Univerzita Karlova v Praze
Filozofická fakulta
Ústav informačních studií a knihovnictví

Diplomová práce

2011 **Bc. Martina Knopová**

Univerzita Karlova v Praze
Filozofická fakulta
Ústav informačních studií a knihovnictví

Studijní program: informační studia a knihovnictví
Studijní obor: informační studia

Bc. Martina Knopová

Bezpečnost dat v informačních systémech

Diplomová práce

Praha 2011

Vedoucí diplomové práce: PhDr. Jan Pokorný, PhD.

Oponent diplomové práce:

Datum obhajoby:

Hodnocení:

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracovala samostatně a že jsem uvedla všechny použité informační zdroje.

V Praze, 7. ledna 2011

……..

podpis diplomanta

Poděkování

Děkuji svému vedoucímu práce PhDr. Janu Pokornému Ph.D. za cenné rady a připomínky.

Identifikační záznam

KNOPOVÁ, Martina. *Bezpečnost dat v informačních systémech [Data security within information systems]*. Praha, 2010. 80 s. Diplomová práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví 2010. Vedoucí diplomové práce PhDr. Jan Pokorný, Ph.D.

Abstrakt

Práce je zaměřena na zanalyzování současných autentizačních metod. Kromě popisu obecných principů je kladen důraz na podrobnou analýzu a přehled implementačních specifik. První část práce popisuje vymezení základních pojmů v oblasti bezpečnosti dat. Hlavní část práce je věnována problematice logické vrstvy ochrany dat – zejména možnostem zabezpečení autentizace uživatelů v informačních systémech. Dále se práce zabývá přehledem a srovnáním tří autentizačních metod. Každá metoda je podrobně popsána, je brán zřetel na možnost budoucího vývoje dané metody. Klíčové kapitoly jsou věnovány jednotlivým autentizačním a obranným mechanismům. Samostatná kapitola je věnována současným bezpečnostním opatřením – zabezpečení autentizačních operací, kryptografickým systémům a jejich principům. Pro praktickou představu byla provedena SWOT analýza jednotlivých metod. Závěr práce shrnuje poznatky získané z analýzy jednotlivých popsaných autentizačních metod a navrhuje adekvátní řešení pro autentizaci uživatelů.

Abstract

The thesis aims on analysis of contemporary authentication methods. Besides description of global principles the emphasis is placed on detailed analysis and summary of implementation specifics. The first part of the document reports on determination of element concepts within

the area of data security. The fundamental part is devoted to problems of logical layer in data security - especially the possibilities of users' security in information systems. The thesis is also providing the reader with summary and comparison of three authentication methods. Each chapter is described in deep detail with consideration the possibilities of future development of specific methods. Key chapters are focused on particular authentication and defensive mechanisms. Separate chapter is analyzing recent safety measures - security of authentication operations, cryptographic systems and their principles. As a practical example SWOT analysis of individual methods was performed. The last part is summarizing the observations achieved while analyzing particular authentication methods described. As a conclusion the author suggests adequate solutions for user authentication.

Obsah

1. ÚVOD DO PROBLEMATIKY

Cloud Computing[1], virtualizace[2], Web 2. O[3], crimeware[4], spam[5], open-source[6], intrenet fraud[7] - toto jsou jenom některé z trendů, kterými se dnes žije v oblasti informační bezpečnosti. Tuto bezpečnost neurčuje zpravidla jediný trend, ale v oblasti ICT musíme být ve střehu na mnoha frontách. Navíc doznívající hospodářská recese zvýšila ještě hodnotu elektronických dat a zveřejnění tajných depeší amerického velvyslaneckého imperialismu a jejich následné využití ve světové politice, tedy bezpečnost důležitých dat má významné slovo i ve světových otázkách. Organizace vládní i nevládní myslí na svou budoucí stabilitu, chrání se před interními a externími hrozbami, kyberteroristické a hackerské útoky jsou na denním pořádku v souvislosti s průmyslovou špionáží.

Zatímco dříve patřila bezpečnost spíše k upozaděným složkám systému, dnes se jedná o alfu a omegu informačních systémů. A to především díky nepřiměřené legislativě, ostrému konkurenčnímu boji, problémům s etickými a ekonomickými škodami způsobenými úniky dat. V současnosti se dynamicky vyvíjejí jednak způsoby obrany a útoků, identifikují se

---

[1] Fenoménem dnešní doby je jednoznačně Cloud Computing. Sdílení hardwarových a softwarových prostředků pomocí sítě. Je jedním z nejdiskutovanějších témat v IT bezpečnosti současné doby. Definice: „přesunující data, aplikace či služby do internetu. Vychází z logiky, že lokální uživatelé (ať již osoby či organizace) nemusí znát technické detaily, navíc se o systémy starat – mohou být skutečně jen uživateli. Myšlenka je revoluční a otevírá úplně nové možnosti v ICT. Často však naráží na nevyřešené bezpečnostní problémy.

[2] "Virtualizací" se v prostředí počítačů označují postupy a techniky, které umožňují k dostupným zdrojům přistupovat jiným způsobem, než jakým fyzicky existují, jsou propojeny.

[3] "Web 2.0 "není jednoznačný pojem. Jedna definice říká, že "web 2.0" je důsledkem nových technologií, a bývá charakterizován jako posun od centralizovaného zpracování/služeb k decentralizaci. Jiná definice říká, že "Web 2.0" je přeměna webu dokumentů na web dat, v platformu pro sdílení dat. Pojmem "Web 2.0" se rozumí nová generace webu, která se vyznačuje prvky parcticipace, konvergence atd.

[4] "Crimeware" jsou zkrátka programy sloužící k odcizování dat, k rozesílání spamu (i z „unesených" počítačů), k monitorování systémů, k průmyslové špionáži, ke krádežím přístupových hesel – a k desítkám dalších činností, které jsou nebo mohou být zneužity k počítačové kriminalitě.

[5] "Spam" je nevyžádané sdělení (nejčastěji reklamní) masově šířené internetem.

[6] "Open-source" je skupina aplikací a operačních systémů, které jsou šířeny bezplatně včetně svého zdrojového kódu.

[7] Termín "Internet Fraud" česky "Internetový podvod" obecně se odkazuje na nějaký druh podvodu, který používá jednoho nebo více online služeb, aby předložila podvodné výzvy k potenciálním obětem, k provedení podvodné transakce.

původy hrozeb a kyberteroristických útoků, analyzuje se množství škodlivých kódů, diferencují se způsoby na zajišťování webové bezpečnosti, shrnují se pozitiva i negativa a společnost se zaměřuje na problematiku ztráty elektronických dat více než kdykoliv předtím. Navíc stále více na významu nabývá problematika škodlivých kódů v informačních sítích, problematika Web 2.O, služeb a fungování moderních webových aplikací, které přinášejí naprosto *novou zkušenost* s různými formami útoku. Stejně tak otázka virtualizace[8] dnes hýbe světem, proto bezpečnost dat v informačních systémech nezůstává jenom otázkou pracovníků v ICT, ale rovněž se stává vysoce řešenou prioritou ve vysoké management, sociologů a rovněž i informační vědců.

Je nesporné, že otázka bezpečnosti dat se velmi zvýšila s nárůstem konceptu "Webu 2.0", který souvisí s obrovským nárůstem uživatelské základny, především v aplikacích sociálních sítí, které se staly novou platformou pro útoky počítačových zločinců. Web 2.0 s počtem svých uživatelů, interaktivním obsahem se stal sociální platformou pro kyberteroristické útoky počítačových zločinců. Interaktivní obsah, sociální sítě s otevřenou propojenou komunitou lidí a skupin nabízí útočníkům nový prostor pro šíření počítačových útoků prostřednictvím *nových kanálů* a také umožňuje provádět útoky *sociálního inženýrství* za účelem profilace a krádeže identity, které představují významné ohrožení informační bezpečnosti.

Dalším důvodem, proč se zabýváme problematikou bezpečnosti dat, je *vzestup* cílených útoků na jednotlivá zařízení, neboť významně narůstá počet nových hrozeb, které jsou stále významnější v jejich komplexnosti, složitosti a kriminálním úmyslu.

Organizace soukromé i veřejné stále více akcelerují na outsourcing, cloud technologie a mobilní řešení. Důležitým vedlejším účinkem zároveň ale je, že více dat je vystaveno *ztrátě* nebo *krádeži.* Tato témata jsou dokonce tak aktuální a dynamická, že se v současnosti probírají témata aktuálními, netradičními a netypickými hrozbami, např. od nových metod pishingu[9] (whaling, TagNabbing) přes nebezpečné bezpečnostní programy, hardwarovou špionáž na úrovni výrobců, až po nebezpečné geografické lokace. Kybernetiční útočníci totiž

[8] Někteří ji považují za řešení bezpečnostních problémů. V otázkách dnešní informační bezpečnosti řešíme virtualizaci jako jedno z hlavních řešení bezpečnostních problémů.

[9] „Pishing" je podvodná technika používaná na internetu k získávání citlivých údajů (hesla, čísla karet)

velmi rychle chápou význam *nových technologií,* jako je Cloud computing a virtualizace, jako využití pro svoji činnost. Dále jsou velmi aktuální otázky monitoringu, které mají velký přesah do legislativy a právních norem. Rozebírají se i nové technologie pomocí těch klasických, jako je např. VPN, IDP či antivirová ochrana, filtr spamu či obsahu. [10]

Informační bezpečnost hýbe světem, s tím jak jsme čím dál více závislí na informačních systémech a jejich provozování. Pojmy, jako "kontinuita provozu", "řízení identit", ochrana před automatizovanými útoky, se stávají a budou stávat čím dál více aktuálními. Jedním z nejžhavějších problémů dnešní společnosti je ochrana před falšováním identity, kde se subjekt vydává za někoho, kým ve skutečnosti není, řeší se tedy otázka *identity člověka* a její bezpečné prokázání na poli bezpečnostních informačních systémů dneška. Řešíme v podstatě *identifikaci jedince* pro provedení různých operací v systémech, neboť máme v rukou ohromně silnou zbraň, která ve „*virtuálním prostředí"* předkládá reálné informace. Zatímco v reálném světě prokazujeme svoji identitu svým vzhledem nebo identifikačním dokumentem. Ve virtuálním světě vycházíme z toho, že nějaký v podstatě *neznámý subjekt* se pokouší prokázat svoji *identitu* a vyžaduje své systémové nároky. Zvláště nyní, kdy je riziko neautentizovaného přístupu k datům stále vyšší, neboť se zvyšuje okruh osob, které mohou mít přístup k těmto datům. Tedy jakákoliv entita, kterou se pokoušíme zařadit ve virtuálním světě, musí mít svou reálnou identifikaci, neboť neexistuje *jiný* způsob určení *totožnosti.* Dalším problémem těchto systémů je jejich *spolehlivost.* Jde zde především i o to, kdo bude *vlastníkem* mojí *identity.*

Z výše uvedených důvodů je bezpečnost informačních systémů velmi širokou oblastí sofistikovaných řešení v dané problematice, funguje na mnoha přístupech a metodách. V druhé kapitole práce budou jasně definovány cíle této diplomové práce. Třetí kapitola bude pojednávat o použité metodologii a informačních zdrojích. Následující kapitola vysvětlí a definuje pojem bezpečnosti v širších souvislostech a provede základní členění jejích forem. Pátá kapitola bude věnována právní úpravě týkající se bezpečnosti dat v národních a mezinárodních souvislostech a bude rovněž představen moderní koncept ochrany soukromí. Sedmá kapitola řeší problém ochrany dat v informačních systémech a rozděluje jednotlivé

[10] Zvláště se klade důraz na bezpečnostní monitoring sítí v kontextu s podezřelými jevy a událostmi, které mají vysokou schopnost odhalit slabá místa systému nebo neznámé útoky.

způsoby ochrany dat. V osmé kapitole se problém ochrany dat zužuje na ochranu logického přístupu k datům – neboť tato oblast tvoří klíčovou a kontrolní část zabezpečení celého systému. Devátá kapitola představí základní rozdělení autentizačních metod v informačních systémech. Desátá, jedenáctá a dvanáctá kapitola je věnována analýzám jednotlivých typů autentizace a představuje její specifika. Třináctá kapitola představuje konkrétní technologie na zabezpečení autentizačních metod. Čtrnáctá kapitola se věnuje problematice kryptování, neboť většina chráněných operací s daty v informačních systémech je chráněna touto technikou. Patnáctá kapitola popisuje možnosti elektronických certifikátů a představuje její dvě hlavní funkce v oblasti bezpečnosti dat. Šestnáctá kapitola je praktickou analýzou popsaných autentizačních technologií a provádí komparaci jednotlivých autentizačních metod a představuje aplikaci získaných poznatků. Cílem této kapitoly je podat souhrnný přehled o racionálním uplatnění získaných poznatků z provedených analýz.

Soupis využitých zdrojů je obsažen v Seznamu použitých zdrojů, který byl vytvořen dle pravidel převzatých z norem ISO 690 a ISO 690-2. V textové části práce je citováno podle prvního údaje záznamu a data vydání, tzv. "Harvardským systémem".

2. CÍLE PRÁCE

Cílem diplomové práce je popsat a zhodnotit problematiku bezpečného uložení dat v informačních systémech. Práce se zaměřuje zejména na problematiku přístupu k *logické vrstvě* ochrany dat. Autentizace uživatelů, o které pojednává tato práce, je *klíčovým prvkem* zabezpečeného přístupu do informačních systémů. Tato práce se zabývá konceptem autentizace, neboť se jedná o hlavní kontrolní složku logického přístupu k datům v informačních systémech. Autentizace se zde řeší proto, poněvadž představuje *nejčastější* hrozbu útoků na tyto bezpečnostní mechanismy a v současnosti je stále více oblíbenou součástí mnoha portálů a webových aplikací. Dále je zaměřena na analýzu jednotlivých metod autentizace uživatelů. Jedním z dílčích cílů je seznámení uživatelů se základními nejběžnějšími používanými autentizačními metodami v informačních systémech, a to především z pohledu jejich fungování a vlivu na bezpečnost. Popsány jsou tři metody autentizace pomocí hesel, autentizačních tokenů a biometrik. Jádrem je přehled autentizačních metod a jejich porovnání. U každé autentizace jsou zmíněny možnosti obrany proti automatizovaným útokům a dalším bezpečnostním a konfiguračním chybám. Jsou zde zahrnuty ty nejčastější a nejkritičtější problémy, se kterými se v praxi setkáváme. Dále je práce zaměřena i na nové technologie zpracování dat, jejich využití, srovnání výhod a nevýhod, především se soustředí na platformu moderních kryptografických metod (ochrany dat), která je predikována jako příslib do budoucnosti v ochraně dat. [11] Taktéž kromě jiných ukazuje biometrické systémy ochrany dat, o kterých se mluví jako o ochraně dat budoucnosti. Práce je zaměřena na *logické* metody pro autentizaci uživatelů v informačních systémech. Práce není zaměřena na *fyzické* (úroveň hardware a zálohování dat) ani *organizační* (doplňková snaha o ochranu systému). V této práci bych ráda uvedla a srovnala autentizační metody uživatelů v informačních systémech, což spadá do logické vrstvy bezpečnosti. *Fyzickou* ani *organizační* úrovní zabezpečení dat se tato práce zabývat nebude.. Tato práce se snaží zohlednit její základní *jádro* fungování a popsat jednotlivé technologie a principy. Práce se v první části zabývá širokou problematikou ochrany dat, soustřeďuje se na dvě klíčové oblasti vstupního získání dat – autentizace V první fázi řízení přístupu ke všem informačním

[11] Máme na mysli nové možnosti v prostředcích moderní kryptografie, která jsou založena na PKI (Public Key Infrastructure)

systémům je jeho správné nastavení.

3. METODOLOGIE A INFORMAČNÍ ZDROJE

Slovo „metoda“ pochází z řečtiny - „meta hodos“ a znamená způsob, jak dosáhnout nějakého teoretického i praktického cíle zkoumání. (např. experimentování, inovační metoda apod.). Z principů a zásad metody umožňuje získání konkrétních údajů o zkoumaných jevech.

Metody vědecké práce můžeme rozdělit do dvou skupin:

1. Metody empirické – jedná se o metody, kterými je možno zjistit konkrétní jedinečné vlastnosti nějakého objektu či jevu. Patří mezi ně – např. pozorování, měření, experimentování.

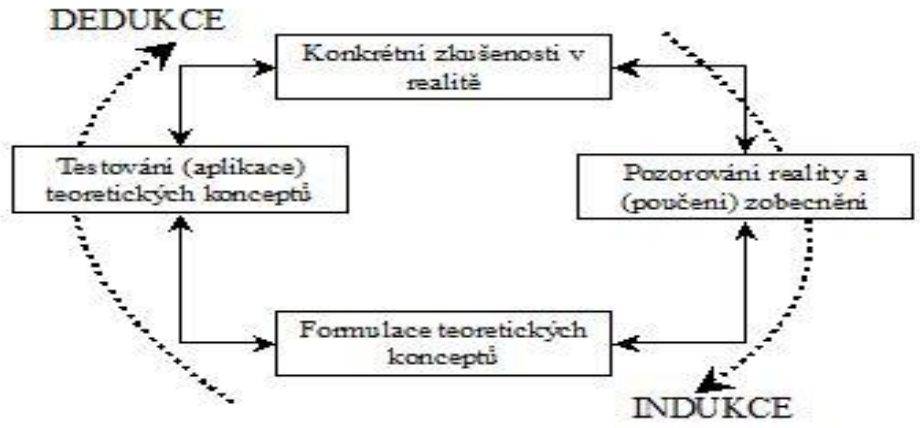
2. Metody logické – zahrnují množinu metod využívajících principu logiky a logického myšlení. Patří k nim např. analýza, syntéza, indukce, dedukce.

V této diplomové práci využívám jak metody empirické, tak metody logické. Z empirických metod je použita výsledná SWOT analýza současně používaných technologií, kde je každá technologie podrobně popsána, znázorněna pomocí tabulek a grafů a nastíněny jsou možnosti vývoje dané technologie. Metoda SWOT analýzy je použita pro sběr a komparaci dat potřebných pro analýzu jednotlivých technologií.

Z *logických* metod jsem si vybrala a používám metody *identifikace, analýzy a dedukce* a deskriptivního přístupu. Metoda identifikace je v práci použita při rozpoznání současných autentizačních metod v současnosti používaných v informačních systémech.

Analýza je proces faktického nebo myšlenkového rozčlenění celku (jevu, objektu na určitou část) a zahrnuje rozbor vlastností, vztahů, faktů, vlastností jevů a procesů a umožňuje rozlišit podstatné od nepodstatného. Jedná se též o proces odhalování nových vztahů a zákonitostí. V práci jsem provedla analýzy *autentizačních* metod uživatelů v oblasti *vstupního* zpracování dat přístupu do informačních systémů.

Dedukcí rozumíme logické vyhodnocování a vyvozování závěrů a jejich testováním v realitě se získávají nové znalosti a zkušenosti. V této práci dedukce používám zejména při vyvozování závěrů z provedených analýz.



Obr. č.1 - Kolbův experimentální cyklus

Tématem bezpečnosti dat v různých aplikacích, použitích vhodných autentizačních metod, se zabývá řada konferencí. Jelikož se jedná často o mezinárodní konference, hlavním jednacím jazykem je angličtina. Výstupy z nich jsou zpřístupněny převážně jako sborníky z konferencí v anglickém jazyce nebo přímo ze soukromých prezentací zúčastněných.

V rámci České republiky proběhla konference CYBER „Kybernetické výzvy a hrozby“ organizované ministerstvem zahraničních věcí, kde se sešli bezpečnostní experti z České Republiky, Francie a Spolkové republiky Německo. Aby sdíleli své zkušenosti, poznatky z oblasti informační bezpečnosti a zaměřili se na interdisciplinární spolupráci mezi specialisty informačních a komunikačních technologií.

Další konferencí, která se uskutečnila v ČR v roce 2010 - konference s názvem „Trendy v internetové bezpečnosti“ pořádaná čtyřmi významnými internetovými servery Konference Security 2010, z dalších např. Security Upgrate 2010. Z dalších pak konference zabývající se jednotlivými odvětvími bezpečnosti, např. konference Cloud Computing atd.

4. POJEM BEZPEČNOST A ZÁKLADNÍ ČLENĚNÍ JEJÍCH FOREM

Pod pojmem bezpečnost rozumíme obvykle ochranu odpovídajících informačních systémů a informací, které jsou v nich uchovávány, zpracovány a přenášeny. Pojem bezpečnost IT zahrnuje takové pojmy, jakými jsou *bezpečnost informačních systémů, ochrana informačních systémů, ochrana informací, ochrana informačních technologií*. Všechny tyto pojmy mají svůj nezanedbatelný význam při popisu a diskuzi o bezpečnosti a ochrany informačních systémů a informací uložených, zpracovávaných a přenášených v takovýchto systémech. Pojem bezpečnost IT ale budeme používat jako obecný pojem, který může reprezentovat kterýkoli z ostatních uvedených pojmů. Mezinárodní normalizační organizace ISO ve svých normách definuje bezpečnost jako zajištěnost proti nebezpečím, minimalizaci rizik a jako komplex administrativních, logických, technických a fyzických opatření pro prevenci, detekci a opravu nesprávného použití informačních systémů. Bezpečný informační systém je takový, který je zajištěn *fyzicky*, *administrativně*, *logicky* i *technicky*. Informační systém je třeba zabezpečovat, protože se jedná o *ochranu investic*, neboť informace je zboží, nutí k tomu právní nebo morální pravidla, činnost konkurence a zákonné úpravy pro ochranu dat.

1. Základní pojmy

Informační systém definujeme jako:

„Množinu prvků ve vzájemných informačních a procesních vztazích (informační procesy).”

Informační systémy zpracovávají data a zabezpečují komunikaci informací mezi prvky. IS se často dělí na:

- systém zpracování dat a komunikační systém.

Předmětem činnosti IS je účinné řešení informačních procesů. Je nutné:

- analyzovat IS v závislosti na informačním prostředí

Proč stavíme bezpečné IS/IT prostředí?

