto jako norma byla délka klíče omezena na 56 bitů. Vedle problému délky klíče, existují některé konkrétní potenciálně slabé klíče, které mohou bezpečnost algoritmu vážně narušit. Jedním z nich je situace, kdy na levé straně je klíč tvořený samými jedničkami a na pravé straně klíč tvořený samými nulami, popř. jejich možnékombinace.V roce 1977 prohlásili Diffie a Hellman, že jednoúčelový počítací stroj, který by byl schopen rozluštit DES za jediný den, by stál asi 20 miliónů dolarů. O čtyři roky později zvýšili dobu na rozluštění na tři dny a cenu stroje na 50 miliónů dolarů. Oba muži tak předpověděli, že algoritmus bude bezpečný pouze do roku 1990. V roce 1988 byl vyvinut čip, který byl schopen prověřit celý milión šifer za vteřinu. V roce 1993 Michael Wiener navrhl počítač v ceně 1 miliónu dolarů, který byl schopen realizovat luštění DESu metodou totálních zkoušek v průměru za 3,5 hodiny. V současné době je bezpečnost použití tradičního DESu o délce klíče 56 bitů nasnadě. Proto během celé existence DESu vzniklo několik „bezpečnějších“ verzí.

Verze DESu

- **Násobný DES** – některé realizace DESu využívají šifrování s klíčem o délce 56 bitů několikrát za sebou. Typickým zástupcem je TripleDES (trojnásobný DES).

- **DES s nezávislými podklíči** – další variantou je metoda, kdy pro každou rundu je použit jiný naprosto nezávislý podklíč o délce 48-bitů, který není generován z 56-bitového klíče, což při 16 rundách prakticky znamená, že klíč má délku 768 bitů.
- **DESX** – je varianta DESu společnosti RSA Data Security, která se stala součástí některých aplikací
- **CRYPT** – varianta DESu použitelná jako jednosměrná funkce pro tvorbu hesel a lehké šifrování.
- **GDES (Generalizovaný / zobecněný DES)** – zobecněný DES byl vytvořen pro urychlení a posílení algoritmu klasického DESu.
- **DES s alternativními S-boxy** – některá řešení umožňují měnit uspořádání či vnitřní řešení S-boxů.

3.3 Asymetrická kryptografie

O dost novější a v současnosti především používaná třída algoritmů však používá pro šifrování a dešifrování různé klíče. Tato kryptografie se jmenuje ***kryptografie s veřejným klíčem***, nebo také ***asymetrická kryptografie*** a její rozvoj se datuje zhruba od roku 1970.

Šifrovací klíč bývá *veřejný* (public key), zatímco dešifrovací klíč bývá *soukromý* (private key) a znám jenom svému držiteli. Tedy zasílaní šifrovaných zpráv konkrétnímu adresátovi je umožněno všem, zatímco dešifrovat je může jenom on sám.

Držitel může svůj soukromý klíč použít k zašifrování kontrolního součtu dat a tím tato data opatří tzv. elektronickým podpisem (viz následující kapitola) - vzhledem k tomu, že je soukromý klíč znám pouze jeho držiteli, může každý dešifrovat a zkontrolovat kontrolní součet jeho veřejný klíč a potvrdit tím jednak integritu dat (tj. že je během přenosu nikdo nezměnil), jednak také autora, protože jediný, kdo mohl použít soukromý klíč k podpisu, je jeho držitel.

3.3.1 Šifrovací algoritmus RSA

Algoritmus RSA, jehož pojmenování vzniklo z prvních písmen příjmení jeho autorů (Rivest, Shamir, Adleman), vznikl v roce 1977. Podstatou algoritmu je skutečnost, že je

velmi obtížné faktorizovat (rozložit) velká čísla, zvlášť když jsou součinem dvou velkých prvočísel. Přesto bezpečnost RSA je přímo úměrně závislá délce klíče.

Historie RSA:

- RSA vznikl v roce 1977 na Massachussets Institute of Technology (MIT). V roce 1983 byl na zmíněný algoritmus vydán U.S. Patent (číslo #4,405,829). Nositelem tohoto patentu byla firma RSA Security, kterou autoři RSA mezitím založili. Patent, jehož platnost byla pouze na území USA, byl udělen na 17 let (do roku 2000) a znamenal, že za jakékoliv komerční využití RSA bylo nutné platit firmě RSA Security licenční poplatky.

Algoritmus RSA patří do skupiny tzv. „asymetrických šifer“, kde existuje „veřejný“ a „privátní šifrovací klíč“. Veřejný klíč slouží k šifrování zpráv směrem k uživateli, privátní k jejich dešifrování. Primárně se tento algoritmus prezentuje jako algoritmus pro výměnu klíčů a tvorbu elektronického podpisu.

Paradoxem asymetrických algoritmů obecně je jejich poměrně vyšší rychlost zpracování při softwarové realizaci, než-li při hardwarové. Sice byla vyvinuta řada mikročipů, které realizují RSA, ale jsou při zpracování 1000x pomalejší než-li algoritmus DES. Při softwarové realizaci je algoritmus pouze 100x pomalejší než-li DES.

Luštění algoritmu RSA:

Existuje několik velmi složitých způsobů luštění algoritmu RSA. Dá se říci, že obecně je možné uvést několik zásad pro luštění algoritmu:

- Znalost jednoho šifrovacího/dešifrovacího páru exponentů daného modulu umožňuje luštiteli faktorizovat tento modul.
- Znalost jednoho šifrovacího/dešifrovacího páru exponentů daného modulu umožňuje luštiteli odvodit jiný šifrovací/dešifrovací pár bez nutnosti faktorizace.
- Doplnění zpráv náhodnými hodnotami slouží jako prevence proti vyluštění RSA metodou luštění s nízkými šifrovacími exponenty.
- Dešifrovací exponent by měl být velký.

Algoritmus RSA lze snadnou využít pro digitální podepisování (viz. následující kapitola) RSA v současnosti představuje celosvětovou normu, kterou formuluje i ISO 9796. Například francouzské a australské bankovnictví je normalizováno na bázi RSA. V USA, díky tlaku různých organizací (v neposlední řadě také NSA) neexistuje žádná norma pro šifrování na bází veřejného klíče.

3.4 Nejznámější šifry z historie

3.4.1 Substituční šifra

Oecně spočívá v nahrazení každého znaku zprávy jiným znakem podle nějakého pravidla. Pravděpodobně nejstarší popis substituční šifry je v Kámasútře, která se datuje do 4. století, ovšem její autor čerpal z pramenů až o 800 let starších.

3.4.2 Caesarova šifra

Je pojmenovaná po Juliu Caesarovi, který ji pravděpodobně používal jako první. Každé písmeno tajné zprávy je posunuto v abecedě o pevný počet pozic. Šifra je z dnešního pohledu velmi snadno luštitelná, protože je jen málo možných klíčů. Ve své době ale představovala nevídanou metodu a osvědčila se velmi dobře.

3.4.3 Vigenèrova šifra

Jedná se o speciální případ polyalfabetické šifry. Vigenèrova šifra používá heslo, jehož znaky určují posunutí otevřeného textu a to tak, že otevřený text se rozdělí na bloky znaků dlouhé stejně jako heslo a každý znak se sečte s odpovídajícím znakem hesla. Caesarova šifra je tedy speciálním případ Vigenèrovy šifry s heslem o délce jeden znak.

3.4.4 Vernamova šifra

Je anglicky často nazývaná *one-time pad*, v českém překladu *jednorázová tabulková šifra*. Jde dosud o jedinou známou šifru, o níž bylo exaktně dokázáno, že je nerozluštitelná. Podobně jako Caesarova šifra i tahle spočívá v posunu písmen, avšak každé písmeno je posunuto o jiný počet pozic, který je navíc zvolen náhodně. Pokud je klíč dokonale náhodný, dlouhý stejně jako zpráva sama (a není použit opakovaně), je tato šifrovací metoda dokonale bezpečná. Délka klíče však pro běžné účely použití této metody zpravidla

znemožňuje, metoda se používá hlavně pro velice specializované účely, např. tzv. *horká linka* spojující za dob studené války Moskvu a Washington používala Vernamovu šifru.

3.4.5 Transpoziční šifry

Transpozice neboli přesmyčka spočívá ve změně pořadí znaků podle určitého pravidla.

3.4.6 Šifrování strojem

Použití mechanických a elektronických strojů přineslo do šifrování zcela nové možnosti. Zejména proto, že stroje jsou schopny velkého počtu opakování určitého úkonu v krátkém čase.

- ***Enigma***

Německo za 2. světové války používalo k utajování zpráv mechanický stroj Enigma, který prováděl poměrně složité operace se vstupním textem, ale zároveň se dal poměrně snadno ovládat. Poláci ovšem ještě před vypuknutím války pracovali na prolomení šifry a jejich zjištění byla později nedocenitelná pro spojenecké armády. Šifra byla již během války zlomena a poskytovala tak německé straně pouze falešný pocit bezpečí. Enigma měla původně 3 kolečka, která se otáčela, podobě jako mechanické počítadlo a každé mělo jinak propojené vstupní a výstupní kontakty, tím se měnil průběh proudu a i výsledné písmeno zašifrovaného textu. Později začalo ponorkové námořnictvo používat čtyřrotorové Enigmy.

Obr.2. Enigma

3.5 Steganografie

Starší sestrou kryptografie je steganografie neboli *ukrývání zprávy jako takové*. Sem patří různé neviditelné inkousty, vyrývání zprávy do dřevěné tabulky, která se zalije voskem apod. V moderní době lze tajné texty ukrývat například do souborů s hudbou či obrázky namísto náhodného šumu.

