Ochrana dat a informačního soukromí
PV080

1 Úvod: Ochrana dat a etika v informačních technologiích

Zavádění prostředků informačních technologií (IT) do existujících či nově budovaných systémů v širokém spektru oblastí lidské společnosti nám přináší mnoho výhod. Prostředky IT nám umožňují například komunikovat se svými blízkými, zaznamenávat audio-vizuální informace ve svém okolí a sdílet je s přáteli např. prostřednictvím sociálních sítí, využívat výhod videotelefonie, orientovat se v neznámém prostředí či být připojen ke globální informační síti takřka kdekoliv prostřednictvím bezdrátového připojení. Na druhé straně zavádění prostředků IT však s sebou přináší i řadu problémů, jejichž důsledky mohou být fatální. Prostředky IT mohou být totiž zdrojem dalších (často skrytých) problémů, které se mohou vyskytovat na různých úrovních.

S prvotními problémy objevujícími se v souvislosti se zaváděním prostředků IT se mohli „pamětníci“ setkat např. v dobách, kdy se výplaty začaly počítat na počítači. Výplaty byly na počítači spočítány daleko rychleji a za menšího úsilí, než za použití předchozích konvenčních metod. Případné opravy a nedostatky se však najednou řešily mnohem déle. Často to byla řešení typu: „My to nemůžeme opravit. Dáme ti chybějící peníze příští měsíc v odměnách.“

A jak je tomu vlastně dnes, v době kdy prostředky IT pronikají do pořád širšího spektra oblastí našeho každodenního života? Jakou roli hraje ochrana dat ve světě protkaném informačními technologiemi? Jaké další související problémy lze v budoucnu očekávat? Které z nich se dotknou „jen“ firem a vládních organizací a které mohou bolet nás jako soukromé osoby? K jakým nedopatřením při nasazení prostředků IT došlo a dochází, čeho se lze vyvarovat a jak?

Co je DES a jak pracuje? K čemu je digitální podpis a k čemu PGP? Lze zajistit bezpečné obchodování na Internetu a jak? Může se v budoucnu stát, že se budete bát svěřit některé údaje o zdravotních problémech svému lékaři?

Prostřednictvím této části kurzu se pokusím zodpovědět co nejvíce obdobných otázek, a také ujasnit pojmy a techniky, které jsou často zmiňovány povrchně a bez náležitého vysvětlení a uvedení souvislostí.

1.1 Bezpečnost a informační soukromí

Bezpečnost (angl. *Security*) je obecně vlastnost prvku (např. IS), který je na určité úrovni chráněn proti ztrátám nebo také stav ochrany (na určité úrovni) proti ztrátám. V oblasti

IT se bezpečnost soustředí především na ochranu činností zpracování, úschovy, distribuce a prezentace informací. Český termín „bezpečnost“ může být v anglickém překladu interpretován také jako „*Safety*“. Na rozdíl od bezpečnosti ve smyslu anglického termínu *Security*, „*Safety*“ spíše znamená, že při specifikovaných podmínkách nedojde ke stavu ohrožení lidského života, zdraví, hodnot a prostředí. Pro zamezení případné víceznačné interpretace budeme v následujícím textu rozumět bezpečnost ve významu anglického „*Security*“, pokud nebude uvedeno jinak.

Soukromí (angl. *Privacy*) je v obecném pojetí charakteristikou života jedince a jeho práva související s možností kontroly informací o sobě, o své činnosti a ochrany proti nežádoucímu rušení[1]. Informační soukromí představuje jeho specifičtější oblast, která se vztahuje především ke zmíněné možnosti kontroly informací, jakými jsou např. osobní data či další relevantní (potenciálně citlivé) informace týkající se určitého jedince. Tento termín se váže i na jiná práva jedince, a tak je jeho přesná definice obtížná. Informační soukromí úzce souvisí se zajištěním ochrany osobních informací, pravidel pro jejich kontrolu a poskytování jiným subjektům atd. Zajištění informačního soukromí podporují bezpečnostních funkce prosazující anonymitu, pseudonymitu, nespojitelnost a nepozorovatelnost.

Ochrana informačního soukromí a osobních dat sehrává důležitou roli. V současnosti je například běžnou praxí, že informace, které o nás „síť“ ví jsou často využívány např. při rozhodování potenciálního budoucího zaměstnavatele o našem přijetí či nepřijetí na pracovní pozici nebo při rozhodování bankovního subjektu zdali nám bude poskytnuta půjčka. Jsou známé také případy, kdy informace publikované dotyčným v sociálních sítích vedly ke ztrátě jeho zaměstnání či k rozvodu. Je tedy patrné, že ochrana informačního soukromí je důvodem pro zajištění bezpečnosti, stejně jako třeba ochrana firemních dat nebo informací vojenské rozvědky. V žádném případě nelze pojmy (informační) bezpečnost a informační soukromí volně zaměňovat, ale ani oddělovat.

1.2 Hodnota osobních dat

Soukromé informace jsou informace, které nechceme sdílet s jinými, nebo u kterých chceme osobně kontrolovat jejich pohyb (tzn., sdílíme je s někým, ale ne s „ostatními“). [KC Laudon, Communications of ACM 9/96]

Roger Needham, profesor University of Cambridge a světově uznávaný odborník v oblasti bezpečnosti, formuloval tuto myšlenku: „Rozhodujícím ukazatelem úrovně ochrany je cena osobních dat „na ulici“ – na černém či šedém trhu.“ U zdravotních dat je cena v Anglii 150-200 liber, v kanadské provincii Quebec podle některých „inzerátů“ 20-60 liber. Podle Needhama by měla cena být výrazně nad 500 liber. Pokud by cena za získání osobních dat byla směšně nízká, mohla by se tato data stát nevýznamnou položkou nákladů pojišťovacích firem, kterým by usnadnila rozhodování, jak vysoké splátky pojistného nasadit tomu či onomu jedinci. Cenu osobních dat a tím i úroveň ochrany ovlivňují tři faktory:

1. výše trestu těm, kdo data jiných řádně neohlídali a spolupodíleli se tak na jejich úniku;

[1] Nežádoucím rušením je zde myšleno rušení ve smyslu jak přímého fyzického přístupu k osobě a jejímu nejbližšímu okolí, tak i rušení nevyžádanou komunikací.

2. výše trestu těm, kdo s nimi neoprávněně manipulují;

3. úroveň ochranných mechanismů.

Čtyřicet let komunistického „pořádku“, který neřadil soukromí občana k nejvíce respektovaným hodnotám, u nás vykonalo své – často nevíme, jakou hodnotu mají naše osobní informace pro stát i mnohé firmy a jaká škoda nám může vzniknout jejich únikem mimo naši kontrolu. Pro zajímavost, v Anglii je ke svým osobním datům a zacházení s nimi necelých 20 % občanů totálně lhostejných, stejný počet velmi obezřetných až paranoidních a okolo 60 % je ochotno část svých práv nechat omezit za „přiměřenou úhradu“ – finanční, věcnou či nejčastěji v podobě výrazného zlepšení služeb. Co to konkrétně znamená?

Ano částečnému omezení práv, když finanční informace budou dostupné komukoliv v rámci banky – za možnost skutečně rychlého a nekomplikovaného obsloužení ve kterékoliv pobočce nebo bankomatu.

Ne výraznému omezení práv zavedením jednotného občanského záznamu ve státním informačním systému. Vzhledem k rozsahu a přehmatům státního aparátu snad nikdo nevěří slibům o zaručení ochrany dat. Hlavní zájem je ale především o zachování práva občana poskytovat aktuální a úplné informace o sobě jen v nutných případech. Pokud občan plní základní povinnosti (neporušuje zákon a platí daně) a nežádá od státu žádné přímé služby, tak má právo být stranou („*to be let alone*“) a kontrolovat pohyb informací o sobě.

1.3 Soukromí

Pokud se jedná o soukromí z technického úhlu pohledu, zajímají nás kromě ochrany důvěrnosti (informačního obsahu) dat následující vlastnosti, které definují různé pohledy na obecný pojem „soukromí“. K důvěrnosti dat jakožto velmi důležitému tématu se budeme věnovat později.

1.3.1 Anonymita

Anonymita je vlastnost systému, který zajišťuje možnost použití zdrojů nebo služeb bez zjištění identity uživatele tohoto systému. Jedná se o poměrně samozřejmou součást pojmu „soukromí“. Anonymita pomáhá např. při eliminaci hrozby profilování uživatelů (angl. *user profiling*).

1.3.2 Pseudonymita

Jedná se o vlastnost systému, který zajišťuje možnost použití zdrojů nebo služeb bez zjištění identity uživatele tohoto systému tak, že uživatel je stále zodpovědný za toto použití. Možnými aplikacemi jsou např. používání služeb s následnými platbami za toto používání bez uvedení vlastní identity při bezproblémových platbách (v případě problémů lze v odůvodněných případech identitu zjistit – např. u banky). Určitá podobnost existuje s poštovními přihrádkami (PO Box), kde pokud nedojde k porušení zákona, tak majitel přihrádky zůstává odesílateli pošty neznámý. Pokud ale dojde ke střetu se zákonem, lze u pošty zjistit skutečnou identitu majitele přihrádky.

1.3.3 Nespojitelnost

Nespojitelnost (angl. *unlinkability*) je vlastnost systému, který zajišťuje možnost opakovaného použití zdrojů nebo služeb s tím, že ostatní si tato použití nebudou schopni spojit (spojení ve smyslu vzájemné souvislosti, může se jednat o postupně i současně poskytované stejné i různé služby). Tato vlastnost se výrazně odlišuje od předchozích dvou v tom, že nezohledňuje identitu uživatele, ale rozsah služeb a zdrojů, které byly použity stejným uživatelem. Možnou aplikací je ochrana soukromí uživatele používajícího současně služeb Internetu a určité telefonní přípojky – komunikační partner by neměl mít možnost zjistit, odkud se daný uživatel na Internet připojuje.

1.3.4 Nepozorovatelnost

Nepozorovatelnost (angl. *unobservability*) je vlastnost systému, který zajišťuje možnost použití zdrojů nebo služeb tak, že ostatní nemohou pozorovat používání daného zdroje nebo služeb. Nepozorovatelnost lze vnímat ve dvou rovinách jako: (1) zaručení anonymity subjektu, který určitý zdroj nebo službu využívá (nejen vůči vnějším pozorovatelům, ale i vůči dalším subjektům, které daný zdroj či službu rovněž využívají) a (2) zaručení nedetekovatelnosti použití daného zdroje nebo služby vůči subjektům, které daný zdroj nevyužívají. Ochraňovanými hodnotami nejsou informace o uživatelích, ale o použití zdrojů nebo služeb. Příkladem aplikace může být ochrana proti tzv. analýze provozu (angl. *traffic analysis*), tj. např. proti pozorování toho, která strana rozesílá nejvíce zpráv v určité době nebo při výskytu určité události.

Pro zvídavé studenty:
http://dud.inf.tu-dresden.de/Anon_Terminology.shtml – rozšířená terminologie informačního soukromí (nad rámec tohoto kurzu)

1.4 Rozsáhlé databáze osobních informací

Seskupováním osobních dat do rozsáhlých databází dochází k tomu, že takovýmto kombinováním dat o určité citlivosti lze získat informace daleko citlivější, které jinak spadají do kategorie s vyššími požadavky na ochranu. Pro seskupování se také používá termín agregace (z angl. *aggregation*). Představte si, že máte k dispozici kompletní informace o zdravotním stavu a finanční situaci

1. manžela nebo manželky;
2. přímého nadřízeného;
3. všech zaměstnanců organizace, kde pracujete;
4. všech obyvatel města/vesnice, kde žijete;
5. všech klientů určité banky nebo zdravotní pojišťovny.

Cítíte ten rozdíl? Jedná se přitom o stejné informace – jen se mění druh a počet osob, ke kterým se vztahují. A představte si, jaký zájem o tyto informace musí mít třeba banka, která poskytuje úvěry a hypotéky, nebo např. pojišťovací agent.

Pravděpodobnost, že budou informace neoprávněně zpřístupněny, záleží na dvou faktorech:

- hodnotě informací,
- počtu osob, které mají k informacím přístup (operátoři i uživatelé systému).

1.4.1 Statistické databáze

Podobné problémy byly poprvé studovány v souvislosti s databázemi údajů ze sčítání lidu v USA. Podobně se také využívají data získaná u nás při sčítání lidu, kdy uvádíte náboženské vyznání i počty televizorů, vybavení mobilními telefony atd. Takové databáze sice obsahují citlivé údaje o jednotlivcích, ale jejich využití má být pouze pro statistické dotazy k vytvoření obrazu o celkových potřebách obyvatelstva a formulování vládní politiky – podpora církví, určení vybavenosti domácnosti podle lokalit atd. Výsledky dotazů v takovýchto databázích nesmějí poskytnout údaje o jednotlivcích.

V roce 1979 se známé odbornici v oblasti bezpečnosti IT Dorothy Denningové podařilo prokázat, že prostředky, které využívala americká vláda pro formulaci dotazů a získávání odpovědí ze statistické databáze sčítání lidu, povolovaly konstrukci takových dotazů, které umožnily získat údajně tajné informace o jednotlivci. Podle přesvědčení vládních činitelů byly takové informace opravdu tajné a dobře chráněné – dokud Denninová nezjistila plat svého šéfa sérií legitimních dotazů v databázi.

Konstrukce série takových dotazů nebývá obvykle jednoduchá. Představte si ale zjednodušeně, že se zpřesňováním dotazu až na [kolik je měst s počtem 17 000-18 000 obyvatel, kde žije jen jeden muž, který je 36letý evangelík slovenské národnosti, jeho 28letá žena žije mimo toto město, 6letá dcera s touto ženou a 15letý syn s oním mužem] dostanete k odpovědi 1. Pak už lze jednoduše zjistit plat tohoto našeho souseda jen doplňováním dotazů o [..., jehož příjem je X-Y měsíčně] a určováním X a Y tak, aby odpověď byla stále 1 a ne 0.

Pokud nám systém spravující databázi pro statistické dotazy umožní podobný postup, pak je to špatný systém. Existují tři druhy protiopatření.

1. *Minimální rozsah dotazu* a to buď s omezením minima
   - celkového počtu záznamů použitých pro tvorbu odpovědí, nebo
   - počtu záznamů použitých pro tvorbu odpovědí na každou automatickou část dotazu.

   Např. první uvedenou techniku využívají databázové systémy novozélandského národního zdravotního systému.

2. *Náhodný výběr* je technika nyní používaná v americké databázi údajů ze sčítání lidu. Každý dotaz je zodpovězen na základě vyhodnocení náhodně vybraných záznamů ze všech existujících záznamů.

3. *Perturbační (zmatečné) techniky* podle některých definic zahrnují i výše uvedený náhodný výběr. Obecně se jedná o přidání pseudonáhodného „šumu“ tak, aby odpovědi byly konzistentní, ale získání elementární odpovědi na sérii podobných dotazů nebylo možné. Často jsou používány dvě metody:

- k záznamům zahrnutým pro vyhodnocení dotazů se přidají další náhodně vybrané podobné záznamy;
- vypočtená hodnota nebo mezihodnoty jsou zaokrouhlovány nebo mírně pozměněny.