1. aktiva (data a IT prostředky) jsou majetkem organizace a mají finanční a v některých případech finančně nevyčíslitelnou hodnotu

2. bezpečný (zabezpečený) IS/IT - organizace zvyšuje prestiž společnosti, pro obchodní partnery může být rozhodujícím faktorem při zadávání zakázky, zvyšuje se konkurenceschopnost společnosti

3. bezpečný IS/IT organizace zajišťuje stabilitu společnosti (úspěšný útok na IS/IT může vést ke zhroucení společnosti, ke konfliktům s legislativou, k oslabení konkurenceschopnosti).

„Národní strategie informační bezpečnosti ČR - Příloha č.2“ (www.micr.cz). Obecně je lze formulovat jako:

1. zachování důvěrnosti („confidentiality“), kdy přístup k aktivům mají pouze autorizované subjekty, tj. osoba, proces nebo zařízení disponující oprávněními k provádění činností v IS/ICT,

2. zachování dostupnosti („availability“), kdy autorizované subjekty mohou na své vyžádání vykonat činnosti a není jim odepřen k činnosti přístup,

3. zachování integrity, kdy ke změně aktiva nemůže dojít neautorizovaným subjektem, nepovolenou činností či nekompletním provedením změn,

4. zajištění prokazatelnosti („authentication“), kdy lze vysledovat jakoukoliv akci, která v systému proběhla s tím, že lze zjistit původce takové akce,

5. zajištění nepopíratelnosti („non-repudiation“), kdy subjekt nemůže odmítnout svoji účast na provádění nějaké akce,

6. zachování spolehlivosti („reliability“), kdy reálné chování systému je konsistentní s chováním systému tak, jak je dokumentováno.

Z toho vyplývá, že data a zařízení je potřeba chránit. Hlavní útoky definujeme:

1. neoprávněné přístupy k informacím

2. zfalšování informací

3. ztráta důvěrnosti (vyzrazení informací)

3. znemožnění přístupu oprávněným uživatelům k informacím

4. znemožnění kontroly informací (jak je s nimi nakládáno)

Z této analýzy vyplývají požadavky na zabezpečení IT a jejich cíle můžeme definovat:

1. autenticita

2. integrita

- dostupnost
- prokazatelnost a nepopiratelnost odpovědnosti
- spolehlivost a důvěrnost.
- optimalizovat jej tak, že navrhneme a realizujeme jeho automatizovanou část.

Postup při stavbě bezpečného IS/IT prostředí:

- určení cíle, jaké úrovně zabezpečení se má dosáhnout
- určení strategie postupu a dosažení cíle
- určení politiky a stanovení pravidel, která povedou k dosažení cíle

Obr. č.2 - Oblasti řešení bezpečnosti

5. PRÁVNÍ ÚPRAVA V NÁRODNÍCH A MEZINÁRODNÍCH INICIATIVÁCH A MODERNÍ KONCEPT SOUKROMÍ

Právo na soukromí a ochranu osobních údajů patří mezi základní lidská práva. Základním vymezením práva v ČR je na ústavní úrovni ochrana soukromí, která je upravena v *Listině základních práv a svobod*, a to konkrétně v č. 7 odst. 1[12], která nařizuje nedotknutelnost osob a jejich soukromí. Základním právním předpisem, který reguluje ochranu osobních údajů, je *zákon č. 101/2000 Sb., o ochraně osobních údajů.* Základní vymezení typologie osobních údajů lze nalézt přímo v *zákoně č. 101/2000 Sb. o ochraně osobních údajů.* Mezi další zákony vztahující se k této problematice patří *Zákon č. 106/1999 Sb. o svobodném přístupu k informacím v platném znění.* Tento zákon upravuje podmínky práva svobodného přístupu k informacím a stanovuje základní podmínky, za nichž jsou informace poskytovány. Dalším významným zákonem na úpravu ochrany soukromí je *Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti v platném znění,* který upravuje zásady pro stanovení utajovaných informací, pro přístup k nim a pro požadavky na jejich ochranu. Základní vymezení a typologie osobních údajů lze nalézt přímo v zákoně č. 101/2000 Sb., o ochraně osobních údajů. Tento zákon definuje pojmy jako jsou *osobní údaj, citlivý údaj, anonymní údaj, subjekt, správce, zpracování osobních údajů, způsob nakládání s osobními údaji* – shromažďování, uchovávání nebo odstranění těchto údajů. S příchodem nově vzniklých technologií vznikly nové typy osobních, kontaktních a identifikačních, citlivých a důvěrných údajů – které se díky nově vznikajícím technologiím a vzrůstajícímu počtu uživatelů stávají dostupnější a snáze šiřitelné. Obrovský objem těchto dat se šíří s minimálními požadavky na finance a dostupné informační technologie.

Česká republika je v oblasti ochrany osobních údajů také signatářem několika mezinárodních smluv, které ratifikovala a které je povinna právně dodržovat, které buď částečně anebo úplně upravují soukromí. Mezi nejdůležitější mezinárodní smlouvy, které je

[12] Citace Listiny práv a svobod. v Ústavě.

Česká republika povinna dodržovat a kterými je vázaná, je *Evropská úmluva o lidských právech* vyhlášená roku 1950 v Římě, která v čl. 8 uvádí, že „každý má právo na respektování svého soukromého života a korespondence, které je nezbytné v demokratické společnosti v zájmu národní bezpečnosti, předcházením nepokojů a zločinnosti nebo ochrany práv a svobod jiných“. Další významnou mezinárodní smlouvou, která se týká pouze ochrany osobních údajů, je *Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat*, která pro Českou republiku nabyla účinnosti dne 1. listopadu 2001.[13] V sekci *Osobní údaje ve společných informačních systémech EU* souvisejí také závazky nad zpracováním osobních údajů ve společných informačních systémech.

Kromě mezinárodních smluv jsou pro Českou republiku závazné také předpisy vydávané v rámci Evropského společenství. Základním dokumentem zabývajícím se problematikou osobních údajů je Směrnice 95/46/ES Evropského parlamentu a Rady o ochraně jednotlivců s ohledem na zpracování osobních údajů o volném pohybu takovýchto údajů, která byla přijata v roce 1995. Dalším krokem směrem do současnosti je *zákon č. 480/2004 Sb. o některých službách informační společnosti*, který stanovuje v kontextu informačních technologií zejména výjimku *nabízení obchodu a služeb.*

Dalším druhem legislativních dokumentů jsou normy a jiné legislativní předpisy. Mezi nejvýznamnější normy vztahující se k naší problematice patří mezinárodní norma ISO/IEC 17799, kde je uvedena specifikace požadavků na systém v oblasti bezpečnosti informací. Jedná se o klíčovou normu pro bezpečnost informačních systémů pro použití dat. Další kategorií jsou právní předpisy v rámci EU, které už specifikují konkrétní oblasti o právní ochraně. Např. Směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích) a směrnice rady č. 2001/264/EC, kterou se přijímají bezpečnostní předpisy Rady Evropy.

V normě BS 7799-2 (Systém managementu bezpečnosti informací – Specifikace s návodem pro použití) jsou uvedeny podrobnější specifikace a instrukce k užití výše uvedené normy ISO/IEC 17799. V oblasti českých norem je požadavkům na systém managementu

[13] Dodatkový protokol k této Úmluvě “Působnost této Úmluvy byla vztažena rovněž na soubory osobních údajů, které se nezpracovávají automatizovaně” pro Českou republiku nabyl účinnosti dne 1. července 2004.

bezpečnosti informací věnována norma ČSN ISO/IEC 27001, která stanoví požadavky na systém managementu informací tak, aby byla organizace schopna vyhodnocovat svá rizika a uplatňovat náležité kontrolní a řídící mechanismy k zachování důvěrnosti, integrity a dostupnosti informací. Další normou je ČSN ISO/IEC 15408, která je věnována informačním technikám, bezpečnostním kritériím pro hodnocení bezpečnosti IT. Tato je doplněna směrnicí pro řízení bezpečnosti IT s větším upřesněním normou ČSN ISO/IEC TR 1335 1-4.

Jako nejčastější příklady *identifikačních údajů* uvádí Emin Tatli, vedoucí Katedry mediální bezpečnosti na univerzitě v německém Weimeru, takové údaje, které "souvisejí s osobní identitou uživatelů, jako je jméno, příjmení, adresa, telefonní číslo, rodinný stav, životopis, přihlašovací jméno, pseudonym a přezdívka používaná na internetu" [TATLI, 2008]. Za *citlivé údaje* na internetu mohou být považována taková data, jako jsou příspěvky na diskusní fóra, citlivé adresáře a aplikace sociálních sítí aj. [TATLI, 2008]. Za důvěrné údaje jsou považována hesla, osobní emaily, soubory aj. Specifické místo mezi těmito typy údajů zaujímá IP adresa, která právně za osobní údaj považována není, avšak jedná se o klíčový údaj při identifikaci počítače i *konkrétního uživatele*.

Kromě právníků, sociologů nebo akademických teoretiků se tímto tématem zabývá řada soukromých organizací, např. mezinárodní organizace Privacy International působící v Londýně, která má za úkol monitorovat bezpečnost stavu informačních technologií, včetně citlivých dat jednotlivých uživatelů a každoročně vydávat zprávu o situaci v jednotlivých zemích a následně tuto zemi zařadit do jednotlivých kategorií dle míry této kontroly. [14] Tato organizace především kritizuje nárůst *sociální* kontroly ve společnosti.

V USA jsou mnohem dále především v ratifikování nových technologií, které se objevují v kybernetickém prostoru. Dokládá to i to, že v roce 2000 vznikl *Zákon o informačních technologiích*[15]. Tento zákon se široce zabývá americkou právní legislativou informačních technologií a Internetu. Mimo jiné se už v roce 2000 zabýval právní úpravou certifikačních autorit a digitálního podpisu. Díky novým Pravidlům 2000 vznikl soubor funkčních požadavků upravujících podobu digitálního podpisu. Tento zákon se rozhodl

[14] http.//www.privacyinternational.org.

[15] V USA zákon nabyl účinnosti 1. října 2000

implementovat „koncepci systémového modelu“, definovat jednotlivé entity a vztahy mezi nimi. [GUPTA, et al, 2005]. Mimo jiné tento zákon specifikoval funkční požadavky na *digitální podpis,* který je jedním z nástrojů ochrany autenticity uživatele na internetu. Kromě jiného je digitální podpis chápán jako mechanismus autentizace, kde digitální podpis ověřuje autenticitu všech dat v dokumentu, jak uvádí např W. Stallings v knize *„Cryptography and Network Security: Principles and Practice“* nebo má šifrovací funkci a zabezpečuje integritu zprávy pomocí kódu, jak uvádí Menezes. [MENEZES, 1993]. Digitální podpis uvádíme jako příklad nové technologie, která byla implementována do mnoha standardů a která je v kompetenci NIST (The National institute of Standards and Technology), která legislativně upravuje standardy pro použití nových technologií. (DeCeW in Woo 2006)

Nový koncept soukromí teď ustupuje od práva „být nechán“ k právu na uplatňování kontroly nad svými osobními údaji, který souvisí i s právními úpravami uváděnými výše. Hlavní myšlenkou nového konceptu soukromí je snaha osamostatnit se od pasivní svobody ze strany vnějších institucí k *aktivní* kontrole svých osobních údajů nebo omezování přístupu k nim.

6. PROBLÉM OCHRANY DAT V INFORMAČNÍCH SYSTÉMECH

Jak informační technologie byla aplikována na moderní organizace, stalo se mnohem snazší shromažďovat, ukládat, manipulovat a šířit informace. Rozvoj informatiky v posledních letech přinesl potřebu shromáždění velkého množství dat v informačních systémech a databázích. Dnes je pomocí počítačů možné naprosto zlikvidovat firmu, svoji obchodní konkurenci, vykrást banku, odstavit jakoukoli síť, narušit vojenskou operaci, formulovat útoky přes síť, ideologicky či myšlenkově propojit lidi kdekoliv ve světě pomocí jakéhokoliv *elektronického zařízení.*

Vzniká tedy potřeba ochrany dat uložených, zpracovávaných a distribuovaných v informačních systémech. Tato data se musí ochránit před *neidentifikovanými* závažnými hrozbami. V případě informačních systémů musí jít o opatření směřující k zajištění trvalé *dostupnosti* nabízených služeb, k řízení přístupu k datům na základě přístupových práv a ochraně přenášených dat.

6.1 Proč data chránit?

Tato doba je založena především na *dostupnosti a integritě informací*, které je potřeba si vyměňovat na veřejné síti. Organizace jsou v podstatě *závislé* na datech, které je potřeba si vyměňovat přes veřejnou síť. Jedná se o online banky, které se neobejdou bez zabezpečení a zajištění integrity a dostupnosti dat na svých serverech. Proč je tak důležité chránit data? *Data jsou nejcennější částí informačního systému, představují nejcennější aktivum každé organizace.* Při nesprávné ochraně se může přihodit, že dojde ke zneužití bankovních účtů, ke konkurenci se mohou dostat podnikatelské plány či konstrukční řešení. V současnosti nás zajímají jednotlivá *datová úložiště*, jež se běžně ve firmách používají.

Nejčastějšími a nejaktuálnějšími důvody, proč chránit data, je především *vzestup* cílených útoků. Narušení dat je i nadále předmětem vážných obav organizací a roste počet podniků, které zaznamenaly více než pět narušení dat během jednoho roku. Dalším důvodem může být to, že neustále roste počet společností, které úspěšně implementovaly technologie pro šifrování dat. Smyslem toho je si uvědomit, co by pro nás znamenalo zcizení či

modifikace dat a jaké hroby z toho plynou. Je množina pravidel a mechanismů pro zabezpečení důvěrnosti, integrity a dostupnosti dat spojená se snahou čelit možným hrozbám zevnitř i zvenčí. Podle [DANEL, 2010].

Cíle útočníků

- krádeže dat
- zničení dat
- destabilizace systému
- blokování místa nebo určitých zdrojů [DANEL, 2010].

6.2 Jaká data máme chránit?

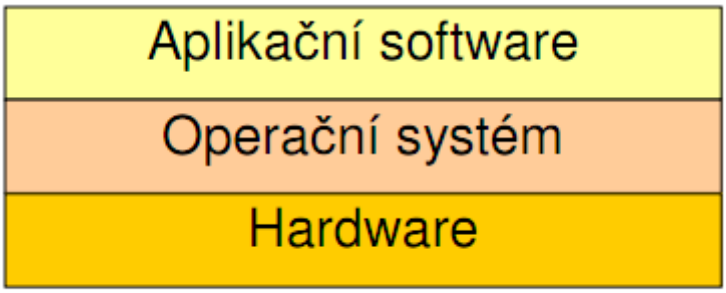
Zde se především jedná o jednotlivé komponenty informačního systému. Jde o bezpečnost *hardware*, bezpečnost *operačního systému* nebo bezpečnost aplikačního *software*. Hardware zahrnuje samotné zařízení, které umožňuje provádět operace s daty. Software je řídící program, který určuje postupnost prováděných operací. Dále se software dělí na několik částí na operační systém (systémový software, který zajišťuje řízení a správu hardwaru a základní systémové operace). Druhým typem je aplikační software, který provádí požadované manipulace s daty, např. napsání textu. [BURDA, 2010].

6.2.1 Hierarchie základních komponent

Hardware obsahuje prostředky, které umožňují manipulaci s daty (procesor, paměti, vstupy, výstupy apod.) Základní příkazy pro ovládání hardwaru jsou nabízeny jako služby pro nadřízenou vrstvu.

Operační systém agreguje základní příkazy do komplexnějších služeb (např. čtení z paměti, tvorba adresářů, mazání souborů apod).

Aplikační software prostřednictvím služeb operačního systému provádí stanovené manipulace s daty. [BURDA, 2010].



Obr. č.3 - hierarchie základních komponent [BURDA, 2010]

6.3 Proti čemu data chránit?

Informační systémy jsou atraktivním cílem elektronického zločinu – proniknutí informací do veřejného oběhu. Data bychom měli chránit především proti *aplikačnímu softwaru, k*terý zahrnuje především:

1. Škodlivý software (“malicious software” = “malware”). Jedná se o takový software, jehož účelem je narušit bezpečnost informačního systému.

Škodlivý software umožňuje:

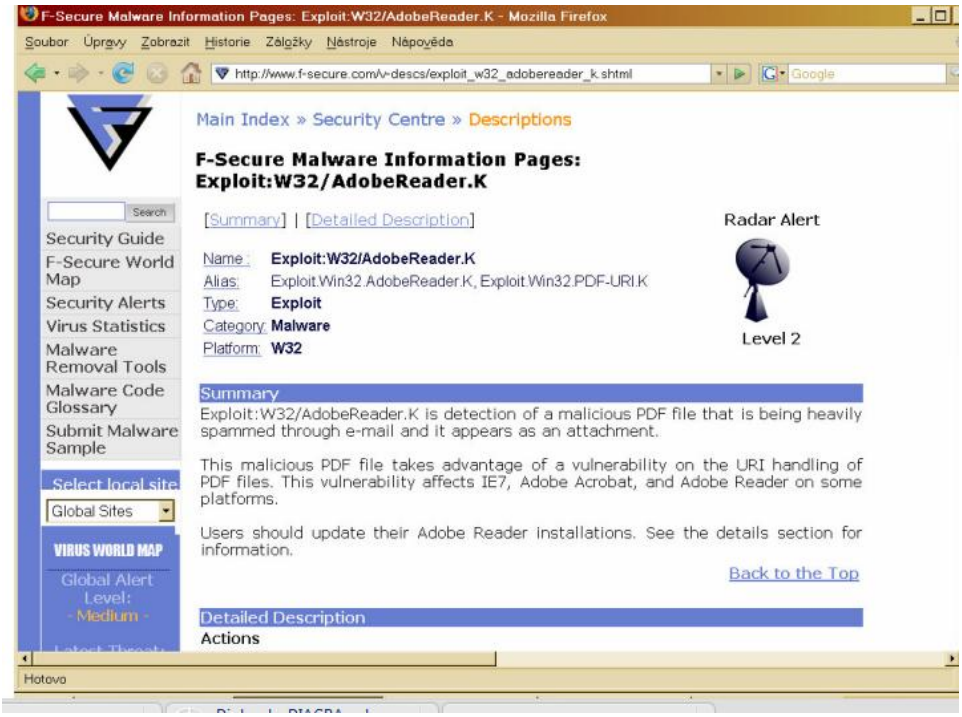
- zničit data a software v počítači
- zablokovat počítač
- získat důvěrné informace
- zneužít počítač

2. Možnosti zneužití počítače:

- zapojení do útoků na dostupnost jiných počítačů (“distributed denial-of-service attack” = “DdoS attack”)
- rozesílání nevyžádané (většinou reklamní) elektronické pošty – tzv. “spam”
- zobrazování nevyžádané reklamy, přesměrování webového prohlížeče na reklamní stránky apod. – tzv. reklamní software (“adware”). [BURDA, 2010].

6.3.1 *Programové ohrožení*

1. **Počítačové viry** – program, který se šíří bez vědomí uživatele
2. **Trojské koně** – skrytá část programu nebo aplikace provádějící funkce, se kterou uživatel nesouhlasí
3. **Červi (worms)** – šíření založeno na bezpečnostních chybách
4. **Back** – doors – vstup do systému bez hesla
5. **Phising** – podvodný email snažící se vylákat důvěrné informace – hesla atd**.**
6. **Hoax** – poplašná zpráva
7. **Spyware** – software sleduje uživatele nebo informace o jeho počítači a data odesílá
8. **Rootkit** – program k zamaskování určitých aktivit na počítači



Obr. č.4 - Bezpečnost aplikačního software [BURDA, 2010] [16]

[16] Ochrana: specializované servery s informacemi, jaké jsou aktuální slabiny a jak se kterému útoku bránit.

(Je tedy zřejmé, že vlastní ochrana dat se skládá z těchto 5 částí.) Tato typologie určuje 5 definovaných způsobů, které rozdělují data na ta, kde rozhoduje to, jaká data chceme chránit a proč. Je tedy velmi důležitá *identifikace dat.*

7. TYPY OCHRANY DAT

7.1 Ochrana fyzického přístupu k nosičům dat

Do této oblasti spadá možnost jednak mechanického útoku na fyzické nosiče, na kterých jsou data uložena a jednak i zajištění proti živelným pohromám. V prvním případě se snažíme zajistit především to, na jakých místech jsou data uložena, aby se k zařízením, na kterých jsou data uložena, nemohla dostat neoprávněná osoba. Jde o to, že pokud útočník má možnost fyzického přístupu k datům, dochází k několikanásobnému riziku zničení dat. Proti přírodním katastrofám se lze bránit především pravidelným zálohováním a duplikacím důležitých částí systému s pravidelným zálohováním dat. [DOSEDĚL, 2002]. Důvodem zajištění fyzické bezpečnosti je možnost zničení dat. Útočník má mnohem více možností ke zničení dat, pokud má k nosičům fyzický přístup. Do této kategorie bezpečnosti spadá například také ochrana proti živelným pohromám, neočekávaným požárům či ochrana proti výpadkům napájení. Také musíme zajistit oprávněnost přístupu před neoprávněnými osobami.

7.1.1 Ochranný mechanismus pro fyzické a přírodní ohrožení

Mezi jednotlivé typy obrany patří:

- **Zálohování** – úplná/inkrementální
- **Zabezpečení** – UPS, přepěťové ochrany
- **Kategorie systémů odolných vůči výpadkům:**

– Fault-tolerant systém – systém odolný vůči výpadkům – výpadek části systému (elektřina, komponenta, síť) nezpůsobí významné přerušení funkce systému; řešení pomocí zdvojení kritických komponent

– Disaster-tolerant systém - systém odolný vůči katastrofám; jako FT řešeno zdvojením, ale i fyzickým oddělením záložního systému [DANEL, 2010].