Steganografie, jedna z mnoho zajímavých metod skrytí informace, jejichž současný rozmach byl způsoben především výpočetní technikou a téměř orwellovským postojem k osobně ochraně některých lidí. Slovo Steganografie pochází z řečtiny (stegos – střecha, úkryt; steganos – ukrytý; graphos – písmo, psát) a dá se volně přeložit jako „ukryté písmo“ nebo „skrytý vzkaz“.

3.5.1 Historie steganografie

Stejně jako se špionáž označuje za druhé nejstarší řemeslo, steganografie je jednou z jejich nejstarších metod. Potřeba skrytého předávání zpráv skrze nepřátelské obležení byla nutná již ve starověkém Řecku. Jednou složila jako nositelka informace vyholená hlava otroka (samozřejmě poté, co se mu nechaly vlasy znovu narůst – dost nepraktické přenosové médium), podruhé to byla vosková tabulka, kde se pod tradiční vrstvou vosku skrývala zpráva vyrytá do dřevěné destičky. Pokročilejší metodou steganografie jsou tajné inkousty, které byly oblíbené především v renesanci a v následujících válečných obdobích. Tajné inkousty se vyráběli především z organických látek, v dnešní době je může úspěšně vyrobit se směsi organické a anorganické látky. Kvalita však je vždy závislá na použitých surovinách a jejich vzájemných poměrech. Přesto v příručkách pro mladé chemiky lze nalézt desítky návodů. Poslední variantou skryté komunikace, která se dnes řadí mezi steganografickou metodu, je skrytá komunikace pomocí masmédií. Této komunikace se využívalo a využívá pro úkolování agentů v terénu, kdy obě strany komunikují pomocí zcela bezvýznamných sdělení (např. informace o počasí, inzeráty, apod.).

3.5.2 Digitální steganografie

Moderní doba si žádá využití moderních metod. Díky rozvoji výpočetní techniky se steganografie začala ubírat dalším zajímavým směrem – *digitalizací*. Právě ***digitální steganografie*** odráží současný trend využití bezpečnostních metod při komunikace skrze internet. Umožňuje snadné skrytí tajné zprávy do multimediálního souboru (obrázek,

video, zvukový záznam), který je na internetu volně vystaven. Těsně po 11.září 2001 americká FBI ke svému velkému překvapení zjistila, že síť AL-Kajdá využívá pro svou komunikaci právě této metody předávání zpráv. Bohužel, každoročně se zvyšující rozpočet FBI za účelem stálého držení kroku s teroristy, není úplně tak efektivní, jak by se dalo očekávat. Vraťme se však k podstatě věci – jak tedy digitální steganografie funguje? Celá její metody je založena na dvou nedokonalostech. První z nich je ta, že lidské oko velmi těžko rozezná posun barvy o jednu v 24-bitovém barevném spektru (16,7 miliónu barev). Druhou nedokonalostí je fakt, že každý obrázek ve své informaci nese určitou dávku šumu, kterou člověk může, ale většinou nedokáže svými smysly rozeznat. To jsou dva z pilířu moderní steganografie. Podívejme se teď podrobněji na skrývání textu do obrázků, což je asi nejčastější požadavek digitální steganografie.

3.5.3 Steganografie a šifrování

Zde je nutné se zastavit a vysvětlit si rozdíl, který je mezi steganografií a šifrováním:

- ***Šifrováním*** se mění obsah zprávy tak, aby běžný uživatel, který nevlastní šifrovací klíč (tj. není příjemcem zprávy) nezískal informaci, která je uvnitř skrytá.
- ***Steganografie*** je pouze metodou, jak danou informaci ukrýt tak, aby se snáze a bezpečněji dostala k adresátovi.

Samozřejmě v praxi se většinou používá steganografie jako posílení šifrovací metody, kdy se šifra ukryje do obrázku a pošle příjemci. Tato varianta je velice praktická především v těch zemích, kde došlo v rámci boje proti terorismu k veřejnému zákazu šifrování.

3.5.4 Vodoznaky a autorské práva

Do souvislosti se steganografií se občas dávají i vodoznaky. Princip vodoznaku je sice velmi podobný, ale jeho smysl je trochu v jiné rovině. Vodoznaky jsou většinou *utajené informace* podobného charakteru jako steganograficky skrytá zpráva, které slouží jako nezvratný důkaz o autorství, jenž si daná společnost vloží do svého díla (obrázku, filmu, apod.). Díky vodoznaku je možné odhalit krádež takovýchto děl (na internetu dosti aktuální téma). Bohužel, díky použití stejného principu je možné se i vodoznaku pomocí jednoduché editace obrázku zbavit.

Výhody:

- snadné praktické použití (ukrytí krátké zprávy do veřejně přístupného média - obrázek, zvuk, apod.);
- vysoká dostupnost steganografického softwaru (shareware, freeware).

Nevýhody:

- pouze pro malé (nerozsáhlé) zprávy;
- pokud je zpráva zachycena, je její obsah prozrazen (není-li použito např. šifrování, apod.), jakákoliv manipulace s obrázkem (otočení, převedení do jiného formátu, apod.) vede ke ztrátě ukryté informace.

4 ELEKTRONICKÝ PODPIS

Elektronický podpis je v dnešní době nová, postupně se zavádějící technologie, jejímž cílem je vedle klasického podpisu postavit nástroj, který dostatečně potvrzuje *autorství* dotyčného člověka. Jedním z nejdůležitějších bezpečnostních požadavků, kladených na proces zpracování, ukládání a přenášení informací, je požadavek na zajištění *integrity* těchto dat, tj. požadavek na zabránění neodhalené a neoprávněné modifikaci dat.

Elektronický podpis může být, stejně jako manuální podpis, použit pro ***identifikaci*** a ***autentizaci*** původce informace. Elektronický podpis může být také použit pro kontrolu, že informace nebyla po podepsání změněna. Tím lze zajistit integritu informace. Na rozdíl od manuálního podpisu však nelze pomocí elektronického podpisu rozlišit originál informace od její kopie.

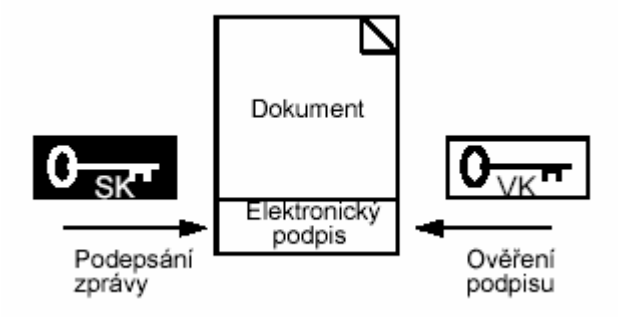
4.1 Funkce elektronického podpisu

- ***Zajišťuje autenticitu dokumentu*** - příjemce dokumentu bezpečně ví, kdo je autorem dokumentu.
- ***Zajišťuje integritu dokumentu*** - příjemce dokumentu má jistotu, že obsah dokumentu nebyl během přenosu nebo zpracování modifikován.
- ***Zajišťuje nepopiratelnost autora elektronického podpisu*** - autor dokumentu nemůže popřít autorství dokumentu ani jeho obsah.

4.2 Vlastnosti elektronického podpisu

- Je spojen s jedním konkrétním elektronickým dokumentem (tj. potvrzuje pravost a autenticitu tohoto dokumentu) a nemůže být použit pro podepsání jiného dokumentu.
- Může být vytvořen pouze tím, kdo zná jisté tajemství (nazývané např. *soukromý klíč*).
- Je nemožné vytvořit jiný dokument, sebeméně odlišný od původního dokumentu, pro který by byl původní elektronický podpis stále platný.
- U dokumentu, podepsaného elektronickým podpisem, kopii od originálu rozlišit nelze.

- Jakmile je jednou elektronický podpis dokumentu vytvořen, kdokoli si může ověřit pravost tohoto podpisu, a to bez nutnosti znát tajemství (soukromý klíč), kterým byl podpis vytvořen.
- Elektronický podpis zachovává téměř všechny vlastnosti manuálního podpisu vyjma jediné – u dokumentu, podepsaného manuálním podpisem, lze rozlišit jeho kopii od originálu.



Obr.3. Podepisování dokumentů elektronickým podpisem

4.3 Certifikační autorita

Aby bylo možné důvěřovat elektronickému podpisu, je třeba mít jistotu, že veřejné klíče, používané pro kontrolu elektronického podpisu, skutečně náleží osobě, která je uvedena v popisu klíče. K tomu slouží tzv. ***certifikační autority***. Certifikační autorita na základě ověření totožnosti vydává certifikát pro veřejný klíč-v podstatě to znamená, že ho opatří podrobnými údaji a tyto údaje i samotný klíč podepíše soukromým klíčem certifikační autority.

4.4 Digitální podpis

Digitalní podpis se vytvoří tak, že se manuální podpis zkonvertuje do podoby elektronického obrazu. Nejenže však digitální podpis nemůže nahradit elektronický podpis, nemůže dokonce nahradit ani samotný manuální podpis. Digitální podpis může být podvržen. Může být duplikován nebo připojen k jinému dokumentu. A nemůže být ani použit ke kontrole, zda dokument nebyl po podepsání modifikován. *Digitální podpis bývá*

někdy zaměňován s elektronickým podpisem. Elektronický podpis je ale širším termínem, který zahrnuje kromě digitálního, také například biometrické prokazování totožnosti (např. otisk prstu) nebo jiné prokazován totožnosti (např. čipová karta). Digitální podpis je speciálním případem elektronického podpisu, kdy k ověření původu dokumentu dochází na základě šifrování.

