7. Aplikovaná kryptografie

Osnova

1. Úvod
2. Úvod do kryptografie
3. Konstrukce digitálního podpisu, zákon o elektronickém podpisu, správa veřejných klíčů, certifikační autority a infrastruktury veřejných klíčů
4. Autentizace uživatelů v počítačových systémech - tajné informace, tokeny, biometriky.
5. Kerberos, bezpečnost v prostředí Internetu.
6. Útoky [*chybí + není v okruhu*]

Výklad

1. Úvod

- Zavádění prostředků informačních technologií (IT) do existujících či nově budovaných systémů v širokém spektru oblastí lidské společnosti nám přináší mnoho výhod (sociálních sítí, využívat výhod videotelefonie, připojení ke globálním informačním systémů atd.). 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.
- **Safety, bezpečí** – stav bytí, ve kterém platí, že za definovaných podmínek nedojde ke stavu ohrožení lidského života, zdraví, hodnot a prostředí (někdo či něco nezpůsobí škodu (mnohdy se chápe se jako chránění proti náhodným událostem)).
- **Security, bezpečnost** – je obecně vlastnost prvku (např. IS), který je na určité úrovni chráněn proti ztrátám nebo také stav ochrany (na určité úrovni) proti ztrátám tedy proti úmyslným škodám.V oblasti IT se bezpečnost soustředí především na ochranu činností zpracování, úschovy, distribuce a prezentace informací: Information security (informační bezpečnost) - ochrana proti úmyslným škodám, nežádoucím akcím na informačních aktivech.
  Pro zamezení případné víceznačné interpretace budeme v následujícím textu rozumět bezpečnost ve významu anglického „Security“, pokud nebude uvedeno jinak.
- **Privacy, soukromí** - 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. 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.
  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 nepozoro-vatelnost. 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.
  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“:
  - **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).

- **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).
- **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 poskyto-vané 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.
- **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 ne-detekovatelnosti použití daného zdroje nebo služby vůči subjektům, které daný zdroj ne-využívají. Ochraňovanými hodnotami nejsou informace o uživatelích, ale o použití zdrojů nebo služeb. Příkladem aplikace může být ochrana proti tzv. analýze provozu (angl. traf-fic analysis), tj. např. proti pozorování toho, která strana rozesílá nejvíce zpráv v určité době nebo při výskytu určité události.

- **Dosažení informační bezpečnosti** je proces **dosažení a udržení dostupnosti, důvěrnosti, integrity, autenticity, zodpovědnosti, nepopiratelnosti a spolehlivosti informací a IT služeb** na přiměřené úrovni.

- **Rozsáhlé databáze osobních dat** - 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)

  Příklady databází:
  - Satistické 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.
    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; 2. Náhodný výběr; 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.

- **Tři dimenze ochrany dat** - i samotné utajení dat je velmi složitým problémem
    - 1. zda tato data mají být utajována
    - 2. zda samotná existence těchto dat je utajována
    - 2. zda samotná existence těchto dat je utajována

  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.
- **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 (ataky tyto pracovníky předem i průběžně prověřovat).
    - Přísně tajná data
    - Tajná data
    - Důvěrná data
    - Citlivá dat
- **Bezpečnost informací – Základní cíle**
    - **D**ostupnost
    - **D**ůvěrnost
    - **C**elistvost
    - **Z**odpovědnost