7.2 Ochrana uložených dat

Musíme zajistit to, aby data byla naprosto nečitelná. V praxi to může znamenat, že útočník přenese disk s daty do jiného počítače s jiným operačním systémem a chce data

analyzovat. Pokud chceme samotná data nějakým způsobem ochránit, musíme je zašifrovat. (tedy využijeme metod kryptografie). To znamená, že zašifrujeme soubory, které chceme ochránit. Tento typ ochrany dat zahrnuje i různé možnosti technických závad a výpadků elektrické energie atd. [DOSEDĚL, 2002].

7.3 Ochrana dat přenášených počítačovou sítí

Pokud data putují v rámci počítačové sítě, jsou vystavena obrovským rizikům. Tento přenos dat je vystaven obrovským rizikům, neboť počítačová síť je téměř nezabezpečeným prostředím. Je nejsnadnějším terčem pro kompromitaci a modifikaci. Patří sem především ovládání počítače, přenos souborů, zabezpečení bezdrátových sítí, webové stránky (např. vybírání elektronické pošty, bankovní služby apod.) Zatímco běžný protokol (http) je nezabezpečený, existuje jeho zabezpečená verze https. K zabezpečení se používá síťová vrstva SSL- Secere Socket Layer. [PARAFRÁZE DOSEDĚL, 2002].[17] U zabezpečení sítí rovněž hrozí virová nákaza, průnik do sítě, útoky typu DoS (Denial of Services), odposlech provozu, přístup k nezabezpečeným kanálům atd.

7.3.1 Softwarová ohrožení

- **Firewall, antivirové programy** – jedná se o tzv. „bezpečnostní bránu“ systému. Je to zařízení či software oddělující provoz mezi dvěma sítěmi (naší domácí a internetem), přičemž propouští jedním nebo druhým směrem data podle určitých předem definovaných pravidel. Brání tak zejména před neoprávněnými průniky do sítě a odesílání dat ze sítě bez vědomí a souhlasu uživatele.

- **Sítě – VPN** (Virtual Private Network) – komunikace se symetrickým šifrováním

- Bezpečnostní politika, plán obnovy činnosti [DANEL, 2010].

Mezi další škodlivý software patří trojské koně[18], viry[19], červi[20] atd.

[17] Použitím protokolu SSL se budeme zabývat v kapitole 12.

[18]Program tvářící se užitečně např. (systém pro pamatování hesel, který kromě své původní činnosti provádí ještě nějakou pochybnou aktivitu na pozadí. (např. sbírá hesla zadávaná uživatelem z klávesnice a jednou za čas je posle po internetu) nebo informuje o použitém software či programovém vybavení.

7.4 Ochrana dat před zničením

Data mohou být smazána či poškozena anebo může být zničen jejich fyzický nosič. Jedinou možnou obranou je systematické zálohování, vytvořit si záložní kopie nebo duplikovat nosiče dat. Ke zničení dat může docházet dvěma způsoby – data mohou být smazána či poškozena přímo na svém nosiči, nebo je samotný nosič fyzicky zlikvidován. Další případ může nastat chybou uživatele nebo chybou systému, fyzickým útokem atd. Jedinou obranou těchto dat je systematické zálohování, které je procesem, v němž vybraná a důležitá data jsou zálohována na jiné médium. Snahou je zálohovat co nejčastěji a pravidelně. Samostatnou důležitou částí ochrany dat nemusí být jenom úplné zničení, ale rovněž velmi nebezpečná je i *modifikace dat.* Tato činnost je mnohdy nebezpečnější než samotné zničení dat, neboť pozměněná data mohou napáchat rovněž velké škody. [DOSEDEL, 2002].

7.5 Ochrana logického přístupu k datům

Patří mezi klíčovou a kontrolní část zabezpečení celého systému. Znamená v prvé řadě to, aby se k datům nedostal nikdo, kdo nevlastní přístupová práva. Tato část ověřuje především identitu uživatele. Je základním stavebním prvkem bezpečnosti systému, při dodržování těchto principů mnohonásobně zvýšíme bezpečnost informačního systému. Musí být zde vyjádřena hierarchie přidělování přístupových práv atd. Tento typ ochrany je pro nás stěžejní částí. [DOSEDEL, 2002].

---

[19] Nachází se v operační paměti počítače a napadá otevírané soubory, šíří je a škodí. Potřebují ke svému šíření hostitele.

[20] Nepotřebují ke svému šíření hostitele. Jedná se o samostatné programy, které ke svému šíření využívají především sítě a internet.

8. PROBLEMATIKA OCHRANY LOGICKÉHO PŘÍSTUPU K DATŮM

Většina informačních systémů využívá nějaký přístup pro uchovávání a přístup k datům. Zabezpečení dat je množina pravidel a mechanismů pro zajištění důvěrnosti, integrity a dostupnosti dat, která je spojena se snahou bránit data *zvenčí.* Zabezpečení dat se skládá ze 3 úrovní [CASTANO, 1995]: fyzické (úroveň hardwaru, zálohování dat), logické (softwarové metody pro autentifikaci/autorizaci) a organizační (doplňková snaha o ochranu systému). V této části bych ráda uvedla a srovnala bezpečnostní koncept autentizace a srovnala jednotlivé *typy* autentizačních metod, které spadají do *logické* vrstvy bezpečnosti. Této problematice se budeme věnovat do hloubky, protože tvoří kontrolní část zabezpečení celého systému. Fyzickou ani organizační úrovní zabezpečení dat se již nyní zabývat nebudeme.

Do podmínek pro *logické* vrstvy bezpečnosti spadají:

- zajištění důvěrnosti dat (secrecy)
- ochrana integrity dat (integrity)
- zajištění dostupnosti dat (availibility) [SOLOMON, 2003, s. 212]:

1. podmínka - zajištění *důvěrnosti* dat spočívá ve snaze zabránit neautorizovanému *úniku* informací. Můžeme si představit např. informační systém banky, který obsahuje databázi aktuálního stavu na účtech klientů. V tomto případě znamená první podmínka bezpečnosti informačního systému zajištění důvěrnosti dat v tom smyslu, že se snažíme zajistit, aby jakýkoliv neautorizovaný subjekt nemohl vniknout do systému a zjistit např. stav účtu vytipovaného klienta. V tomto smyslu *ochrana důvěrnosti dat* znamená, že systém zajišťuje *oprávnění* konkrétní osoby k přístupu k účtu a především ochranu před neoprávněným vniknutím na účet.

2. podmínka - ochrana *integrity* dat spočívá v zabránění neautorizované nebo nepatřičné modifikaci dat. V případě informačního systému banky ochrana integrity dat zabraňuje v *modifikování* stavu na účtu a zabraňuje tak proniknutí jiným než autorizovaným subjektům. Zabraňuje neoprávněnému manipulování s daty.

3. podmínka – zajištění *dostupnosti* dat – (nebo služeb informačního systému) znamená, že autorizovaným uživatelům *nebude odmítnut* přístup a že systém nebude zabraňovat zpracovávat příkazy autorizovaných subjektů a zajišťuje tedy kontinuitu dat a neustálou *dostupnost*.[21] Napadá se především to, co není možné regulérně využívat.

8.1 Identifikace, autentizace a řízení přístupu

Ochrana logického přístupu k datům je založena tom, aby do systému neměl přístup uživatel, který k tomu nemá dostatečná přístupová práva. Pro tento účel musíme tedy dostatečně ověřit *identitu* uživatele. Systém tedy potřebuje *důkaz,* že se jedná o tu osobu, která se za ni prohlašuje. Před vlastní autentizací uživatele musí proběhnout *identifikace,* v níž uživatel potvrdí, že je skutečně tím, za koho se vydává.

V praxi je potřeba rozlišovat dva pojmy – **autorizaci a autentizaci**, které jsou nesprávně považovány za synonyma. *Autorizace* je proces, při němž se ověřují (server či jiná entita) dostatečná práva pro přístup do určité oblasti pro vykonání akce. Dalším problémem je autentizace dat, které jsou *ochranou* jejich *integrity*, která spočívá v tom, že zabráníme neautorizované nebo nepatřičné modifikaci dat jiným než *autorizovaným* subjektům. A tedy tím zabráníme např. modifikaci stavu na účtech jiným než autorizovaným subjektům.

Abychom se v celé problematice orientovali, musíme si tedy ujasnit základní pojmy. *Autentizace* tedy znamená *ověřování pravosti* identity **(kdo je to).** Dalším pojmem je autorizace, která znamená *oprávnění* pro určitou činnost **(co může).** Je důležité zde zmínit, že autentizace je základním předpokladem autorizace. To znamená, že v prvé řadě nás musí systém *rozeznat* od ostatních subjektů, a pak nám přidělí určitá práva. (tedy oprávnění pro určitou činnost).

Při výběru autentizace musíme mít na paměti důležité autentizační metody. Na bezpečnost systému to má obrovský vliv, neboť časová prodleva, či není-li určitá metoda dostatečně rychlá, způsobuje obrovské komplikace a dochází tak k falešným přijetím či neoprávněným odmítnutím v systému.

---

[21] Kde patří mezi stále oblíbené útoky typu Denial of Service – odepření služby. Zákeřnost těchto útoků spočívá v tom, že není napaden cíl, ale přístupové zdroje k němu.

Vedle autentizace a autorizace existuje mnoho dalších metod, jak zajistit bezpečnost IS. Např. fyzické přístupy k nosičům dat, zálohování, pořizování dalších kopií, obnovy ze záloh, auditní záznamy atd. Avšak jednoznačná *autentizace a autorizace* uživatele musí předcházet všem dalším aktivitám uživatele v informačním systému a musí zajistit *ochranu důvěrnosti a integritu* autentizační informace.

Otázkou zůstává, jaký je reciproční vztah mezi *identifikací* a *autentizací*. Jakým konceptem zůstává identifikace? Jde o to, že *předmět* musí poskytovat svoji identitu. To znamená, že poskytování identity se provádí např. pomocí uživatelského jména, bitu čipové karty, umístěním obličeje nebo mávnutím rukou na kameru. Nejzákladnějším prvkem pro autentizaci, autorizaci a odpovědností a snahou o další procesy je poskytování *identity*.

9. AUTENTIZACE UŽIVATELŮ V INFORMAČNÍCH SYSTÉMECH

Autentizace *ověřuje identitu* objektu porovnáním jednoho nebo více faktorů s databází platných identit (jinými slovy, uživatel účtu, entity). Schopnost *subjektu* a systému zachovat mlčenlivost o ověřování faktoru pro identity, přímo odráží úroveň bezpečnosti tohoto systému.*"Identifikace a autentizace* jsou vždy společně jako jeden dvěma kroky procesu. Poskytování identity je první krok a poskytování autentizačních faktorů vede ke kroku druhému. Bez obou si objekt nemůže získat přístup k systému - ani jeden prvek sám o sobě není užitečný." [STEWART, 2008]. Musíme si vybrat vhodnou autentizační metodu, která slouží jako ochrana před *falšováním identity*. Především to musí být metoda dostatečně rychlá, která nezpůsobuje množství komplikací. Dále je nutné si vybrat metodu dostatečně spolehlivou, aby nedošlo k falešným přijetím či *neoprávněným* odmítnutím [SCHMEH, 2003, 179]. Dále musí jít o metodu dostatečně důvěryhodnou, kde se daří riziko odmítnutých operací výrazně eliminovat a čtvrtou podmínkou je to, že není možné měnit zadání a výstupy autentizace. Optimální autentizace je závislá na těchto čtyřech možnostech, ale v praxi se používá i *kombinace dvou nebo tří* autentizačních způsobů. Díky správně nastaveným autentizačním požadavkům *eliminujeme* výrazně množství útoků na autentizační protokoly.

V prvé řadě to mohou být útoky na autentizační zařízení, které se snaží přesvědčit zařízení, aby se domnívalo, že neoprávněná entita je entitou oprávněnou. V další řadě se pak jedná o útoky na *fyzickou bezpečnost*, které v současné době představují obrovské riziko, neboť jejich cíle jsou velmi nákladné a obrana proti nim je velmi obtížná.[22] Dalším typem útoku jsou útoky na fyzickou bezpečnost, kde se jedná o útoky na bezpečnost prostředí, využívané např. hojně v sociálním inženýrství. [23] [PARAFRAZE PRIBIL, 2009]

[22] Jedná se o útoky invazivní a poloinvazivní, které jsou velmi náročné na provedení. Jejich cílem je změnit chování celého systému, např. chování autentizačního čipu. Nebo metody poloinvazivní, jako např. „odposlech" elektromagnetických vln.

[23] Např. tyto útoky mohou mít podobu instalace falešných čteček apod.

9.1 Základní rozdělení autentizačních metod

Autentizační metoda vyjadřuje to, co od uživatele potřebujeme získat, *čím se uživatel musí prokázat* pro ověření identity. [HOEPER, 2010] Jedním z dále popisovaných způsobů je zvolení si metody *silné autentizace*, která výrazně přispěje do ochrany dat běžných uživatelů. Autentizace uživatelů v počítačových systémech informuje o kvalitě nasazení autentizační metody a je vnímána jako nejdůležitější, nejfrekventovanější a nejpoužívanější autentizační metoda obecně a je významným měřítkem kvality bezpečnostního nasazení systému.

1. První kategorií je, co uživatel zná - (typicky se jedná o nějaké *tajemství* či *kód* uživatele, nejčastěji ve vyjádření či formě textového řetězce, tzn. *heslo, PIN*, *přístupovou frázi* apod. Výhodou je, že se nejedná o fyzický objekt, ale o abstraktní znalost. Uživatel v této kategorii sdílí znalost daného tajemství se systémem a ten dokáže rozhodnout, zda uživatel je opravdu tím, za koho se vydává.

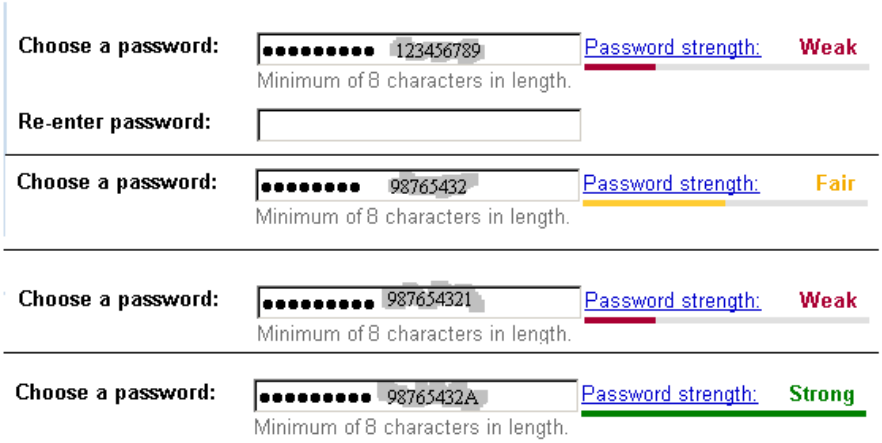
2. Druhou kategorií je, co uživatel má - většinou se jedná o nějaký fyzický objekt, označovaný jako *token*. Výhodou tokenu je, že ho lze velmi obtížně zkopírovat, jeho ztráta je obtížně zjistitelná a je schopen uchovávat a zpracovávat náhodné informace s velkou entropií (míra informace). Jedná se např. o čipovou kartu, USB klíč atd. K jeho použití musí existovat příslušná čtecí zařízení, což zvyšuje náklady při zavádění systému do praxe.

3. Třetí kategorií je, co uživatel je – Ve třetí kategorii se jedná o nějaké automatizovaně zhodnotitelné biologické informace - tzv. *biometriky*. Systém posuzuje *fyziologické vlastnosti těla uživatele*, případně jeho *chování*. (Tradičně jde o otisk prstu, vzorek hlasu, styl písma apod.). Nevýhodu je, že biometrické informace jsou jen velmi obtížně měřitelné (značně ale závisí na tom, co je měřeno) a právě přesnost měření výrazně ovlivňuje celkovou bezpečnost mnoha biometrických systémů. [WINDLEY 2005, s. 50- 61].

Bez kvalitního nasazení jakékoliv autentizační metody postrádá smysl další technika ochrany dat – a tou je šifrování neboli metoda postavená na kryptosystémech. Tato technika je jednou (mimo jiných) z nejvýznamnějších a nejpoužívanějších technik současnosti.

10. AUTENTIZACE POMOCÍ HESEL

Je nejrozšířenější a nejvyužívanější autentizační technikou, při níž uživatel zadává své *přihlašovací jméno v kombinaci s heslem.* Pro úspěšné přihlášení do systému vůči autentizační autoritě je *haš* hesla uloženého v systému a konkrétní způsob zadaných údajů závisí na autentizačním protokolu. Mluvíme-li o autentizaci pomocí hesel, budou nás zajímat místa uložení hesel a použití kryptografie, která zabezpečuje hesla proti *přečtení.* [CYBERSECURITY, 2009], Jedním z prvních prohřešků, kterých se uživatelé často dopouštějí, je např. používání slabých hesel, hesel sdílených anebo hesel napsaných na psacím stole - a celá investice do zajištění ochrany bezpečnosti dat je marná.



Obr. č.5 – Síla hesla

Zdroj: http://en.wikipedia.org/wiki/File:PassWord_Strength.png

V prvé řadě je potřeba říct, že použití hesel funguje na principech kryptografie, o kterých se zmíníme v kapitole č. 14 a jejich ukládání v šifrované podobě. Dalším faktorem, kterým dosáhneme alespoň optimální míry zabezpečení, je nastavit určitou *kvalitu* hesla. Pro kvalitu je rozhodující počet znaků abecedy a délka hesla. Uživatel předkládá systému heslo, které je řetězcem znaků společně se svou identifikací (loginem). Tato metoda zabezpečení je používána ve velkém množství aplikací. Doporučovaným způsobem pro zvyšování bezpečnosti hesla je obměňování základní množiny znaků a jejich kombinací. Jak např. uvádí Barbara Guttman v knize *"An introduction to Computer security"* [GUTTAMAN, 1995, str. 180].

Systém tyto autentizační údaje kontroluje společně s údaji, které má o daném uživateli k dispozici. V praxi to funguje tak, že uživatel zadá heslo do systému, systém zná databázi uložených hesel všech uživatelů a po příjmu hesla porovná zaslané heslo s kopií ve svém seznamu a zašle uživateli odpověď. Principem tedy je, že systém kontroluje a porovnává heslo uživatele s údaji ve své databázi pro vyhodnocení konkrétní identity [KRHOVJÁK, J., MATYÁŠ, V. 2007]. Naproti tomu, jak uvádí J. Stamp, v systému bohužel neexistuje bezpečnější způsob ochrany hesel v elektronickém monitorování. (S výjimkou použití vyspělejší autentizace, např. na základě kryptografických metod anebo tokenů). "Můžeme zlepšit jenom zabezpečení hesel" [STAMP, 2006 s. 174]. Nejdůležitější je tedy zohledňovat expirační dobu hesel, omezit minimální počet pokusů pro přihlášení. Nebo použít tzv. "Strong password" – které zahrnuje minimální počet znaků, povinné kombinace čísel a písmen nebo zákaz používání smysluplných slov. Problémem hesel je především mnoho hesel do různých systémů a *nejednoznačnost identity*. (V jiném systému pod stejným uživatelským heslem vystupuje někdo jiný.)

10.1 Statická

Obecně považována za nejslabší metodu autentizace. Některé výzkumy dokonce uvádějí, že až 80% statických hesel lze prolomit do 1 minuty.[24] Jsou častými prostředky identifikace na základě znalostí osobních identifikačních čísel nebo kódů. Používání klasických hesel zná každý z nás ze své každodenní praxe, jedná se o klasické přihlašování do informačních systémů, výběrů z bankomatů apod. V současnosti se prosazují i hesla dynamická, která jsou o něco spolehlivější než hesla klasická – statická. [RAK (et al.), str. 88].

10.2 Dynamická

Dynamická hesla jsou vždy jiná, ale lze je odvodit z nějakého typu *znalosti*.[25] Dynamická hesla částečně odstraňují nedostatky klasických statických hesel. Při každém přihlášení se heslo podle předem stanoveného algoritmu mění a nemůže být znovu použito v původní podobě. Tím je znesnadněn přístup neautorizovaného uživatele. Dynamická hesla se

[24] http://www.rekonix.cz/rekonix/cs/page.php?n=vasco/autentizace.html

[25] Znalost může být např. minulá jména a příjmení, jména rodičů, data a místa narození atd.

mění v závislosti na čase a místě použití hesla. Použití hesla je možné charakterizovat např. poštovním směrovacím číslem, jménem společnosti apod. Jelikož je tato technika odvozená z nějakého typu znalosti, může být snadno zapomenuta nebo chybně interpretována. Uživatel hesla si může sám zadat úroveň zabezpečení hesla. Automatizovaný výpočet dynamického hesla je realizován pomocí speciálních prostředků SW, nazývaných Personal Digital Assistant (PDA), který může být zabudován např. do čipové karty [RAK, (et al.), str. 88].

10.3 Jednorázová

Jednorázová hesla (one-time pasword - OTP) je heslo platné pouze pro jeden login nebo jednu transakci. Jednorázová hesla zabraňují řadě nedostatků, které jsou spojeny s tradičními (statickými) hesly. Největší výhodou jednorázových hesel je, že *nejsou náchylná k útokům pomocí přehrání* tzv. replay útokům,[26] jsou vhodná všude tam, kde se budeme přihlašovat do nezabezpečeného počítače. Řeší hned několik problémů. Např. jak uvádí J. Weckert [WECKERT, J. 2005, s. 166]: k problémům s použitím hesel patří *elektronické sledování*[27] a přístup k *souboru s hesly*[28]. Tomu procesu se říká "sociální inženýrství" [29][BEAVUR, K. STUART, M. 2010, 89-90]. Nejmodernější metodou jsou způsoby založené na tzv. *šifrovacím klíči*[30] [*The Eletronic supervisor: New technology, new tensions*"U.S. Congress, Washington DC] Obecně jsou právě jednorázová hesla ohrožena útoky sociálního inženýrství, např. phising,[31] který byl použit Přestože jednorázová hesla jsou v některých ohledech bezpečnější, než ostatní typy hesel, jsou stále zranitelná vůči *man-in-the middle*

[26] Pokud útočník dokáže zaznamenat OTP, které bylo již použito, nebude již moct heslo použít, protože nebude platné.