Některé algoritmy digitálního podpisu

-RSA

-DSA

5 AUTENTIFIKACE

Řešení bezpečnosti a ochrany dat v informačních systémech je velmi rozsáhlou problematikou a ochrana přístupu (autentifikace) k systémům a zdrojům organizace představuje jen jednu část. I když je to jen *část z celkové bezpečnosti informačních systémů*, použití hesel a přístupů představuje vysoké procento bezpečnostních selhání, a to až 71% z dnes registrovaných průniků do systémů. Neautorizovaný přístup obyčejně znamená vysoké finanční ztráty a poškození jména organizace. Největší rizika, kterým musí dnes čelit profesionální informační systémy přichází ze vnitř organizace.

5.1 Autentifikace - jako základ informační bezpečnosti

Dnešní technologie klient/server poskytuje kompaktní data a další kritické informace přes Internet a veřejné sítě až k samotnému PC, případně mobilnímu telefonu. Organizace jsou tak nuceny investovat do technologií, které by ochránili soukromé, velmi důvěrné informace před neautorizovaným přístupem. Prudký nárůst počtu PC a datových sítí, ve kterých se sdílejí data a zdroje, explozivní nárůst počtu mobilních uživatelů a všeobecná potřeba informací vyžaduje od organizací, aby investice do bezpečnostních technologií pokládaly za jedny z nejprioritnějších.

Denně používané síťové aplikace jsou zranitelné neautorizovaným průnikem stejně, jak data uložená v lokální síti, nebo stažená z Internetu.

Názvosloví

- **Identifikace:** Identifikace uživatele je proces, ve kterém se uživatel představí systému jako platný uživatel.
- **Autentifikace:** Proces, který určuje skutečnou, pravou identitu uživatele, který se snaží o přístup do systému.
- **Autorizace:** Tento proces určuje, které aktivity budou povoleny. Běžně je autorizace v kontextu s autentifikací. Jakmile se uživatel autentifikuje, jsou mu přiděleny určitá oprávnění.
- **Autentifikátor:** Přenosné zařízení nebo software určený na autentifikaci uživatele. Autentifikátor pracuje na bázi výzva-odpověď, na bázi sekvencí kódu "pouze čas" a

"čas a událost", případně jiných technikách. Autentifikátorom může být token, čipová karta, nebo jiné zařízení.

Autentifikace a identifikace uživatelů, případně zařízení a serverů při přístupu ke zdrojům organizace se stává nevyhnutelnou především v případě bankovních operací a finančních transakcí (elektronické bankovnictví), elektronického obchodu, pro vzdálené a mobilní uživatele, v oblasti státní zprávy, bezpečnosti a armády, při práci s důvěrnými informacemi ve zdravotnictví a pod.

5.2 Typy autentifikací

- **autentifikace heslem** - založenou na znalosti hesla, které je utajené a známé jen uživateli.
- **autentifikace předmětem** - založenou na vlastnictví identifikačního předmětu.
- **biometrická autentifikace** - založenou na biometrických charakteristikách osoby.

Podle počtu použitých metod k autentifikaci rozlišujeme:

- *Jednofaktorová autentifikace* - použití jedné metody,
- *Dvoufaktorová autentifikace* - použití kombinace dvou metod, např. token heslo,
- *Třífaktorová autentifikace* - použití tří metod autentifikace.

5.2.1 Hesla a osobní identifikační čísla

Hesla a osobní identifikační čísla se přidělují individuálním subjektům, ne jejich skupinám. *Důvěrnost hesel* (osobních identifikačních čísel) pak bývá zajišťována individuální účtovatelností a dalšími administrativními opatřeními, např. zakazujícími uchovávání hesel jinde než v paměti subjektu a připouštějícími používání pouze obtížně uhodnutelných hesel, případně i aplikací mechanismů generujících jednorázově použitelná hesla (na bázi seznamů jednorázově používaných hesel mnoho let pracovala bankovní síť SWIFT – Society for World-wide Interbank Financial Transfers).

Jestliže heslo má být použito pro autentizaci subjektu žádajícího přístup do počítače, potom musí být v počítači dostupný jeho vzor, aby bylo možno zadané heslo kontrolovat.

Uchovávání seznamu hesel je ovšem *bezpečnostní problém*. Kompromitované heslo může použít neoprávněný subjekt k „maškarádě“, k útoku vedeném formou falšování své identity. Proto se místo pamatování hesel (osobních identifikačních čísel) v původní podobě uchovávají v počítači výsledky jejich zpracování jednosměrnými funkcemi (snadno se spočítá výsledek, obtížně se k výsledku hledá jednoznačně odpovídající vstup). Zadané heslo (PIN) se zpracuje stejnou funkcí a autentizační bezpečnostní funkce porovnává výsledky a ne originály.

Přenos hesel nezabezpečenou sítí (běžná lokální síť, telefonní spoj) v otevřené podobě je velmi zranitelný z hlediska požadavku zachování soukromí a důvěrnosti. Jejich šifrováním problém zasílání hesla nevyřešíme, útočník může šifru hesla odchytit a replikovat ji stejně jako by to udělal s jeho originální hodnotou. Jedním možným řešením tohoto bezpečnostního problému je použití mechanismu „výzva–odpověď“. Následujícím způsobem, který umožňuje přenášenou autentizační informaci dynamicky měnit: uživatel i vzdálený počítač znají tajné heslo P a oba umí řešit vhodnou jednosměrnou hašovací funkci *a*. Jakmile uživatel požádá vzdálený počítač o povolení přístupu (udá mu své jméno), vzdálený počítač ho vyzve k dodání důkazového materiálu potřebného pro autentizaci udané identifikace tím, že mu zašle nějakou náhodnou hodnotu R. Uživatel odpoví vzdálenému počítači hodnotou získanou aplikací jednosměrné hašovací funkce *a* na hodnoty hesla P a výzvy R, tj. *a* (P, R). Vzdálený počítač nyní provede stejný výpočet a udanou identitu uzná za autentickou, pokud oba vypočtou stejnou hodnotu.

5.2.2 Magnetická a čipová karta

Magnetická karta

Používá se jako ***identifikační bezpečnostní mechanismus*** již poměrně dlouho a v mnoha aplikacích (bankomaty, placení v obchodech, řízení přístupu do zabezpečovaných prostorů). Formát takové karty a magnetického proužku na ní definuje mezinárodní norma ISO 7810. Magnetická karta obvykle poskytuje paměť přibližně pro řádově stovky bitů dat. Může obsahovat např. informaci identifikující uživatele, číslo jeho bankovního účtu apod. Pro ověřování prohlašované identity uživatele magnetické karty se používá nějaký typ aplikace osobního identifikačního čísla. V on-line systémech lze osobní identifikační čísla ověřovat centrálně, nemusí se tudíž pamatovat na magnetické kartě. PIN bývá kombinován s informací

identifikující uživatele, případně s její částí, aby se útočníkům zabránilo sestavovat si seznamy osobních identifikačních čísel a jejich šifer. Magnetické karty *lze snadno falšovat* nebo *neoprávněně kopírovat*. Jako ochranný prostředek před falšováním se používají např. hologramové obrázky na lícní straně karty. Existuje řada propracovaných prostředků chránících magnetické karty před jejich neoprávněným kopírováním.

Čipová karta

V nedávné době se vyvinuly *karty s mikroprocesory*, pamětmi RAM a ROM, vesměs nazývané ***čipové karty*** (smart cards). Čipové karty poskytují *větší paměťovou kapacitu než magnetické karty* a navíc poskytují nezanedbatelný zpracovatelský výkon přímo na kartě. Umožňují uložená data fyzicky chránit. Kontakty na vnitřní obvody se realizují prostřednictvím plošek, realizovaných na povrchu čipové karty. Jejich pozici, rozměr karty a protokoly, používané pro řízení komunikace mezi čipovou kartou a snímačem čipové karty, zavádí norma ISO/IEC 7816. Čipové karty lze obtížně kopírovat, vnitřní uspořádání čipových karet bývá výrobci karet tajeno.

První generace čipových karet z druhé poloviny 80. let obsahovala jednoduché 8bitové procesory a poskytovala relativně omezenou kryptografickou funkcionalitu. Čipové karty druhé generace jsou vybavovány výkonnějšími procesory, mají více paměti a poskytují větší variantu kryptografických funkcí. Poslední typy čipových karet dokáží realizovat výpočty, potřebné pro digitální podpisy, ve zlomcích sekund. ***Čipové karty druhé generace*** se typicky používají jako interaktivní identifikační zařízení. Mohou obsahovat i tajný kryptografický klíč uživatele. Proto dříve než čipová karta umožní provádění svých funkcí, uživatel používající čipovou kartu musí zadat svůj PIN (na nějakém terminálu a snímači karet). Karta se tak chrání před krádeží. Ve Francii čipové karty již vesměs vytlačily z používání magnetické karty jako platební karty. Existují obchodní systémy s elektronickými pokladnami založené na používání čipových karet. Jsou dostupné čipové karty realizující digitální podpisování v reálném čase. Čipové karty lze používat jako kalkulačku s displejem pro výpočet identifikační informace při autentizaci. Příkladů použitelnosti čipových karet lze uvést mnoho.

Obr.4. Čipová karta

5.2.3 Biometrická identifikační zařízení

Biometrika je poměrně novým oborem, který se vyvinul jako možnost ***využití tělových identifikátorů*** (otisk prstu, geometrie dlaně, apod.) pro jednoznačné určení, ***tzv. identifikování osoby***. To dává naději, že již nebude nutné sebou neustále nosit snadno zcizitelnou čipovou kartu nebo pamatovat si několika místné kombinace hesel. Podívejme se blíže na specifikum a samotné metody identifikace uživatelů.