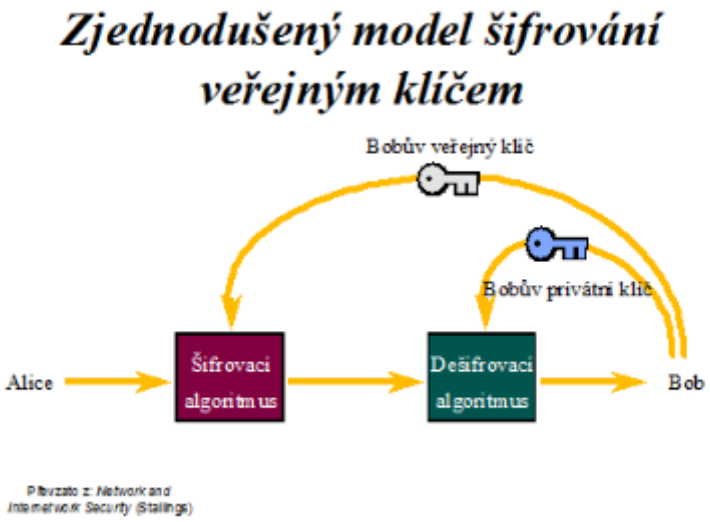
2. Úvod do kryptografie

Kryptografie slouží k zajištění podpory mnohých aspektů bezpečnosti. Nejčastěji jsou to **důvěrnost** a **integrita**, ale nelze opomenout ani **dostupnost** a **zodpovědnost**.

- **Zajištění 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.
  Známým příkladem šifrování je jednoduchá šifra Julia Cesara.
  Šifrování a **dešifrování**. U šifrování je podstatné, aby zašifrovaný text bylo možné pomocí šifrovacího klíče opět převést zpět do čitelné podoby. Tomuto procesu říkáme dešifrování.
- **Zajištění integrity** -
- **Zajištění dostupnosti** -
- **Zajištění zodpovědnosti** -

- **Kryptografií** - pak označujeme vědu (nebo snad umění?) zabývající se tvorbou šifro- vacích a dešifrovacích algoritmů. Takže pak mluvíme o kryptografických algoritmech, klíčích, zařízeních atd.
- **Kryptoanalýzou** - se rozumí obor, který se snaží šifry překonávat a hledat jejich slabiny.
- **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: 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.
  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: 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.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.



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. 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. všem 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

3+4. Autentizace uživatelů a dat, digitální podpis

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:

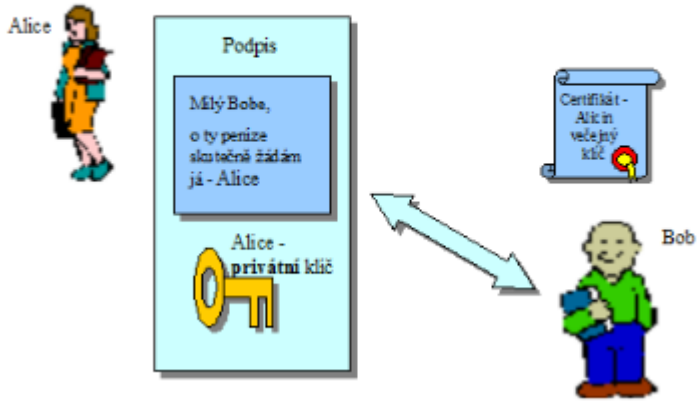
- Na základě **výlučné znalosti** (co kdo zná) – tyto metody jsou poměrně velmi dobře známy, jedná se o použití tajných hesel, PINů, algoritmů atd.
- Podle **vlastnictví specifických předmětů** (tokeny) (co kdo má) – tyto metody jsou také široce rozšířeny, jsou to např. magnetické a čipové karty, ale i běžné klíče k zámkům a speciální zařízení jako jsou tzv. autentizační kalkulátory.
- **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.
- **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.

- **Biometrické systémy** - sou 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.

- **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)

Co je digitální podpis?



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 pro vytváření podpisu) a podepisovaná data jsou vstupními daty pro podpisový algoritmus, jehož výstupem je digitální podpis daných dat, tento podpis pak lze připojit ke zprávě. Správný digitální podpis může vytvořit jen ten, kdo má k dispozici soukromý klíč. Pro ověření podpisu je nutné mít veřejný klíč podepsaného subjektu. Digitální podpis nedává sám o sobě žádnou záruku o době jeho vytvoření.
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. hash (kontrolní součet datového souboru), který je vlastně přesnou reprezentací (charakteristikou) dat. Tento hash je vlastně výstupem jednocestné kryptografické hašovací funkce aplikované na data.
- Poté se tento hash podepíše daným asymetrickým šifrovacím algoritmem (RSA) 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 hashe) 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.
Najznámejší podpisový algoritmus RSA se používá taky na asymetrické šifrování. V současné době sa používá modulo o délkách 1024 až 4096 bitů.
Digitální podpis se používá k zajištění:

- autenticity dokumentu
- integrity dokumentu
- nepopiratelnosti zodpovědnosti autora podpisu

Zaručený elektronický podpis

- Je jednoznačně spojen s podepisující osobou (jen fyzická osoba!)
- Umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě
- Byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou
- Je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat

Elektronický podpis vs. značka

- Elektronický podpis - podepisující osoba je fyzická osoba, která je držitelem prostředku pro vytváření elektronických podpisů a jedná jménem svým nebo jménem jiné fyzické či právnické osoby; pro ověření podpisu je vydáván certifikát (veřejného klíče).
- Elektronická značka - označující osobou fyzická osoba, právnická osoba nebo organizační složka státu, která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou; pro ověření podpisu je vydáván systémový certifikát (veřejného klíče).
- Technologicky jde o totéž
- Jen úroveň ochrany soukromého klíče je jiná.

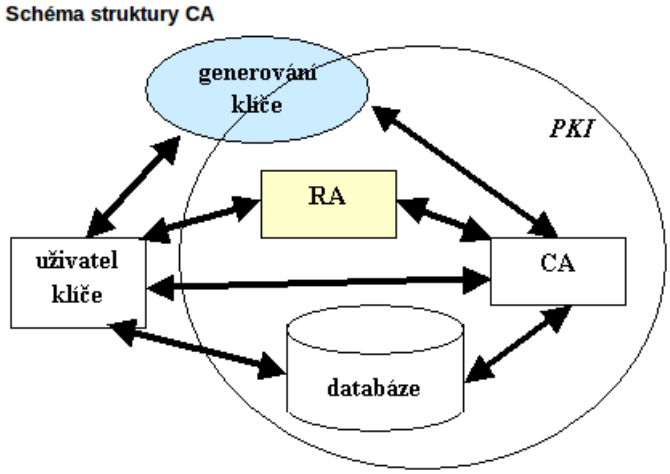
- **Zákon o elektronickém podpisu**

  Zákon o elektronickém podpisu č. 227/2000 Sb. (změněn zákony č. 226/2002, 517/2002 a 440/2004 Sb.).
  „Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě“

- **Elektronickým podpisem tak může být i pouhé jméno napsané na klávesnici.**

- **Správa veřejných klíčů** - veřejné klíče jsou ve správě podpůrné struktury **PKI** (Public Key Infrastructure). PKI je systém technických prostředků, služeb a organizačních opatření určených ke správě veřejných klíčů.
  PKI je založena na prvcích:
  - bezpečnostní politika (BP) – definuje pravidla pro provoz celé infrastruktury PKI
  - procedury – definice postupů pro generování, distribuci a používání klíčů
  - produkty – HW/SW komponenty pro generování, skladování a používání klíčů
  - autority – prosazují plnění BP s pomocí procedur a produktů

  Komponenty PKI:
  - **certifikační autorita** (CA) – poskytovatel certifikační služby, vydavatel certifikátu
  - **registrační autorita** (RA) – registruje žadatele o vydání certifikátu a prověřuje jejich identitu
  - **adresářová služba**– prostředek pro uchovávánía distribuci platných klíčů a seznam zneplatněných certifikátů (CRL)