[27] Pokud jsou hesla přenášena do počítačového systému, mohou být snadno elektronicky monitorovány. Tato situace může nastat v síti sloužící k předávání hesel, nebo na počítači v samotném systému.

[28] Pokud soubor hesel není chráněn silnou kontrolou přístupu, je možné tento soubor stáhnout. Heslo soubory jsou často chráněny jednosměrným šifrováním. Hesla nejsou k dispozici systémovým administrátorům nebo hackerům (pokud úspěšně obejdou kontroly přístupu).

[29] Jedná se o manipulování lidí do provádění akcí nebo nebo vyzrazení důvěrných informací.

[30] Tyto moderní způsoby a mnoho dalších moderních metod jsou založeny na kryptografických metodách. Více v knize: [*The Eletronic supervisor: New technology, new tensions*"U.S. Congress, Washington DC]

[31] Nachytání uživatele tím, že nabídnou uživateli jedno nebo více možností hesel, která již byla použita v minulosti.

útokům. Např. v roce 2005 došlo k incidentu ve Švédsku, kdy byli takto napáleni zákazníci švédské banky. V roce 2006 byl tento typ útoku použit na klienty banky USA[32]

[32] http://en.wikipedia.org/wiki/One-time_password

11. AUTENTIZACE POMOCÍ TOKENŮ

Autentizační token je zařízení, pomocí kterého se může uživatel přihlásit do systému – podmínkou je, že uživatel jej musí mít v okamžiku přihlášení u sebe. Tokeny mají více forem – nejběžnější jsou čipové a paměťové karty, USB tokeny a autentizační kalkulátory. Minimální funkcí všech tokenů je možnost uložení citlivých údajů, některá sofistikovaná zařízení obsazená kryptoprocesorem jsou schopna provádět kryptografické výpočty. Tokeny nabízejí obecně bezpečnější a efektivnější metodu autentizace, než hesla a společně s biometrikami jsou považovány za silné *autentizační metody*. [KRKOŠKA, 2009] Problematika autentizačních tokenů se zabývá pokročilými druhy ověřování/prokazování identity jedinců. Např. se používají při přihlašování do počítače nebo u internetových bankovních aplikací. S tím souvisejí i použité komunikační protokoly, jejichž bezpečnost je v takovém případě zásadní. [KRHOVJÁK et al c2010]

Autentizační tokeny jsou zařízení, která mohou uživatelé nosit neustále s sebou za účelem autentizace do systému. Mají buď specifické vlastnosti (tvar, elektrický odpor, elektrickou kapacitu) nebo obsahují specifické tajné informace (např. kvalitní heslo nebo kryptografický klíč) nebo jsou dokonce schopny provádět specifické (obvykle kryptografické) výpočty. Ačkoli některé techniky jsou založeny výhradně na něčem, co má uživatel k dispozici, je většina technik popsaných v této sekci kombinací s něčím, co uživatel zná. Tato kombinace může poskytnout podstatně silnější zabezpečení, než jenom něco, co uživatel ví nebo má sám. Naproti tomu se velmi málo ví, že kromě klasických dvou přístupů ke zpracování informací, popsaných níže, existují tokeny, které mohou být klasifikovány také z hledisek *zdrojů, bezpečnosti a rozhraní*[33] [PARAFRÁZE MAYES, 2008 295- 298].

Podrobné rozčlenění k nastudování se objevuje v knize *"Smart cards, tokens, security and applicatios"* Velmi zajímavě o tom pojednává zejména kapitola 13- *RFID and*

[33] Z angličtiny, dá se přeložit jako "člověk uprostřed" nebo "člověk mezi". Podstatou je snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem. Musí se využít tzv. *důvěrných autorit* nebo-li třetích stran.

Contactless Technology, kde se tokeny realizují u procesů v řadě *bezpečnostních mechanismů*, za účelem zvýšení zabezpečení zdrojů.

11.1 Paměťové tokeny

Paměťové tokeny *uchovávají,* ale nezpracovávají informace. Jedná se o speciální čtecí/zapisovací zařízení umožňující kontrolovat psaní a čtení dat z a do tokenu. Nejběžnějším typem paměťových tokenů je *magnetická karta* s tenkým proužkem magnetického materiálu, umístěná na povrchu karty např. (na zadní straně kreditní karty). Společné použití paměťové tokeny pro přihlášení do počítačových systémů je bankomat (ATM) karty. Toto používá kombinace něčeho, co *uživatel vlastní (kartu),* s něčím, *co uživatel zná (PIN*).

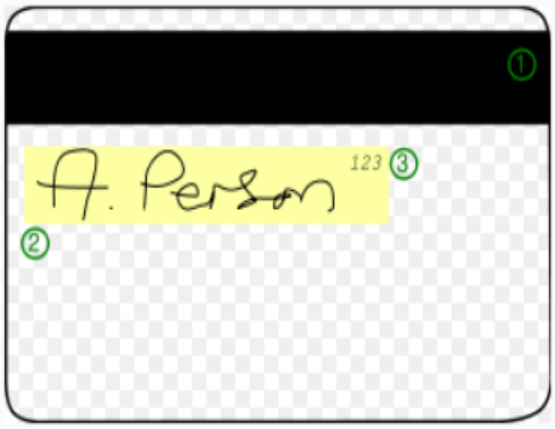
Některé počítačové ověřovací technologie jsou založeny výhradně na vlastnictví tokenu, jsou ale méně časté. Systémy používající pouze tokeny, jsou daleko více rozšířené a mohly by být použity v jiných aplikacích, např. pro fyzický přístup. [GUTTMAN, ROBACK 1995, s. 183]

Paměťové tokeny, které ještě používají PIN, poskytují mnohonásobně vyšší bezpečnost, než hesla. Kromě toho, tento druh karet je levný na výrobu. Pokud chce hacker napadnout či získat tuto informaci, *musí získat token, platné heslo a uživatelské jméno.* Tudíž musí znát kombinace (obzvláště proto, že většina ID uživatelů jsou obecně známy). Tokeny jsou vyžadovány pro fy*zické* vstupy a výstupy, to má dopad v tom, že např. lidé budou nuceni odstranit tokeny, když opustí počítač. To může velmi usnadnit ověřování [ROSS, 157-159].

Rozmístění základních ochranných prvků na kartě znázorňuje následující obrázek.

(1 – logo banky, 2 – čip, 3 – hologram, 4 – číslo karty, 5 – logo vydavatele karty, 6 – platnost karty, 7 – jméno majitele platební karty)

Obr. č. 6 - Přední strana platební karty



(1 – magnetický proužek, 2 – podpisový vzor, 3 – CVC kód)

Obr. č. 7 - Zadní strana platební karty

11.2 Inteligentní klíče

Rozšiřují funkčnost a vlastnosti paměťových tokenů. Autentizace pomocí tzv. *inteligentních tokenů* je jednoduchá. Jsou založeny na principu tzv. *přenosného klíče* obsahujícího vložený čip, který je schopen ukládat i zpracovávat data. Samotný token obsahuje jeden nebo více integrovaných obvodů. Inteligentní token obvykle vyžaduje, aby uživatel použil něco, co zná (např. PIN nebo heslo), aby se mohl "odemknout" pro použití. Pro použití - pro autentizaci - je inteligentní klíč dalším příkladem autentizace založené na něčem, co uživatel vlastní (tj. token sám).

Většina inteligentních tokenů jsou používány místo statických uživatelských jmen a hesel, neboť nabízí silnější a pohodlnější způsob pro uživatele na identifikaci a autentizaci přístupu k počítačům a sítím [INTRODUCTION TO INFORMATION TECHNOLOGY, s. 487].

Používají se např. v aplikacích *elektronického bankovnictví* nebo se používají jako *bezpečný klíč* k ověření uživatele pro komunikaci na veřejné síti mezi uživatelovým počítačem s bankovním systémem. Při této aplikaci jsou bankami implementovány kryptografické algoritmy a tajné klíče na čipové kartě [HANSMANN, 2003, s. 62, 50, 331]. Inteligentní tokeny mohou být založeny na bezkontaktních nebo kontaktních technologiích a doplňují stávající bezpečnostní systémy.

11.3 Klasifikace tokenů na základě vlastností

- *1. fyzické charakteristiky* - Inteligentní tokeny lze rozdělit do dvou skupin: čipové karty a jiné typy tokenů. Čipová karta vypadá jako kreditní karta, ale obsahuje vestavěný mikroprocesor. Čipové karty jsou definovány mezinárodní standardní organizací ISO. Inteligentní tokeny, které nejsou čipové karty, můžou vypadat jako kalkulačky, klíče nebo jiné přenosné předměty. Existuje několik typů karet, každá je specifická pro konkrétní aplikaci. Jeden z typů těchto karet se využívá připojením k počítači na nákup přes internet např. (e-commerce),[34] Konkrétnější rozdíl vysvětluje např. Amit Dhir v knize "The digital consumer technology handbook." [DHIR, 2004, s. 185]

- *2. Inteligentní rozhraní*. Inteligentní tokeny mají buď manuální nebo elektronické rozhraní. Manuální nebo elektronické rozhraní (human-interface) mají displej nebo/a klávesnici a umožní lidem komunikovat s kartou. Inteligentní tokeny s elektronickým rozhraním musí být čteny speciálními čtečkami. Čipové karty, jako je popsáno výše, mají elektronická rozhraní. Smart žetony, které vypadají jako kalkulačky, mají obvykle manuální rozhraní. [United States, General Accounting Office, 2004, str. 165]

- *3. Používané protokoly.* Existuje mnoho různých protokolů, inteligentní klíč lze použít pro autentizaci. Obecně platí, že mohou být rozděleny do tří kategorií: statická výměna hesel, dynamické generátory hesel a výzva-odpověď. Token, který používá dynamický generátor hesel, pro protokol vytváří jedinečnou hodnotu, např. že se mění periodicky (každou minutu) [35] [United States, General Accounting Office, 2004, str. 165]

Jednorázová hesla jsou schopná odstranit problém s elektronickým monitorováním a tokeny, které vyžadují použití PIN, pomáhají tak snížit riziko jejich padělání.

---

[34] Rozdíl mezi nimi je, že méně kontaktní verze obsahuje anténu cívky. To vysílá a přijímá data bez nutnosti navázat kontakt s čipovou tou. Základní funkce obou typů čipových karet je stejný. Se zavedením combicard (kontaktní i kontakt-méně funguje na ne kartu), může čtečka karet přijímat oba typy karet výslechu a interakce

[35] Technology assessment: cybersecurity for critical infrastructure protection, str. 165

Příkladem by mohl být token obsahující IC s Obě bezkontaktní a kontaktní rozhraní, jako jsou karta Baclays OnePulse.[36]

Obr. č.8 – Barclays karta

[36] Tyto karty se používají ve Velké Británii.

12. AUTENTIZACE POMOCÍ BIOMETRIK

Informační bezpečnost se týká zajištění důvěrnosti, integrity a dostupnosti informací ve všech formách. Existuje mnoho nástrojů a technik, které podporují řízení bezpečnosti informací a systémů založených na biometrii, které se vyvinuly na podporu některých aspektů informační bezpečnosti.

"Jak už bylo řečeno, *identitu osoby prokazujeme pomocí vlastnictví* (identifikační doklady, karty, čipy, nazývané často v anglické praxi souhrnným termínem *toked-based identification* apod.), *znalostí* (hesla, identifikační kódy) a podle *měřitelných biologických* (biometrických) charakteristik (fyzický vzhled, tvar, hlas, otisky prstů, struktura DNA). To, co máme, nám může být odcizeno nebo napodobeno: to, co známe a umíme, může být odpozorováno, uhodnuto nebo jinak získáno. Obojí tak může být zneužito další osobou nebo skupinou osob. Aby případné riziko bylo minimální, v praxi se často kombinuje "vlastnictví" se "znalostmi" s cílem zajistit bezpečnější osobní identifikaci. "[RAK, (et al.), 2008].

Biometrické systémy výrazně podporují aspekty identifikace, autorizace, autentizace v informační společnosti. Jain (et al.) (2000) definuje biometrické bezpečnostní systémy jako "*Modelový systém umožňující osobní identifikaci stanovením pravosti specifických fyziologických nebo biologických vlastností uživatele* [MALTONI, JAIN, 2004; s. 269]. Naopak Schneiner ho považuje za "*efektivní bezpečnostní systém, který musí obsahovat kombinaci minimálně dvou z těchto tří prvků*: *něco, co jste, co víte, nebo něco, co je"* [SCHNEIER, 2000, s. 136]. Biometrické údaje se vyskytují v několika různých formách, které mohou být snadno *získány, digitalizovány, přenášeny, uchovávány a porovnávány* pomocí biometrických autentizačních zařízení. Biometrické údaje jsou součástí širšího systému bezpečnosti. Základní fáze biometrického zabezpečení zahrnují následující procesy: *získávání dat* (ze šablony založené na datech, údajích), *analýzu* (s jiným biologickým charakteristika), *extrakci* (ze šablony založené na údajích), a *uchovávání*. [SCHNEIER, 1999; s. 136].

Nicméně biometrické techniky nejsou samy o sobě zárukou dokonalého zabezpečení. Jenom kombinací dvou nebo více bezpečnostních znaků dochází k určité pravděpodobnosti, že bude efektivní. Ve stati *"Cryptography in plain text. Privacy Law and Policy Reporter|"*

Clarke poukazuje na to, že je potřebné kombinovat i jiné techniky s biometrickými údaji, nabídnout vlastnosti bezpečného systému, a to techniky jako: *utajení* (soukromí), *integriu,* a *autentizaci*.[CLARKE, 1998; s. 24-27].

Jednu z dalších definic nám může poskytnout Paul Reid, který biometrický systém označuje jako ”fyziologické nebo psychologické zvláštnosti, které mohou být změřeny, zaznamenány a kvantifikovány.” Dále uvádí, že “v biometrických systémech je třeba tyto informace zaznamenat. Tyto záznamy se označují jako “zápis”. Tento zápis slouží na vytváření šablony. Šablony jsou obvykle dlouhý řetězec alfanumerických znaků, které popisují funkce fyzického znaku” [REID, 1998; s. 6]. Na základě tohoto “zápisu” biometrické systémy stále více získávají na popularitě jako způsob, jak poskytnout osobní identifikaci. Osobní identifikace je v současnosti velmi důležitá v mnoha aplikacích a na popularitě získává především díky vzestupu a používání všech typů bezpečnostních autentizačních mechanismů a je častým cílem podvodů a krádeží identity. V posledních letech se ukazuje, že tato otázka je hlavním problémem společnosti. Jednotlivá hesla, PINy, identifikace klíčového slova a osobní otázky mají nedostatky, které omezují jejich použitelnost v široce síťové společnosti. Výhodou biometrických systémů je, že mohou vytvořit neoddělitelnou vazbu mezi jednotlivcem a částí dat. Nevýhodou biometrických systémů je jejich proklamovaná invazivita a obecná rizika, která mohou vzniknout, pokud s biometrickými údaji není správně zacházeno. Existují osvědčené postupy, které mohou poskytnout vynikající matematickou analýzu mezi daty a identitou tím, že biometrické údaje představují “slib”, který není-li dodržen, může to vést k nesmírným rizikům pro soukromí jednotlivce [PARAFRÁZE FLEMING, 1998; s. 2005].

Např. podle Zhanga se biometrické formy zaměřují na *verifikaci a identifikaci identity*. Biometrické technologie jsou zaměřeny na měření *fyziologických vlastností lidského těla*, např. (otisk prstu, geometrie ruky) nebo chování člověka (např. dynamika podpisu nebo vzorek hlasu). Jedná se o měření *autorizovaným způsobem*. Aktuálností je to, že některé systémy jsou již komerčně dostupné a používají se pro snímání otisků prstů nebo systémy, které například porovnávají vzorky oční duhovky [ZHANG, 2002, s. 217].

Biometrické technologie v současnosti doplňují velmi lákavou vlastnost mechanismu autentizace. *“V současné době většina biometrických autentizací tvoří uzavřený soběstačný systém, ve kterém jsou veškeré etapy v procesu ověřování provedeny a kontrolovány v*

uzavřeném prostředí", jak poukazuje např. [PAGANI, 2005, s. 56]. Biometrické techniky v současné době doplňují významnou část mechanismu autentizace a hrají významnou roli v bezpečném uložení tajných identifikačních údajů. Nejvýznamnější rozdíl mezi biometrickými a tradičními technologiemi je *odpověď* systému na autentizační požadavek. Rozdíl je v tom, že biometrický systém neurčuje identitu člověka absolutně, ale s určitou pravděpodobností odpoví, zda-li se jedná o daného jedince.

12.1 Typy biometrických autentizací

Biometrické technologie se liší ve složitosti, schopnosti a výkonnosti. Existuje mnoho typů biometrických prvků v současné době v provozovaných, a mnoho dalších typů by mělo přijít, nebo se dále rozvíjet ve velmi blízké budoucnost (DNA, hologramy). Uvádím tedy zde typy biometrických systémů, které jsou dnes k dispozici k roku 2010 a nejčastěji využívány mezinárodními systémy na ochranu bezpečnosti.

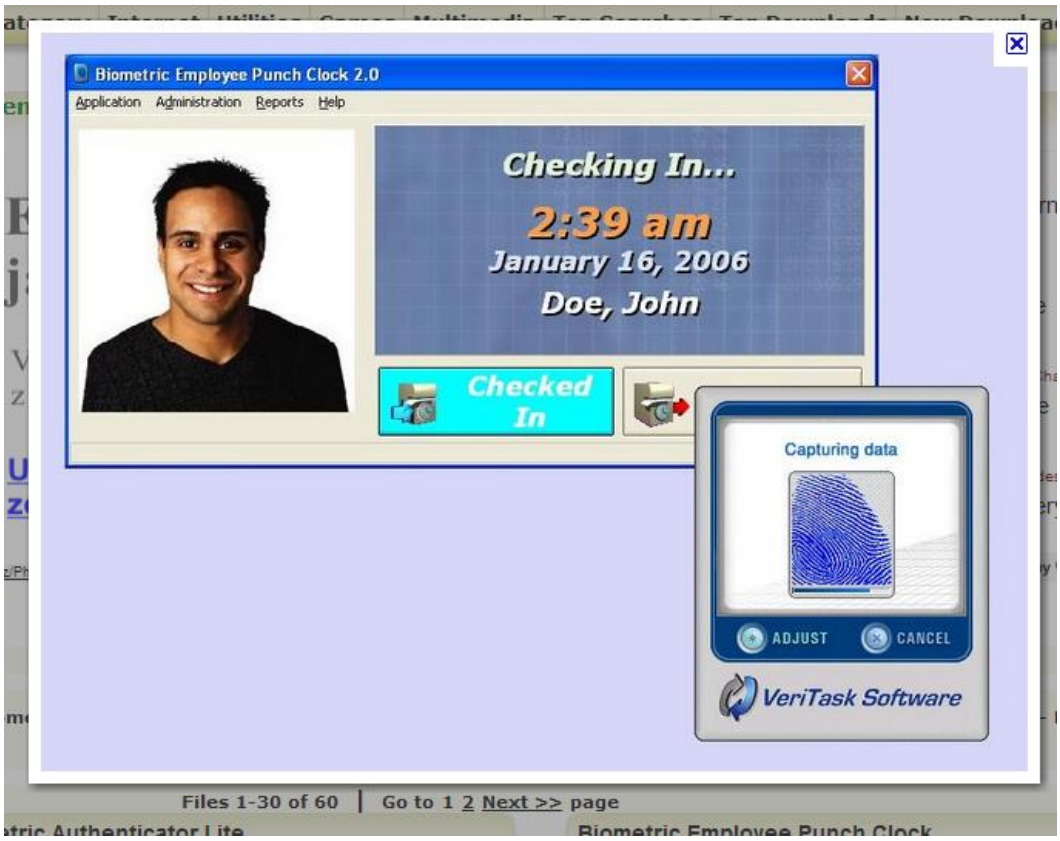
Nejčastějšími z nich jsou: (uvádím zde příklady 6 hlavních technologií). K hlavním biometrickým technologiím patří: rozpoznávání obličeje, otisků prstů, geometrie ruky, duhovky, sítnice, uznání/verifikování podpisu, RFID čip, implantát, rozpoznávání hlasů mluvčích, ověření. Do biometrických technologií v rámci současného vývoje patří: žilní vzorce, DNA, tvar ucha, tělesný zápach, holografie a scan těla. [VACCA, 2007; s.]

Každý z následujících typů zařízení zachytí data v jiné podobě a pod jiným mechanismem. Povaha biometrických údajů a způsob, jakým jsou nabyty, určuje *invazivitu protokolu* pro zápis a ověření. Způsob nabytí a související nejistoty v procesu měření může vytvořit individuální prostor k útoku tím, že manipulují s mechanismem zachycování nebo nahrazením biometrických údajů. [FLEMING, 1998; s. 2005] Nejistota na přesnost získávání a porovnávání biometrických údajů, zvyšuje rizika od různých druhů spojené s falešnými přijetí a chybného odmítnutí biometrických pověření.

1. Otisky prstů [FINGERPRINT] **:** Tato unikátní technologie využívá jedinečnosti konečků prstů. Snímá se buď obraz otisku prstu, jednak formou optického snímání nebo kapacitního snímání. Generace biometrických šablon je založena na sladění detailů charakteristických rysů otisků prstů. Jedná se o jednu z nejvíce komerčně dostupných technologií. [JAIN, BOLLE, PANKANTI, 1999, s. 43] Touto problematikou se nezabývají jenom nejnovější články nebo sborníky z konferencí, ale vychází i obrovské množství

monografií zaměřujících se na podstatu, cíle a aplikace těchto technik. Jednou z takových je i monografie Anila K. Jaina *"Biometrics: Personal Indentification in Networked Society",* která toto téma otisků prstů a počítačové bezpečnosti široce analyzuje v kontextu moderní síťové společnosti [JAIN, BOLLE, PANKATI, str. 43. 2005].