Typickým příkladem perturbačního protiopatření je např. technika zvaná *k-anonymity*, která zabraňuje možnosti re-identifikace subjektu na základě pseudo-identifikátorů (tj. neunikátních atributů jako například věk nebo datum narození) tím, že jednoznačná hodnota přiřazená určitému atributu subjektu je buďto

- generalizována (tj. nahrazena rozsahem do něhož tato hodnota spadá) tak, aby existovalo alespoň k subjektů s hodnotou stejného atributu v daném rozsahu, nebo
- odstraněna.

Problém inference (odvození), který jsme zde diskutovali, je definován jako odvození informací o vyšší citlivosti zpracováním a analýzou skupiny informací o nižší citlivosti nebo také nepřímý přístup k informacím bez přímého přístupu k datům, která tyto informace reprezentují.

V současném digitalizovaném a propojeném světě se stává pořád složitějším identifikovat zdroje, které jsou využívány k získávání osobních informací a budování statistických databází. Obrovský potenciál k tomuto účelu mají webové technologie, obzvláště pokud bereme v potaz, že na jejich bázi vyrostly služby jako např. *Facebook* nebo *Google Analytics*.

Problémem zajištění soukromí v rozsáhlých statistických databázích a v dalších podobných prostředích se detailně zabývá oblast označována jako „*privacy-preserving data mining*“.

1.5 Tři dimenze ochrany dat

I samotné utajení dat je velmi složitým problémem. Když se poprvé objevil AIDS, tak mnohá zdravotnická zařízení ve světě postupovala tak, že záznamy pacientů HIV pozitivních převedla mimo dosah běžných uživatelů zdravotnického informačního systému. Pak je ale jednoduché odvodit, že pacient, jehož záznam nemůže „běžný“ lékař získat, je pacientem HIV pozitivním. Opět se jedná o inferenci. A obdobný je i triviální problém u víceúrovňových systémů (viz horizontální členění dále v kurzu), kdy může činnost uživatele na nižší úrovni odhalit fakta odpovídající úrovni vyšší. Téměř klasický případ bývá uváděn při zápisu souboru. Pokud se uživatel na úrovni „důvěrné“ pokusí ve víceúrovňovém systému uložit soubor DOCS/IRAN/MISSILES/FORM.DOC a obdrží systémové hlášení, že soubor již existuje a uživatel nemá právo jej přepsat, pak lze jednoduše odvodit, že soubor již vytvořil a využívá někdo na úrovni vyšší.

Při utajování datové položky je třeba zvážit tři dimenze:

1. zda tato data mají být utajována,
2. zda samotná existence těchto dat je utajována,

3. zda i důvod utajení těchto dat je utajován.

Řešení první dimenze je nejjednodušší – přístup k datům mají jen oprávněné osoby. Technik k realizaci tohoto požadavku existuje několik. Další dvě dimenze vyžadují více zamyšlení a kreativní řešení. Ochrana před inferencí je jedním ze stále ne zcela vyřešených témat při návrhu bezpečných víceúrovňových databází. Pro některé situace vystačí perturbační techniky, jindy zase důsledné vedení auditního záznamu a jeho průběžné hodnocení pro zjištění pokusu o útok na data prostřednictvím inference. Žádné z dosavadních řešení však není všelékem.

1.6 Síla informací

S příchodem mnohoznačně definované informační společnosti se mění nejen podmínky pro bankovnictví, vzdělávání, obchodování či nakladatelskou činnost, ale také pro armádu a národní bezpečnost. Využití počítačů přináší nesčetné výhody, ale i nová rizika – ve všech oblastech, kam jsou informační technologie zaváděny. Pro zajímavost se podívejme na oblast, která je obestřena nezvykle mnoha „kdyby“, „když“ a „až“ – informační válečnictví (angl. *information warfare*).

Obrana každé země závisí nejen na armádě, ale i na tajných službách. Koneckonců i armáda jako taková má své výzvědné služby. Vždy se pracuje na základě dvou nosných principů:

- Dosáhnout vlastní *informační dominance*, tzn. mít správné informace na správném místě ve správný čas.
- Zamezit nepřátelské straně v dosažení informační dominance.

Vzpomeňte jen lekcí z historie. Dávným bitvám snad vždy předcházelo chytání „jazyků“, jejichž mučení bylo kruté i na tehdejší poměry. Není snad potřeba příliš rozvádět úspěšnou kryptoanalýzu německých šifrovacích strojů Enigma polskými a britskými kryptografy během 2. světové války, která tak podle některých odhadů byla zkrácena o 1-2 roky. A s příchodem radaru se posunulo získávání informací o nepříteli za hranici dohledu oka. Netrvalo ale dlouho a přišlo se na to, že lze vysílat klamavý zpětný signál „od neexistujících letadel“. Střely dnes také nejsou řízeny jen množstvím prachu a orientací hlavně při výstřelu. A copak nelze rušit nebo dokonce „nahradit“ řídící signál střely nepřítele signálem vlastním? Moderní války se nevyhrávají zničením co největšího počtu bojových prostředků nebo vojáků v primární fázi. Na to je dost času ve fázi sekundární, kdy vojáci a bojové prostředky nepřítele ve zmatku nevědí co dělat nebo přímo útočí na sebe navzájem. V primární fázi je důležité právě způsobit onen zmatek (maximálně eliminovat příjem a hlavně výměnu informací na straně nepřítele) a přitom si udržet zdroje informací o činnosti a vybavení nepřítele i schopnost dodat informace včas svým jednotkám.

Rozvoj moderních technologií a jejich integrace do prakticky všech oblastí lidské společnosti má za následek i změnu charakteru novodobého válečného konfliktu. Tento jev je podmíněn postupným zaváděním informačních technologií také v armádě. Navigace, komunikace a synchronizace jednotek, navádění střel či paprsků, získávání senzorových dat, detekce a lokalizace nepřátelských pozic či detekce narušení prostoru – zde všude dnes armáda využívá prostředků na bázi informačních technologií. Dalším pozorovatelným jevem je robotizace armády čili postupné nahrazování lidských zdrojů dálkově řízenými

či částečně nebo plně autonomními bojovými prostředky (např. bezpilotní letouny nebo autonomní střelecké věže schopné eliminovat narušitele v plně automatickém režimu). Nasazování těchto prostředků v konečném důsledku vede k postupné asymetrizaci vojenského konfliktu a člověk se tak ocitá na bitevním poli tváří v tvář proti stroji.

Na druhé straně, zavádění informačních technologií do čím dál širšího spektra prostředků našeho každodenního života a možnost vzdálené interakce s těmito prostředky prostřednictvím komunikační sítě přispěla k tomu, že válečný konflikt lze vést také v rovině kybernetického prostoru. Moderní válečný konflikt tak může být veden výlučně v kybernetickém prostoru a v materiální rovině se projevovat nepřímo např. narušením vnitřní infrastruktury krajiny či organizace. Dopady takovéto činnosti často nemusí být snadno detekovatelné a ve výsledném efektu se mohou projevit až s odstupem času v ekonomické rovině. Důsledky kybernetické války se mohou projevovat také přímou ztrátou na životech (např. v důsledku manipulace navigačních systémů, meteorologických údajů, lékařských přístrojů, železničních systémů či dopravní signalizace).

Charakteristickou vlastností informační války je, že může být vedena malou skupinou jedinců či jednotlivcem třeba z opačné strany planety, její dopad může být plošný, zatímco její pravý původce či fakt, že došlo k cílenému útoku, nemusí být nikdy odhaleny.

2 Co je bezpečnost?

Bezpečnost nemusí pro každého znamenat to samé. Bude jiná pro armádu, jiná pro banky a nemocnice a jiná pro správce rubrik „hezké chvíle“ v inzertních časopisech.

Jsou dvě zásadní sféry aplikací bezpečnosti. Ta prapůvodní je vojenská, kde se např. kryptografické techniky (tedy bezpečnostní mechanismy) uplatňují již po tisíciletí. Význam bezpečnosti ovšem v posledním desetiletí výrazně stoupá i ve sféře obchodní, komerční či soukromé. Požadavky jednotlivých sfér se často významně liší a přestože vojenské aplikace daly oboru bezpečnosti IT počáteční uplatnění, dnes se musí i vojenští činitelé často přizpůsobit. Velká přeorganizovanost armády (v určitém smyslu ústící do nepřehlednosti) vytváří potřebu zajistit určitý systém ve zpracování a využití informací. Ten v zásadě spočívá v

- *zajištění vlastní informační dominance* – je třeba mít správné informace na správném místě ve správný čas,
- *minimalizaci nepřátelské informační dominance* – omezit šíření vlastních informací k nepříteli, případně dokonce zajistit dodání špatných (klamavých) informací.

2.1 Hierarchické členění informací

Ve složitých (přeorganizovaných) strukturách není systematizace jednoduchá záležitost. Částečné řešení přináší hierarchická klasifikace informací. Pro minimalizaci nepřátelské informační dominance je důležité svěřovat pracovníkům jen nejpotřebnější informace (a taky tyto pracovníky předem i průběžně prověřovat). Pak je nasnadě, že důvěrnost je zásadním požadavkem v obdobných systémech. Hierarchické členění (viz Tabulka 1) je jednoduchým modelem vhodným pro tento účel.

Počet úrovní a klasifikace informací na určitou úroveň záleží na požadavcích organizace. Tomuto tématu budou později věnovány asi dva díly, nyní jen zjednodušeně –

Přísně tajná data
Tajná data
Důvěrná data
Citlivá data

Tabulka 1: Hierarchické členění dat podle citlivosti.

uživatel prověřený pro určitou úroveň má obvykle možnost přistupovat k informacím na úrovni své a všech nižších. Jedna z nejčastěji aplikovaných bezpečnostních politik je založena na modelu *Bell-LaPadula*:

- Procesy nesmějí číst data na vyšší úrovni (tzv. jednoduchá bezpečnostní vlastnost, též *NRU – no read up*).
- Procesy nesmějí zapisovat data do nižší úrovně (tzv. *-vlastnost, též *NWD – no write down*).

Tyto dvě základní vlastnosti a formální aparát pro sledování stavu bezpečnosti stroje tvoří podklad pro budování víceúrovňových systémů. Model má drobné nedostatky, přesto je důležitým mezníkem v oboru bezpečnosti. Dnes je na základě tohoto horizontálního pohledu hodnocena úroveň bezpečnostních technik a aplikací, celý obor bezpečnosti je tímto pohledem do značné míry ovlivněn.

Řešení je ale opravdu jen částečné, poněvadž je umělé a neodráží skutečnou situaci. I v armádě se řeší problémy s ohledem na původ protivníka, druh krizové situace apod., nikoliv s ohledem na začlenění informací o protivníkovi do určité kategorie. Např. americká armáda má dnes „nastavenu“ úroveň *přísně tajné* rozšířenou o oborové podúrovně, jako třeba přísně tajné nukleární, přísně tajné chemické, přísně tajné kryptografické atd.

Další problémy mohou souviset se způsobem prosazování takovéto bezpečnostní politiky. To, že nelze zapisovat data do nižší úrovně, je např. u tajných služeb dosti ošemetné – část zpravodajské sítě může padnout díky zrádci na vyšší úrovni, o jehož přístupu k materiálům na nižší úrovni nejsou správci těchto materiálů informováni. Kdyby se údaje o přístupu (požadavek zodpovědnosti) zapisovaly, pak lze srovnáním těchto údajů u „odstraněných“ agentů zjistit, kdo si jejich materiály prohlížel. V praxi se na tyto souvislosti přichází obvykle jen náhodou.

2.2 Případ od případu

V komerční sféře je běžné, že práce se člení podle obchodních případů, rozmístění poboček atd. *Často sice záleží na utajení informací (před konkurencí), nejdůležitějším požadavkem je však integrita dat.* Nemusí se vždy jednat o integritu ve striktním pojetí, ale o *smysluplnost a správnost* využívaných informací. Modelem, který je nejčastěji citován pro komerční bezpečnost, je model *Clark-Wilson*, který formalizuje stoleté zkušenosti z obchodování a účetnictví. Model formalizuje pohled na data a operace nad daty při zachování integrity, ale i pojmy jako auditní záznam a řízení přístupu.

To, že se v komerční sféře řeší problémy s ohledem na „téma“ (obchodní partner či případ apod.), vede k odlišnému přístupu ke zpracování informací. Svou roli samozřejmě

hraje i menší rozsah drtivé většiny firem a potřeba pružného jednání. Pokud komerční pohled hodně zjednodušíme, pak jej lze shrnout do vertikálního modelu členění informací.

Hrozby vojenským systémům pocházejí primárně od vnějších činitelů, kdežto komerčním systémům hrozí větší nebezpečí od vlastních pracovníků. Vždyť i celý systém podvojného účetnictví je kontrolním systémem proti neúmyslným a často i proti úmyslným chybám (pokud knihu zápisu pro kreditní a debetní pohyby vedly dvě různé osoby/skupiny).

Zaměstnanci mohou, kromě zadávání nesmyslných informací do firemních IS, také informace roznášet „po hospodách“ i konkurenci. Tady je pak nasnadě zájem firem, aby zaměstnanci nevěděli více, než je pro jejich práci nezbytně nutné. Informace jsou pro armádu velmi důležité, pro komerční organizace však naprosto nezbytné. Také interakce pracovníků armády s okolním světem je podstatně menší než u pracovníků komerční organizace. Důležitým aspektem pro úschovu a zpracování informací v komerční sféře jsou právní závazky a do značné míry i *podpora zákazníka*.

K výše uvedenému přistupuje potřeba zajištění bezpečnosti při plně elektronickém obchodování. Téměř vždy je třeba zajistit integritu dat, často i ve spojení se zajištěním důvěrnosti. A to jsme se ještě nedostali k *autentizaci* (ověření původu) dat, zajištění *nepopiratelnosti původu* zprávy nebo jejího *přijetí* atd.

Uvedené zjednodušení vojenského a komerčního pohledu na využívané informace může být v některých ohledech násilné, pro popsání rozdílu v pohledech na různé aspekty bezpečnosti je však výstižné. Svět není černobílý, ale výše popsané rozdíly mohou být pro pochopení mnohých otázek užitečné. Je důležité si uvědomit, že „bezpečnost“ nemusí pro každého znamenat to samé. Bude jiná pro generála, jiná pro šéfa pobočky banky a jiná pro správce databáze inzertní služby Annonce, např. rubriky „hezké chvíle“. Tady se pak dostáváme k trendu posledního desetiletí – *soukromé* bezpečnosti. Není to sice úplně novinka (už César si dopisoval s Kleopatrou šifrovaně), ale je zřejmé, že význam nabývá právě s dostupností počítačů i pro osobní potřebu. Pak lze příliš vtíravému pronikání do osobního života účinně bránit často právě zase počítačem.

Základní pravidlo počítačové bezpečnosti:
Stoprocentní ochrana bývá téměř vždy nemožná a musíme se spokojit s určitým kompromisem.