Verifikace, neboli ověřovací proces, je základním „kamenem úrazu“ veškerých biometrických metod. Ověřovací proces vždy vyžaduje, aby se uživatel přihlásil do systému, např. použitím PIN-kódu. Teprve poté je provedeno porovnání sejmutého záznamu se záznamem z databáze. Pro samotný verifikační proces je podstatný počet povolených pokusů, než bude daný žadatel systémem definitivně odmítnut jako nepovolaná osoba. A právě ***počet pokusů může být tou největší bezpečnostní dírou daného identifikačního zařízení***. Neboť je nutné zvolit takový počet, aby oprávněný uživatel byl systémem jasně rozpoznán, ale jakýkoliv útočník získal příliš málo možností i údajů o systému, který by mu pomohli systém prolomit.

Dalším problémem je ***tzv. ukládání výsledků verifikačního procesu***, neboť je nutné mít nějakou evidenci pokusů o přihlášení se, během používání systému.

Zde existují dva možné přístupy:

- připojení daných zařízení do sítě s centrálním počítačem a ukládání všech pokusů o přihlášení se do centrální databáze;

- uchovávání veškerých pokusů o přihlášení v paměti daného identifikačního zařízení. To sebou nese problém uchovávání omezeného počtu transakcí (pokusů o přihlášení),

což se řeší přepisem nejstarších pokusů těmi nejnovějšími.

- **Verifikace otisku prstu**

Již kriminální věda přišla s ***daktyloskopií***, která nám říká, že na vnitřním povrchu prstů jsou drobné, vyvýšené, brázdovité útvary, které vytvářejí různé vzory. Tyto vzory se pak dělí do tří hlavních kategorií - *smyčky, přesleny a oblouky*. Podstatná je frekvence výskytu, neboť je vědecky dokázáno, že smyčky obsahuje 65% ze všech otisků, přesleny něco kolem 30% a oblouky jen asi 5% všech otisků. Pro porovnávání otisků prstů se pak používají identifikační body, tzv. markanty, které se nacházejí v rýhách vzoru. Identifikační bod se může skládat z některých následujících objektů:

- ***rozdvojení*** - konce dvou rýh vytvářejí vidličku, krátká rýha, ukončovací rýha,
- ***ohrazení*** - spojení dvou rýh vytvářející vidličku na obou koncích, izolované body, roztrojení, atd.

Je přirozené, že některé z těchto bodů se vyskytují častěji než ostatní. Např. krátké rýhy, rozdvojení a ukončovací rýhy jsou daleko frekventovanější než roztrojení, izolované body a ohrazení. Proto se při daktyloskopii (porovnávání otisků prstů) sleduje, jak přítomnost identifikačních bodů, tak i jejich umístění v daném otisku. Otisk prstu obsahuje v průměru 100-200 jednoznačně identifikujících bodů. V praxi však není stanoven přesný počet bodů nutný k rozlišení mezi dvěma otisky. Podle tohoto postupu pak známe několik přístupů k verifikaci otisku prstu. Některé metody se pokoušejí emulovat tradiční daktyloskopii (porovnávání charakteristických markantů prstu), jiné používají *metodu přímého porovnání otisku prstu jako celku, další používají jedinečné řístupy založené například na moaré obrazcích, ultrazvuku, atd*. Některé umožňují *detekovat živý prst*, jiné ne. Poměrně vysoká přesnost (malý výskyt nesprávného přijetí) těchto zařízení může být nevýhodná v případech používání nedisciplinovanými uživateli (velký výskyt nesprávného zamítnutí). Ověřování otisků prstů je vhodné tehdy, je-li k dispozici odpovídající výklad, nácvik používání systému a kontrolované prostředí. V současné době existuje nejvíce různorodých zařízení sloužících pro identifikaci pomocí otisků prstů.

- **Verifikace tvaru ruky**

Zařízení pro jednoznačnou identifikaci pomocí ruky (dlaně) jsou založeny *na měření fyzikálních charakteristik ruky a prstů z hlediska třídimensionální perspektivy*. V prvopočátcích tato metoda byla založena na pouhém jednoduchým měřením délky 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. Základem těchto zařízení bývá ***speciální skener***, který produkuje 3-dimensionální fotografie a redukuje tato data až do 9 bytové hodnoty. Tato metoda je tedy velmi vhodná pro aplikace, kde je omezená paměť pro ukládání těchto dat, jako jsou čárové kódy. Geometrie ruky nám nabízí poměrně dobrou vyváženost z hlediska výkonnostních charakteristik i relativní snadnosti používání. Tato metoda je vhodná pro větší databázi uživatelů nebo pro uživatele s ne příliš častým přístupem (takoví uživatelé bývají méně disciplinovaní z hlediska správného používání biometrického systému, což může vést k častějšímu zamítnutí žadatele). A právě díky jednoznačnosti charakteristik ruky lze docílit poměrně vysoké přesnosti systému. Biometrické systémy založené na snímání geometrie ruky jsou používány v různorodých aplikacích. Nejvíce rozšířené jsou v ***docházkových systémech***. Pro mnoho biometrických projektů je verifikace geometrie ruky obvykle prvním systémem, o kterém se při návrhu uvažuje.

- **Verifikace obličeje**

Verifikace obličeje ***je dnes nejvíce zkoumanou metodou***, neboť problematika identifikace osob dle tváří je velmi obsáhlá. 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. Obraz v počítači může být někdy uložen jako matice jasových úrovní, častěji je však diskriminován nějakou funkcí, která snižuje redundanci dat. Neuchovává se tedy přesná poloha očí, nosu a rtů, ale ukládá se jen vzdálenost očí, vzdálenost rtů od nosu, úhel mezi špičkou nosu a jedním okem, atd. V současné době je známo několik technik rozpoznávání tváří. K těm významnějším a nejvíce používaným patří metoda ***měření geometrických vlastností a metoda porovnávání šablon***. Rozpoznávání obličeje člověka vždy velmi lákalo. Všeobecně se věří, že po zdokonalení systému rozpoznávání obličeje, by mohli odpadnout mnohé, méně efektivní systémy (např. docházkový systém do zaměstnání – proslulé *„píchačky“*). Je však pravdou, že během výzkumů se velmi často špatně

specifikovaly požadavky, což vedlo k nízké funkčnosti a efektivitě systému. Jsou však známy i případy, kdy byly požadavky na systém tak přemrštěné, že bylo obtížné, respektive naprosto nemožné takový systém realizovat. Proto je nutné si uvědomit jak vysoké nároky je nutné klást na daný identifikační systém. Je obrovský rozdíl v realizaci systémů, který porovnává dva statické obrazy a systému, který ověřuje totožnosti jednotlivce nacházejícího se ve skupině lidí. Atraktivnost rozpoznávání obličejů je z hlediska praktického užívání pochopitelná, ovšem je nezbytné být realistický ohledně vyhlídek této technologie. Doposud neměli obličejové rozpoznávací systémy v praktických aplikacích velký úspěch.

- **Verifikace hlasu**

Ověřování totožnosti pomocí lidského hlasu lze definovat jako ***elektronickou metodu 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. Metoda ověřování hlasu je také známa pod jinými jmény jako je autentizace pomocí hlasu či otisk hlasu. Jednou z nejúspěšnějších technik pro ověřování hlasu je ***porovnávání vzorků pomocí analýzy signálů řeči – spektrum***. Některé ověřovací technologie zakládají své autentizační rozhodnutí na *analýze vět*. Je přirozené, že věta má více akustické informace, než-li jednotlivá slova, potažmo slovo. Slova bývají krátká a neobsahují dostatečnou akustickou informaci, která by spolehlivě odlišila mluvčího. Mimoto více informace umožňuje vyšší kvalitu *srovnávacího procesu* pro absolutní shodu. Věty zná pouze autentický mluvčí a mohou jimi být i množiny slov, které je mluvčí schopen vyslovit opakovaně test za testem. Uživatelé si často vytvářejí svoje vlastní tajné autentizační věty a bezpečnost systému je částečně rozšířena, protože neoprávnění uživatelé (podvodníci) neví, kterou větu použít, natož jakým hlasem ji vyslovit. Testy ukazují, že "hacker" (viz. Kapitola 6), který nezná příslušnou autentizační větu autorizovaného uživatele je odmítnut systémem ve více jak 99% případů. Ačkoliv výzkum v této oblasti začal ji v 70. létech, komerční využití rozpoznávání lidského hlasu jako biometrické metody sloužící k jednoznačné verifikaci osob nastává až v současnosti. Verifikace hlasu se dnes používá především ke vzdálenému přístupu do informačních systémů (většinou prostřednictvím telefonu). Uvědomíme-li si jak častá je hlasová komunikace v každodenní činnosti každého z nás, je verifikace hlasu poměrně zajímavá biometrická technika. Významnost ověřování hlasu mezi biometrickými technikami

spočívá v její rychlosti, spolehlivosti, jednoduchosti na použití a nízké ceně. Charakteristickým příznakem současných systémů pro ověřování hlasu je, že ověření může být za určitých okolností (nastydnutí, šum okolí, atd.) mnohem komplikovanější než u jiných biometrik, což vede k názoru, že verifikace hlasu je v některých případech pro uživatele méně přijatelná. Přesto, lze vzhledem k významu této techniky, předpokládat její významný rozvoj.