Nespornou výhodou této technologie je odpadnutí potřeby hesel. Uživatelé už nemusí vyťukávat hesla, místo toho jim je přístup umožněn pouhým dotykem. Několik států už kontroluje otisky prstů nových žadatelů o sociální služby nebo dávky, aby příjemci nemohly podvodně získat výhody pod falešnými jmény. Stát New York má v současné době více než 1 500 000, kteří jsou zaevidovaní v takovém systému [VACCA, 2007; s. 2005].



Obr. č.9 - Příklad biometrické autentizace zaměstnanců
Zdroj: http://www.filebuzz.com/files/Biometric_Authentication/1.html

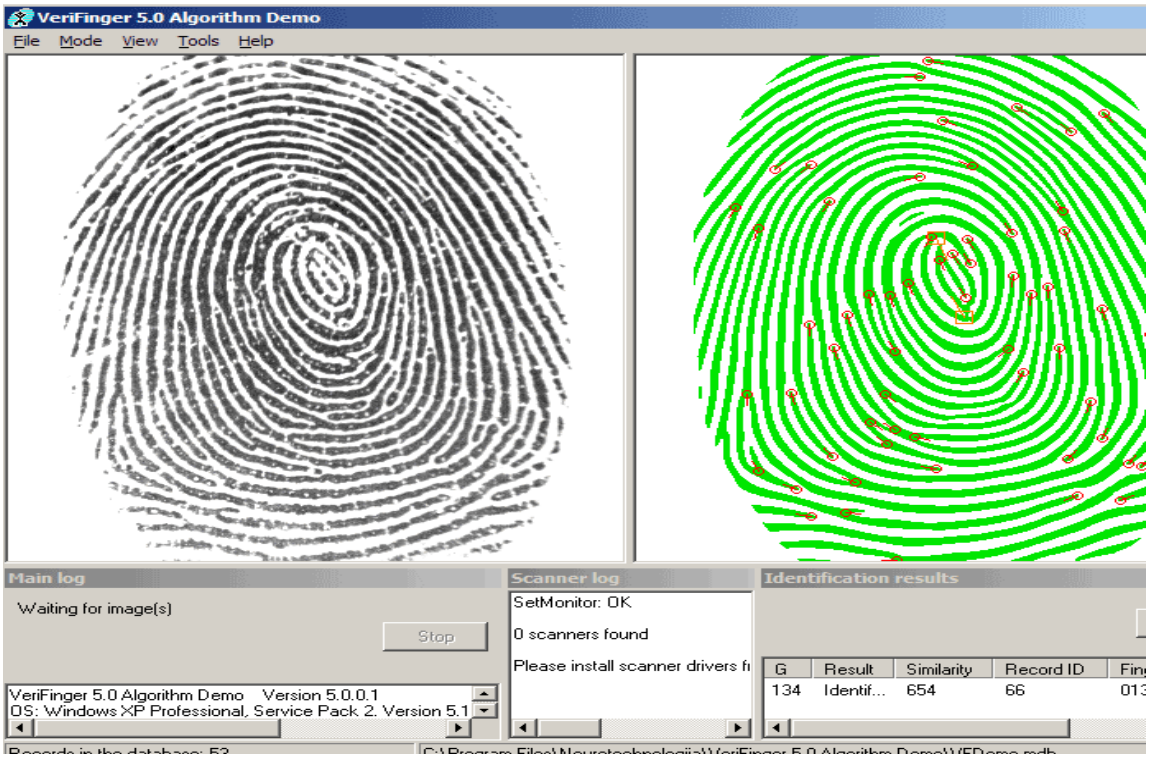
2. Rozpoznání obličeje: [FACE RECOGNITION] Např. Rakover a Cahlon ve své knize „Face recognition: congnitive and computational prosesses" navrhují např. identifikaci osoby pomocí infračerveného záření. Podle nich lze identifikaci osoby provést různými způsoby, jako je snímání obrazu obličeje ve viditelné oblasti spektra, pomocí fotoaparátu

nebo pomocí infračerveného vzorku obličeje emisemi tepla. *„Rozpoznávání obličeje funguje na viditelném světle modeluje/kopíruje klíčové funkce z centrální* ***části*** *obličeje. Pomocí širokého sortimentu kamer, systémy reagující na viditelné světlo, extrahují vlastnosti z pořízených snímků, které se v průběhu času mění, aniž by se snímaly povrchní rysy jako je výraz obličeje či vlasů"* [RAKOVER, CAHLON, str. 35, 2001].

Existuje několik přístupů k modelování obličeje snímků ve viditelném spektru. Nejčastěji se používají analýzy hlavních komponent, místní funkce analýzy, neuronové sítě, elasticko-grafové teorie a multi rozlišující analýzy. Některé analýzy jsou zaměřené na stacionární zachycení uživatele, za účelem zachycení obrazu, ačkoli mnoho systémů dnes používá real-time proces detekce osob a vyhledávání obličeje automaticky. Více o typech jednotlivých a způsobech jejich použití nalezneme u Johna R. Vaccy a jeho knize „Biometric technologies and verification systems" [VACCA, 2007; s. 226]

Uživatelé metodu biometrických měření označili podle průzkumů jako nejméně rušivou a agresivní[37] [BOULGOURIS, N.V., 2009, str. 47]. Abychom se tedy zpětně vrátili k tomu, jak přesně funguje metoda rozpoznávání obličeje. Funguje na základě testování různých částí oka. Snímač oční sítnice pomocí biometrické šablony vytvoří záznam vzoru kapiláry cév v zadní části oka. Skenování lze provádět na dálku pomocí vysoce rozlišujícího fotoaparátu a díky šabloně vytvoří proces podobný sítnici skenování [LEELAND, 2008; s. 12, 57]. Tyto metody a mnohé další popisuje jeden z nejnovějších výzkumných materiálů nazvaný *"Face Recognition : New Research"* od autorky Katherine B. Leelandové, která se v současnosti zabývá mimo jiné i způsoby behaviorální korelace a antropologickými výzkumy v této oblasti a metodikami zpracovávání těchto dat.

[37] Více se o jednotlivých průzkumech dočteme v knize "Biometric: Theory, Methods, and Applications od N.V. Boulgourise, která obsahuje obrovské množsví detailů jednotlivých měření a výsledky výzkumů. Např. srovnávací průzkumy biometrických technik ověření identity na základě neuronové sítě.



Obr. č. 10 - Identifikace pomocí otisků prstů

Zdroj: http://www.filebuzz.com/files/Biometric_Authentication/1.html

3. Rozpoznávání mluvčích (SPEAKER RECOGNITION] Tato technika využívá akustické vlastnosti řeči, které se liší mezi jednotlivci. Tyto akustické vzory odráží jednak anatomie (velikost a tvar krku a úst), a jednak charakteristiky chování, (styl mluvení). Zařízení těchto principů používá 3 styly vstupu. Většina aplikací verifikace mluvčích používá dependentní vstup a je využíván vždy, když existuje podezření z podvodníků. *„Různé technologie pro zpracování a ukládání hlasových příkazů obsahují skryté Markovy modely, maticové algoritmy, neuronové sítě, maticové reprezentace a rozhodovací stromy.“* [KESHET, BENGIO, 2009, str. 215]

Z pohledu uživatelů je tato technika vnímána jako neinvazivní. Tato technologie potřebuje přidaný hardware a za pomocí mikrofonů a hlasem přenosných technologií, umožňuje např. rozpoznávání dlouhých vzdáleností přes běžné telefony. (Drátové nebo bezdrátové linky) [FLEMING, 1998; s. 63, 65].

4 Snímání duhovky a sítnice [EYE BIOMETRICS: IRIS AND RETINA SCANNING]

Jedná se o metodu, která se používá na oční duhovky, která je barevným prostorem obklopující zornici oka. Vzorky duhovky jsou získávány prostřednictvím video systému založeného na snímání obrazu. Skenovací zařízení pro duhovky se používají především v personálních aplikacích po několik let. Tato technologie funguje dobře v obou způsobech, jak verifikaci, tak identifikaci uživatelů. (v systémech provádějí jedno nebo mnoho vyhledávání v databázi). Stávající systémy mohou být dobře využity i v přítomnosti brýlí a kontaktních čoček. Tato technologie se rovněž nepovažuje za invazivní, neboť nenastává fyzický kontakt se scannerem. Snímání duhovek bylo používáno např. pro práci s jedinci z různých etnických skupin a národností. [REID, 2004 s118, 122] Jedním z výborných článků zabývajících se touto tématikou, je monografie „*Biometrics for network security"* od autora Paula Reida, kde představuje tuto koncepci jako nejslibnější metodu biometrik. Nazývá ji téměř „Svatým Grálem".

Obr. č. 11 - Příklad digitálního snímání sítnice

Zdroj: http://www.shutterstock.com/pic-767857/stock-photo-digital-retina-scan-of-a-blue-eyed-woman.html

5 Geometrie ruky a prstů [HAND GEOMETRY]

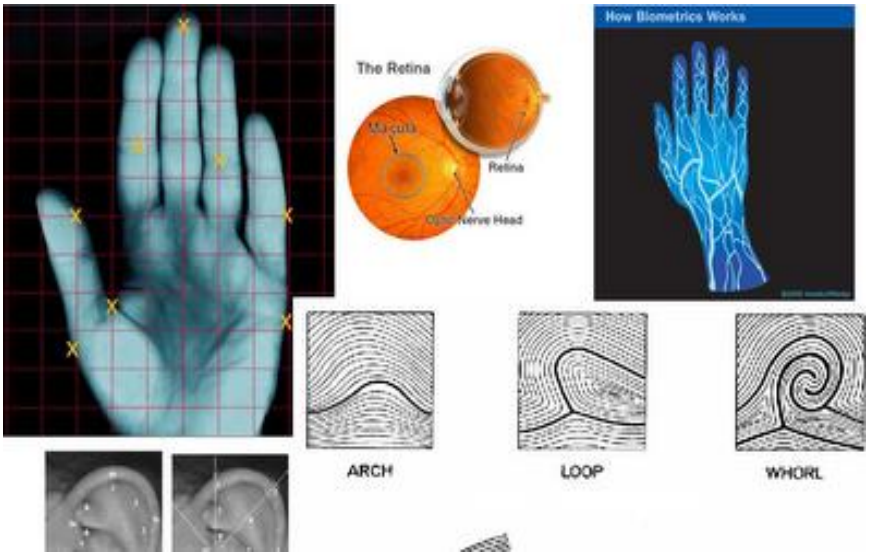
Tyto metody personální identifikace jsou dobře známy. Ruční rozeznávání bylo k dispozici více než 30 let. Pro dosažení osobního ověření, změří systém fyziologické vlastnosti

buď prstů, nebo celých rukou. Geometrie ruky je atraktivní metodou autentizace z řady důvodů. Mezi faktory měření patří délka, šířka, tloušťka a plocha rukou. *"Zajímavou charakteristikou je, že některé systémy vyžadují malý biometrický vzorek, (pár bytů)."* [FLEMING, 1998; s.63, 65].

"Geometrie ruky se prosadila v řadě aplikací. Měří např. čas docházky, fyzické kontroly přístupu anebo osobní ověření autenticity žádosti." [BOLLE, str. 45, 2003] Nicméně, neexistuje zde množství literatury věnované výzkumu záležitostí souvisejících s ověřováním geometrie ruky, místo toho hodně z dostupných informací je ve formě patentů nebo použití zaměřených na popis. Výrazné výjimky jako prototyp systému popsaný [JAIN (et. al.)] např. 3D profilu ruky nebo identifikačních přístrojů.

6 Ověřování podpisu [SIGNATURE RECOGNITION AND KEYSTROKE DYNAMICS]

Tato technologie používá dynamickou analýzu podpisu k ověření osoby. Tato technologie je zaměřena na měření rychlosti, tlaku, úhlu a využívání osobou, která vytvořila podpis. Největšího úspěchu a využití dosáhla aplikace v *elektronickém obchodě*, kde je podpis uznávanou metodou osobního ověření. [ADVANCES IN BIOMETERICS: THIRD INTERNATIONAL CONFERENCES, ICB, 2009, str. 157-160]



Obr. č.12 – Geometrie ruky
Zdroj: http://jacinthnote.blogspot.com/2009_08_01_archive.html

12.2 Využití a potenciál biometrických technologií

Biometrické technologie mají obrovský potenciál pro využití ve všech nových technologiích. Již nyní se uplatňují v odvětví obchodu, veřejných sférách na letištích a ve většině systémů elektronické identifikace a autentizace. V biometrických technologiích se totiž střetává několik oblastí zájmu, které vytvářejí pole pro interakci třech hlavních otázek – *soukromí, uvědomění a souhlasu*, které ale rovněž mohou přispět k rizikům, která pocházejí z těchto systémů.

Souhlas obecně nepovažuji za riziko, neboť podle mě není takový problém snadno ho získat v souvislosti s biometrickými údaji. To předpokládá, že uživatel jako odpovědná osoba, má nějakou kontrolu nad tím, jak jsou jejich údaje uloženy a zpracovány anebo že používá nějakou vhodnou úroveň poskytované ochrany uživatele v rámci systému. Např. použití silného šifrování pro ochranu biometrických údajů při uchovávání může být dobrým příkladem takovéto ochrany. Musí být samozřejmě vytvořen nějaký konsenzus se všemi stranami zapojenými do používání veřejných systémů a musí existovat osoby, které jsou odpovědny za chování jednotlivců. Zde se nabízí úplně jiná otázka. Pokud uživatel nemá jinou možnost než použít biometrický systém, může být skutečně donucen, aby dal souhlas k jeho použití?[38] [FLEMING, 1998; s. 69-75].

Na obrovský potenciál a využití této technologie jako velmi aktuální a užitečné zareagovala např. Albánie , kde k datu 14. 1. 2009 schválila biometrické údaje jako nezbytný požadavek pro zavedení biometrických prvků do cestovních dokladů na urychlení procesu liberalizace vízové politiky, kdy samotná vláda tento způsob označila za "*jeden z nástrojů na zlepšení migrační politiky a především za zkvalitnění boje s organizovaným zločinem a korupcí*."

V globálním měřítku může být dalším významným krokem v této oblasti připravený projekt Indie na čipování kreditních karet pro ekonomicky slabší obyvatele, *"kde čipové karty budou obsahovat osobní údaje držitele včetně jeho fotografie a otisků prstů."* Budou fungovat na principu klasických kreditních karet a budou propojeny s bankovním účtem držitele karty.

[38] Encyclopedia of Multimedia Technology and Networking, Volume 1, Stewart T. Fleming, Biometrics Security. Str. 67

(údaj z 8. 1. 2009). Dalším příkladem může být Rusko, kde Moskevské oddělení Federální migrační služby modernizuje své služby a kromě standardních pasů zavádí paralelně biometrické pasy, což by mělo přispět k odbourání zprostředkujících společností, které komerčně nabízejí Rusům vyřízení biometrického pasu. Dále, podle Moskevského oddělení Federální migrační služby: *"rovněž zavádí elektronická víza pro cizince a dále elektronický systém hlášení pobytu cizinců v moskevských hotelích,"* [ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ, 2010]. Mezi další země, které v současnosti vysoce využívají těchto technologií a implementují je do svých státních identifikačních systémů, patří Německo, USA a Bosna a Hercegovina.

Biometrie totiž nabízí jedinečné výhody. Biometrická data bývají použity k identifikaci vás jako vás. Tokeny, čipové karty, magnetické karty, id karty, fyzické klíče, atd. jsou především předměty, které mohou být jednoduše odcizeny nebo duplikovány, hesla mohou být zapomenuta, zpozorována nebo sdílena. Navíc v dnešním elektronickém světě to znamená pamatování si obrovských množství hesel, osobních identifikačních čísel pro počítačové účty a bezdrátové telefony, webové stránky atd. [FLEMING, 1998; s. 69-75].

Rizika bezpečnostních aplikací jsou velká pro napadení soukromí jedinců. Vliv biometrických technologií na společnost a potencionální rizika pro soukromí a ohrožení identity bude do budoucnosti vyžadovat zprostředkování a zavedení velkého množství právních předpisů. Řešením je důkladné zvážení biometrických údajů za účelem použití a právní ochranou. Důkladné zvážení významu biometrických údajů i to, jak by mělo být právně chráněno, je nyní potřeba v širším měřítku [FLEMING, 1998; s. 69-75]

Z této diskuze vyplývá jedna velmi podstatná věc. A to, že technologický vývoj je stále v předstihu před etickým nebo legálním zabezpečením.

"Biometrie nepředstavuje tajemství," [SCHNEIDER, 1999]. Pokud jsou biometrické údaje ohroženy, vyvolává to značný problém pro jednotlivce. Pokud tyto údaje poškodí jedince, pak budou nebezpečné i samotné systémy zahrnující jejich prověření. Biometrické údaje nemohou být nikdy zrušeny, a tudíž musí jím být přikládána nejvyšší ochrana. Otisky prstů na biometrické bázi jsou snadno ohrozitelné a můžou být dokonce odcizeny bez vědomí

dotyčné osoby. Rozšířené třídy útoků jsou známy jako **spoofing**[39], kdy se naruší integrita biometrického systému. Naopak biometrie slibuje rychlý, snadný, přesný, spolehlivý a méně nákladný způsob autentizace pro různé aplikace [JAKOBSSON, MAYERS, s. 80].

Zatímco biometrické bezpečnostní systémy mohou nabídnout vysoký stupeň zabezpečení, principy tradičního systémového inženýrství jsou stále zapotřebí k zajištění vysokého stupně zabezpečení. Problémem však může být entropie a zní plynoucí nepřesnosti při měření. V praxi lze u každého člověka najít u jakýchkoli dvou měřených vzorků rozdíly, a tak nemůže být porovnání nikdy stoprocentní.

[39] spoofing- třída útoku na biometrický bezpečnostní systém, v němž se zlými úmysly individuální snahy obejít korespondence mezi biometrické údaje získané od jednotlivce a jednotlivých sám. Přesné techniky pro spoofing se mohou lišit v závislosti na konkrétním typu biometrického zapojeny. Obvykle však tyto metody zahrnují použití nějaké formy protetických jako falešná prst, záměna high-rozlišení obrazu duhovky, masku, a tak dále.Stupeň pravdivosti protetických liší v závislosti na přesnosti biometrických zařízení, které je falešné a svobody, že útočník má v interakci s přístrojem.

13. ZABEZPEČENÍ AUTENTIZAČNÍCH OPERACÍ

13.1 Technologie

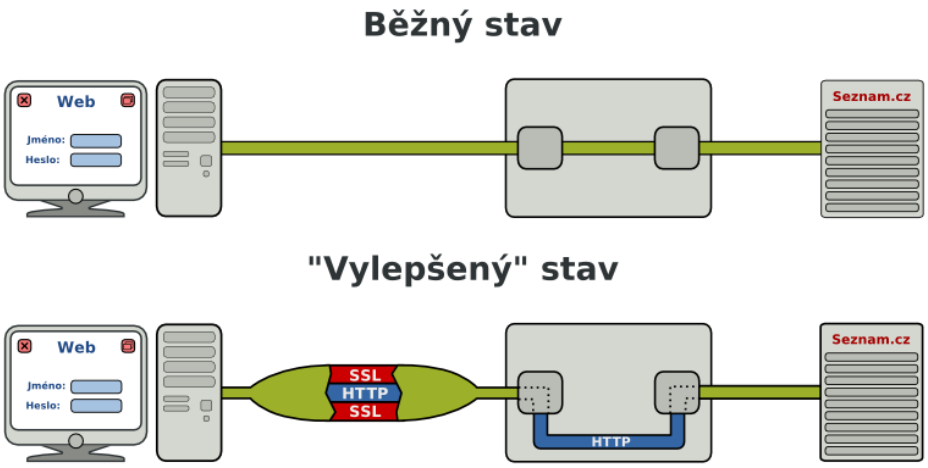
Veškerá komunikace v prostředí internetu, která má probíhat bezpečným způsobem, má na výběr dvě technologie. Jedno je použití systému. Jeho charakteristikou je, že důvěryhodnost komunikace je založená jen na vztahu *odesílatele a příjemce*. V jistých situacích však tento způsob není vyhovující. Jakmile chceme komunikovat se státními institucemi anebo servery, které jsou prakticky mimo náš dosah, otvírá se prostor pro systém bezpečnostních certifikátů. Z technického hlediska je tento systém označovaný zkratkou SSL - Secure Socket Layer.

13.1.1SSL

SSL slouží v prvé řadě jako ochrana dat uživatelů. Jedná se o technologii, která zabezpečuje *zabezpečené připojení. SSL* neboli Secure Socket Layer je vrstva ležící mezi aplikační a transportní vrstvou a zajišťuje bezpečnost komunikace šifrováním. Slouží k autentizaci komunikujících stran. Zajišťuje tedy bezpečnost datové komunikace šifrováním a slouží k autentizaci komunikujících stran. Tento protokol je založen na asymetrické kryptografii, kdy si obě komunikující strany vygenerují dvojici klíčů - veřejný a soukromý klíč. Veřejný klíč je možné zveřejnit, a pokud tímto klíčem kdokoliv zašifruje jakoukoliv zprávu, bude ji moci rozšifrovat jen majitel použitého veřejného klíče svým soukromým klíčem.