2.3 Zásadní kroky pro zajištění bezpečnosti

Při prvním pohledu na řešení problémů informační bezpečnosti musíme mít na paměti tři zásadní skupiny úkonů, které je (téměř) vždy potřeba provést:

Analýza hrozeb. V tomto bodě je potřeba zvážit, co všechno by mělo být chráněno, a především vyhodnotit, jaké hrozby hrozí ochraňovaným hodnotám. Tento krok je směrodatný pro další postup, často však nelze než vycházet z analýzy empirických poznatků o problémech v okolí, jiných útocích na podobné hodnoty atd. Chybně provedená analýza hrozeb má za důsledek téměř vždy chybně navržená bezpečnostní opatření. Hodnoty pak mohou být chráněny velmi nákladným, ale naprosto nesmyslným a neúčinným způsobem.

Specifikace bezpečnostní politiky a architektury. Bezpečnostní politika stanoví, co mají dosáhnout a zajistit ochranná opatření. Zahrnuje požadavky, pravidla a postupy, určující způsob ochrany a zacházení s ochraňovanými hodnotami. Architektura

na vysoké úrovni popisuje strukturu celého komplexu opatření a jednotlivým částem přiřadí bezpečnostní funkce.

Popis bezpečnostních mechanismů. Zde jsou rozepsány techniky pro implementaci bezpečnostních funkcí nebo jejích částí. Účinnost mechanismu musí být v souladu s bezpečnostní politikou a přiměřená odpovídajícím hrozbám.

2.4 Základní cíle

Podívejme se na některé základní prvky bezpečnostní politiky a jejich provázanost s bezpečnostní architekturou (ne vždy jsou potřebné všechny uvedené prvky).

Důvěrnost. Cílem zabránit zjištění sémantického obsahu dat nepovolanými (neautorizovanými) osobami. Můžeme se o to snažit např. obecně utajením existence informací (značně obtížné), kontrolou přístupu k místům, kde se data nacházejí maskováním mezi jinými soubory nebo změnou dat do jiné podoby, kterou nelze změnit zpět bez znalosti patřičné (tajné) informace – klíče. Tento poslední způsob se běžně označuje jako šifrování a budeme se mu věnovat dále v tomto kurzu.

Integrita. Data bez povolení majitele (autorizované osoby) nesmí nepozorovaně změnit svůj stav (tzv. slabá integrita) nebo jej nesmí změnit vůbec (tzv. silná integrita). Povšimněme si, že pokud bude na dobré úrovni zajištěná důvěrnost, pak je zajištění integrity snazší.

Dostupnost. Autorizovaní uživatelé by měli mít přístup k datům a službám co nejméně komplikovaný. Dobře chráněná data, co se důvěrnosti a integrity týče, která nelze použít při řádné práci, ta nám nebudou příliš platná. Dostupnost dat zaručuje, že požadovaná data jsou v požadovaném čase na požadovaném místě. Dostupnost lze tedy v tomto smyslu vnímat také jako předpoklad k dosažení informační dominance.

Zodpovědnost. Za veškeré své činy a chování v systému mají uživatelé zodpovědnost vůči majiteli dat. Tato zodpovědnost nemusí být přímá (majitel nekontroluje každého uživatele osobně), ale v případě potřeby musí vždy existovat možnost zjistit, kde a kým (příp. i za jakým účelem) data v určitou dobu byla použita.

2.4.1 Nevhodnost doplňkové bezpečnosti

V praxi se často setkáváme s postupem, kdy se při budování systému nebo tvorbě aplikace těsně před odevzdáním zákazníkovi zjistí, že „by tam mělo být nějaké zabezpečení“. Nejprve je pracně vybudován rozsáhlý systém a teprve dodatečně se přichází na to, že bude potřeba "nějak"zajistit ochranu spravovaných informací. Tak se dodatečně vyčlení několik procent z rozpočtu a začne se doplňovat. Důsledky a výsledky jsou stejné, jako doplňování jedné z pozapomenutých stěžejních funkcí systému těsně před dodáním zákazníkovi.

Doplňková bezpečnost (angl. *add-on security*) v naprosté většině případů neposkytuje stejnou míru ochrany jako bezpečnost budovaná pro začlenění v prvotní specifikaci systému. Důsledkem pozdního doplnění specifikace o zajištění bezpečnosti může být vybudování ochrany na nižší úrovni (než by za stejné peníze poskytla ochrana budovaná plánovitě) nebo překročení rozpočtu, mnohdy obojí.

2.4.2 Co všechno může být bezpečnost

Bezpečnost nespočívá jen v pořízení a nainstalování ochran do systému. I v počítačových systémech hraje významnou roli **fyzická bezpečnost** – jde o to zjistit, kdo má fyzický přístup k prvkům systému (bez ohledu na hardwarovou či softwarovou ochranu) nebo jaký může být dopad přírodních katastrof. Dokonalá ochrana uživatelských stanic je mnohdy k ničemu, pokud je k systému připojena konzola, ze které operátor může neoprávněně (a nepozorovaně) sledovat informace na uživatelských obrazovkách. A dokonale šifrovaná data na serveru, z něhož někdo bez problémů ukradl celý pevný disk, ta již řešení podnikové strategie asi také nepomohou.

Tady přicházíme k dalšímu aspektu – **bezpečnosti personální** – která je jedním z pilířů dobré ochrany. K ochraně dat nemusí být příliš platné bezpečnostní řešení „na míru“ od renomované firmy, pokud k obsluze systému s přístupem k důležitým datům najmeme špióny konkurence nebo původce krádeží dat z několika bank.

Při návrhu bezpečnostní politiky je třeba si uvědomit, že mnohé hrozby nelze přímo odvrátit, ale buď jen snížit pravděpodobnost jejich „úspěšné“ realizace nebo s minimálními ztrátami (zdržením) zajistit následnou nápravu. Data je možné lehce duplikovat a záložní kopie bezpečně ukládat na vzdáleném místě. Nikdo nemůže zabránit šíření moru a virů, můžeme však udělat hodně pro to, aby nedošlo k nákaze našich dat. Zajištění bezpečnosti nikdy neznamená zajištění úplné ochrany, nýbrž minimalizaci rizik na tolerovatelnou úroveň.

2.5 Příklad z praxe

Pojďme se podívat na skutečný případ budování bezpečnosti v celostátní počítačové síti Národního zdravotního systému (NHS) v Anglii. Předběžný odhad nákladů – pouze na zavedení šifrovacích služeb pro zajištění důvěrnosti dat – je téměř 20 milionů liber, na roční údržbu a provoz padnou zhruba 3 miliony liber. Podle názoru mnohých expertů budou skutečné náklady několikanásobně vyšší, i když se opominou investice na zajištění jiných, pro medicínskou praxi životně důležitých, funkcí spolehlivé počítačové sítě. Dvě zásadní předpokládané hrozby jsou:

- možnost neautorizovaného připojení jedinců (hackerů) k síti a
- možnost odposlechu zasílaných informací.

Kritiku tohoto přístupu lze shrnout uvedením dvou údajů:

- podle posledních údajů z nezávislého auditu Národního zdravotního systému je jen 6 % případů narušení bezpečnosti způsobeno zvenčí,
- podle slov vedoucího oddělení UNIRAS, která je zodpovědná za vyhodnocování incidentů v oblasti bezpečnosti IT v celé vládě, byla v letech 1994/95 jen 2 % případů narušení bezpečnosti způsobena zvenčí.

Zkuste se na základě těchto údajů zamyslet nad tím, zda zajištění důvěrnosti je opravdu stěžejním problémem, případně které jiné hrozby nebyly zohledněny a o jaké prvky by měla být doplněna bezpečnostní politika takové rozsáhlé sítě.

2.6 Informační bezpečnost ve zdravotnictví

Medicína je velmi specifický obor lidské činnosti a rozhodně se jí rozvoj v oboru informačních technologií nedotkl tak, jako třeba žurnalistiky nebo obchodu. (Naštěstí?!) Samozřejmě – s počítači se i v lékařské praxi setkáváme téměř denně. Nelze ovšem čekat, že nahradí člověka do takové míry jako třeba v dopravě. Doktor není jen opravář těl, ale často i duší a lidských vztahů. Návštěva lékaře není pro většinu z nás nikdy obyčejným aktem jako třeba koupě piva nebo příjem výplaty.

Pokud chceme hovořit o bezpečnosti IT v medicíně, tak na prvním místě musíme zmínit bezpečnost ve smyslu anglického „*Safety*“ – předpoklad, že při specifikovaných podmínkách nedojde ke stavu ohrožení lidského života, zdraví, hodnot a prostředí. Ano, jde právě o ten lidský život. Kolik přístrojů je dnes v nemocnici obsluhovaných počítačem nebo s jeho zásadní podporou? K ohrožení života může dojít *přímo*, podobné případy jsou ale podle odborné literatury velice výjimečné, spíše extrémní. Jsou např. zaznamenány případy, kdy chyba v programu způsobila zvýšení dávek ozáření, kterému pak pacient podlehl. Lapidárně řečeno – pro počítač je číslo jako číslo. To je také příčinou chyb vedoucích k *nepřímému* ohrožení, kdy počítač nebo jím řízený přístroj dodají chybné výsledky vyšetření/analýzy, na jejichž základě lékař stanoví chybný léčebný postup.

2.6.1 Důvěryhodnost a důvěrnost

Mnohých případů léčby na základě chybných dat se lze vyvarovat zajištěním důvěryhodnosti (např. autentizací) předávaných informací. U informací na papíře lékař obvykle pozná rukopis specialisty z nemocnice nebo alespoň razítko ap. Jak ale pozná původ digitalizovaných informací? Přece nebude při obdržení výsledků z laboratoře telefonovat, ověřovat a zjišťovat kdo, kdy, jak a koho!? Právě bezpečnostní mechanismy jako třeba digitální podpis by měly lékaři umožnit zodpovězení všech otázek současně s přijetím laboratorní zprávy. S jakou úrovní spolehlivosti, to už závisí na implementaci a také přístupu všech pracovníků, kteří budou takovému systému předávat data nebo jej spravovat. Důležitý je také audit práce s daty (kdo viděl nebo dokonce měnil výsledky testu). Právě důvěrnost zdravotních informací je dnes velice aktuálním a ožehavým tématem.

Pacient má rozhodně právo očekávat, že lékař nikomu nesdělí žádné jeho osobní zdravotní informace, které získal při lékařském výkonu. Morální závazek lékaře je zde jasný, ne vždy však je dobře zakotven i v zákonech. Podle mého osobního názoru by lékař měl mít povinnost střežit takto získané informace stejně, jako kněz střeží informace spadající pod zpovědní tajemství. Bez souhlasu pacienta by pak rozhodně neměl tyto informace žádným způsobem předávat dál, ani pro potřeby soudu nebo policie.

Jak má však lékař dodržet takové závazky, když musí zdravotní pojišťovně sdělit, jaké zákroky provedl? Jaké závazky pak mají pracovníci pojišťovny? Na jaké úrovni pak lze udělat smysluplný kompromis? Podobné otázky je vždy nutno řešit při tvorbě *administrativních* dat, která v medicíně jsou v 90 % založena na datech *klinických*. České zdravotnictví se ale v současné době potýká s řadou existenčních problémů, takže lze očekávat, že důsledné řešení obdobných otázek zůstane až na další století.

2.6.2 Bezpečnost v klinických informačních systémech

V medicínské informatice bývá sice požadavek na ochranu dat často explicitně zmiňován, obvykle však bez podrobnější specifikace bezpečnostní politiky. Objevilo se donedávna jen několik návrhů k principům bezpečnostní politiky. Zásadní význam má až publikace „*Security in Clinical Information Systems*“, kterou vydala British Medical Association (BMA) v lednu 1996. Zásadní přínos tohoto výsledku práce specialistů BMA a zvláště Rosse Andersona (Cambridge University) je ve stanovení devíti základních principů bezpečnostní politiky pro klinické informační systémy. Přístup, který vyžaduje BMA i od vedoucích činitelů ministerstva zdravotnictví a Národního zdravotního systému, se často kříží s některými „představami“ o jednotném zdravotním záznamu, který by byl přístupný např. i pracovníkům ministerstva. Jejich zájem je zřejmý, ale nebude asi ani vzdáleně podobný představě pacienta. Také model práce zdravotnictví v Británii je rozdílný od českého – přesto – podívejme se na jednotlivé principy:

Každý identifikovatelný klinický záznam musí mít seznam řízení přístupu s vyjmenováním lidí nebo skupin lidí, kteří mohou záznam číst a přidávat k němu data. Systém musí zamezit přístupu kohokoliv, kdo není na tomto seznamu.

1. Doktor může otevřít nový záznam, kde je uveden jen on a pacient na seznamu řízení přístupu. Pokud je pacient jen na speciálním vyšetření, pak může doktor na seznam zařadit i jeho ošetřujícího lékaře.

2. Právě jeden z lékařů na seznamu řízení přístupu musí být označen jako odpovědný a pouze on může seznam měnit a může k němu přidávat jen odborné zdravotnické pracovníky.

3. Odpovědný lékař musí pacientovi sdělit, kdo je na seznamu řízení přístupu při vytvoření nového záznamu, při jakýchkoliv změnách a kdykoliv je odpovědnost za záznam předávána jinému lékaři. Pacientův souhlas musí být výslovný, s výjimkou řešení nouzových stavů a specifikovaných statutárních případů.

4. Nikdo nesmí mít možnost smazat klinické informace, dokud neuplynula předepsaná doba pro jejich úschovu.

5. Všechny přístupy ke klinickým záznamům musí být zaznamenány s udáním informací kdo a kdy se záznamem pracoval. Auditní záznam všech mazání musí být neustále udržován.

6. Informace ze záznamu A mohou být připojeny k záznamu B tehdy a jen tehdy, když seznam řízení přístupu záznamu B je obsazen v seznamu pro A.

7. Musí být zavedena účinná opatření proti agregaci osobních zdravotních informací. Pacienti, k jejichž seznamu řízení přístupu má být přidána další osoba, musí být zvlášť upozorněni, pokud již tato osoba má přístup ke zdravotním informacím velkého množství lidí.

8. Počítačové systémy, které pracují s osobními zdravotními daty, musí mít subsystém, který efektivně prosazuje výše uvedené principy. Účinnost tohoto subsystému musí být podrobena hodnocení nezávislými experty.

2.6.3 Požadavky lékařů

Při využití počítačů jsou lékaři velmi vnímaví uživatelé. Trpí sice obvyklou „nemocí“ požadavku na jednoduchost obsluhy atd., ale jsou si jasně vědomi možností, které jim počítače přinášejí. Je to do jisté míry dáno kvantem informací, které během svého vzdělání a každodenní praxe musejí lékaři vyhledávat, zpracovávat a využívat. Vědí, do jaké míry je spolehlivost (důvěryhodnost) informací zásadní pro jejich práci a také vědí, že jejich pacientům záleží na tom, aby ne každý (úředník) věděl o jejich nejniternějších problémech.