- **Verifikace podpisu**

Ověřování totožnosti pomocí podpisů zná většina lidí z banky. Princip je jednoduchý. Podepíšeme se a bankovní úřednice dle vlastního uvážení buď to vyžádá další identifikaci nebo považuje náš podpis v porovnání s podpisovým vzorem za jednoznačný identifikátor a vyhoví naší žádosti. Otázkou však je, jaká je důvěryhodnost uvážení samotné úřednice. A proto, pro lepší kontrolu a komfort byl vyvinut systém ***identifikace pomocí podpisu***. K tomu je zapotřebí, aby se dotyčná osoba podepsala (napsala svoje jméno nebo iniciály) na speciální podložku pomocí speciálního pera. Systém ověřuje podpis osoby na základě porovnání s uloženým podpisovým vzorem, který popisuje jak byl popis napsán. Není tedy důležitá podoba podpisu či tvar písmen, i když o to jde samozřejmě také, ale ***důraz je kladen na dynamiku podpisu, provedení tahů, sílu, kterou tlačíme při psaní na podložku, rychlost psaní apod.*** To vše podává jednoznačnou charakteristiku libovolného podpisu. Technologie rozpoznávání je založena na porovnávání změny tlaku, zrychlení v jednotlivých částech podpisu, zarovnání jednotlivých částí podpisu, celkovou rychlost, dráhu a dobu pohybu pera na a nad papírem. Verifikace podpisu má oproti jiným biometrickým metodám výhodu v tom, že lidé jsou zvyklí se podepisovat při transakcích spojených s ověřením identity a zpravidla nevidí na zavedení této verifikační biometriky nic neobvyklého. Zařízení pro verifikaci podpisu jsou ***poměrně přesná*** a obvykle se používají na místech, kde se podpis vyžadoval ještě před zavedením biometrického systému. Přesto současnosti je těchto zařízení v porovnání s jinými biometrickými systémy používáno poměrně málo.

- **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 je spojen s

nervy, jejichž signály vystupují z oka pomocí očního nervu. Oční nerv, společně s artérií sítnice, vystupují 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. Obrázky sítnice mají stejné charakterizační vlastnosti jako např. otisky prstů.***Verifikace sítnice je velice přesnou biometrickou metodou***, 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. A právě z těchto důvodů, přestože samotná metoda vykazuje velmi dobré výsledky, má verifikace sítnice problémy z hlediska přijatelnosti ze strany uživatelů. Použití této metody se tím redukuje jen na vrcholně bezpečné kontrolní systémy. Velkým kladem ověřování pomocí sítnice je značná spolehlivost a velmi obtížná napodobitelnost. Nevýhodou je jistá subjektivní nepříjemnost, daná samotným uživatelem.

- **Verifikace duhovky**

Stejně jako např. otisky prstů nebo obraz sítnice, i *duhovku oka má každý člověk jedinečnou.* Avšak, zatímco existuje asi 60 odlišných forem otisků, které mohou být různě kombinovány na jednom otisku, v případě duhovky je počet různých vzorů - forem duhovky vyšší než-li 400. Nalezení dvou identických duhovek náhodným výběrem je tedy mnohonásobně méně pravděpodobné, než nalezení dvou identických otisků prstů. Duhovky dvou identických dvojčat jsou samozřejmě rozdílné a jedinečné. Ve skutečnosti dokonce i obě duhovky jednoho člověka jsou rozdílné a jedinečné. Z tohoto pohledu neexistuje jiná biometrická charakteristika člověka, která by byla více rozlišovací než právě duhovka. Snímání obrazu duhovky oka je v porovnání se snímáním obrazu sítnice oka uživatelsky příjemnější metoda. Kromě toho, verifikace duhovky se vyznačuje velmi vysokou přesností. Z tohoto důvodu lze verifikaci duhovky oka použít i pro identifikaci uživatele. Snadnost použití prozatím nebyla hlavním kritériem při vývoji těchto zařízení, avšak v dohledné době lze v této oblasti od systémů pro verifikaci duhovky očekávat výrazná zlepšení.

6 POČÍTAČOVÁ KRIMINALITA

Snaha maximálního využití informačních technologií má však i své negativní stránky. Je již obecným jevem, že jakmile se objeví nový vynález, najdou se lidé, kteří ho využijí k páchání trestné činnosti. Nejinak je tomu s výpočetní technikou, přesněji s informačními technologiemi. Tak se objevila i ***počítačová kriminalita***, představující nový druh trestné činnosti. S ní se musí dnes počítat všude tam, kde narůstá využívání výpočetních technologií a rozvíjí se informační průmysl. Počítačová kriminalita je jistě výrazným jevem dnešní doby, ale zájem o informace, byť byly zpracovávány, přenášeny a uchovávány jiným způsobem, je mnohem staršího data. Jen jsme byli zvyklí, a stále tak to i chápeme, tyto jevy nazývat jinými pojmy (vyzvídání, vyzrazování atd.), zejména podle způsobu uplatnění informací. To ostatně platí obecně dodnes. S postupně stále se rozšiřujícím zaváděním výpočetní techniky rostla a roste však míra jejího zneužívání a do jisté míry zastiňuje klasické formy práce s informacemi a jejich zneužívání. Počítačová kriminalita má řadu výrazných charakteristik, které ji odlišují od kriminality klasické. Ve většině případů počítačové kriminality se neobjevují takové prvky, jako je násilí, použití zbraně, újma na zdraví osob apod. Zatímco však u klasické kriminality se měří doba spáchání trestného činu na minuty, hodiny, dny, trestný čin v oblasti počítačové kriminality může být spáchán v několika tisícinách sekundy a pachatel ani nemusí být přímo na místě činu.

6.1 Hacker

Relativně samostatnou oblast v útocích proti programovému vybavení a datům uloženým v informačních systémech tvoří tzv. skupina ***"hackerů" - průnikářů***, *kteří se snaží obejít zabezpečení informačního systému a neoprávněně do něj vniknout*. Na začátku takového průniku je recese a touha dokázat, že hacker je "lepší" než použitý bezpečnostní systém.

Téměř „oficiální policejní definice“ Doc. Ing. Ivo Látala, CSc., z Policejní akademie České republiky, zní: „Hackeři (průnikáři) – osoby, které pronikají do ochraňovaných systémů, přičemž jejich cílem je prokázat své vlastní schopnosti, kvality, aniž by měly zájem získat informace nebo systém narušit. Hlavní je překonávat ochranné bariéry, což považují za zábavu, dobrodružství, provázené ‚sportovním nadšením‘, aniž by očekávaly osobní veřejné uznání. Stačí jim, jestliže se o jejich činu hovoří. Snad by vyhovovalo srovnání se žháři, kteří mají požitek z pozorování ohně, nebo se dokonce podílejí na jeho likvidaci.

Hackerství je jejich koníčkem, u počítačů vysedávají po dlouhý čas a získaná data nebo programy využívají spíše pro svoji potřebu nebo pro přátele.“

Činnosti, které pravý hacker provádí a kterými získává uznání a respekt, jsou:

- získání a zpřístupnění zdrojového kódu programů
- odhalení slabin informačního systému a zpřístupnění příslušných informací
- publikování užitečných informací na Internetu
- pomoc při administraci a provozu diskuzních skupin, seznamů mailů, archivů atd.
- pomoc při testování nových programů (tzv. beta verzí)

6.1.1 Typy útoků používané hackery

Jak je známo, hackeři (v dnešním slova smyslu) útočí na *vzdálené počítače či servery*, aby k nim získali aspoň nějaký přístup. Podívejme se tedy na krátký popis útoků, kterými hackeři zaměstnávají "nebohé" adminy.

- ***Brutal Force Attack - útok hrubou silou***

  Celkem snadný způsob útoku, i když časově nejvíce náročný. K útoku hrubou silou se využívá různé password crackery, jako třeba ***Hydra*** pro Linux, nebo např. **wwwhack** pro Windows. V podstatě jde o to, že tyto *"louskače hesel"* se vrhají na server a zkouší různé kombinace znaků jako hesla (či uživatelská jména), popř. berou hesla ze slovníku (-> wordlist attack). Slovníkový útok ale nezabere, pokud je daný uživatel dostatečně chytrý, aby si nedával hesla typu 'abcdefgh'.

  Pak zabere snad jen skutečný *brutal force attack*, který může trvat pekelně dlouho v případě silného hesla. Počítejte se mnou: vezměme jen klasickou anglickou abecedu malých písmen, tj. 25 znaků. Pokud máme desetimístné heslo, pak počet kombinací je 25^{10} = 95,367,431,640,625 možností, čili nějakých 95,4 biliard! A dejme tomu, že jsme na rychlé lince a hádáme 10 hesel za sekundu, to jest přibližně 95,4 biliard hesel za **302408 let**! Takže pokud nechcete předávat jedoucí počítač z generace na generaci, podívejte se po jiném útoku. (I když s rozvojem kvantových počítačů se tato rychlost o hodně zvyšuje. Ale to budete muset mít soubor s hesly v tomto počítači. A nebo zrychlit přenos dat sítí...

Tato metoda je celkem nebezpečná i v tom, že moderní systémy si takovéto útoky zaznamenávají do logů, protože jsou snadno vypátratelné.

- ***Útoky na hardware***

  Sem patří útoky jako ***sniffing, keylogging*** a podobné. ***Zkráceně - odchytávání dat***. Aby hacker mohl úspěšně odchytávat data, je pro něj důležité znát o daných počítačích či sítích co nejvíce. Zde se vyplatí investovat do bezpečnosti a používat přinejmenším šifrované spojení. A pokud se hacker dostane do prostor s počítači (viz výše), může to být úplná katastrofa. Takový hardwarový keylogger vypadá jako obyčejná redukce na klávesnici. A pokud vám přepne síťovou kartu do tzv. *promiskuitnho módu*, budete mít co dělat, abyste vypátrali děravé místo. Odposlouchávat se dá mnoha způsoby. K náročným způsobům, které asi mezi "obyčejnými" hackery nejsou využívány, patří třeba odposlech elektromagnetických signálů vydávaných klávesnicí po každém stisknutí klávesy či dokonce elmg. vyzařování monitoru! A když už máme útoky na hardware, proč by nemohly být:

- ***Útoky na software***

  Tyto útoky jsou velmi časté. Možná i nejčastější. Zde se využívá nedokonalosti programů či síťových protokolů k průniku do systému. Podívejme se na některé:

  - **Buffer overflow** - Asi *nejčastější typ chyby*, kterou využívají piráti. Princip je v tom, že máte rezervovanou pro proměnnou určitou paměťovou oblast a zapíšete do ní něco většího. To se "přečnívá", může být vykonáno jako příkaz. A toho už se dá pěkně zneužít...