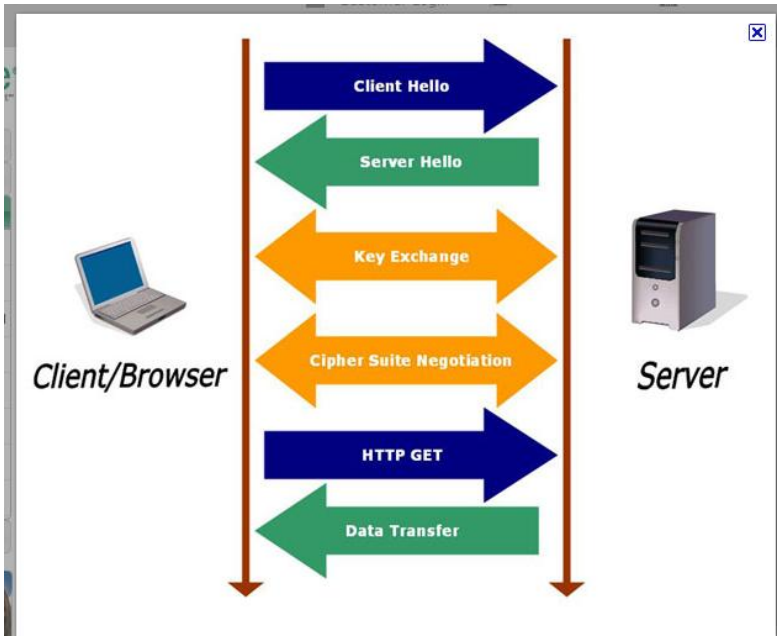
Funguje na principu zahajování komunikace klientem, ve kterém klient pošle serveru požadavek na SSL spojení, s několika doplňujícími informacemi a server pošle klientovi odpověď na jeho požadavek, který obsahuje stejný typ informací, které klient požaduje a certifikát serveru. Server tedy odešle spolu s odpovědí klientovi svůj certifikát a klient následně ověří pravost tohoto certifikátu. Podle přijatého certifikátu si klient ověří autentičnost serveru. Na základě dosud obdržených informací vygeneruje klient základ šifrovacího klíče, kterým se bude šifrovat následující komunikace. Z tohoto základu tedy vygenerují jak server, tak klient šifrovací klíč a klient a server si navzájem potvrdí, že jakákoliv jejich komunikace bude od této chvíle šifrována tímto klíčem. Od této doby obě

entity komunikují již přes šifrované spojení a bez tohoto klíče žádný požadavek na server se od této doby neodešle.



Obr. č.13 - Na obrázku je vidět ,že uživatel si pouze myslí, že se připojuje k serveru, zatímco je napojen na záškodnické zařízení

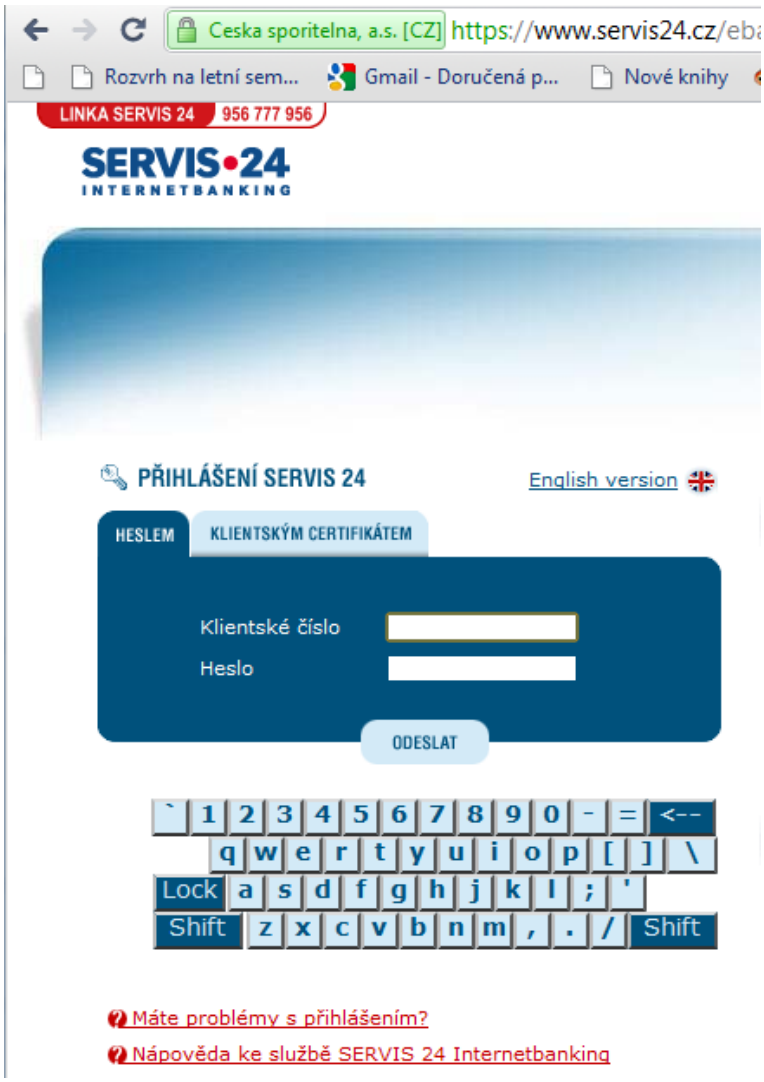
Zdroj: http://www.abclinuxu.cz/images/clanky/barton/ssl_inf_nakres.png



Obr. č.14 - Ukázka jak SSL pracuje. Obr. Klient prokazující svoji totožnost serveru.

Zdroj: https://ssl.trustwave.com/support/support-how-ssl-works.php

Protokol SSL se nejčastěji využívá pro bezpečnou komunikaci s internetovými servery pomocí HTTPS, což je zabezpečená verze protokolu HTTP. Po vytvoření spojení (session) je komunikace mezi serverem a klientem šifrovaná a je tedy zabezpečená. Využívá se tedy ve všech aplikacích, kde je potřeba šifrované komunikace, např. v elektronickém bankovnictví, při šifrování a podepisování, v e-mailu, všude tam, kde je potřeba využití bezpečnostních certifikátů a kde je potřeba zabezpečit komunikaci po celou dobu spojení. Další hlavní oblastí, kde se setkáváme s SSL, je *internetbanking.* Smyslem je to, že si uživatel musí být jistý, že je skutečně spojený s webovým serverem banky a ne nějakého podvodníka.



Obr. č.15 - Příklad se zabezpečeným protokolem https.
Zdroj: https://www.servis24.cz/ebanking-s24/dispatcher

13.1.2PGP

Jedná se o počítačový program, který umožňuje šifrování a podepisování. PGP umožňuje šifrovat a dešifrovat zprávy, digitálně je podepisovat a ověřit identitu odesílatele. Tato technologie měla dokonce takový vliv, že byla standardizována a byla umožněna spolupráce mezi několika jejími verzemi a podobným software. PGP bylo později přijato jako internetový standard pod názvem OpenPGP. Nyní se jedná o otevřený standard dodržovaný PGP, GnuPG (GNU Privacy Guard nebo také GPG). Nejčastěji se s ním setkáváme s použitím při šifrování e-mailů a celkově na zvýšení bezpečnosti e-mailové komunikace.

PGP umožňuje šifrovat a dešifrovat zprávy, digitálně je podepisovat, ověřovat identitu odesílatele a spravovat klíče. Základy této technologie jsou postaveny na asymetrické kryptografii, které se budu podrobněji zabývat v dalších kapitolách. Ve stručnosti bych ráda zmínila, že při použití asymetrická kryptografie pracuje na principu použití dvou různých klíčů, kdy šifra používá dva různé klíče a výstupem je zašifrovaná zpráva.

Právě zacházení se soukromým klíčem je nejkritičtějším bodem této technologie. Pokud počítač používá více lidí, je nutné si privátní klíč chránit dobrým heslem.

PGP má dvě základní užitečné funkce. Jednu jsme právě zmínili, tj. šifrování dat a druhou funkcí je digitální podpis, kde je princip velice podobný technologii šifrování. Odesílatel připojí ke zprávě určitý dodatek, tzv. „message digest“, který zašifruje svým elektronickým klíčem, čímž vznikne elektronický podpis. Příjemce si obstará veřejný klíč odesílatele zprávy, dešifruje přiložený podpis a porovná je s tím, jak by měl vypadat podle jeho výpočtu. Pokud oba výsledky souhlasí, můžeme zprávu považovat za autentickou. S pomocí PGP lze data odesílat *důvěrně*. Podporuje tedy ověřování zpráv a kontrolu jejich integrity.

Jako praktický příklad uvádím e-mail zašifrovaný pomocí PGP, který vypadá následovně:

```
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-2
Version: GnuPG v1.4.7 (MingW32)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org

hQQOA1JM4l3mJzWUEA//WSGo8I/9QSA5w4usYfXhm8jN9Y7mWT5370x/CMlaeXLX
```

```
tHgu6wto6UjXma08yemwlUhH6t1BmBjy1Etmrj9G+PWuCHpOs+FmInPPHZ2TojYn
onUonaz99PyVzLTvv+yg7rxN07zJaCuHIMbPHo+yY1+Y33PslOzcln8NzlKzBHA6
zD6bhD0VCN/WvE15fJdQOGTWCxEGDqWiBoOTCyMYJDd8/beT6eYduOVboZLXDooe
MGitYJnMhFZD5C0TazxnFGvI8nwqA1+nbcxlUp1iBcDBohm1aaIwA9MigvP7Yt/9
4kz2VZJdW4iN2AyhOP9Y9QAQzJ5DSOGm5TNoX9EL+Y2gPJYZz4COPizwRj7VxXkV
kgjQNyZbG597dPwRHJdICc0YKHJB6cL+0ve/tmOmf+XfFOxAxiJ+8f1Iu5j2+m6X
SdahM3cA0pDXJS9kHWidjx3D9RbheEnewm7nKde6J9TwiW9LIEY65ChvPasbwv79
gT8LPXYu54lEpQWcwdVJsgMTgU9+YYXQ7MmdqBdUMroPSdyF3YCzElixE//CoIsy
XQ01Zr8a/oabgv9xhIEjpON9qR1WbHNBp3PLliXUSpIvGe+IB2hIjKRcB9mSCp69
D61vWOdqygc6S//SMlBNJYhJLWwHjYa8U+anEi8PyZt6pafAsmUejk8HFOMRh14P
/jDHvLpy9k57k/erKK2eEiPV2JWKk7/4lGNLZWsyqKK2kEEsRgVSQR2/qdMpHZTo
aR6tbYkCrYbSeAqfqPrNabTZ0KdxT19GA7ouShevtjkmdayJ5Z+aUhbG6hNakitF
EwaIdjJNgzn302WUSex2SR7wjZpgkmppk8tFXpAOgZS+mLJTJ7bsgZzt2LUot0lf
1GNmwIc7s85wGDm+Ep2Nv+Xgh3BtS+NXLe7gPdrp022RdgRDNeuG8PxBo/IE7WfO
JP5RuDn5irWSzWNECx103ZgJB3E/ntoQWbShCMPS4OWowDIHBHwpNxofRwL91ZCt
kH7eAFJ1a0/vc5z3gwt4XZ7C8K37YQUacto0MvBNryiITYZs3riTXKhvyfQs9Hmk
zri0q+zvVU5/r21x1tm1335r6q007A4Rl0M5I9p0CAFr3hFODQe3Y2bNL4s8r+8b
PEmrkdTKYcuAmeAHopGdVGcNjyVPohNYpavQsxF6EHjnWnIKPueh11ZaD9ERcQ9g
BGi5AC3N7hNrsBqocME4I8/Stqc9/8RUUfue6WkGre+B+OKfg27wRjGu19e7uA3w
9yyowLiFoVVZSt2jqVM2TiN+rdQTX7BICmpXU3lJ+CIdGImPdNAxVu2lrhwAACPX
eFXJGpsQ/aBBKb2t/hWCulRbhdRuXjl8NKB8Wb6334ACNr7KFCW5tb6s9zqAwwGK
AD7UFYFSbcvrKRCxDusectaJF37VdV1d6JcOBdAzHFx9Cu4nZpVxPlWqwCg=
=18gY
-----END PGP MESSAGE-----
```

Zdroj: *vlastní*

14. KRYPTOGRAFICKÉ SYSTÉMY

Je důležité říct, že většina principů zabezpečené autentizace uživatele funguje na potřebě šifrování dat. Dvě stěžejní potřeby v ochraně dat obsahují dvě následující kapitoly, ve kterých jsou popsány prostředky autentizace, které souvisejí s potřebou šifrování dat. Všichni, kdo používají nové technologie, zmiňují šifrování jako nezbytnou potřebu transparentních mechanismů pro uživatele. Proto je možné tvrdit, že šifrování dat v pohybu (data-in-motion), a tedy i šifrování obecně je rozšířené.

Kryptografie v informačních systémech se používá jako nástroj ochrany dat ve všech etapách jejich zpracování. Logická obdoba trezoru, ve kterém jsou uloženy cenné informace. Trezor však poskytuje ochranu proto, že je fyzicky odolný, zatímco šifrovaní činí určitými algoritmy změny z *čitelné informace na nečitelnou.* **"***Šifrovací algoritmus je funkce sestavená na matematickém základě a provádí samotné šifrování a dešifrování dat."* [CLARKE, str. 189, 2008] *Šifrovací algoritmus obecně upravuje data tak, aby je nemohly číst běžnými prostředky nepovolané osoby. Takže důležitou funkcí tohoto "trezoru" je, aby i při odcizeni takto zašifrovaných dat nedošlo k úniku informací. Šifrovací klíč říká šifrovacímu algoritmu jak má data (de)šifrovat, podobá se počítačovým heslům, avšak neporovnává se zadaná hodnota s očekávanou, nýbrž se přímo používá a vždy tedy dostaneme nějaký výsledek, jehož správnost závisí právě na zadaném klíči"*[STAMP, str. 51, 2005]. Délka klíče ovlivňuje kromě jiného časovou náročnost při útoku hrubou silou – což je kryptoanalytická metoda, kdy postupně zkoušíme všechny možné hodnoty, kterých klíč může nabývat. Nešifrovaný text bude informace, kterou chceme zašifrovat. Zašifrovaný text bude informace po zašifrování [WINDLEY, str. 171, 2005].

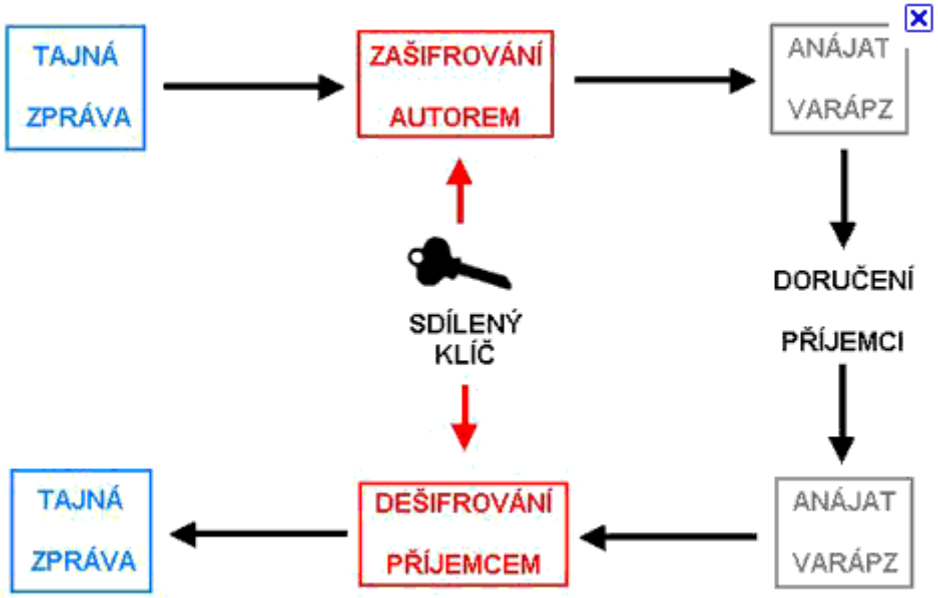
Kryptografické metody lze dělit podle několika hledisek, uvedu pouze nejpoužívanější a nejzásadnější. Jako první bych uvedla rozdělení na šifry jednosměrné a obousměrné. *"Šifrování dat pomocí několika nezávislých šifrovacích schémat "tzv. multi-šifrování" bylo navrženo v různých souvislostech, bývá využíváno například k ochraně proti částečné klíčové expozice anebo dešifrování, neboť představuje práh přístupu k datům."* [BRUGGEMANN, str. 188, 204] Šifrování můžeme rozdělit na několik typů. V prvé řadě to může být rozdělení na obousměrné a jednosměrné. *"Rozdíl je v tom, že u obousměrného šifrování při znalosti správného klíče jsme schopni dešifrovat výsledek a získat zpět originál. Zatímco*

u *jednosměrné tento zpětný proces provést nelze (a obvykle se ani nepoužívá žádný klíč)"* [HANSMANN, 190, 2003]. Ačkoli se na první pohled jednosměrné šifry mohou zdát nevyužitelné, své uplatnění mají. Nejčastěji slouží k ukládání hesel, čímž se zabrání jejich odhalení i po zpřístupnění jejich uložené verze, ale zároveň zůstává možnost ověření hesla zadaného uživatelem – zadanou hodnotu stačí zakódovat a porovnat s uloženou variantou. Obdobou jednosměrných algoritmů jsou výtahy zpráv a digitální podpisy. Obousměrné šifry používáme všude tam, kde chceme mít možnost zpřístupnit původní text – ale jen vybrané skupině lidí, znajících příslušný klíč. Daleko podrobněji o těchto postupech pojednává kniha *"Basic methods of cryptography"* od J. Lubbe [LUBBE, str. 202,1998].

14.1 Symetrická kryptografie

Jednou z definic symetrické kryptografie, která se mi líbila, neboli kryptografie založené na symetrických šifrách, je definice z knihy *"NET Security and cryptography"* od P. Thorsteinsona a je následující: *"Symetrická šifra je šifra, ve které se k šifrování a dešifrování používají stejný klíč nebo klíče, které jsou matematicky příbuzné jednomu takovým způsobem, že jde lze snadno vypočítat jeden klíč ze znalosti druhého, což je skutečně jediný klíč..."* [GUTTAMAN, str. 65, 1995].

Podle volné parafráze z knihy *"Information theory, coding and cryptography"*, ze které vycházím v následujícím textu, se v podstatě jedná o to, že předpoklad je v tom, že existují dvě základní entity, tedy uživatel a systém. Tyto dvě entity mají společný klíč, kterým se šifrují a dešifruji autentizační data. Existují tedy dva klíče, které musejí být odděleny od šifrované zprávy, neboť se používá jen jeden klíč pro šifrování a dešifrování, tento druh techniky se tedy nazývá *tzv. "symetrická kryptografie nebo kryptografie jednoho klíče nebo privátní klíčová kryptografie.* [BOSE, 2007 s.283]



Obr. č.16 - příklad výměny klíčů u symetrické kryptografie
Zdroj: http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&clanekID=245

Tedy smyslem toho je, se používá jeden klíč k šifrování i dešifrování textu. Algoritmy symetrické neboli algoritmy s jedním klíčem se tedy především používají k šifrování a dešifrování zpráv. Tedy naprosto praktický příklad. Příjemce potřebuje rozšifrovat zprávu. K tomu, aby příjemce rozšifroval zprávu, potřebuje mít identickou kopii klíče (identické klíče). Naprosto logicky - pokud příjemce nemůže potkat odesílatele osobně, a musí získat klíč, musí být klíč nějakým způsobem předán příjemci. Proto největší problém symetrické kryptografie je *distribuce klíčů*. Nicméně, algoritmus jednoho klíče je velmi efektivní zejména v předání velkých objemů dat. V symetrické kryptografii jde tedy o to, že jsou dvě strany, které si vyměňují klíče pomocí stejného algoritmu. Tento klíč bývá čas od času měněn. Šifrovací algorimus je přístupný veřejnosti, takže proto by měl být silný a dobře vyzkoušený. Velikost klíče[40] je zásadní pro vytvoření silného šifrování. [41][PARAFRÁZE NA VACCA, 2007, s.283]

[40] Americká Národní bezpečnostní agentura NSA bylo ještě v 90. letech přijatelné použít klíč o velikosti 40 bitů. Dnes, nejbezpečnější systém používá 128-bitové klíče nebo dokonce klíče ještě delší. [Information theory, coding and cryptography, BOSE s. 283, rok.]

[41] [Information theory, coding and cryptography, BOSE s. 283, rok. 2007]

Při tvorbě symetrických kódů je výhodou rychlost algoritmu. Na straně příjemce i odesílatele musí nastat určitý konsenzus pro distribuci klíče. Při tvorbě symetrickych kryptografických algoritmů se používají dvě základní techniky: substituce a transpozice. Podstatou substituce je, že nahrazuje znaky otevřeného textu jinými znaky, čímž vzniká šifrovaný text. V podstatě hlavni úlohou celé symetrické kryptografie je bezpečné přenesení zprávy od odesílatele k příjemci a v tomto případě se týká bezpečné distribuce tajných klíčů. Tedy hlavní nevýhodou symetrické kryptografie je nutnost velkého množství klíčů a potřeba jejich distribuce. Na druhou stranu nejsou kladeny žádné nároky na výpočetní náročnost symetrických šifer.[PARAFRÁZE NA BOSE, 2007 s.283, 284]

Symetrická kryptografie je především *prostředkem* k požadavku bezpečného přenosu zpráv v počítačových sítích, protože obsah zprávy není možné číst bez tajného klíče třetí osobou, ať už záměrně nebo náhodně. Symetrická kryptografie se používá v informační bezpečnosti a může být použita jako nástroj k otázkám a řešení integrity a ověřujícím požadavkům. Ještě, abychom si vysvětlili, jakou roli hraje autentizační kód zprávy (zde čerpám podle autorů Peeringa a Tygara), který je velmi důležitý při verifikaci zprávy. Funguje tedy na následujícím principu: odesílatel vytvoří souhrn zprávy nebo **autentizační kód zprávy (MAC)**, zašifruje ho tajným klíčem a odešle se zprávou. Příjemce pak dešifruje MAC, který mu byl odeslán a oba dva porovná. Pokud jsou klíče identické, pak zpráva, která byla přijata, musí být shodná s tou, která byla odeslána. Více o využití autentizačních kódů zprávy (MAC) najdeme v knize “Secure broadcast communication in wired and wireless networks” [PARAFRÁZE NA PERRING, TYGAR, 2003, od str. 214]

14.1.1 Key management

Hlavní potíž se symetrickými režimy, jak uvádí např. J. Hope, je, že tajný klíč musí být vlastněn oběma stranami a proto musí být přenesen od tvůrce k více lidem. Kroky vedoucí k zajištění bezpečného mechanismu pro tvorbu a předání tajného klíče, jsou označovány jako **Key Management.** Jedním ze zajímavých článků, který o Key Managementu pojednává podrobněji, je článek *“The Ten Key Management Issues of the Third Wave”*[PARAFRÁZE NA HOPE, J.,str. 15, 16, 17.] Nebo můžu doporučit knihu *“Foundation of security: what every programmer needs to know”,* která se od kapitoly 13, od strany 227 rovněž zabývá touto problematikou.