Dva zásadní požadavky – důvěryhodnost a důvěrnost informací – jsou zásadní charakteristiky lékařské praxe po tisíciletí. Osobně si myslím, že právě tento fakt dodává spolupráci lékařů a odborníků na bezpečnost IT hodně na zajímavosti. Ať už to budou aplikace na ochranu důvěrnosti informací o pacientech, na zajištění důvěryhodnosti laboratorních výsledků a zpráv o nových léčebných postupech a šetřeních nebo anonymizace dat pro výzkum a výuku nových adeptů oboru, popř. i pro plánovače ministerstva zdravotnictví.

3 Úvod do kryptografie

V kryptografii se obvykle pro popis komunikace označují komunikující strany jako ***A*** (Alice) a ***B*** (Bob) a také se musejí samozřejmě zvažovat „ti zlí“ – obvykle se jako hrozba zmiňuje odposlech (angl. *eavesdropping*) a zlá strana odposlouchávající komunikaci mezi Alicí a Bobem se označuje jako ***E*** (Eva).

3.1 Šifra, algoritmus, klíč

Kryptografie slouží k zajištění podpory mnohých aspektů bezpečnosti. Nejčastěji jsou to *důvěrnost* a *integrita*, ale nelze opomenout ani *dostupnost* a *zodpovědnost*. Zatím zůstaňme u důvěrnosti. Snahou Alice je ochránit svá důvěrná data před zraky nepovolaných slídilů, ať už jsou tyto data uložena v Aliciných elektronických zařízeních (např. v počítači, mobilu, paměťové kartě apod.), online (např. služby Dropbox, Ubuntu One apod.) nebo se jedná o data, které posílá Alice Bobovi. Alice proto využívá nástrojů kryptografie, aby zajistila, že požadovaná data nebude moci číst nikdo jiný ale pouze ten, komu na to dá Alice výslovné svolení.

V minulosti vystupovali v roli Alice a Boba především diplomaté, vojáci, obchodníci či milenci. Dnes již bychom si bez zachování důvěrnosti pomocí kryptografie těžko dokázali představit např. fungování e-shopů, mobilních telefonů, platebních karet či vzdálené odemykání a zamykání automobilů nebo elektronických bran.

Pro zachování důvěrnosti informace převádíme její srozumitelnou podobu do podoby nesrozumitelné tak, aby se ztratila její informační hodnota. Tuto transformaci nazýváme šifrováním.

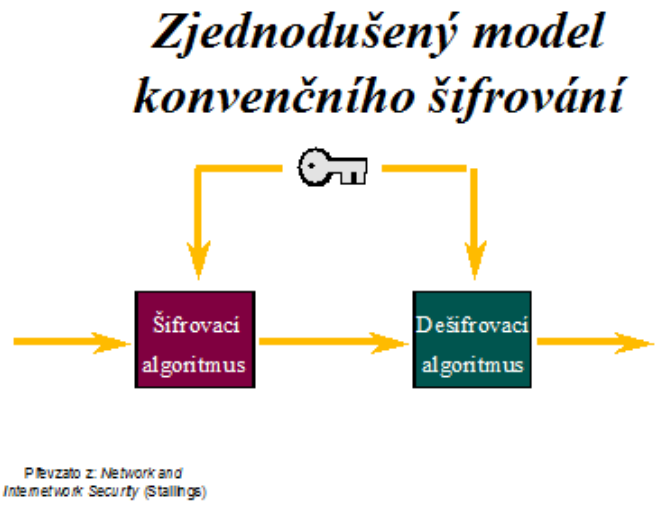
Přáním Alice většinou je, aby její data nemohl prohlížet nikdo jiný (ať už na počítači nebo při přenosu) – pokud mu k tomu Alice nedá výslovné svolení. Ale sama Alice aby mohla podle potřeby zase změnit podobu nazpět. Po dlouhou dobu jako Alice vystupovali hlavně diplomaté, vojáci, obchodníci a milenci.

Známým příkladem šifrování je jednoduchá šifra Julia Cesara. Ta funguje na principu substituce každého písmena textu následujícím písmenem abecedy – „posunutým“ o 3

pozice. Písmeno „A“ se tak šifrováním převede na „D“, písmeno „B“ pak na „E“ atd. Je ale jasné, že takovýto postup neukrývá informace příliš bezpečně. Některá písmena se totiž v textu vyskytují častěji než jiná. Není tak velkým problémem vyhodnotit relativní výskyt písmen v zašifrovaném textu a srovnat jej s průměrnými hodnotami pro písmena daného jazyka. Na základě charakteristické početnosti výskytu písmen (latina má jiné charakteristiky než čeština) pak lze odhalit, která písmena se zašifrovala na která písmena zašifrovaného textu. Vše lze pak doladit metodou pokusů a omylů, nejlépe za použití počítače.

V obdobném druhu šifer jsou patrné dvě věci: každé písmeno se nahradí jiným, způsob náhrady je určen nějakým číslem (u Césarovy šifry trojkou) a také všeobecným povědomím o písmenech v abecedě a jejich řazením.

U šifry Julia Cesara je šifrovacím algoritmem náhrada písmen a parametr 3 je *šifrovacím klíčem. Šifrováním* tedy rozumíme převod *nešifrovaných* (otevřených) dat na data *šifrovaná* pomocí šifrovacího systému, který se skládá z šifrovacího algoritmu a šifrovacího klíče. U šifrování je podstatné, aby zašifrovaný text bylo možné pomocí šifrovacího klíče opět převést zpět do čitelné podoby. Tomuto procesu říkáme *dešifrování* (viz Obrázek 1).



Obrázek 1: Model symetrického šifrování.

Kryptografií pak označujeme vědu (nebo snad umění?) zabývající se tvorbou šifrovacích a dešifrovacích algoritmů. Takže pak mluvíme o kryptografických algoritmech, klíčích, zařízeních atd. A *kryptoanalýzou* se rozumí obor, který se snaží šifry překonávat a hledat jejich slabiny. Obor označovaný jako *kryptologie* pak spojuje tyto dva sourozence – siamská dvojčata.

V kryptologii se používá nejen operací šifrování a dešifrování jako operací reverzibilních, ale také např. hašování – „srážení“ rozsáhlých dat na malý, leč reprezentativní řetězec. Tento řetězec (hašovací hodnota čili haš) má zásadní význam třeba u digitálního podpisu a problematika hašování má v oboru kryptologie velmi privilegované postavení.

Kryptografie i celá počítačová bezpečnost jsou záležitosti stavění překážek a hledání děr. *Základní pravidlo kryptografie je, že ochrana spočívá v tajnosti klíče, a nikoliv v tajnosti algoritmu.* Bezpečnost algoritmu je jeho schopnost odolat úsilí protivníka získat přístup k nezašifrovanému textu či spíše k šifrovacímu klíči. Absolutně bezpečný algo-

ritmus by měl garantovat, že ze zachyceného zašifrovaného textu nelze bez klíče získat nezašifrovaný text. Jediným známým algoritmem s touto vlastností je *Vernamova šifra*, kde je nezašifrovaný text kombinován operací XOR s náhodnou neopakující se posloupností dat stejné délky a dešifrování se provede opakováním operace XOR na zašifrovaná data a onu posloupnost. Nevýhoda je zřejmá – délka klíče je stejná jako délka šifrovaného textu. Z tohoto důvodu se této metody používá jen výjimečně (i když dnes kapacity současných paměťových médií lze pro absolutně bezpečné šifrování vhodně využít).

Dobrý algoritmus je terčem analýz a „útoků“ ze všech stran roky (2-3 se pokládají za minimum), kdy se ho pokouší desítky špičkových odborníků nějak pokořit. *Neveřejný algoritmus je nedůvěryhodný algoritmus.* Pro Alici nemá velký smysl chránit klíč od málo robustních dveří – Eva může třeba jen jednoduše vyšroubovat panty. Většinu uživatelů zajímá hlavně použitelnost algoritmů a ve věci konstrukce algoritmů se spoléhají na odborníky v kryptologii a bezpečnosti. Každým rokem se konají desítky kryptologických konferencí, z nich nejvýznamnější jsou americké Crypto spolu s Eurocryptem a Asiacryptem/Auscryptem. Existuje také Mezinárodní asociace pro kryptologický výzkum (IACR – www.iacr.org), která výše uvedené konference (spolu)pořádá. Odpověď na otázku „který algoritmus je nejlepší“ neexistuje, lze se ale pokusit ve sbornících najít, které algoritmy mají nějaké slabiny, jak algoritmy vhodně používat nebo pro co je naopak raději vůbec nepoužívat. Vždy se vyplatí hledat pravdu na všech stranách a zjistit si o algoritmech i jejich aplikacích co nejvíce detailů od co nejvíce lidí.

Neformální pravidlo by se asi dalo formulovat takto – *pokud nejsou všechny zásadní detaily o algoritmu známy alespoň dva roky a nejsou o něm publikovány alespoň dva tucty nezávislých analýz a přednášek na konferencích IACR, tak nemá smysl o nasazení algoritmu vůbec uvažovat.* Přinejmenším ne v prostředí, kdy nemáte skutečně spolehlivou ochranu přístupu k vašim počítačům nebo kdy posíláte data po veřejných linkách.

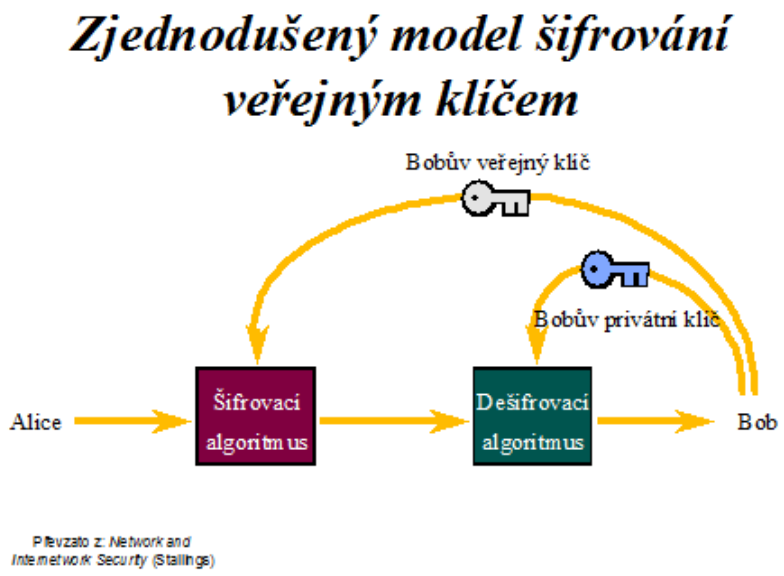
3.1.1 Symetrické a asymetrické algoritmy

Kryptografické algoritmy se v zásadě dělí na dvě velké skupiny:

- **symetrické** algoritmy, kde se pro zašifrování i dešifrování používá stejný kryptografický klíč;
- **asymetrické** algoritmy, které používají odlišný klíč pro zašifrování (veřejný klíč) i pro dešifrování (soukromý klíč).

Obě skupiny lze dále členit podle způsobu transformace dat a jiných detailů – např. šifry proudové (zpracováván bit po bitu) či blokové (data zpracovávána v blocích). Význam rozdělení algoritmů na dvě prvně uvedené skupiny není v rozdělení algoritmů na dvě různé třídy bezpečnosti, ale v problémech ohledně správy klíčů a obecně i výkonu. Lze totiž – zjednodušeně – říct, že symetrické algoritmy jsou rychlejší. Zato si musíte s každým, s kým chcete komunikovat při využití šifrování, domluvit kryptografický klíč a obě strany jej musí pečlivě opatrovat. Asymetrické algoritmy jsou na tom sice s výkonem hůře, zato ale stačí spolehlivě zveřejnit svůj veřejný klíč a chránit si jen svůj soukromý klíč. Ono spolehlivé zveřejnění veřejného klíče a jeho případné zrušení v případě porušení nebo krádeže soukromého klíče je velice problematická záležitost. U rozsáhlých skupin komunikujících účastníků někdy může být celkově výhodnější jednodušší způsob šifrování symetrickou cestou. Nejčastějším praktickým řešením bývá tzv. *hybridní systém*, kde jsou

prostředky asymetrických algoritmů použity k autentizaci a ustavení společného klíče pro následné symetrické šifrování – tento systém je uplatněn např. v SSL (viz podkapitola 5.2).



Obrázek 2: Model asymetrického šifrování.

Ale zpět ke klíčům – velmi jednoduchým příkladem na vysvětlenou mohou být klasické visací zámky. Pro symetrickou kryptografii si můžeme celou situaci představit tak, že každá z komunikujících stran A, B, C a D musí obvykle mít k dispozici zámky i klíče všech ostatních stran. Pokud chtějí tajně komunikovat všechny tyto strany společně, pak jim stačí po jedné kopii zámku a klíče. Pak ale nemá A žádnou jistotu, zda zprávu obdržela od C nebo od D. Takže obvykle má každá ze stran různé klíče ke komunikaci s různými partnery. Pokud chce Alice poslat tajnou zprávu Bobovi, pak musí vzít klíč se zámkem A-B, zprávu tímto klíčem zašifrovat a poslat Bobovi (viz Obrázek 3). Ten musí mít klíč k zámku A-B a zprávu odemknout – dešifrovat (viz Obrázek 4).

V případě využití asymetrické kryptografie každá strana opatruje jen svůj soukromý klíč a kdokoliv může použít všeobecně přístupné prostředky (v našem případě připravené zámky) pro zašifrování zprávy. Je ovšem důležité mít na vývěsce prostředky správně označené, neumožnit jiným stranám změny prostředků atd. (Eva nesmí nahradit věci označené „A“ svými vlastními, ani je změnit, poškodit atd.) Tady přicházejí ke slovu věci jako certifikáty kryptografických klíčů, o kterých se dozvíme dále v tomto kurzu a ke kterým se vztahuje i podstatná část Zákona č. 227/2000 Sb. o elektronickém podpisu.

3.1.2 Délka klíče

Častým ukazatelem úrovně ochrany – i když někdy velice zavádějícím – je délka použitého kryptografického klíče. Pokud vezmeme jeden konkrétní a kvalitní algoritmus, tak platí, že čím delší je použitý klíč pro šifrování, tím lepší je úroveň ochrany. Pro případného útočníka, který nemá k dispozici dešifrovací klíč, totiž vede cesta k překonání šifry přes vyzkoušení všech možných hodnot klíče, případně hledání slabin algoritmu. Pokud útočník zná vyloženou „díru“ v algoritmu, pak vám nepomůže ani milionbitový klíč... A nevadí,

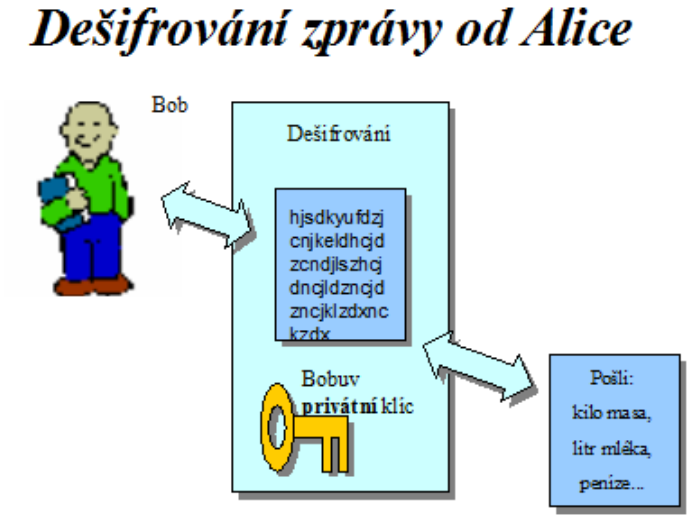
Obrázek 3: Schematické znázornění šifrování veřejným klíčem.