  - **DoS** neboli Denial of Service = *odepření služby*. Skrze tento útok dochází ke zpomalení či až k úplnému odstavení počítače. Tyto útoky můžou být vedeny buď na síťové rozhraní počítače nebo na samotný počítač.

    - Mitnick Attack - tento útok moc typický a používaný není, ale přesto ho tu zmíním. Hacker se snaží uhádnout číslo paketu a podstrčit jiný se stejným číslem.

    Tak to byly některé typy útoků, které hackeři využívají. Samozřejmě zde nejsou všechny.Jak je známo, hackeři jsou tvorové vynalézaví a pokaždé najdou něco nového.

6.1.2 Sociální chování hackerů

Hackeři jsou spíše uzavření, nevynikají komunikativností, nejsou vhodní pro kolektivní práci. V pracovním kolektivu nebývají příliš oblíbení. Zaměstnavatel pro jejich výbornou znalost technologií trpí některé jejich výstřelky a dá se říci, že jsou na své pozici stabilizováni, nepočítá se ovšem s nimi na pozice vedoucích či manažerů. Hacker *neuznává nadřazené autority*, systémem nadřízenosti a podřízenosti v zaměstnání pohrdá. Hackeři rádi hrají počítačové hry, oblékají se především s ohledem na své pohodlí (nikoliv požadavky firmy).

6.1.3 Morální hodnoty hackerské komunity

Hackeři věří ve svobodu jedince a jsou ochotni pomoci jiným (na základě svého vlastního rozhodnutí). Elektronický svět je pro ně výzva a je zaplněn problémy, které čekají na pokoření (vyřešení). Hacker žádný problém neřeší dvakrát – jednou vyřešený problém již pro něj není zajímavou výzvou. Sdílení informací a ***know-how*** pro vyřešení problémů je nedílnou součástí hackerské komunity a přispět vlastním know-how je morální povinností pravého hackera. Svět hackerů je založen na reputaci. Nový člen komunity získá svoji pozici v této komunitě až poté, co projeví své schopnosti, ale také svoji ochotu podílet se na ideálech komunity hackerů. Hacker nebere, ale dává. Věnuje svůj čas, svoji kreativitu a výsledek svých znalostí ve prospěch vyřešení problémů.

Mezi nejznámnější hackery patří ***Kevin Mitnick***.

Velmi problematický je však *postih* takového průnikáře. Pouhý fakt, že nepovolaná osoba vnikla do systému, by byl obtížně kvalifikovaný jako trestný čin, k případné trestní postižitelnosti je důležité prokázání nějakého dalšího úmyslu. Pokud se však nezjistí a neprokáže, že informace byla použita anebo se její použití chystalo, je trestně právní postih průnikáře omezený. Je obecně známo, že mnozí průnikáři provozují svou činnost jako "koníčka", že proniknutí do systému berou jako určitou intelektuální výzvu, to vše bez hmotných nebo jiných ambicí.

Od skupiny "hackerů" se odlišuje jiná skupina, tzv. ***"crackeři"***, kteří se zabývají narušením ochrany programů (např. proti neoprávněnému kopírování). V literatuře jsou často tyto dva termíny zaměňovány i když zaměření každé skupiny je k jinému cíli. K tomu je třeba poznamenat, že osoba může být jak "hackerem", který se snaží vniknout do cizí databáze,

tak i "crackerem", který vymyslí a zrealizuje odblokování určitého programového vybavení. Činnost obou dvou skupin je však nepřijatelná a mnohdy porušuje platná zákonná ustanovení.

6.2 Cracker

Policejní definice (z již citované přílohy časopisu POLICISTA) zní: Crackeři, což jsou spíš patogenní osobnosti, jimž se nejedná jen o překonání ochranných překážek, ale po průniku různým způsobem nabourávají informační systémy, získávají data, aniž by snad měli zájem je využít pro svůj prospěch. Potěšení mají spíše z destrukce systému.

Crackeři mají ve skutečnosti velice často ***zájem* využít úspěch pro svůj prospěch** (šíření nelegálního software atd.) a mají potěšení z překonání ochranných překážek. Jen malá část skutečných crackerů vyhovuje policejní definici - tedy tomu, že motorem jejich akcí je pouze potěšení ničit. Nicméně jsou takoví a lze o nich tvrdit, že se pohybují ve své činnosti na hranici mezi crackery a hackery. Říká se mu zpravidla v hackerské komunitě ***samuraj.*** Pokud se tento útočník *naboural do systému a* následně vysvětlí správci, např. pomocí e-mailu ze superuživatelského accountu, jak k nabourání došlo a jak má správce tuto díru „záplatovat“.

Příkladem takové skupiny na hranici mezi hackery a crackery může být známá velice aktivní Československá skupina Binary Division, která se specializovala na pozměňování webů. V roce 2000 napadla například weby ISDN, stránky slovenského HZDS a web českého ministerstva vnitra. Její útoky ochromily i služby freemailových serverů Post v Česku i na Slovensku, členové skupiny napadli i České noviny a řadu dalších serverů.

6.2.1 Warez

Speciální podskupinou crackerů je skupina warez d00dz (dud – falešný, padělaný), která se zabývá *překonáním ochrany proti kopírování, úpravou komerčních programů, luštěním ochranných kódů a následnou distribucí nelegálního, copyrightem chráněného software*. Jednotlivé skupiny soutěží o prvenství v překonání překážek, kterými jsou hry, programy, CD atd. chráněny. Typické pro tyto skupiny je vytváření vnitřního hierarchického uspořádání a dělba úloh jednotlivých členů.

Skupiny *warez* si postupně vytvořily svůj vlastní jazyk, lépe řečeno slang.

Typické je zejména:

- ***náhrada písmene S za $*** : Compu$erve, Micro$oft; systematické nahrazení písmene 's' označujícího množné číslo písmenem 'z' (passwordz, passez, utilz, MP3z, distroz, pornz, sitez, gamez, crackz, serialz, downloadz, ...);
- ***použití zdůrazňující předpony k*** (snad jako kilo) (k-cool velice chladnokrevný, k-awesome – hrozně děsivý, k-korun – drahý);
- ***nahrazení o-0*** (c00l, l0zer, b00t, d00d …);
- ***vzájemná záměna ph a f*** (phone => fone, freak => phreak);
- ***používání znaků #!$ při doplňování textů*** ("Hey Paul!#!$#$!#!$");
- ***využívání fonetického čtení/zápisu*** (You are => u R, For You => 4U…);
- ***nadměrné používání VELKÝCH PÍSMEN;***
- ***pro českou komunitu je typické nepoužívání diakritiky a používání anglických*** (i méně obvyklých) ***zkratek***.

6.3 Rhybář a rhybaření (Phishing)

Těžiště zájmu rhybářů nejsou čísla telefonních karet, ale ***krádež obecnějších privátních citlivých informací patřících jedinci***. Těmito údaji mohou být především *údaje o platební kartě* (nejběžnější objekt zájmu) nebo *krádež přístupového jména a hesla*, s jejichž pomocí lze na dálku manipulovat s bankovním kontem. Hlavním metodou phishingu je sociální inženýrství a vzhledem k tomu proti němu vlastně neexistuje dobře fungující automatická ochrana. Nejčastěji je prováděn ***pomocí e-mailů*** (ale i pomocí falešných webových stránek), které vypadají naprosto legitimně a mají snahu vypadat oficiálně – správná adresa odesílatele (na první pohled), veškeré formální náležitosti jsou také splněny, a obsah, který vás žádá např. o potvrzení nebo doplnění vašich bankovních údajů… Pokud však odpovíte a do e-mailu vložíte svá data – jste chyceni do sítě rhybářů. ***Obraně proti phishingu je v současné době věnována značná pozornost***. Dokonce současný americký prezident Bush zařadil boj proti němu do svého volebního programu a slibuje podepsat návrh zákona určující mj. relativně přísný způsob potrestání pro každého, kdo vlastní cizí přihlašovací údaje s cílem způsobit trestný čin. Předpokládá zřejmě, že útočníci si to přečtou, zaleknou se a získaná data raději zničí.

6.4 Lama

Možná se vám stalo, že vás již někdo nazval lamou. Lamou rozumíme člověka, který je v nějakém určitém oboru nešikovný, začínající, vše kazící. Lama je počeštěná verze anglického výrazu lammer (resp. *lamer*). Původ označení *lammer/lamer* pravděpodobně vznikl ve skateboardovém slangu jako synonymum pro *luser* (pochází z loser = ztracená existence, poražený). Slovo lame má pak tyto významy: chromý, kulhavý, nepřesvědčivý, neuspokojivý, zchromit, zmrzačit..., ale v počítačovém slangu označuje především osobu, která získává ze ***serverů data, ale nikdy žádné nenahrává a nikomu neposkytuje***. Lammerem je v komunitě pohrdáno, je protikladným označením k pojmu **elita** nebo **guru** (komunitou uznávaný expert pro konkrétní oblast např. Linux, grafiku, …). Lamou jsou nazýváni také lidé, kteří se až moc často ptají na různé triviálnosti. Ale pozor – lamou můžou některé výše uvedené skupiny nazývat všechny ostatní, kteří nejsou přímo v jejich komunitě, a to bez ohledu na skutečné schopnosti takto označených.