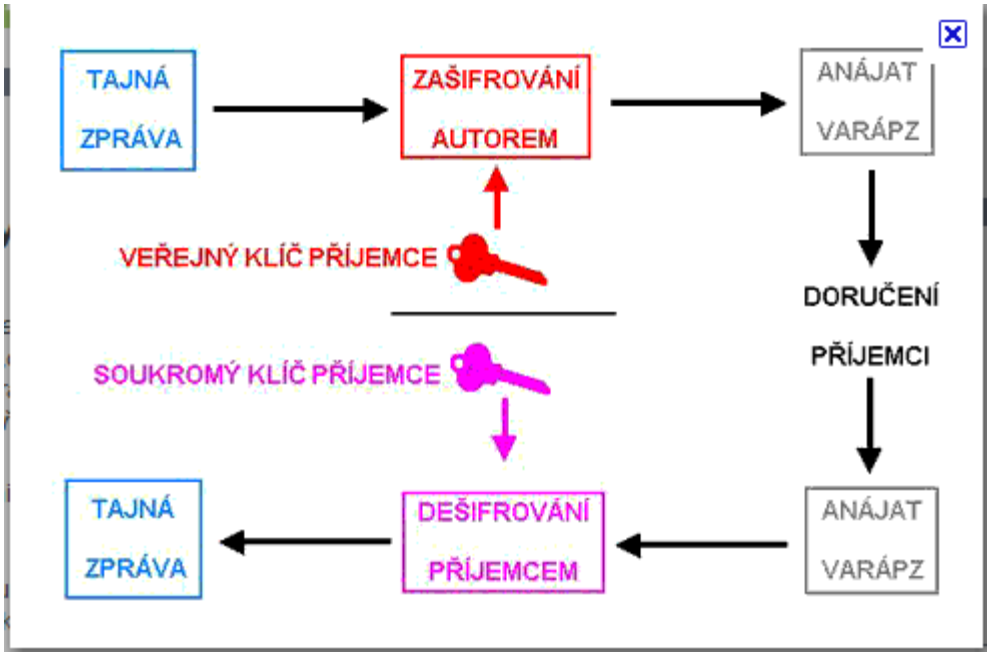
14.1.2 Public key infrastructure

Stejně tak existují dva typy symetrických algoritmů a steam šifry. Pro symetrickou kryptografii je problémem již několikrát zmiňovaná *výměna klíčů nebo jejich distribuce*. Např. Chcete-li použít metodu symetrické kryptografie mezi Vámi a někým jiným na internetu (nebo nějaké jiné nedůvěryhodné sítě), musíte mít prostředky k bezpečné výměně tajného klíče. Musíte vymyslet mechanismus mezi včetně dopravy disku s klíčem, čtení po telefonu, nebo pomocí jiné sítě předávající klíče. Nicméně preferovanou metodou je nasazení kompletní **Public Key Infrastructure.** Řešení, které využívá asymetrické kryptografie k výměně symetrického kryptografického klíče. Pro výměnu tajného klíče se používají jednotné komunikační relace, které se pak likvidují. *"PKI je jednoduchý koncept, jak nasadit různé aspekty různých kryptografických mechanismů do jednoho, kompletního, reálného řešení. Každý člen sítě na síti v symetrické kryptografii potřebuje mít sdílený tajný klíč se všemi členy v zájmu podpory zabezpečené komunikace."*[STEWART, 2008, 181-185]

14.2 Asymetrická kryptografie

Asymetrická kryptografie nebo také (kryptografie s veřejným klíčem). *"Jedná se o skupinu kryptografických metod, která je vytvořená pro účel ochrany informací a její principy se používají k šifrování a dešifrování zpráv."* [BANDYOPADHYAY, ADI, TAI-HO86-89] Oproti symetrické kryptografii je základní rozdíl v tom, že se k šifrování i dešifrování používá jediný klíč. Doslovnou definici nám poskytuje Kahate v knize *"Cryptography and network security"* a jedná se *o " V asymetrické kryptografii, také označována jako "kryptografie veřejného klíče" jsou použity dva různé klíče (které tvoří dvojici klíčů). Jeden klíč je používán pro šifrování a pouze další odpovídající klíč musí být použit pro dešifrování"* [KAHATE, 2003, str. 154] Vlastními slovy bychom řekli, že vychází z infrastruktury veřejných klíčů a implementuje použití dvou různých matematicky svázaných klíčů, které jsou vytvořeny současně ve vzájemné interakci. Další obdobnou definici nám poskytuje např. Dobda *"Asymetrická kryptografie vznikla z potřeby komunikace na neutajeném komunikačním kanále, kde jsou k dispozici dva klíče tvořící klíčový pár se schopností šifrovat a dešifrovat informace."* [DOBDA, 213, 1998] Podle nás, je tedy jejich matematický vztah je založen tedy na tom, jestli chce uživatel (entita) získat soukromý klíč k rozkódování nějaké operace zašifrované veřejným klíčem a pokud tato operace vyžaduje veřejný klíč, bude potřebovat k invertování operace soukromý klíč.

Základním znakem asymtrické kryptografie je fakt, ze veřejný klíč se může libovolně rozšiřovat, často je ukládán na určené servery veřejných klíčů. Viz problematika veřejných klíčů (kapitola elektronický a digitální podpis). Information Security and Assurance: 4th International Conference, ISA, 2010, konkrétně kapitola " *A Cryptosystem for Encryption and Decryption od Long Confidential Messages".* [BANDYOPADHYAY, ADI, TAI-HO86-89]



Obr. č.17 - Příklad výměny klíčů u asymetrické kryptografie
Zdroj: http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&clanekID=245

Šifrovací klíč pro asymetrickou kryptografii má dvě části. Jedna část se používá pro šifrování zpráv, (kterou příjemce zprávy nemusí znát), druhá pro dešifrování. (kterou odesílatel šifrovaných zpráv zpravidla vůbec nezná). Ve výsledku to znamená to, entita, která zprávu zašifruje, nemusí s dešifrujícím příjemcem zprávy sdílet žádná tajemství, čímž eliminují potřebu výměny klíčů. Tato vlastnost je tedy základní výhodou asymetrické kryptografie [DASWANI, KERN, KEASAVAN, s. 221]. *"Když uživatel zasílá data do systému, na vstupu do systému je zašifruje tzv. veřejným klíčem, naopak u výstupu ze systému, jakmile potřebuje provést tzv. dešifraci dat, používá soukromý klíč,"*[DASWANI, KERN, KEASAVAN, s. 223]. Tedy jednoduše, jestliže chceme entitě, uživateli, poslat zprávu musíme hledat veřejný klíč této entity, pomocí něhož zprávu zašifrujeme. *"Příjemce jako jediný je tedy schopen danou zprávu dešifrovat svým soukromým klíčem."*[DASWANI, KERN, KEASAVAN, s. 222].

Více o problematice asymetrických veřejných klíčů najdeme v obsáhlé knize *"Foundation of security: what every programmer needs to know"*. Kryptografie s veřejným klíčem využívá asymetrii k vytvoření matematických funkcí, které jsou založeny na dvou predikátech. Asymetrická kryptografie je na rozdíl od kryptografie se symetrickým klíčem založená na principu matematických funkci a jednosměrného šifrování [DASWANI, KERN, KEASAVAN, s. 223].

Provedení samotné operace, tedy dešifrování, je velmi obtížné, neboť nelze tuto informaci dešifrovat bez znalosti určitých informací, které by ji umožnily dešifrovat. Obtížnost tohoto šifrování je v tom, že když bude chtít někdo jiný zjistit postup, jakým jsme informaci šifrovali, bude muset prověřit všechna možná množství jednotlivých kombinací.

Představme si uživatele, který bude chtít dešifrovat informaci, bez znalostí, které k tomu nutně potřebuje. Například, jestli dva lidé, kteří se navzájem neznají a chtějí na dálku komunikovat soukromě na internetu, aby se museli setkat osobně anebo mluvit spolu po telefonu, aby se dohodli na klíči. Asymetrická klíčová kryptografie umožňuje způsob, jak jim to umožnit bez nutnosti takovýchto řešení.

Nejpoužívanějším algoritmem je RSA, který se považuje se "*za jeden z matematicky nejdokonalejších algoritmů a funguje na prvočíselnosti a faktorizaci (rozložení) velkých prvočísel. "*[SWAMINATHA, ELDEN 2003, 116] Tento algoritmus byl normalizován několika standardizačními organizacemi a ve Spojených státech dokonce patentován. Patent před několika lety vypršel a nyní je algoritmus volně šiřitelný. V současnosti jsou velké naděje vkládány do systému založených na bázi eliptických křivek. Jedna se o algoritmy, které dokáží provádět kryptografické operace několikrát rychleji než RSA při zachovaní stejné bezpečnosti. [BOYLES, str. 330, 2010] Nově se algoritmy RSA se zabývá např. monografie *"CCNA Security Study Guide "*od Tima Boyle.

S asymetrickou kryptografií dochází k problému *distribuce veřejných klíčů*. "*Tento mechanismus slouží k identifikaci identit v rámci distribuce veřejných klíčů. Slouží k ověření subjektu, zda získal vhodný veřejný klíč jiného subjektu. Řešením je ustanovení důvěryhodných autorit, tzv. certifikační autority (CA) nad kterými existuje centrální dohled a které jsou uspořádány do hierarchické struktury s jasně definovanými vztahy podřazenosti a nadřazenosti,"* [STEWART, CHAPPLE, 2008, str. 375, 376].

Nevýhodou této metody je větší pomalost než v případě symetrického systému. Je nutná jistá kontrola nad klíči, neboť útočník by mohl čistě hypoteticky nahradit veřejný klíč svým klíčem za účelem dešifrování zpráv napadnuté strany. Víme, že velkou výhodou asymetrické kryptografie je především schopnost umožnit *"šifrování dat a především realizaci digitálního podpisu. Každá entita má dva klíče. První soukromý se používá pro dešifrování zprávy nebo vytváření digitálního podpisu."* [STEWART, CHAPPLE, 2008, str. 375]. Asymetrická kryptografie pak sama o sobě neřeší autenticitu veřejného klíče. Je důležité rozhodnout, zda daný klíč opravdu patří dané entitě. Hlavní výhodou je menší počet klíčů než je tomu u kryptografie symetrické [STEWART, CHAPPLE, 2008, str. 381]. Velmi kvalitní a podrobné informace poskytuje týkající se tzv. certifikačních autorit a distribuce veřejných klíčů kniha, z které jsem čerpala informace do této kapitoly: "*CISSP: Certified Information Systems Security Professional Study Guide"* od autorů J. M. Stewarta a Mika Chapple, v kapitole deset se pojednává o PKI and Cryptographic Applications.

14.2.1 Využití asymetrických šifer

Kryptografie s veřejným klíčem se výrazně používá v oblasti ochrany informací. Aplikace se osvědčuje k ověření autentizace formou tzv. Digitálního podpisu nebo ke kontrole integrity zpráv, kde se použitím asymetrické šifry problém výrazně zjednodušuje, neboť závislost těchto dvou klíčů je nezjistitelně složitá. Např. pokud chci jako odesílatel zprávy ověřit autentičnost zprávy (tedy zjistit, jestli zpráva skutečně pochází od toho, od koho ji očekáváme), musím mít k dešifrování zprávy k dispozici tajný klíč odesílatele. *"Veřejný klíč není utajován, takže zde existuje potencionální riziko, že téměř kdokoli může tento veřejný klíč zjistit a podvrhnout falešnou zprávu."* [DOBDA, 1998, str. 216]. Toto riziko, např. u symetrických šifer není možné. Druhý, veřejný klíč používaný k dešifrování zprávy, musí příjemce získat důvěryhodným způsobem. A dále uvádí: *"Při aplikaci asymetrické šifry, která v tomto případě využije autentizační spojení, se zobrazuje šifrovaná zpráva pomocí asymetrické šifry a je nejdříve zašifrována tajným klíčem odesílatele (provádí autentizaci) a pak veřejným klíčem příjemce. Příjemce tedy provede opačný postup dešifrování, a je-li zpráva po dešifrování čitelná, lze prohlásit, že je autentická."* Nevýhodou asymetrické šifry je její pomalost, a proto se nepoužívá pro šifrování dlouhých zpráv. U tohoto způsobu se používá metoda kombinace symetrické a asymetrické šifry, kde se symetrická šifra používá k samotnému šifrování a dešifrování zpráv, zejména pro její rychlost a asymetrická šifra se používá pro bezpečný přenos klíče symetrické šifry [DOBDA, 1998, str. 218].

15. ELEKTRONICKÉ CERTIFIKÁTY

Jedná se o jednu z forem autentizace a šifrování. Elektronický podpis[42] dokáže bezpečně zajistit *identifikaci* odesílatele. Certifikační autorita je organizace, která funguje jako důvěryhodná třetí strana u asymetrické kryptografie. V prvním případě certifikáty zajišťují funkci *ověření* identity podepsané osoby, ve druhém případě pomocí kryptografie zajišťují provázání mezi *klíčem osoby* a *identitou osoby*.

15.1 Funkce podpisu

Elektronický podpis se vyrábí tak, že se ze vstupního dokumentu spočítá *kontrolní součet.* Jeho specifičnost je v tom, že na výstupu poskytne řetězec, ze kterého je možné odvodit původní postup. Především dokládá *integritu* podepsaného dokumentu a autentizaci podepsaného. Pro některé účely je navíc vyžadován zaručený elektronický podpis pouze s předepsanými typy certifikace, tedy „založený na kvalifikovaném certifikátu“ digitálního podpisu (u odesílatele) se vytváří ve dvou krocích:

„1. Spočte se otisk (hash) podepisovaného textu.

2. Otisk dokumentu se za pomocí soukromého (privátního) klíče podepisujícího zašifruje.

Výsledkem druhého kroku je digitální podpis. Ten se pošle spolu s podepisovaným textem

příjemci. Jeho ověřování (verifikace) se na straně příjemce provádí ve třech krocích:

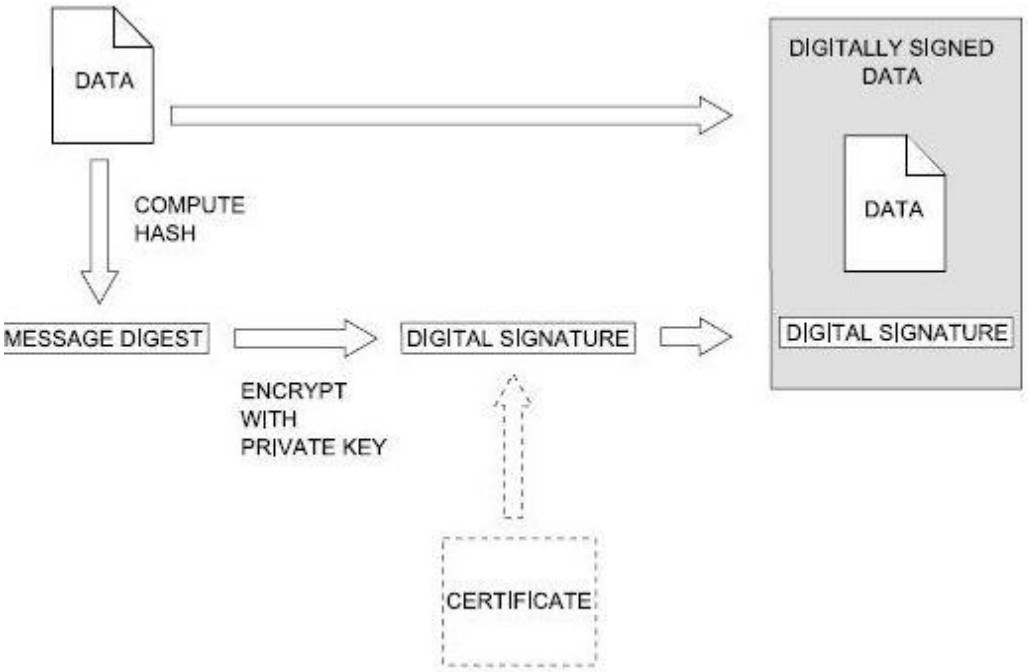
1. Příjemce samostatně spočte otisk z přijaté zprávy.

2. Příjemce dešifruje přijatý digitální podpis veřejným klíčem odesílatele.

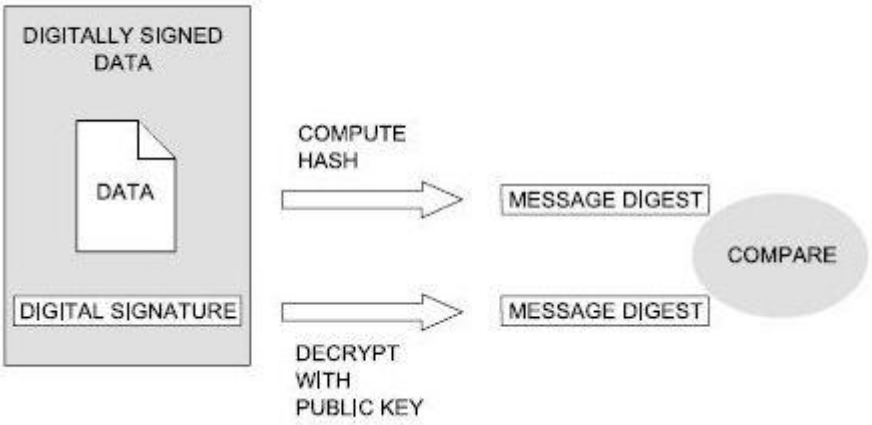
3. Příjemce porovná výsledek získaný z bodu 1 s výsledkem získaným z bodu 2. Pokud jsou stejné, pak mohl digitální podpis vytvořit pouze ten, kdo vlastní soukromý klíč odesílatele

[42] Pojmy digitální a elektronický podpis budeme považovat za synonyma, i když právní úpravou se jedná o zcela odlišné věci.

– tedy odesílatel. A navíc tato skutečnost prokazuje, že zpráva nebyla během přenosu pozměněna, tj. zajišťuje i integritu zprávy.“ [DOSTÁLEK, VOHNOUTOVÁ, 2006]



Obr. č.18 - Schéma podepisování



Obr. č. 19 - Schéma verifikace

15.2 Funkce šifrovací

Celý tento systém je založen na tom, že každý uživatel vlastní certifikát a dvojici klíčů. Jeden klíč se nazývá veřejný a může se volně distribuovat mezi další uživatele. Druhý klíč se nazývá soukromý (privátní) a ten si naopak vlastník certifikátu musí pečlivě střežit a předejít jeho zneužití. Asymetrická kryptografie zde hraje tu roli, že pro šifrování se používá privátní klíč a pro dešifrování veřejný. Zprávu tedy uživatel podepisuje svým tajným klíčem a tuto zprávu (digitální podpis) může za pomoci veřejného (dešifrovacího) klíče ověřit kdokoli. Důležité je tedy popsat proces vytváření a ověřování podpisu u odesílatele a příjemce.

16. SWOT ANALÝZA POPSANÝCH AUTENTIZAČNÍCH TECHNOLOGIÍ

16.1 Analýza SWOT

Pomocí SWOT analýzy jsou v diplomové práci symbolicky vyjádřeny výstupy analýzy provedených autentizačních metod a jejich komparace. Zkratka SWOT je odvozena z počátečních písmen analyzovaných oblastí (Strenghts – silné stránky, Weaknesses – slabé stránky, Opportunities - příležitosti, Threats - hrozby), umožňuje vyjádřit komplexní výsledek informací získaných v průběhu diplomové práce. Cílem interní analýzy je zhodnotit silné a slabé stránky jednotlivých technik a na základě těchto poznatků zjistit a zhodnotit jednotlivé silné a slabé stránky autentizačních metod. Tuto metodu analýzy lze aplikovat ve veškerých veřejných organizacích a institucích k odstranění nedostatků, které omezují podnik v soutěži schopné konkurence [TOMEK, 2007, s. 80].