že zbytek světa o díře neví nebo že dokonce neví, jaký algoritmus jste použili. Pokud je ale algoritmus skutečně dobrý, pak delší klíč znamená pro útočníka zdržení ze dvou důvodů:

- jednak musí vyzkoušet víc možných hodnot klíče (jednobitový klíč může nabývat dvou hodnot – 0 a 1, dvoubitový čtyř – 00, 01, 10 a 11... a co třeba stobitový?);
- pro algoritmy s variabilní délkou klíče také delší klíč znamená delší dobu potřebnou pro provedení výpočtu.

Uvádění bezpečnosti jen délkou klíče bez uvedení algoritmu je velice ošemetné, některé hranice ale lze zhruba načrtnout. Pro symetrické blokové šifry (DES, IDEA, RC4 atd.) se dnes má za to, že oblast 70 bitů je běžně překonatelná během několika hodin vládními superpočítači asi pro 15-20 zemí světa. A s Internetem lze dnes také provádět výpočty distribuované na stovkách i tisících strojů, takže tato hranice je překonatelná i pro odhodlaný tým „nevládních“ odborníků. Ovšem cena za vyluštění jedné takové zprávy, jako byla ta v *DES Challenge* je značná, čili se není potřeba obávat, že by třeba DES nebyl „dost dobrý“ pro běžnou potřebu jednotlivce nebo malé firmy pro šifrování dat, která chceme chránit dnes, ale netrápí nás jejich zveřejnění za měsíc. Dnes již ovšem máme k dispozici nový standard pro symetrickou blokovou šifru – AES (viz níže). U dobrých symetrických blokových šifer se má za to, že hranice 100 bitů je pro klíč dostatečnou zárukou bezpečnosti nejméně pro 3-4 další roky. Zde je taky vhodné poznamenat, že alternativa trojitý DES nabízí ochranu ekvivalentní asi 112 bitům.

Pro asymetrické algoritmy je situace značně komplikovanější. Asi nejznámějším algoritmem je RSA (nazvaný dle svých otců – Rivesta, Shamira a Adlemana), u kterého je dnes překonatelná hranice někde pod 800 bitů. Většinou se tedy pro RSA doporučují klíče buď s délkou 1024, nebo raději 2048 bitů. Pro algoritmy nad eliptickými křivkami se dnes uvádí, že cca 170 bitový klíč dává stejnou bezpečnost jako u RSA s klíčem okolo 1000 bitů, resp. klíč sym. alg. 80 bitů.



Obrázek 4: Schematické znázornění dešifrování privátním klíčem.

3.1.3 Advanced Encryption Standard

2. října 2000 se celý kryptografický svět od amerického NIST (National Institute of Standards and Technology) dozvěděl, že z pětice finalistů při výběru kryptografického algoritmu pro nový americký standard AES (Advanced Encryption Standard), následovníka DES, byl vybrán algoritmus Rijndael. Autory tohoto algoritmu jsou Vincent Rijmen a Joan Daemen. Rijndael sice nepatřil mezi nejlepší z hlediska odhadu bezpečnosti (společně s dalším finalistou RC6 byla bezpečnost hodnocena jako „adekvátní“ a nikoliv „vysoká“ jako u dalších tří finalistů), ale jeho hodnocení z jiných hledisek jej činilo ideální volbou dle mnoha expertů. Důležité je také rozhodnutí NIST nezavádět druhý, tzv. záložní algoritmus, což byla varianta zvažovaná jak kvůli možnosti rychle nasadit jiný algoritmus v případě nenadálého selhání primárního algoritmu, tak údajně i z jiných důvodů (např. že žádný z amerických návrhů v soutěži neuspěl). Důvodovou zprávu k výběru algoritmu a další podrobné informace najdete na www.nist.gov/aes.

3.2 Kryptografie jako zbraň

Masové rozšíření Internetu a potřeba řídit bezpečné elektronické obchodování s sebou přinesly potřebu větší dostupnosti kryptografie. Dodnes je ale s exportem šifrovacích produktů mnohde zacházeno jako s exportem zbraní. Je pravda, že silná kryptografie představuje významnou „zbraň“ – schopnost utajit (zašifrovat) nebo naopak dešifrovat komunikaci může rozhodnout výsledek konfliktu. Vládní zájmy se zde soustřeďují do dvou oblastí:

- mít jistotu, že používání kryptografických systémů nesníží schopnost dopadnout nežádoucí osoby a skupiny osob;
- zajistit, aby používání kryptografických systémů nepůsobilo proti národním zájmům dané země.

Uvádí se, že např. vládě USA se takto daří v oblasti kryptografických a hlavně kryptoanalytických objevů udržovat náskok přibližně 10-15 let před civilním světem (a dalšími zeměmi). Americká NSA (National Security Agency), která má dvě zásadní poslání (srovnejte s principy uvedenými v úvodu článku): Získávat vládě USA přístup k informacím komunikovaným mimo území USA a také pomáhat v tom, aby nebylo možno získat přístup k informacím vlády USA. NSA je snad nejméně známou, ale velmi důležitou tajnou službou USA. NSA disponuje nejvýkonnějšími počítači, jaké jsou na povrchu této planety nasazeny a toto platí po celou dobu její existence. Má analytické pracovníky snad všude, kde jen lze získávat nějaké informace důležité pro USA. Prvním Američanem zabitým ve válce ve Vietnamu byl právě pracovník NSA. Pro ilustraci o práci NSA stojí za přečtení rozhovor s jejím bývalým pracovníkem Perry Fellwockem na www.euronet.nl/∼rembert/echelon/nsa-elint.htm, nebo bezpečnostní manuál pro pracovníky NSA na www.cl.cam.ac.uk/∼rja14/Papers/nsaman.pdf.

4 Autentizace uživatelů a dat, digitální podpis

4.1 Autentizace

Autentizace uživatele je obvykle prvním krokem, který každodenně provádíme na začátku naší práce s počítačem. Primárním cílem autentizace je zabránit neautorizovaným uživatelům v používání počítačového systému. Sekundárním cílem je znalost systému, který uživatel s ním vlastně pracuje – tak, aby systém mohl řídit přístup uživatele k datům a službám podle daných pravidel.

Autentizační metody v zásadě dělíme do tří, resp. čtyř skupin:

1. Na základě výlučné znalosti (co kdo zná) – tyto metody jsou poměrně velmi dobře známy, jedná se o použití tajných hesel, PINů, algoritmů atd.

2. Podle *vlastnictví specifických předmětů (co kdo má)* – tyto metody jsou také široce rozšířeny, jsou to např. magnetické a čipové karty, ale i běžné klíče k zámkům a speciální zařízení jako jsou tzv. autentizační kalkulátory.

3. *Biometriky (co kdo je)* – tyto metody nabízí automatizované metody verifikace nebo identifikace (rozpoznání identity člověka) na základě fyziologických charakteristik jako jsou například otisk prstu či hlas. Takové charakteristiky jsou jedinečné a měřitelné. Používaly se mnoho let pro zvláště kritické kontroly (armádní a vládní systémy) a v posledních letech můžeme pozorovat širší nasazení biometrické autentizace.

4. *Kombinací výše uvedených metod* – takto lze dosáhnout výrazného zvýšení spolehlivosti autentizace. Typickým příkladem je použití bankovní karty v kombinaci se znalostí PINu.

   Zatímco první dvě skupiny lze použít jen k verifikaci identity, biometrické techniky můžeme použít na dvě rozdílné aplikace: na verifikaci (identity) a na identifikaci. *Verifikace* je proces, při kterém subjekt předkládá svou identitu (např. vložením karty nebo zadáním hesla) a na základě této identity se srovnávají aktuální biometrické charakteristiky s uloženými charakteristikami, které této identitě odpovídají

podle záznamů autentizační databáze. Při *identifikaci* (nebo také *vyhledání*) naopak člověk identitu sám nepředkládá. Systém prochází všechny (relevantní) biometrické záznamy v databázi, aby našel patřičnou shodu a identitu člověka sám rozpoznal.

4.2 Biometrické systémy

Zatímco první dvě z výše uvedených skupin jsou počítačové i širší veřejnosti poměrně dobře známy, o biometrikách zatím koluje mnoho nepřesností a proto se o nich zmíníme šířeji.

Biometrických technologií existuje mnoho a jsou založeny na *měření fyziologických vlastností* lidského těla (např. otisk prstu nebo geometrie ruky) nebo *chování člověka* (např. dynamika podpisu nebo vzorek hlasu). Některé technologie jsou teprve ve stadiu vývoje (např. analýza pachů či rozmístění žil na zápěstí), avšak mnohé technologie jsou již relativně vyzrálé a komerčně dostupné (např. systémy porovnávající otisky prstů nebo vzorek oční duhovky). Systémy založené na fyziologických vlastnostech jsou obvykle spolehlivější a přesnější než systémy založené na chování člověka, protože jsou lépe opakovatelné a nejsou ve velké míře ovlivněny daným jedincem (psychickým stavem) jako např. stres nebo nemoc.

Nejvýznamnější rozdíl mezi biometrickými a tradičními technologiemi je odpověď systému na autentizační požadavek. Biometrické systémy nedávají jednoduché odpovědi typu ano/ne. Heslo buďto je „abcd“ nebo ne, magnetická karta s číslem účtu 1234 jednoduše je nebo není platná. Podpis člověka však není vždycky naprosto stejný, stejně tak pozice prstu při snímání otisku se může trochu lišit. Biometrický systém proto nemůže určit identitu člověka absolutně, ale místo toho řekne, že s určitou pravděpodobností se jedná o daného jedince.

4.2.1 Chyby a variabilita v biometrických systémech

Mohli bychom vytvořit systém, který by vyžadoval pokaždé téměř 100% shodu biometrických charakteristik. Takový systém by však nebyl prakticky použitelný, neboť naprostá většina uživatelů by byla téměř vždy odmítnuta, protože výsledky měření by byly vždy alespoň trochu rozdílné[2]. Abychom tedy udělali systém prakticky použitelný, musíme povolit určitou variabilitu biometrických charakteristik. Současné biometrické systémy však nejsou bezchybné, a proto čím větší variabilitu povolíme, tím větší šanci dáváme podvodníkům s podobnými biometrickými charakteristikami.

Variabilita tedy určuje, jak hodně podobná musí být biometrická data, aby systém uživateli povolil přístup. Tato variabilita je obvykle nazývána jako (bezpečnostní) *prahová hodnota* nebo (bezpečnostní) *úroveň*. Je-li povolená variabilita pouze malá, pak bezpečnostní úroveň nazýváme vysokou a je-li povolená variabilita větší, pak bezpečnostní úroveň nazýváme nízkou.

Existují dva typy chyb, které biometrické systémy mohou udělat:

- *nesprávné odmítnutí* (angl. *false rejection*) neboli chyba prvního druhu nastane, pokud je oprávněnému uživateli odmítnut přístup (protože biometrický systém nepovažuje současná biometrická data dostatečně podobná uloženému registračnímu vzorku)

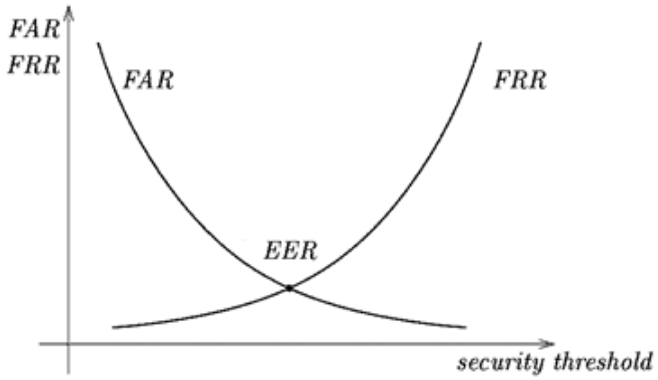
[2]Stoprocentní shoda napovídá, že jsme se dostali k velmi zdařilé kopii (podvrhu).

- *nesprávné přijetí* (angl. *false acceptance*) neboli chyba druhého druhu nastane, pokud je přístup udělen neoprávněnému uživateli (protože systém považuje podvodníkova biometrická data dostatečně podobná biometrickým datům nějakého oprávněného uživatele)

V ideálním biometrickém systému by byl počet nesprávných odmítnutí i počet nesprávných přijetí nulový. V reálném systému jsou však tato čísla nenulová a závisí na nastavené bezpečnostní úrovni. Čím vyšší je tato úroveň, tím více je nesprávných odmítnutí a méně nesprávných přijetí a čím nižší je bezpečnostní úroveň, tím více je nesprávných přijetí a méně nesprávných odmítnutí. Počty nesprávných přijetí a nesprávných odmítnutí jsou tedy nepřímo úměrné.

Rozhodnutí jak vysokou bezpečnostní úroveň použít je závislé především na účelu celého biometrického systému. Správná míra tolerance musí být kompromisem mezi použitelností a bezpečností použitého systému. Biometrický systém u vchodu do zábavního parku Disney bude typicky používat nižší úroveň bezpečnosti (tj. vyšší míru tolerance) než systém u vchodu do centrály CIA.

Počet nesprávných odmítnutí a nesprávných přijetí se obvykle vyjadřuje jako procentuální podíl z celkového počtu oprávněných a neoprávněných přístupů. Tyto poměry se anglicky označují jako *false rejection rate* (FRR) a *false acceptance rate* (FAR). Čím nižší jsou tato čísla, tím přesnější je dané zařízení. Některá biometrická zařízení (nebo jejich obslužný software) vyžadují bezpečnostní úroveň jako parametr rozhodovacího procesu při požadavku autentizace. Jiná zařízení vrací skóre z nějakého intervalu a výsledné rozhodnutí je ponecháno aplikaci. Pokud zařízení podporuje několik bezpečnostních úrovní nebo vrací skóre, můžeme vytvořit graf závislosti FRR a FAR na nastavené bezpečnostní úrovni. Příklad takového grafu ukazuje následující obrázek (viz Obrázek 5):



Obrázek 5: Křivka FAR/FRR.