Jak je z výše uvedeného textu patrné, není jednoduché se vyznat ve spletité síti hackerských vztahů, jejich skupin a na nich parazitujících a navazujících undergroundových a víceméně zločinných skupin. Nejčastější chybou médií je nesprávné a nespravedlivé použití pojmu hacker na všechny, kteří způsobují lidem a počítačovým firmám různé druhy ztrát (finanční, prestižní, …). Počítačová kriminalita může postihnout značnou šíři osobního i společenského života. Výpočetní technika je nasazena do řízení a správy státu, v armádě, policii, ekonomice, průmyslu i zemědělství, ve zdravotnictví a jinde.

7 BEZPEČNOSTNÍ POLITIKA

Základní otázky při tvorbě bezpečnostní politiky jsou :

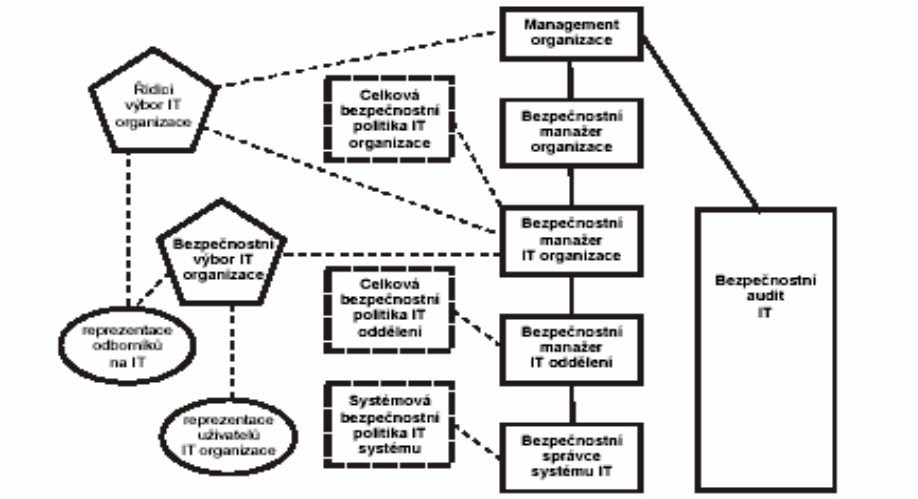
- *co vyžaduje ochranu.*
- *Proti jakým hrozbám je ochrana budovaná.*
- *Jak budeme chránit to, co vyžaduje ochranu.*

Dělení bezpečnostní politiky :

- ***Celková bezpečnostní politika IT.***
- ***Systémová bezpečnostní politika IT.***

7.1 Celková bezpečnostní politika IT

Uvádí specifikaci ***cílů zabezpečení, definici citlivých dat a klasifikaci těchto dat a definici ostatních citlivých aktiv IT a definici odpovědností za ně.*** Definuje bezpečnostní infrastrukturu organizace a potřebné síly mechanismů pro implementaci bezpečnostní funkčnosti. Specifikuje omezení, která musí bezpečnost IT organizace respektovat. Je vytvářena nezávisle na právě používaných informačních technologiích, a to v časovém horizontu obvykle pěti až deseti let. Celková bezpečnostní politika IT je ***veřejný závazný dokument přijatý vedením organizace*** jako vnitroinstitucionální norma. Jeho cílem je ochrana majetku, pověsti a činnosti organizace. Musí být úplný (otázky a konflikty lze vyřešit odkazem na jeho paragrafy), stručný a srozumitelný. Musí jasně stanovit hierarchické vazby odpovědností a pravomocí, specifikuje povinnosti a práva jak pro lidi, tak i pro data.



Obr.6. Přehled bezpečnostní infrastruktury IT organizace

Generické role *bezpečnostní infrastruktury organizace*, které uvedený obrázek odpovídá, lze charakterizovat následující výčtem:

- ***Bezpečnostní výbor IT organizace***

- řeší interdisciplinární problémy bezpečnosti IT;
- dává řídicímu výboru organizace odpovědnému za používání IT strategické podněty k řešení z hlediska bezpečnosti;
- formuluje bezpečnostní politiky, získává jejich schválení od řídícího výboru organizace odpovědného za používání IT;
- definuje bezpečnostní program a monitoruje jeho implementaci;
- schvaluje administrativní opatření a přijaté standardy;
- dozoruje implementace bezpečnostních programů podle systémových bezpečnostních politik;
- hodnotí účinnost bezpečnostních politik;
- prosazuje zvyšování bezpečnostní uvědomění;
- doporučuje potřebné zdroje (lidi, peníze, znalosti atd.).

- ***Bezpečnostní manažer IT organizace***

- jednoznačně stanovená role s *odpovědností za bezpečnost IT* organizace;

- spolupracuje s bezpečnostním výborem IT organizace a je jím metodicky řízen;

- řídí implementaci bezpečnostních programů;

- jedná se o hlavní řídicí orgán v oblasti udržování bezpečnosti IT v rámci organizace, metodicky řídí bezpečnostní správce systémů IT.

- ***Bezpečnostní správce systému IT***

- *výkonný bezpečnostní orgán;*

- spolupracuje s bezpečnostním manažerem IT organizace a je jím metodicky řízen;

- odpovědný za provozování bezpečnostních funkcí podle systémové bezpečnostní politiky;

- vyšetřuje bezpečnostní incidenty a reaguje na ně;

- může být sdruženou rolí s rolí administrativní správy systému.

- ***Bezpečnostní auditor IT***

- *kontrolní orgán.*

7.1.1 Dokumentace celkové bezpečnostní politiky IT

Dokument lze zpracovat podle následující osnovy:

- ***popis organizace o poslání a koncepcí IT organizace***

  Stručně se popisuje *poslání organizace a funkce IS* v organizaci, uvádějí se výsledky analýzy závislosti organizace na jejím IS a analýza právní stránky problematiky. Dále se popíše skutečné, tj. stávající provozní prostředí a předpokládané provozní prostředí chráněné vypracovávanou bezpečnostní politikou. Uvedou se dosud stanovené zodpovědnosti a pravomoci, stávající bezpečnostní struktura organizace. Důležité jsou *výsledky analýzy dat zpracovávaných IT organizace*, zvláště pak určení citlivých informací a míry jejich ochrany – klasifikace. Popisují se služby IT dostupné uživatelům a specifikace aplikačních rozhraní z hlediska bezpečnosti, síla

dosud používaných ***bezpečnostních mechanismů***. Pro celkovou bezpečnostní politiku jsou důležité závěry analýzy personální otázky bezpečnosti, charakteristiky uživatelů, manažerů a správců IS. Definuje se provozní dokumentace a popisují se netechnická bezpečnostní opatření, administrativní, fyzická, personální a jiná aplikovaná opatření.

- ***Rámcový plán a harmonogram vybudování celkové bezpečnostní politiky***
- ***Cíle celkové bezpečnostní politiky***

  Uvedou se explicitně vyjmenované bezpečnostní cíle v pojmech *důvěrnosti, integrity, pohotovosti, autenticity, odpovědnosti, spolehlivosti aktiv a informačních technologií* organizace.

- ***Specifikace potřebné struktury zodpovědnosti a pravomocí***

  Vypracování bezpečnostní infrastruktury organizace včetně rolí, funkcí, odpovědností a povinností pracovníků (správců / administrátorů).

- ***Identifikace (kritických) aktiv, zvláště pak citlivých dat***
- ***Identifikace obecných hrozeb***
- ***Výsledky orientační analýzy rizik***
- ***Popis stávajícího stavu zabezpečení***
- ***Cíle a strategie havarijních plánů***
- ***Doporučení, jak dosáhnout bezpečnostních cílů***
- ***Omezení respektovaná bezpečnostní politikou***

  Popisují se návaznosti na relevantní zákony (ČR, EU …), vyhlášky a předpisy, včetně analýzy práv a povinností v oblasti nakládání s informacemi, návaznosti na relevantní mezinárodní a národní normy bezpečnosti IS a doporučení.

- ***Časové plány implementace a pravidelných akcí, revizí/oprav***
- ***Návrh a koncepce programu školení a osvěty***

  Cílem je založit program školení a osvěty v oblasti bezpečnosti IS specifický pro organizaci. Školení bývají typicky realizována alespoň počátečně z části i spoluřešiteli bezpečnostní politiky. Program musí být konzistentní s celkovou i

systémovou bezpečnostní politikou a musí napomoci jejich prosazování. Systém kursů musí pokrýt všechny úrovně pracovníků organizace od vrcholového managementu až po koncové uživatele.

7.2 Systémová bezpečnostní politika IT

Definuje ***způsob implementace celkové bezpečnostní politiky IT v konkrétním informačně technologickém prostředí***. Vypracovává se obvykle pro *časový horizont dvou až pěti let.* Stanovuje soubor principů a pravidel pro ochranu IS (proto se o ní hovoří rovněž jako o *bezpečnostní politice IS*) a jím poskytovaných služeb, zabývá se volbou konkrétních technických, procedurálních, logických a administrativních bezpečnostních opatření v závislosti na konkrétních IT a částečně i volbou fyzických a personálních bezpečnostních opatření, pokud tyto mohou ovlivnit bezpečnost IS. Implicitně se zabývá *bezpečností elektronické (počítačové) části* IS. Bezpečnost neelektronické části IS řeší tam, kde by neelektronická část IS mohla výrazně ovlivnit bezpečnost elektronické části. Vše řeší v harmonické návaznosti na již existující a prosazovaná bezpečnostní opatření.

Systémová bezpečností politika IT konkrétně sděluje:

- ***jak chránit (organizovat a distribuovat) konkrétní aktiva***
- ***stanovuje konkrétní bezpečnostní cíle***
- ***vyjmenovává konkrétní hrozby zjištěné analýzou rizik***
- ***definuje konkrétní bezpečnostní opatření, tj. funkce prosazující bezpečnost*** – autorizace, autentizace, audit, klasifikace dat, řízení přístupu apod., které jsou již implementovány nebo se musí implementovat.