16.2 SWOT Č. 1 HESLA

Strenghts (silné stránky)	Weaknesses (slabé stránky)
◆ nevyžaduje instalaci speciální HW nebo SW komponenty při přihlašování uživatele	◆ uživatelé si své heslo musí pamatovat v okamžiku, kdy se přihlašují do více systémů
◆ uživatel se může přihlásit odkudkoliv a nepotřebuje k tomu žádná speciální autentizační zařízení	◆ kladeny značné nároky na paměť uživatele
◆ ochranu hesel zesilují kryptografické systémy (zajišťují větší bezpečnost klíče)	◆ závislé na uživateli (nejslabší složkou systému je lidský faktor)
◆ jednoduchost používání a spravování	◆ používání mnoha hesel
◆ levná	◆ slabá forma ochrany
◆ pohodlný mechanismus pro zrealizování	◆ uhádnutí nebo prolomení ochrany
◆snadno zapamatovatelná	◆odchycení hesla na softwarové úrovni
◆ rychlá	
Opportunities (příležitosti)	**Threats (hrozby)**
◆automatické generování hesel	◆ většina uživatelů používá pro přístup do systémů stejná hesla
◆ bezpečnostní příručka	◆ velká šance na prolomení hesla
◆ vhodná kombinace číslice a písmena – pokud to aplikace dovoluje	◆ nevhodné pro zabezpečení lokální počítačové sítě (více cílů)
◆ používání delších hesel (hesla o více znacích)	◆ konstantní identifikace/ověřování informací
◆ širší kombinace možných bitů (vhodný 64bitový klíč)	◆ registrace hesel zdarma=použití hesel pro marketingové účely nikoliv bezpečnostní (výsledkem je šíření hesel)
◆ kombinace s jinou autentizační metodou	◆ sociální inženýrství
◆ zabezpečovací technologie šifrování	◆ krádež identity

16.3 SWOT č. 2 - TOKENY

Strenghts (silné stránky)	Weaknesses (slabé stránky)
◆ rychlá zjistitelnost ztráty tokenu ◆ úspěšná autentizace je podmíněna použitím tokenu ◆ autentizační informaci nelze sdílet tak jednoduše jako heslo ◆ jednoduchost používání a spravování ◆ nelze snadno zkopírovat ◆ většinou obsahuje šifrovací klíč chráněný pinem ◆žádné HW nebo SW úpravy na straně klienta ◆ jednorázový kód (při zasílání ověřovacích SMS- např. mobilní telefon) ◆chrání uložené kryptografické údaje	◆ fyzická ztráta, zničení ◆ mechanické poškození ◆ falešná odmítnutí ◆ počítačové viry ◆ vyžaduje tajné informace ◆ potřeba speciální čtečky ◆ bez tokenu není autentizace možná, uživatel jej musí mít stále při sobě ◆ porucha nemusí být vždy jednoduše zjistitelná uživatelem ◆potřeba token fyzicky vlastnit
Opportunities (příležitosti)	**Threats (hrozby)**
◆obtížné kopírování ◆ bezpečné uložení tajné informace-klíč uložený v kalkulátoru ◆ při opakovaném chybném zadání PINu se zablokují ◆ některé při pokusu o o násilné vniknutí do přístroje dokonce zničí uchovávanou informaci	◆ v případě poruchy nebo ztráty je uživatel odkázán na servisní středisko a nemůže autentizace využívat ◆ softwarové chyby ◆ PKI obsahuje velmi dlouhé řetězce znaků a na rozdíl od hesel nejdou tak snadno zapamatovat ◆ zneužití různých chyb v aplikacích ◆ nová rizika

16.4 SWOT Č. 3 – BIOMETRIKY

Strenghts (silné stránky)	Weaknesses (slabé stránky)
◆ ověření identity osoby je vysoké ◆ velmi vysoká spolehlivost ◆ používána v bezpečnostních aplikacích (kriminalistika, armáda) ◆ využívání vícefaktorové autentizace (kombinování alespoň s jednou z výše uvedených metod) ◆ měřitelnost – charakteristika by měla být opakovaně měřitelná ◆ nízká míra oklamání systému podvodnými technikami ◆ nemohou být ukradeny ani ztraceny	◆ především behaviorální charakteristiky často podléhají změnám (hlas, podpis) ◆ stoprocentní ověření osoby není možné ◆ stále ve fázi vývoje, především co se týče přesnosti a rychlosti ◆ nemožnost registrace všech osob (osoby s chybějícími orgány) ◆ zavádění dodatečných informací (které zvyšují náklady a složitost systému a snižují bezpečnost ◆ nutnost neustálé údržby přístrojů
Opportunities (příležitosti)	**Threats (hrozby)**
◆ prosazuje se ve veřejném sektoru (bankovnictví, kontrola pasů) ◆ uživatel si nemusí pamatovat žádné informace ◆ biometriky nejsou tajné (jako např. heslo) ◆ musí být vždy aktuální a snímány v průběhu autentizace	◆ možnost okopírování ◆ nedostatečná legislativní úprava ◆ odpor některých uživatelů k biometrikám, něchtejí se podrobit měření, ani ukládání dat do systému ◆ biometrická data nejsou tajná a bezpečnost systému nemůže být založena na jejich utajení ◆ mohou výrazně narušit soukromí uživatele ◆ etické faktory a legislativní omezení ◆ obsahují mnoho citlivých informací

	◆ ztráta anonymity

16.5 Srovnání autentizačních metod

V rámci této práce jsme představili tři metody, které podporují a pomocí nichž zajišťují autentizaci svých uživatelů. Z uvedeného textu bychom již měli mít přibližnou představu o výhodách a nevýhodách jednotlivých autentizačních metod. Autentizace pomocí hesel by se dala považovat za jednoduchou a flexibilní variantu s rozumnou mírou zabezpečení za předpokladu, že zná uživatel heslo. Mezi problémy těchto hesel často patří jednoduchost, snadná zapamatovatelnost a často neopatrné chování ze strany uživatelů nebo nevhodné nastavení hesla ze strany správců systému. Prvním řešením může být optimální nastavení a druhým zvýšená pozornost uživatelů systému. Kvůli velké rozšířenosti autentizace pomocí hesel se na internetu bohužel vyskytuje velké množství nástrojů na prolomení hesla a je zde velké nebezpeční prolomení hesla ze strany internetových útočníků.

Autentizační tokeny se dají považovat za metodu kvalitnější, technologicky vyspělejší s využitím možností PKI (Public Key Infrastructure), která se zvyšuje díky dlouhodobému vývoji především privátního sektoru organizací, které využívají vlastností moderních autentizačních protokolů a umožňují používat různé čtečky a typy karty. Rovněž ale vznikají nové formy útoků, které souvisejí se ztrátami tokenů uživateli nebo tokeny získané útočníky.

Autentizační metody biometrik propagují nový rozměr autentizačních metod uživatelů. Nejenom identifikují uživatele jako jedinečnou osobu, ale především rozlišuje osobu reálnou od stroje. Podle nás představují nebezpečnější formu autentizace vyskytující se v současných autentizačních metodách. Tento fakt tvrdím z toho důvodu, že je zde nejmenší míra pravděpodobnosti získat falšovanou identitu a vydávat se tudíž za jinou osobu. Rovněž zde vstupuje do hry řada nových konceptů, rozvíjejí se nové technologie na podporu biometrických autentizačních systémů, které jednak jdou ze strany komerčních firem, jednak ze strany národních států, kde přispívají k vyšší míře bezpečnosti. Problémem se zde stává bezpečný přenos a uložení dat a jednak etické faktory a současná legislativa, která zaostává za těmito moderními mechanismy.

16.6 Zhodnocení

Nejslabším místem systému zůstává lidský prvek, který dokáže efektivně vynulovat výhody jednotlivých přístupů například napsáním svého hesla na lístek na monitoru počítače anebo používáním jednoduchým hesel, jako je např. jméno rodinného příslušníka, místo pobytu atd. Částečným řešením může být kombinace autentizačních metod a využívání některé silnější autentizační metody v kombinaci s autenizací pomocí hesel. Používáním více metod najednou může zkomplikovat či znemožnit jakýkoliv útok na systém. Pro systémy s vyšší bezpečností by měly být povinností vyžadovat autentizační tokeny, která by mohla být v kombinací s biometrikami.

17. ZÁVĚR

Ve své práci jsem se hlouběji zaobírala, do jaké míry v posledních letech splynula oblast informačních systémů a internetu, jako specifického média, kde vládne stále, přese všechny snahy, absolutní volnost uživatele k legitimním činnostem, ale také ke zneužití tohoto média vůči ostatním uživatelům. Tato volnost je aktuálně předmětem střetu zájmů uživatelů, autorských svazů a jednotlivých států. Zabývat se ochranou dat uživatelů již dávno není výsadou pouze úzkého okruhu jedinců, nicméně internet s nárůstem počtu svých prostředků, poskytuje útočníkům ideální příležitost. Uživatelé se přizpůsobili volnosti internetu, omezené nedostupnosti ilegálního obsahu a naučili se data sdílet ilegálně. Domnívám se, že s pronikáním informačních technologií blíže k jednotlivým uživatelům a s rozšiřováním jejích možností v reálném životě, se stále více setkáváme s potřebou, či dokonce nutností, provádět úkony na základě *autentizace*. Zpravidla se jedná o ověření *identity* uživatele na základě znalosti, dovednosti, biologických znaků či použití technického prostředku. Jednotlivé možnosti autentizace se mohou pro zvýšení bezpečnosti navzájem kombinovat.

V současnosti je nejvíce rozšířena autentizace uživatele na základě *skryté znalosti*, obvykle se jedná o znalost uživatelského jména a příslušného hesla. To přináší do celého systému autentizace jednoduchost. Uživatel si zpravidla tyto údaje pamatuje, má je vždy s sebou a nemusí disponovat dalšími technickými prostředky. Uživatel je tudíž připraven se autentizovat prakticky kdykoliv a za jakékoli situace. Odvrácenou stranou je pak možnost odposlechnutí či jiného získání těchto údajů a jejich následného zneužití. V případě autentizace pouze na základě skryté znalosti se jedná o krádež identity uživatele, která je zpravidla zřejmá až po jejím zneužití. Autentizace na základě skryté znalosti je na jednu stranu jednoduchou metodou, ale na druhou stranu je zcizení těchto znalostí velmi obtížně identifikovatelné. Na straně autentizační služby se uplatňují různé metody zabezpečení.

Domnívám se, že nejlepší úrovně zabezpečení lze dosáhnout kombinací bezpečnostních opatření na straně uživatele i autentizační služby. V současné době se také prosazují bezpečnostní mechanismy na síťové úrovni. Jedná se zpravidla o více či méně automatizované sledování chování počítačové sítě a včasný zásah při neobvyklé aktivitě.

Ve své práci jsem se snažila specifikovat, do jaké míry lze pomocí autentizace osob zajistit jejich bezpečnost. Biometrické charakteristiky jsou založeny na *automatizovaném měření* a porovnáním biometrických charakteristik člověka. Biometrické (behaviorální), to jest na chování založené vlastnosti, které jsou pro každého člověka jedinečné, a tudíž využitelné k *ověření identity*. Cílem této práce bylo srovnání autentizačních metod, které jsou běžně dostupné ve výzkumných laboratořích vysokých škol, ve všech veřejných organizacích a institucích. Např. v běžné praxi pomocí otisků prstů se využívají čtečky otisků prstů, které se řadí mezi kvalitnější typy běžně využívaných autentizačních zařízení na profesionální úrovni, například jako autentizační metoda zajišťující přístup do objektů. V této oblasti může být využita např. biometrická autentizace v knihovnách jako software, který využívají knihovny pro rozpoznávání tváře. Na základě provedených SWOT analýz jsem srovnala jednotlivé metody z hlediska chybovosti, uživatelské přívětivosti a náročnosti na využití. Zároveň se pokouším přiblížit, jaký význam má testování a srovnávání jednotlivých technologií, jaká metoda je vhodná pro případná nasazení v praxi jako náhrada za jinou autentizační metodu a která naopak vhodná není, protože její použití by mohlo vést k nespokojenosti uživatelů nebo snížení bezpečnosti.

Požadavky na zajištění bezpečnosti se liší systém od systému. Je důležité znát *požadavky,* které potřebujeme klást na autentizační systém, jak velká budou bezpečnostní rizika, a jaké jsou požadavky technické a finanční. Do technických požadavků můžeme zařadit *kvalitu zpracování*, *standardizaci, splnění norem, obtížnost obsluhy a rychlost* autentizace. Jiné požadavky budou kladeny na systém řízení přístupu do jaderné elektrárny, kde selhání bezpečnostního systému může vést až k vážnému ohrožení lidských životů a jiné při řízení přístupu do studentů do počítačové studovny. Další vlastnosti, které mohou ovlivnit volbu zvolené autentizační metody v informačním systému, je *cena* – náklady na pořízení potřebného vybavení, náklady na provoz systému a údržbu a také *chybovast* např. biometrická data, na rozdíl od jiných autentizačních metod nejsou nikdy 100% shodná. Z tohoto důvodu musíme povolit určitou variabilitu mezi náklady na provozinformačního systému a rizikem bezpečnosti.

Nastudováním všech uvedených dostupných metod jsem dospěla k přesvědčení, že za nejvhodnější a nejefektivnější variantu při řešení bezpečnosti se dá považovat autentizační metoda založená na kombinaci hesla a nejnovějších trendů. Mezi vybranými metodami pak

zvolit nejvhodnější metodu pro praktickou implementaci, kterou následně ověřit v praxi a bezpečně ochránit všechna uložená data. Systémy silné autentizace využívající mechanismů jednorázových hesel v kombinaci více autentizačních faktorů, nalézají uplatnění v široké škále řešení v oblasti informačních technologií. Pro některé oblasti je jejich nasazení *efektivnější*, pro některé méně. Nejvhodnější nasazení jsou zároveň nejpřímočařejší a nejsnazší na implementaci. Mezi důležité obecné vlastnosti všech systémů při řešení autentizace jsou zejména – *škálovatelnost,* to znamená, že je systém vhodný jak pro malá, tak velká distribuovaná řešení, možnost komfortní administrace – delegování administračních pravomocí, seskupování uživatelů a zařízení, detekce pokusů o napadení systému atd. Dále sem patří moderní algoritmy, např. využití technologie při generování hesel, zabezpečení strategických aplikací a webových aplikací. Nejefektivnější platformou v současnosti jsou šifrovací technologie, které se masově používají v domácích počítačích na ochranu dat (souboru, e-mailů), v elektronickém bankovnictví, v systémech platebních karet. Do budoucna tato technologie může sehrát významnou roli v např. v oblastech elektronických voleb či elektronických peněz.

Na začátku práce jsem se zaměřila na popis obecných postupů a kritérií a rozčlenila jednotlivé typy ochrany dat a jejich specifikace, možnosti jejich uložení a obecné činnosti informačních systémů. Podařilo se mi popsat většinu dosud známých autentizačních metod využívaných v současnosti pro autetentizaci žadatele o přístup do systému. U jednotlivých metod jsem se pokusila uvést jejich princip, vlastnosti a příklad využívání v praxi.

SEZNAM OBRÁZKŮ

SEZNAM POUŽITÝCH ZDROJŮ

BANDYOPADHYAY, Samir Kumar ; KIM, Tai-hoon. A Cryptosystem for Encryption and Decryption od Long Confidential Messages. In *Information security and assurance : 4th international conference, ISA 2010, Miyazaki, Japan, June 23-25, 2010 : proceedings*. New York : Springer, 2010. S. 86 - 97. ISBN 9783642133640.

BEAVER, Kevin ; MCCLURE, Stuart. *Hacking for Dummies*. 3rd ed. Indianapolis : Wiley, c2010. 408 s. ISBN 076455784X.

Biometric authentication : ECCV 2004 International Workshop, BioAW, Prague, Czech Republic, May 15th, 2004 : proceedings. Edited by Davide Maltoni, Anil K. Jain. Berlin : Springer, 2004. xiii, 341 s. ISBN 3-540-22499-8.

Biometric solutions : for authentication in an e-world. Edited by David D. Zhang. Norwell : Kluwer Academic Publishers, 2002. ISBN 9781402071423.

BOSE, Ranjan. Information theory, coding and cryptography. 2nd ed. New Delphi : Tata McGraw-Hill Publishing, 2008. 277 s. ISBN 0071231331.

BOYLES, Tim. *CCNA security study guide*. Indianapolis : Wiley, c2010. xxxii, 516 s. ISBN 9780470527672.

BURDA, Petr. 2010. RE: Žádost o informace [elektronická pošta].Message to: Martina Knopová: 15.12. 2010. 17:15:37 [cit. 2010-17-12].

CISSP: Certified Information Systems Security Professional study guide. Edited by Ed Tittel, Mike Chapple, James Michael Stewart. San Francisco, Calif. ; London : SYBEX, 2003. xlv, 783 s. ISBN 0782141757.

CLARKE, Roger. *Cryptography in Plain Text*. Canberra : Xamax Consultancy, 1998. ISBN 0644475307.

Česko. Úřad pro ochranu osobních údajů. In *Úřad pro ochranu osobních údajů* [online]. Osobní údaje ve společných informačních systémech EU.

Praha : ÚOOÚ, [cit. 2010-11-11]. Dostupné na www: <http://www.uoou.cz/uoou.aspx?menu=0&submenu=10&loc=624>.

Česko. Zákon č. 101 ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů. *In Portál veřejné správy České republiky* [online]. Praha, Ministerstvo vnitra, c2003-2010 [cit. 2011-11-12]. Dostupné na www: <http://portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_number1=101/2000&PC_8411_l=101/2000&PC_8411_ps=10#10821>.

Česko. Zákon č. 106 ze dne 11. května 1999 o svobodném přístupu k informacím. In *Portál veřejné správy České republiky* [online]. Praha, Ministerstvo vnitra, c2003-2010 [cit. 2010-11-11]. Dostupné na www: <http://portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_number1=106/1999&PC_8411_p=3&PC_8411_l=106/1999&PC_8411_ps=10#10821>.

Česko. 2000. Zákon č. 227 ze dne 29. června 2000 o elektronickém podpisu a změně některých dalších zákonů (zákon o elektronickém podpisu). In *Sbírka zákonů České republiky* [online]. 2000, částka 68, s. 3290-3297. Dostupné také z WWW: <http://aplikace.mvcr.cz/archiv2008/sbirka/2000/sb068-00.pdf>.

Česko. 2004. Zákon č. 480 ze dne 29. července 2004 o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). In *Sbírka zákonů České republiky* [online]. 2004, částka 166, s. 9470 9475. Dostupné také z WWW: <http://aplikace.mvcr.cz/archiv2008/sbirka/2004/sb166-04.pdf>.

Česko. Zákon č. 412 ze dne 21. září 2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. In *Portál veřejné správy České republiky* [online]. Praha, Ministerstvo vnitra, c2003-2010 [cit. 2010-11-11]. Dostupné na www: <http://portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_number1=412/2005&PC_8411_b=412/2005&PC_8411_ps=10#10821>.

Česko. Zákon č. 480 ze dne 29. července 2004 o některých službách informační společnosti. [online]. In *Portál veřejné správy České republiky* [online]. Praha, Ministerstvo vnitra, c2003-

2010 [cit. 2010-11-01]. Dostupné na www: <http://portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_number1=480/2004&PC_8411_b=480/2004&PC_8411_ps=10#10821>.

DANEL, Roman. 2010. RE: Žádost o informace [elektronická pošta].Message to: Martina Knopová: 1.12. 2010. 15:35:16 [cit. 2010-2-12].

DASWANI, Neil. *Foundations of security : what every programmer needs to know*. Berkeley, CA : Apress ; New York : Distributed to the book trade worldwide by Springer-Verlag, c2007. xxvii, 290 s. ISBN 9781590597842.

Evropská komise. *EUR-Lex : přístup k právu Evropské unie* [online]. Směrnice údajů 95/46/ES. [cit. 2010-11-11]. Dostupné na www: <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008D0393:CS:HTML>.

Evropská úmluva o lidských právech, čl. 8. Ministerstvo vnitra České republiky**.** [online]. [cit. 2010-11.11]. Dostupné na www: http://www.mvcr.cz/clanek/mezinarodni-spoluprace-92.aspx?q=Y2hudW09Mg%3D%3D

Global privacy protection : the first generation. Edited by James B. Rule and Graham Greenleaf. Cheltenham, UK ; Northampton, MA : E. Elgar, c2008. vii, 318 s. ISBN 1848440634.

GUPTA, Kailash N. [et al.]. *Digital Signature: Network Security Practices*. New Delphi : Prentice-Hall, 209 s. ISBN 8120325990.

GUTTMAN, Barbara ; ROBACK, Edward A. *An introduction to Computer Security*. Gathersburg : National Institute of Standards and Technology, 1995. 276 s. ISBN 100788128302.

HOPE, Jeremy ; HOPE, Tony. Competing in the third wave : the ten key management issues of the information age. United States : Harvard Business School Press, 1997. 253 s. ISBN 0875848079.

Image pattern recognition : synthesis and analysis in biometrics. Edited by Světlana Yanushkevich. Singapore : Word Scientific Publishing, 2007. 407 s. ISBN 9789812569080.

KOLB, Rubin, McIntyre: Organizational Psychology. An experimental Approach. 1979

Nádeníček, Petr. Pravdy o elektronickém podpisu a šifrování 1. In Svět sítí [online]. c2010-2011 [cit. 2011-01-06]. Dostupné z www: <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&clanekID=245>.

PAAR, Christof ; PELZL, Jan. *Understanding cryptography: a textbook for students and practitioners*. Heidelberg : Springer Verlag, 2010. 372 s. ISBN 9783642041013.

PERRING, Adrian, TYGAR, James D. *Secure broadcast communication in wired and wireless networks*. Boston : Kluwer Academic Publishers, c2003. xix, 214 s. ISBN 0792376501.

Phishing and countermeasures : understanding the increasing problem of electronic identity theft. Edited by Marcus Jakobsson, Steven Myers. xxvi, 700 s. ISBN 0471782459.

PŘYBIL, Tomáš. 2010. RE: Žádost o informace [elektronická pošta].Message to: Martina Knopová: 03.11. 2010. 18:17:43 [cit. 2010-11-12].

REID, Paul. *Biometric for network security.* Upper Saddle River, NJ : Prentice Hall PTR, 2004. xx, 252 s. ISBN 9788131716007.

STALLINGS, William. *Cryptography and network security : principles and practice*. 4th ed. Upper Saddle River, N.J. : Pearson/Prentice Hall, c2006. xvi, 680 s. ISBN 0131873164.

STAMP, Marc. *Information security Principles and Practice*. San José State University : Wiley Interscience, 2005. 366 s. ISBN 07817566286.

STEWART, James Michael. *CompTIA Security+Review Guide*. Indianopolis : Wiley Publishing, 2008. 288 s. ISBN 9780470404843.

TOMEK, Gustav ; VÁVROVÁ, Věra. 2007. *Marketing od myšlenky k realizaci*. 2007. 1. vyd. Praha : Professional Publishing, 2007. 308 s. ISBN 978-80-86946-45-0.

VACCA, John R. *Biometic technology and Verification Systems.* Amsterdam ; Boston : Butterworth-Heinemann : Elsevier, c2007. xxvii, 625 s. ISBN 9780750679671.

WINDLEY, Phillip. *Digital Identity*. Cambridge : O´Reilly Media, 2005. 254 s. ISBN 0596008783.