Křivky FAR a FRR se protínají v bodě, kde se FAR a FRR rovnají. Tato hodnota se anglicky nazývá *equal error rate* (EER) nebo také *crossover accuracy*. Toto číslo nemá velké praktické využití (zřídkakdy chceme, aby se FAR a FRR právě rovnaly), ale je možné ho použít jako ukazatel přesnosti daného zařízení. Pokud máme dvě zařízení s ERR 1 % a 10 %, víme, že první zařízení je přesnější (tj. má menší chybovost). V praxi nejsou tato srovnání tak jednoduchá především proto, že není jednoduché získat srovnatelná FAR a FRR pro jednotlivá zařízení. Výrobci často uvádějí pouze nejlepší dosažitelné hodnoty (např. FAR < 0.01 % a FRR < 0.1 %). Tyto hodnoty však nejsou dosažitelné zároveň (tj.

při určité bezpečnostní úrovni). Navíc jsou to hodnoty získané při testech v laboratořích a s profesionálními uživateli (často přímo s vývojáři). Hodnoty získané při nezávislých testech s neprofesionálními uživateli se od publikovaných hodnot samozřejmě podstatně liší (často i z desetin procent na desítky procent). Proto je při interpretaci jakýchkoli takovýchto hodnot obezřetnost určitě na místě.

4.3 Digitální podpis

Digitální podpis se podpisu klasickému, ručnímu, v lecčem podobá a v lecčem také liší. Podoba spočívá především v použití, jakožto prvku stvrzujícího zhlédnutí podepsaného dokumentu (*autenticita* dokumentu) s tím, že toto stvrzení lze prokázat i později (*nepopiratelnost*). Liší se především ve dvou aspektech:

1. Digitální podpis je vždy závislý na podepisovaných datech – podpisy různých dokumentů jsou vždy různé, kdežto ruční podpisy jedné osoby jsou i na různých dokumentech jeden jako druhý. Tímto digitální podpis perfektně zaručuje *integritu* podepsaného dokumentu.

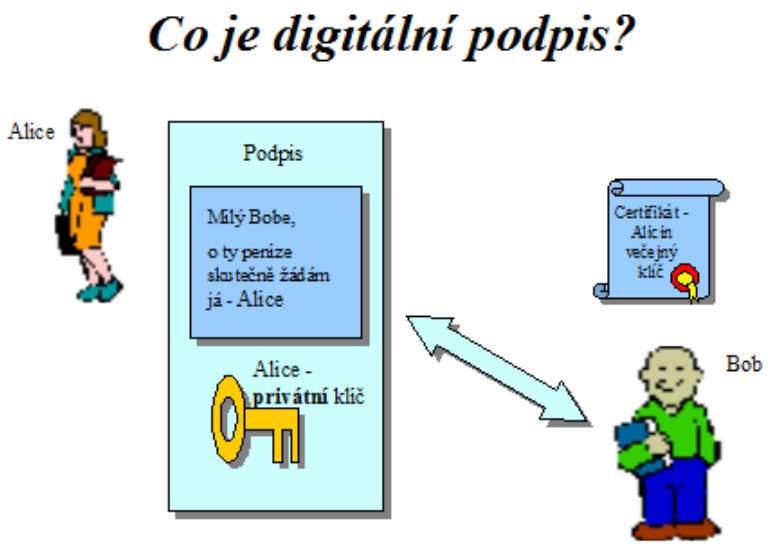
2. Ruční podpis tvoří vždy člověk (i když jej lze samozřejmě padělat), kdežto digitální podpis tvoří vždy počítač. Člověk má tedy omezenou kontrolu nad tím, co a kdy se vlastně podepisuje. Jednak nemá naprostou jistotu, že jsou podepisována data, o kterých si myslí, že jsou podepisována; také ale mohou být podpisy vytvářeny i bez vědomí uživatele (např. prostřednictvím Trojských koní).

Při podpisu digitálního dokumentu je důležitá jeho bitová reprezentace, nikoliv grafická podoba. Digitální podpis je pak také charakteristický řetězec bitů, nikoliv třeba oskenovaný ruční podpis. Pro tvorbu digitálního podpisu je potřebný jednak podepisovaný dokument, ale především jeden z páru klíčů používaných při asymetrické kryptografii. Privátní (soukromý) klíč a podepisovaná data jsou vstupními daty pro podpisový algoritmus, jehož výstupem je digitální podpis daných dat, tento podpis pak lze připojit ke zprávě.

Ve skutečnosti se ale v praxi digitální podpis vytváří následujícím způsobem (protože aplikace asymetrického algoritmu na rozsáhlé datové soubory je časově značně náročná). Nejdříve se vytvoří tzv. haš (kontrolní součet datového souboru), který je vlastně přesnou reprezentací (charakteristikou) dat. Tento haš je vlastně výstupem jednocestné kryptografické hašovací funkce aplikované na data. A až poté se tento haš podepíše daným asymetrickým šifrovacím algoritmem za pomoci privátního klíče.

Poté si každý, kdo zná patřičný veřejný klíč podepsané osoby, může ověřit platnost digitálního podpisu aplikací tohoto veřejného klíče, podepsaných dat (či haše) a digitálního podpisu za použití tzv. verifikačního algoritmu. Pokud je výsledek verifikace podpisu daných dat v pořádku, tak můžeme mít jistotu, že zpráva byla podepsána vlastníkem privátního klíče a že po podepsání již nebyla modifikována.

Správná znalost veřejného klíče (a komu patří) je tedy kritická pro používání digitálního podpisu.



Obrázek 6: Schematické znázornění digitálního podepisování.

4.4 Certifikáty veřejných klíčů

Jak jsme si již říkali u asymetrické kryptografie i u digitálního podpisu, hlavním problémem správy používání veřejných klíčů je jejich integrita a spojení s dalšími informacemi o držiteli klíče atd. Částečným řešením je použití certifikátů, které spolehlivě vážou veřejný klíč k oněm dalším informacím. Spolehlivé vázání je u certifikátů řešeno digitálním podpisem – operací s privátním klíčem entity, která takto vlastně „prohlašuje“ vazbu za důvěryhodnou. To, jaká je konkrétně důvěryhodnost, záleží na mnoha faktorech a bude z různých hledisek různá – stejně jako je různá důvěra dvou jedinců ve výrok pronesený třetím jedincem. Nejčastější podoba certifikátů odpovídá standardu X.509 (mj. i certifikáty ve vašich prohlížečích).

```
Certificate  ::=  SEQUENCE  {
    tbsCertificate          TBSCertificate,
    signatureAlgorithm      AlgorithmIdentifier,
    signature               BIT STRING  }
TBSCertificate  ::=  SEQUENCE  {
    version         [0]     Version DEFAULT v1,
    serialNumber            CertificateSerialNumber,
    signature               AlgorithmIdentifier,
    issuer                  Name,
    validity                Validity,          -- notBefore, notAfter
    subject                 Name,
    subjectPublicKeyInfo    SubjectPublicKeyInfo,  -- algID, bits
    issuerUniqueID  [1]     IMPLICIT UniqueIdentifier OPTIONAL,
    subjectUniqueID [2]     IMPLICIT UniqueIdentifier OPTIONAL,
    extensions      [3]     Extensions OPTIONAL
                    -- sequence of: extnID, crit, value }
```

Část certifikátu dle X.509.

Otázkou často je, zda ono certifikování svěříme nějaké „důvěryhodné“ instituci – tzv. třetí straně, nebo zda jej provádíme přímo sami. Oba postupy mají své výhody i nevýhody. Obvykle platí, že odborníci na bezpečnost preferují postup, kdy mají kontrolu nad tím, komu vlastně věří a proč, sami – například podpisem PGP klíčů svých partnerů pro komunikaci. Toto ale nelze předpokládat u všech uživatelů. Tady je vhodnější cesta oněch třetích stran nazývaných pro tento účel certifikační autority. Je pak potřeba mít na paměti, že veškerou důvěru při ověřování vazeb klíč-držitel, často spojených s ověřováním držitele, takto uživatelé svěřují certifikační autoritě. Pokud takovýto postup vyhovuje (certifikační autoritou je někdo skutečně důvěryhodný, popř. je to skupina určená vedením podniku pro všechny jeho zaměstnance atd.), pak je tato cesta schůdnější – pro uživatele certifikátů. Je třeba si uvědomit, že pro opravdu spolehlivou certifikační autoritu, nabízející své služby na Internetu bez omezení a v kvalitě, které mají uživatelé alespoň minimální důvod věřit, se pohybují náklady na zahájení provozu asi na 2-5 mil. dolarů a náklady na roční provoz okolo miliónu.

U certifikátů podle X.509, které nalezly svoje uplatnění v zajištění bezpečnosti na Internetu, je potřeba brát v úvahu to, že sice odpovídají standardu co se položek certifikátu týče, ale jejich implementace může být odlišná pro různé typy aplikací a platforem. Tak je tomu částečně i u certifikátů pro webové prohlížeče.

5 Prostředky ochrany dat pro běžné uživatele

5.1 Výsledek jednoduchého odhadu rizik

Pod pojmem *riziko* rozumíme nejčastěji (existují různé definice) vyjádření pravděpodobnosti výskytu specifické škody (realizaci bezpečnostní hrozby).

Analýza rizik je činnost, jejíž výsledkem je výpočet pravděpodobnosti výskytu škod. *Odhad rizik* je pak povrchnější, předběžná činnost, jejíž výsledkem je přibližný odhad pravděpodobnosti výskytu škod. Cílem analýzy rizik je určit optimální poměr mezi možnými hrozbami (či spíše jimi způsobenými ztrátami) a náklady vynaloženými na bezpečnostní opatření, která by tyto ztráty měla omezit. Analýza rizik se vlastně nezabývá jen vlastní analýzou, ale zahrnuje určení, případně odhad rizik a poté vlastní analýzu rizik. S analýzou je pak úzce spojeno řízení a kontrola rizik.

Určení či odhad rizika závisí na možných hrozbách a zranitelnostech systému. Zjištění všech potenciálních hrozeb a určení typu a účinnosti protiopatření není snadný úkol. Jiné hrozby jsou důležité pro armádu, jiné pro školy nebo pro redakce časopisů.

Představme si nejmenovaný rešeršní časopis (a online službu) umožňující odběrateli získat dokonalý přehled o trendech a vývoji v oblasti bezpečnosti elektronického obchodování a souvisejících oblastí (počítačová a komunikační bezpečnost, kryptografie, techniky ochrany duševního vlastnictví atd.). Tento časopis monitoruje významné časopisy, knihy a konference v daných oborech po celém světě.

Při tvorbě časopisu formou teleworkingu se jedná (minimálně) o tyto druhy použití Internetu:

- Komunikace s vydavateli monitorovaných publikací probíhá z cca 80-90 % po Internetu.

- Mnohdy (cca 10-20 %, s rostoucí tendencí) jsou vlastní publikace v elektronické formě a rešeršní pracovníci nebo šéfredaktor je získávají po Internetu.
- Rešerše jsou zaslány do redakce prostřednictvím emailu.
- Veškerá komunikace mezi editory a korektory také probíhá prostřednictvím emailu.
- Finalizované rešerše jsou ukládány do databáze, jejíž jedna kopie se používá přímo pro podporu webové verze časopisu.
- Uživatelé/čtenáři přistupují k online verzi časopisu přes jeho webové stránky. (V budoucnu budou např. také dostávat informace o nových rešerších emailem v případech, že rešerše obsahují zvolená klíčová slova nebo patří do vybraných kategorií.)

Po zvážení bezpečnostních rizik a jejich možného dopadu na průběh projektu a chod firmy vyplynuly následující priority ochrany proti:

1. **Nedostupnosti online verze.** Tento aspekt je hodnocen jako nejkritičtější, protože by přímo ovlivnil spokojenost zákazníků. Nedostupnost může nastat jednak neúmyslným poškozením některé komponenty systému nebo cíleným útokem.
2. **Ztrátě rešerše před naplněním databáze.** Zde by se jednalo nejspíše o ztrátu části rešerší (rešerše jsou zpracovávány po částech tak, jak přicházejí k editorům). Může k ní ovšem dojít během kterékoliv z 5-8 emailových transakcí, kterými každá rešerše před zařazením do databáze projde. Opět může nastat jak cíleným útokem, tak i nezaviněným systémovým selháním.
3. **Ztrátě nebo poničení rešerše v databázi.** Ztráta celé databáze, jedná-li se o zdrojovou databázi pro webový server, bude mít samozřejmě za následek nedostupnost online verze. Zde máme na mysli především ztrátu nebo poničení obsahu části rešerší.
4. **Nedostupnosti firemních dat.** Zde není kritická nedostupnost firemních dat po dobu několika hodin ani dnů (k čemuž již mimochodem v minulosti došlo), ale spíše nedostupnost „trvalá“, kdy by nebylo možno data obnovit ze záloh a muselo by se přistoupit k pracné rekonstrukci dat z papírových archivů, poznámek a zdrojů všech členů týmu.

Další hrozby jako např. zjištění obsahu (ztráta důvěrnosti) rešerše před jejím oficiálním publikováním nebo monitorování komunikace mezi členy týmu nemají v běžných případech zásadní dopad na průběh projektu. Ale i tak jsou mezi členy týmu dnes k dispozici prostředky, kterými lze v případě potřeby některé tyto hrozby eliminovat.

Zálohování dat – jak vnitrofiremních, tak i databáze rešerší a souborů s rozpracovanými rešeršemi – je podle výše uvedeného seznamu nejvyšší prioritou pro zajištění ochrany dat. Dalším významným prostředkem ochrany dat je zajištění integrity dat – k tomuto účelu jsou dnes již běžně dostupné stovky aplikací. Toto jsou dvě zásadní položky pro technické zajištění bezpečnosti. Dalším faktorem, který do velké míry ovlivní úroveň bezpečnosti zpracování dat, je ale i dobrá organizace práce. Tato na první pohled „trivialita“ je velmi důležitým faktorem – šéfredaktor bez dobré organizace práce může lehce přicházet každý měsíc o několik desítek rešerší, pokud nemá kontrolu nad tím, kdo a jaké

rešerše má dodat. Při našem projektu by právě takovéto ztráty dat byly jistou cestou k pozvolnému krachu projektu. K těmto ztrátám ale může docházet nejen při emailových transakcích, ale i třeba nepozorností nebo působením Trojského koně v lokální síti „kamenné redakce“.

Když se nad seznamem možných bezpečnostních problémů zamyslíme z pozice toho, kdo má rozhodnout o tom, zda použít nebo nepoužít teleworking řešení, tak zjistíme zásadní poznatek – pro tento projekt nemá s ohledem na bezpečnost téměř žádný význam, jestli je prováděn výše popsaným teleworking přístupem nebo by byl případně prováděn v kancelářích jedné budovy.

Proč tomu tak je? To ještě nemáme do detailů ověřeno, za podstatné ale považujeme faktory:

1. Firma a její první projekt jsou od počátku budovány na principech teleworking řešení.
2. Jedná se o relativně malý projekt s jasným cílem, produkty a možnostmi řešení.
3. Většina členů firmy jsou profesionálové v oboru bezpečnosti a umí rozlišit která data, proti čemu a jak chránit (neboli hlavně provést primitivní klasifikaci dat).
4. Nepracuje se většinou vyloženě „na cestách“, kde přicházejí v úvahu mnohé další bezpečnostní problémy.