Systémová bezpečnostní politika IT musí být v *souladu s celkovou bezpečnostní politikou* organizace a s celkovou bezpečnostní politikou IT organizace, musí respektovat současný stav provozovaného systému i jeho plánovaných rozšíření. Z celkové bezpečnostní politiky IT přebírá stanovení kategorie minimální síly bezpečnostních mechanismů a konkrétně definuje, jak implementovat bezpečnostní funkce.

Pokud je organizace nebo její IS příliš rozsáhlý a různorodý, je vhodné vypracovat samostatně systémovou bezpečnostní politiku fyzické ochrany, systémovou bezpečnostní politiku

technické ochrany (elektronika, software), personální systémovou bezpečnostní politiku, komunikační systémovou bezpečnostní politiku atd.

Generickou strukturu dokumentu, který je prezentací systémové bezpečnostní politiky a výchozím materiálem pro zahájení její implementace do bezpečnostního programu, přibližuje následující osnova:

- ***Analýza současného IS respektující použité IT.***
- ***Výsledky analýzy rizik IS.***
- ***Výsledky analýzy zranitelných míst IS.***
- ***Popis hrozeb pro IS.***

  Aby se zajistilo, že popis hrozeb bude vyčerpávající, je vhodné postupovat podle předem stanoveného systému. Může se použít aplikačně orientované třídění (ztráta důvěry, odposlech, zlomyslný operátor, modifikace dat, maškaráda, zneužití autorizace...) nebo generické třídění podle nějaké normy (třídění podle použitých bezpečnostních funkcí):

- ***Technická bezpečnostní politika.***

  Uvádí se konkrétní zákony, standardy, normy, pravidla, použité praktiky pro řízení zpracování citlivých informací, pro používání hardwaru, pro používání softwaru, de jure a de facto normy.

- ***Personální bezpečnostní politika.***
- ***Administrativní bezpečnostní politika.***

  Uvádí se soubor vnitroorganizačních norem a předpisů.

- ***Udržovatelnost IS z hlediska bezpečnosti.***

  Jedná se o výčet *kritických činností* a odpovídajících opatření pro akce typu registrace uživatelů, inovace softwaru apod.

- ***Formální model bezpečnosti IS.***

  Uvádění formálního modelu je volitelné podle toho, zda se požaduje odpovídající úroveň zaručitelnosti bezpečnosti IS.

- ***Definice souboru relevantních bezpečnostních opatření.***

  Uvádějí se specifikace bezpečnostních funkcí zabezpečovaného IS včetně identifikace jimi pokrývaných hrozeb.

- ***Použité bezpečnostní mechanismy.***

  Vhodně systematicky tříděný výčet, např. podle kategorií – *logické, technické, fyzické bezpečnostní mechanismy*.

- ***Havarijní plán.***

- ***Bezpečnostní dokumentace.***

- ***Plán implementace systémové bezpečností politiky, bezpečnostní program*.**

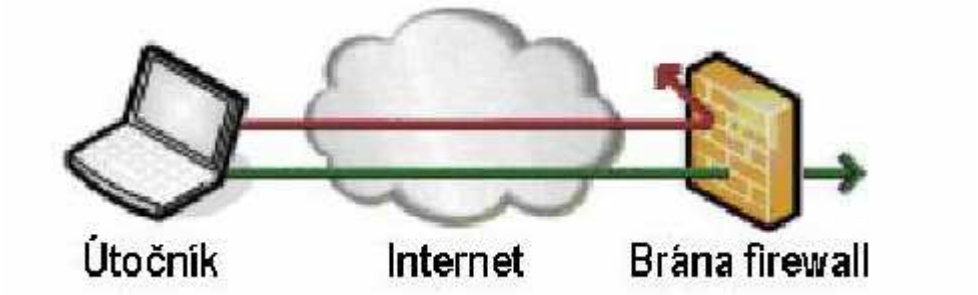
  Uvádějí se detailní pracovní plány implementace přijatých bezpečnostních funkcí, priority, náklady a časové plány, specifikace projekčních aktivit (závazné zdroje a odpovědnosti, kontrolní dny, zprávy o stavu řešení, oponentury). Součástí bezpečnostního programu je plán školení pro celý tým IT organizace, kam patří vývojáři IS, provozní pracovníci, bezpečnostní manažer, bezpečnostní správci, pracovníci odpovědní za autorizaci ostatních pracovníků, koncoví uživatelé atd. Stanovují se provozní a správní procedury a podmínky akreditace bezpečnostního programu, tj. připraví se hodnocení jeho implementace.

Proces tvorby bezpečnostní politiky není jednorázový. Dobrá bezpečnostní politika nikdy nevzniká jednorázovou akcí, neboť se mění chráněná aktiva, mění se informační technologie, mění se motivace a zkušenosti útočníků atd. Životní cyklus tvorby bezpečnostní politiky lze zjednodušeně vyjádřit následujícími (opakovaně) prováděnými kroky -

- ***posouzení vstupních vlivů;***
- ***analýza rizik***;
- ***vypracování bezpečnostní politiky;***
- ***implementace bezpečnostní politiky;***
- ***nasazení bezpečnostní politiky, kontrola její účinnosti a vyslovování závěrů.***

7.3 Deset kroků k vyššímu zabezpečení

- Používání brány firewall pro připojení k Internetu
- Instalování aktualizace
- Používání aktuálního antivirového softwaru
- Používání silných hesel
- Zajistění fyzického zabezpečení
- Opatrné procházení webu
- Používání e-mailu bezpečně
- Pravidelné zálohování a provádění obnovy
- Bezpečné připojení vzdálených uživatelů
- Zabezpečení bezdrátové sítě



Obr.7. Brána Firewall

ZÁVĚR

V současnosti jsme svědky bouřlivého rozvoje výpočetní techniky. Ten, kdo sleduje novinky z oblasti informatiky, mi jistě dá za pravdu. Při některých činnostech si již ani nedovedeme představit, že bychom se bez této techniky mohli obejít, natož jaké možnosti nám její rozvoj ještě přinese. V počítačových systémech jednotlivých institucí se soustřeďují informace ze všech oblastí života společnosti i jednotlivce. Proto poškození funkce počítačových systémů, nejen celostátně budovaných, ale i lokálních, může vést k dezorganizaci v mnoha sférách lidské činnosti. Nezanedbatelné je také stále vzrůstající využívání soukromých osobních počítačů a jejich zapojení do počítačových sítí. Prostřednictvím počítačů je možné sledovat informace, vyhodnocovat získané informace, dotazovat se v mnohdy rozsáhlých informačních databázích, které mohou být navíc vzájemně propojeny. V současné době není žádnou zvláštností přenos informací mezi jednotlivými státy a mezi jednotlivými kontinenty.

Pod názvem mé bakalářské práce „Význam IT v průmyslu komerční bezpečnosti“, si možná každý představí něco trošku jiného, neboť se jedná o velice obsáhlé téma, které není blíže specifikováno. Já jsem se rozhodla tuto práci směřovat především k ochranně informačních systému a dat. Mým cílem bylo poukázat na jejich důležitost v životě každého z nás. V jednotlivých kapitolách jsem chtěla široké veřejnosti srozumitelnou formou nastínit problematiku šifrování, eletronického podpisu, identifikačních systémů jako jsou hesla, magnetické nebo čipové karty či biometrie. Rovněž jsem jsem se zabývala zabezpečením informačních technologií v organizacích a blíže je popsala v 7. kapitole.

Využívání služeb jako je internet nebo platební karty se stalo běžnou součástí našeho života, aniž bychom si uvědomovali, jak dlouhý a složitý vývoj za nimi stojí.

SEZNAM POUŽITÉ LITERATURY

[1] HANÁČEK P., STAUDEK J.: Bezpečnost informačních systémů, Úřad pro státní informační systém, 2000, 127 s.

[2] JAŠEK, R.: Ochrana znalostí a dat v podnikových informačních systémech, Skripta FAME – UTB ve Zlíně, 2000, 115 s.

[3] DOBDA L.: Ochrana dat v informačních systémech, GRADA, 1998

[4] Kriminalistika (Čtvrtletník), Ministerstvo vnitra ČR [online]. [cit. 1998-2005]. Dostupné z http://www.mvcr.cz/casopisy/policista/prilohy/pc_krimi.html

[5] Specialista, ISSN 1801-4739 [online]. [cit. 2005-2006]. Dostupné z http://www.specialista.info/search.php?rsvelikost=sab&rstext=all-phpRS-all&rstema=10

[6] Camo spol. s r.o.: Bezpečnost IT – Autentifikace [online]. [cit. 2006]. Dostupné z http://www.camo.cz/descr.php?id=ajc

[7] Wikipedia.: Kryptografie [online]. [cit. 2006]. Dostupné z http://cs.wikipedia.org/wiki/%C5%A0ifrov%C3%A1n%C3%AD

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES Advanced Encryption Standard

CRYPT Varianta DESu

DEA - 1 Data Encryption Standard

DES Data Encryption Standard

DESX Varianta DESu

DSA Digital Signature Algorithm

GDES Generalizovaný DES

IS Informační systémy

IT Informační technologie

PC Personal computer

PIN Personal Identification Number

RAM Random Acces Memory

ROM Read Only Memory

RSA Rivest Shamir Adleman

RSA Rivest Shamir Adleman

SWIFT Society for World – Wide Interbank Financial Transfers

Triple DES trojnásobný DES

Firewall Zařízení (hardwarové, softwarové), které různým způsobem zajišťuje PC, popř. síť před vnějším světem (např. chrání data, přístup na zařízení atd.)

SEZNAM OBRÁZKŮ