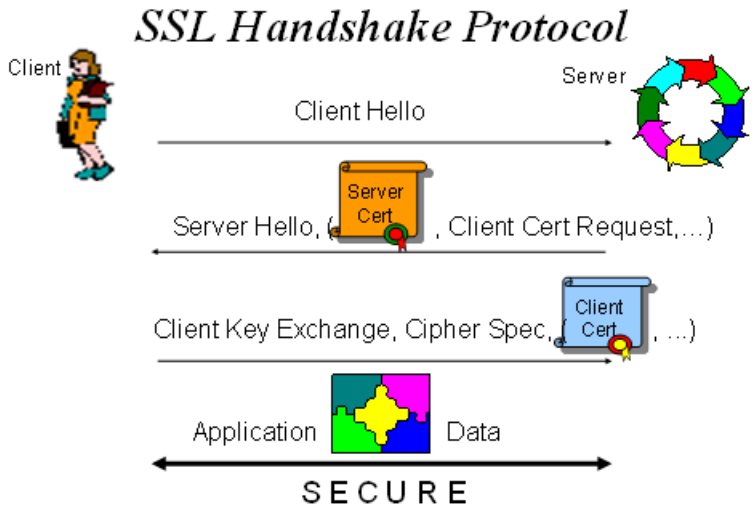
5.2 Použití certifikátů – bezpečnost internetové komunikace

Asi nejznámější internetovou aplikací certifikátů je jejich využití v bezpečné internetové komunikaci zajištěné prostřednictvím protokolové sady SSL/TLS (Secure Socket Layer/Transport Layer Security). Toto řešení nám pro téměř všechny aplikační protokoly (HTTP, telnet, FTP atd.) může poskytnout:

- **Služby autentizace** - server se vždy musí prokázat předložením certifikátu, který klient může a nemusí akceptovat; autentizace klienta není povinná a záleží na serveru, zda ji vyžaduje.
- **Zajištění důvěrnosti obsahu komunikace** - šifrováním dat přenášených kanálem, kdy je po autentizaci ustaven šifrovací klíč pro symetrické šifrování (k dispozici jsou algoritmy RC4 se 40b a 128b klíči, RC2 se 128b klíčem, IDEA se 128b klíčem, DES s 56b klíčem a trojitý-DES se 168b klíčem – ten ale odpovídá jen 112b „úrovni bezpečnosti").
- **Podporu integrity** - data jsou vždy doprovázena autentizačním kódem zprávy (MAC – Message Authentication Code), kterým je 128b výstup hašovací funkce MD5.

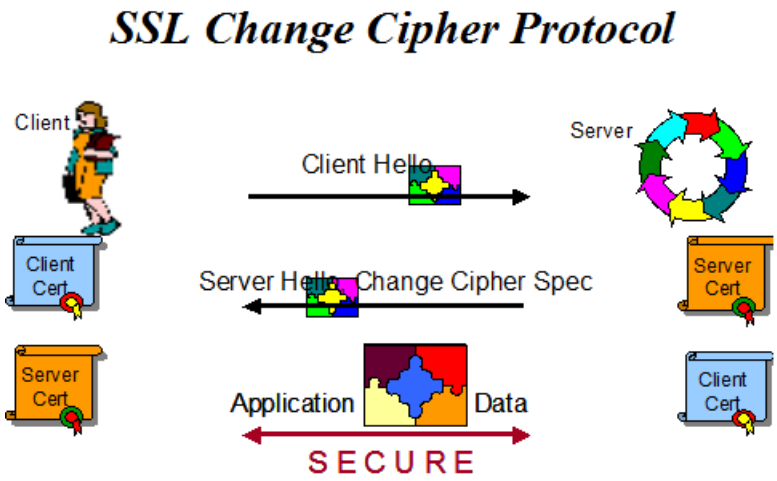
SSL je bezpečnostní protokol, či spíše soustava protokolů, které navrhla (bývalá) firma Netscape pro zajištění bezpečné komunikace v Internetu. TLS je nástupce protokolu SSL vyvíjen v rámci internetových standardů komunitou IETF (Internet Engineering Task Force). Spojení zabezpečené prostřednictvím protokolové sady SSL/TLS je možné provozovat nad libovolnou spolehlivou spojovanou službou (např. TCP). Na začátku komunikace klienta (např. WWW prohlížeče) a serveru (např. WWW serveru) je potřeba

dohodnout kryptografické a další parametry pro následující komunikaci, verzi protokolu, způsob dohody a předání šifrovacích (symetrických) klíčů pomocí šifrovacího algoritmu s veřejným klíčem. Tato fáze se nazývá *SSL (resp. TLS) Handshake Protocol* (viz Obrázek 7).



Obrázek 7: Ustavení zabezpečeného spojení.

Poté již probíhá mezi oběma stranami bezpečná komunikace. Protokol dále umožňuje změnu způsobu šifrování a dalších parametrů komunikace kdykoliv v jejím průběhu pomocí fáze *SSL (resp. TLS) Change Cipher Protocol* (viz Obrázek 8).

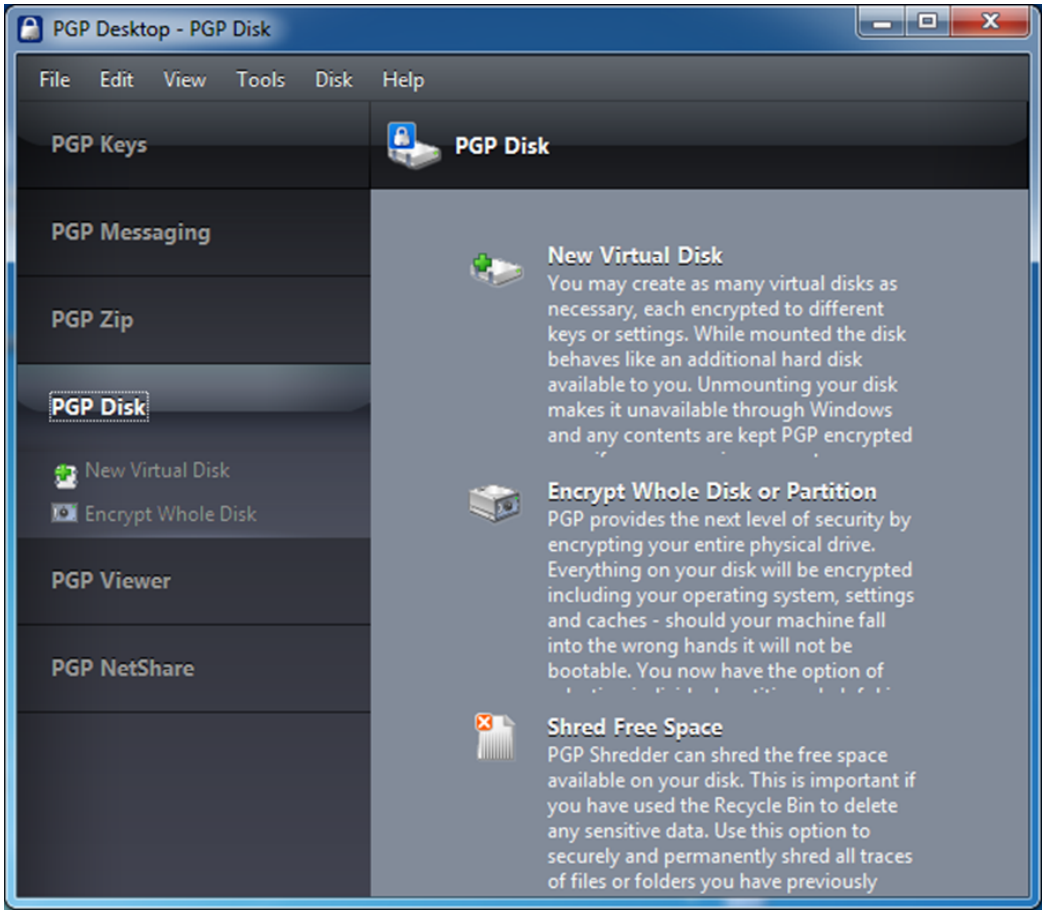


Obrázek 8: Změna parametrů ustaveného zabezpečeného spojení.

Další informace k používání SSL (resp. TLS) protokolu a certifikátů lze dnes získat na mnoha místech, např. u bank, které jej využívají k zabezpečení komunikace s klientem při tzv. internetovém bankovnictví.

5.3 PGP

Asi jen stěží najdete někoho, kdo se ochomýtá okolo oboru počítačové bezpečnosti a nikdy neslyšel o PGP (*Pretty Good Privacy* – Zatraceně dobré soukromí). PGP se stalo bezesporu fenoménem pro mnohé uživatele služeb Internetu, především pak e-mailu. Co všechno PGP umožňuje? Nejnovější verze umožňují spoustu vylepšení a dodatků jako např. certifikační server (umožňující aplikaci hierarchického modelu certifikace/důvěry), spolehlivé mazání souborů, šifrování dat na pevném disku, aplikace pro správu bezpečnostní politiky pro SMTP, má přibalen i personální firewall atd. Důležitá informace ovšem je, že 30 denní zkušební verze PGP je k dispozici zdarma v rámci produktu PGP Desktop (viz Obrázek 9) společnosti Symantec. Po uplynutí zkušební doby je však možné produkt nadále bezplatně využívat, avšak pouze s omezenou funkčností. Produkt PGP Desktop nabízí v omezeném režimu funkci šifrování a podepisování souborů. I v omezeném režimu je však velmi užitečným pomocníkem především díky jednoduchému vytváření a distribuci digitálních certifikátů a díky možnosti šifrovat pomocí asymetrické kryptografie. To lze v praxi využít zejména při zasílání důvěrných dat komunikujícím stranám. Požadovaná data jednoduše zašifrujeme pomocí veřejného klíče požadované strany obsaženého v importovaném certifikátu a odešleme.



Obrázek 9: Ukázkové okno produktu PGP Desktop.

V kostce - PGP umožňuje jednoduché šifrování souborů symetrickou šifrou vámi zvoleným klíčem, digitální podpis souborů (vytvoří se haš souboru a ten se podepíše va-

ším soukromým klíčem) a zašifrování souborů „asymetrickou šifrou“ (uvozovky uvedeny proto, že ve skutečnosti se používá bloková symetrická šifra s náhodně vygenerovaným klíčem, který je po zašifrování vlastního souboru teprve zašifrován zvoleným veřejným klíčem). V zájmu rychlosti přenosu je při šifrování využita komprese a pro aplikace jako je třeba e-mail se využívá kódování dat přes Radix-64. V podstatě tedy vše co potřebujete pro bezpečnou komunikaci e-mailem, distribuci zašifrovaných souborů přes FTP a WWW či digitální podpis jakýchkoliv dat.

To je tedy ono pověstné PGP? Ano a ne - výše uvedený výčet funkcí není vyčerpávající a je také třeba zvážit fakt, že dnes se nejedná jen o samotné PGP, ale o tisíce programů umožňujících např. šifrované telefonování po Internetu, propojení PGP a programů pro e-mail atd. Více o funkcích PGP a jeho nástaveb se můžete dočíst např. na www.pgp.cz, www.pgp.net nebo www.pgpi.com, podívejme se nyní ve zkratce na zásadní věci, o kterých je dobré při používání PGP něco vědět.

5.3.1 Klíče

Prvním zásadním krokem, na který při instalaci PGP narazíte, je vygenerování páru klíčů. Stejné klíče lze samozřejmě používat na různých platformách - klíč vytvořený na laptopu Mac nebo Wintel lze bez problémů používat pod Unixem.

Nejprve si řádně zvažte, kolik párů klíčů budete chtít používat. Tedy hlavně se jedná o ochranu soukromých klíčů těchto párů. Můžete stejný klíč používat na všech strojích a systémech, které používáte. Můžete také zvolit různé klíče pro různé úrovně bezpečnosti (jiné pro vaše osobní stroje pod vaší výhradní kontrolou a jiné pro firemní počítače, kde používáte internetové spojení).

Podle způsobu očekávaného použití zvolených klíčů zvolte vhodnou délku klíčů a také jejich popisné údaje. Stávající hranice bezpečnosti RSA klíčů je něco pod 800 bitů, takže doporučuji pro klíče, které budete běžně používat v blízké budoucnosti, volit v rozmezí standardních 1024-2048 bitů. Větší délka má smysl v případech, kdy váš klíč má být vazbou pro budoucí aplikace nebo klíče a také kdy rychlost kryptooperací nehraje velkou roli (pamatujte - čím delší klíč, tím pomalejší operace s ním). Pro popisné údaje je samozřejmě vhodné jméno a dále je silně doporučován e-mail, lze ale volit jakékoliv jiné údaje (poštovní adresa ap.). Pokud budete používat stejný klíč pro e-mailovou komunikaci prostřednictvím více adres (ať již skutečné e-mailové schránky nebo jen přesměrování pošty), uveďte všechny adresy v dodatečných popisných údajích a pro dokonalé zajištění vazby těchto adres tyto vždy podepište.

Rozšíření vašich veřejných klíčů je dalším stěžejním krokem.

- Nejspolehlivější mechanismus samozřejmě je, když klíč svým partnerům předáte osobně (např. na paměťové kartě) nebo osobně předáte alespoň jeho vytištěnou ASCII podobu nebo otisk (haš) a poté zašlete klíč i elektronickou cestou - partner pak může podle vytištěné informace zkontrolovat, zda dostal skutečně ten pravý klíč. Pro tyto účely je např. vhodné uvádět otisk klíče na vizitkách atd.

- O něco méně spolehlivou metodou je klíč poslat elektronickou cestou a haš sdělit telefonicky, pokud druhá strana zná váš hlas, případně je schopna vás „prověřit“ otázkami, na které můžete okamžitě správně odpovědět jen vy. Méně důvěryhodnou alternativou této metody je čistě elektronická cesta, kdy tyto otázky přijdou

zašifrovány vámi dodaným veřejným klíčem, vy je musíte dešifrovat (čili být schopni použít soukromý klíč) a zodpovědět během krátkého časového intervalu (s mírnou nadsázkou pak lze předpokládat, že jste na ně skutečně odpověděli vy).

- Klíče může podepsat a tak „akreditovat“ někdo z vašich přátel, kteří mají svoje PGP klíče již dostatečně rozšířeny. Podle toho jakou důvěru ve vás a vaše klíče mají a jakou důvěru ve vaše přátele mají jejich partneři, tak dalece se bude důvěřovat vašim klíčům. PGP je z tohoto hlediska velmi propracovaný mechanismus - tranzitivní důvěru lze pomocí PGP spravovat velmi šikovně.

- Klíče lze pak také rozšířit na servery PGP klíčů (viz např. www.pgp.cz), kam ale může poslat falešné klíče každý (zkuste si najít např. klíče z whitehouse.gov), zpřístupnit přes vaše WWW stránky atd. Ve všech těchto případech je ale vhodné mít klíče podepsány jinými akreditory, příp. rozšířeny spolehlivými způsoby - tyto metody jsou vhodné pro širokou veřejnost, vaši důvěrní přátelé by měli získat vaše klíče spolehlivější cestou.

Analogicky pak získejte veřejné klíče všech stran, se kterými chcete do budoucna bezpečně komunikovat. Případně si také zjistěte, zda existuje nadstavba nad PGP pro e-mailové klienty, se kterými pracujete.

Velmi důležitým rysem PGP je to, že většina verzí je dostupná nejen jako zkompilované balíky, ale také jako zdrojový program. Je tím umožněna nezávislá kontrola, které se mnozí kutilové a hackeři (v kladném slova smyslu) rádi oddávají a případné nedostatky pak mohou prezentovat na veřejnosti. Princip je zde v podstatě stejný jako u kryptografických algoritmů - rozsáhlá a neomezená kontrola odbornou veřejností odhalí více chyb než jednorázové (ať už jakkoliv dlouhé) otestování sebelepšími odborníky.

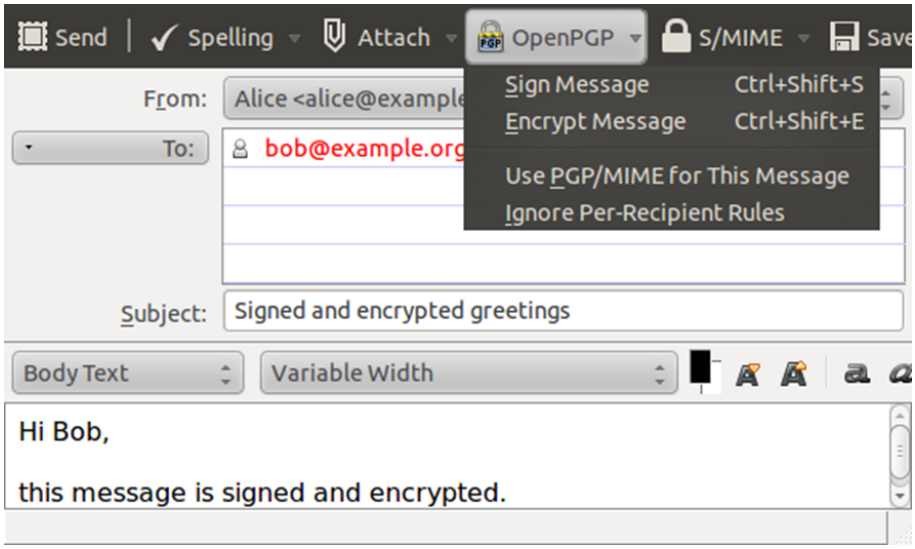
PGP je nástroj, který umožnil internetové komunitě bezpečnou výměnu informací. Je ideálním zhmotněním myšlenky části tohoto kurzu - bezpečnostní nástroj, který nám umožňuje zatraceně dobrou ochranu informačního soukromí.

5.3.2 GnuPG – bezplatná alternativa PGP

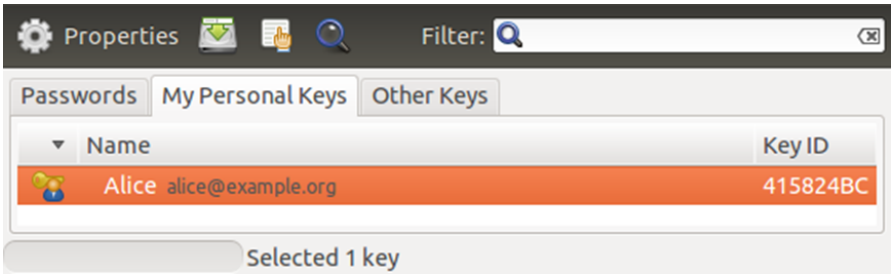
Jak již bylo řečeno, původní návrh PGP je v současné době k dispozici jako proprietární software „PGP Desktop” společnosti Symantec, která nabízí tento produkt bezplatně pouze v omezené míře, Alternativním, zcela bezplatným, řešením postaveným na standardu OpenPGP (RFC 4480)[3] je Gnu Privacy Guard (zkráceně GnuPG nebo GPG). GnuPG je nástrojem příkazové řádky, který neposkytuje grafické uživatelské prostředí. Existuje však řada grafických nadstaveb zpřístupňujících funkce GnuPG prostřednictvím uživatelsky přívětivého grafického rozhraní. Příkladem takového nástroje je např. Enigmail, což je plugin integrující nástroje balíku GnuPG přímo do rozhraní e-mailového klienta Mozilla Thunderbird. Po instalaci nástroje Enigmail je možné snadno podepisovat a šifrovat odesílané zprávy přímo z rozhraní Thunderbirdu (viz Obrázek 10).

Pro linuxové grafické prostředí Gnome je k dispozici nástroj Seahorse, který umožňuje snadné vytváření digitálních certifikátů a usnadňuje práci s vlastními certifikáty či importovanými certifikáty třetích stran (viz Obrázek 11).

[3]OpenPGP je otevřený standard umožňující budovat nástroje využívající principy PGP bez nutnosti jejich licencování.



Obrázek 10: Ukázkové okno nástroje Enigmail.



Obrázek 11: Ukázkové okno nástroje Seahorse.

6 Systémy pro poskytování anonymity

Pro zabezpečení komunikace na Internetu se v současné době aktivně využívá šifrovacích mechanizmů. Tyto technologie ale zabezpečí pouze vlastní obsah přenášených dat, takže útočník není schopen získat otevřenou podobu informací, které jsou předmětem komunikace. Je ale schopen zjistit od koho ta či ona zpráva pochází a komu byla adresována. Znalost takové informace může být v různých prostředích značně nežádoucí, protože může útočníkovi poskytnou jistou znalost o pravděpodobném obsahu přenášených dat. V důsledcích potom může různým způsobem poškodit komunikující strany.

Naproti tomu lze vyžadovat existenci takového prostředí, kdy nemusí být zabezpečen vlastní obsah dat, ale útočník nemá možnost se dozvědět, kdo tato data odeslal a kdo byl jejich příjemcem. Pokud např. zachytí zprávu „Sejdeme se v 10 hodin na náměstí“, ale nebude mít informaci o tom, kdo komu tuto zprávu poslal, tak je pro něj prakticky bezcenná. Ideální je tyto dva přístupy skloubit dohromady a vytvořit takové prostředí, kde je zajištěna jak anonymita komunikujících partnerů, tak i důvěrnost a integrita přenášených dat.

Terminologie, která se v této oblasti používá, je popsána v první kapitole (viz Kapitola1), ale v souvislosti se systémy pro poskytování anonymity se můžeme setkat s alternativní definicí anonymity. (Pozn.: další části textu vycházejí z článku *Anonymita a ochrana*

informačního soukromí, Kumpošt, Matyáš, *VII. ročník konference Internet a konkurenceschopnost podniku*. Univerzita Tomáše Bati ve Zlíně, 2005, 5 s. ISBN 80-7318-269-6.)

6.1 Anonymita

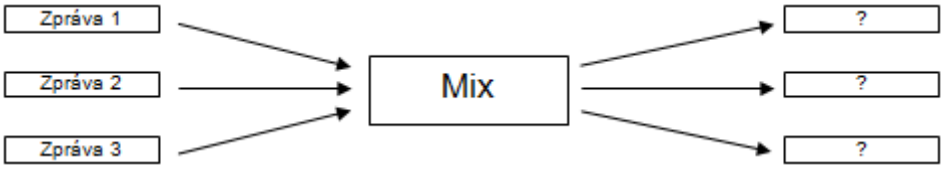
Anonymita je stav, kdy není možné identifikovat subjekt v rámci množiny všech uvažovaných subjektů (anonymitní množina). Jedná se o úplné odstranění všech identifikačních informací daného subjektu. Dále lze uvažovat anonymitu odesílatele (tj. množinu všech možných odesílatelů dané zprávy) nebo anonymitu příjemce (tj. množiny všech možných příjemců dané zprávy).

6.2 Mixy

Autorem prvotního návrhu mix systému byl Chaum v roce 1981. Navrhovaný systém měl sloužit k anonymnímu posílání elektronických zpráv.

Celý proces mixování v tomto prvotním návrhu je poměrně jednoduchý. Mix přijme několik zpráv od uživatelů, kteří chtějí anonymně poslat email. Následně z těchto zpráv odstraní veškeré informace, které by mohly vést k identifikaci uživatelů (a další informace, především časové, využitelné k různým útokům) a takto zpracované zprávy odešle. Základním problémem při zajištění anonymity (a částečně i ostatních aspektů ochrany soukromí) je totiž možnost odlišení jedné pozorované entity (např. emailu) od ostatních – tento problém spadá do otázek tzv. analýzy provozu (traffic analysis). Analýza provozu je útok, kdy se útočník snaží získat nějaké identifikační informace pouhým sledováním provozu na síti.

Příchozí zprávy do mixu jsou zašifrovány veřejným klíčem mixu, aby byl utajen i vlastní obsah zprávy. Mix, jakožto vlastník odpovídajícího privátního klíče, je schopen takto zašifrované zprávy dešifrovat a poté provést příslušné operace vedoucí k odstranění veškerých identifikačních informací o odesílateli zprávy. Takto upravené zprávy jsou dále zpracovány (typicky odeslány na další mix nebo přímo příjemci) v okamžiku, kdy je splněna určitá „prahová“ podmínka. Podmínka, která ovlivní odeslání zpráv z mixu má značný vliv na celkovou míru anonymity poskytovanou daným systémem a také chrání uživatele před různými typy útoků na mixovací systémy nebo celé mixovací sítě.



Obrázek 12: Schematické znázornění mixovacího uzlu.

Vzhledem k procesu, kterým systém zpracovává data a zajišťuje tak určitou míru anonymity, dochází k velkým prodlevám při zpracování zpráv. Zpracování zprávy přes síť mixů může trvat řádově až hodiny. Tato latence je akceptovatelná v případě zasílání elektronické pošty a obecně zpráv. V případě systémů pracujících v reálném čase (ssh připojení, prohlížení www stránek, ftp apod.) je tento přístup nepoužitelný, protože je vyžadována okamžitá reakce na požadavky uživatelů. V těchto situacích se používá systémů založených na Onion routingu.

6.3 Onion routing (cibulové směrování)

Návrh systému Onion Routing byl poprvé představen v roce 1996 jako metoda pro skrytí směrovacích informací v aplikacích, které vyžadují síťové propojení bez přílišných prodlev. Přístup použitý v tomto systému spočívá ve vytvoření speciální šifrované vrstvené datové struktuře (odtud název cibule), která je v síti zpracována při průchodu přes zvolené směrovače. Každá „slupka“ takové struktury je zašifrována klíčem daného směrovače, a tedy pouze tento uzel je schopen provést úspěšné „sloupnutí“ vnější vrstvy. Dešifrováním získá informaci o adrese dalšího uzlu v síti, na který mají být data odeslána. Aplikováním stejného postupu dojde na konci datové cesty k tomu, že poslední uzel získá po dešifrování již ta data, která jsou určena pro příjemce zprávy.

Vlastnímu přenosu dat předchází tzv. ustavení komunikační cesty – inicializační fáze, kdy dojde k vytvoření sdílených symetrických klíčů mezi odesílatelem dat a každým uzlem po cestě k příjemci. Odesílatel potom použije tyto symetrické klíče k vytvoření jednotlivých zašifrovaných vrstev. Každý uzel v síti zná pouze množinu svých předchůdců a následníků a dále do sítě „nevidí“. Výhoda je v tom, že pokud útočník úspěšně zaútočí na konkrétní uzel, získá pouze informaci o dalším skoku, ale následně již nebude schopen zprávu dále sledovat. Pro úspěšný útok je nutné mít pod kontrolou všechny uzly v síti a schopnost poslouchat datový provoz na všech koncích sítě. Nicméně návrh tohoto systému si neklade za cíl být odolný proti takto silnému typu útočníka.

Aby při průchodu sítí nedocházelo ke „zmenšování“ datové struktury vlivem dešifrování vnějších vrstev, přidává každý uzel určité množství náhodných dat tak, aby byla celková velikost cibule vždy konstantní. Tento přístup snižuje riziko útoku na systém Onion Routing pouhým odposlechem provozu.

Zástupcem tohoto typu systému pro poskytování anonymity je systém TOR – The Onion Routing (http://www.torproject.org). Jedná se o druhou generaci Onion Routing systému, která se od původního návrhu liší řadou nově přidaných funkcí vlastností a vylepšení.

Mezi hlavní novinky systému TOR můžeme zařadit např. zajištění tzv. dopředné bezpečnosti (*forward secrecy*), kdy není možné zpětně dešifrovat odposlechnutou komunikaci. Novinkou je též testování integrity přenášených dat a spolehlivější budování komunikačního okruhu (*telescopic circuit building*). Je zde řešena i anonymita serverů, ke kterým se uživatelé připojují. Tato technologie se jmenuje *Rendezvous point* a *Hidden services* (místa setkání a skryté služby). Server má možnost své služby poskytovat prostřednictvím uzlů sítě TOR, takže klienti nevidí skutečnou adresu. Velikou výhodou tohoto přístupu je kontrola připojených klientů na straně serveru a tím pádem i účinná ochrana proti případným útokům typu DoS.

6.4 Anonymní proxy

Další možností pro zajištění „jisté“ míry anonymní komunikace je použití nějaké anonymní proxy. Seznam takových serverů lze snadno vyhledat pomocí Google. Pokud pak v prohlížeči nastavíte tuto proxy, tak bude vaše skutečná IP adresa skryta za adresou proxy serveru. Službám na internetu se bude zobrazovat IP adresa proxy serveru, která se zpravidla ještě s určitou frekvencí mění. Tento způsob je poměrně snadný, nicméně z pohledu uživatele nemusí být příliš bezpečný. Tím, že veškerý provoz směrujeme přes něčí server, tak dáváme svá data k dispozici neznámým lidem. Jakékoliv přihlašovací

údaje odeslané z formuláře budou dostupné provozovateli proxy serveru. Je tedy vhodné použít takovou proxy, která podporuje i SSL provoz a poté používat výhradně šifrovaný protokol https.

6.5 Tunelování provozu

Maskování identity uživatele lze také dosáhnout, pokud máme přístup ke vzdálenému serveru umožňujícímu tunelování provozu. Typicky se jedná o zařízení, na němž běží např. VPN nebo SSH server s povoleným „*port forwarding*“ apod. Pokud máme vzdálený přístup k takovému zařízení, je možné se k němu připojit a komunikovat s „ostatním světem“ tak, že se náš provoz navenek jeví jako pocházející z daného vzdáleného zařízení. Výhodou tohoto řešení je, že s jeho pomocí je možné poměrně snadno maskovat svou pravou identitu vůči koncové službě (např. místu, odkud je spojení realizováno), V praxi však použití samotného tunelování provozu může vést k většímu riziku odhalení skutečné identity uživatele, než např. použití anonymní proxy. To z toho důvodu, že tunelování vytváří permanentní spojení mezi zařízením uživatele a zařízením, z něhož se uživatel jeví, že komunikuje (tzv. výstupní bod neboli „*exit node*“). Dalším důvodem je, že uživatel obvykle musí být vůči vzdálenému systému autentizován, čili vzdálený systém má určitou explicitní znalost identity uživatele. Maskování identity pomocí tunelování provozu nelze považovat za anonymizaci v pravém slova smyslu, ale jedná se o maskování identity ve smyslu pseudonymity. Je to z toho důvodu, že mezi skutečným zařízením uživatele a zařízením sloužícím pro maskování identity uživatele existuje implicitně přímá vazba, kterou je možné snadno detekovat.