- **Certifikační autority**

  Certifikát

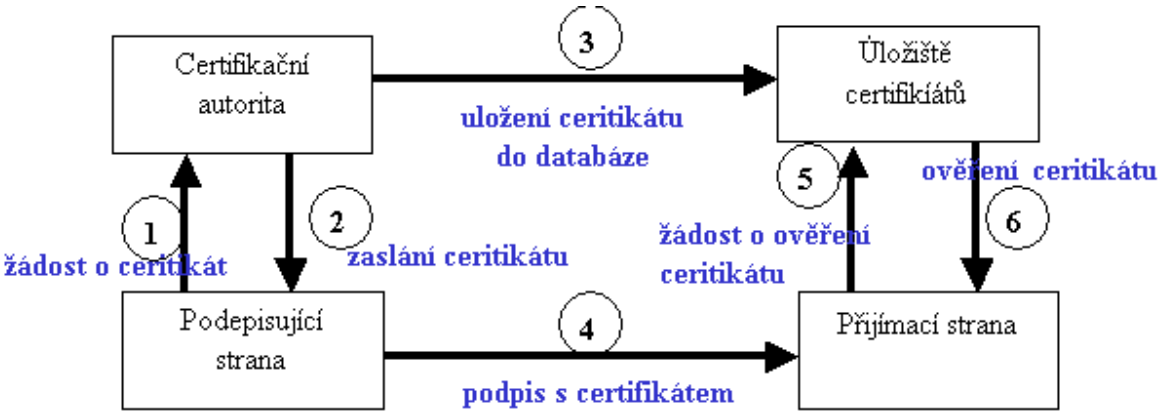
  - Certifikát–veřejný klíč uživatele podepsaný soukromým klíčem důvěryhodné třetí strany
  - Certifikát spojuje jméno držitele páru soukromého a veřejného klíče s tímto veřejným klíčem a potvrzuje tak identitu osoby
  - Poskytuje záruku že identita spojená s vlastníkem daného veřejného klíče není podvržená
  - Případně také představuje doklad o tom, že totožnost držitele veřejného klíče byla ověřena

  Certifikační autorita - struktura:

  - CA vydáva certifikáty na základe požiadavku od registračnej autority
  - RA overuje identitu žiadateľa, posiela požiadavku na vystavenie certifikátu
  - Revokačná autorita – umožňuje predčasné zrušenie platnosti certifikátu (e.g. v případě kompromitace privátního klíče)
  - Vrcholy stromů tvoří kořenové certifikační autority (e.g. Symantec, Comodo, z českých PostSignum, První certifikační autorita)
  - Podobu certifikátov špecifikuje štandard X.509

  Certifikační proces probíhá v následujících krocích:

  - 1. Odesílatel podepisovaného dokumentu žádá CA o digitální certifikát pro svůj veřejný klíč
  - 2. CA ověřuje identitu žadatele (prostřednictvím RA) a certifikát vydává
  - 3. CA ukládá certifikát do veřejně přístupného on-line repozitáře
  - 4. Odesílatel podepisuje dokument svým privátním klíče a odesílá jej s připojeným certifikátem
  - 5. Příjemce ověřuje digitální podpis veřejným klíčem odesílatele a požaduje ověření digitálního certifikátu v repozitáři příslušné CA
  - 6. Repozitář vrací zprávu o stavu odesílatelova certifikátu



- **Infrastruktury veřejných klíčů**
  PKI - popísané v casti Správa veřejných klíčů
  PKI spája verejný kľúč so subjektom prostredníctvom vydania certifikátu certifikačnou autoritou. Jej hlavnou úlohou je digitálne podpísať verejný kľúč patriaci danému človeku – a to pomocou vlastného privátneho kľúča samotnej CA, takže závisí na dôveryhodnosti konkrétnej autority. Tento podpis potvrdzuje - certifikuje vlastníctvo daného verejného kľúča.

Autentizace uživatelů v počítačových systémech (autentizace spočívá v ověření, že autentizovaný je tím, za koho se vydává.)

Tajné informace (co kdo zná)

Hesla, PIN, passphrase, identifikace obrazové informace …

Aby autentizace tajnou informací byla bezpečná je nutné dodržet:

- informace musí být opravdu tajná, tj. nikdo jiný než oprávněný uživatel by ji neměl znát
- autentizační informace by měla být vybrána z velkého prostoru možných hodnot
- pravděpodobnost všech hodnot z prostoru by měla být pokud možno stejná
- pokud dojde ke kompromitaci autentizační informace, musí být možné nastavit novou jinou autentizační informaci

Hesla

- Skupinová (uživatelská role) – málo používané, bezpečnost mizivá
- Unikátní pro danou osobu (heslo = userid)
- Neunikátní (používaná společně s userid)
- Jednorázová (ať už unikátní či nikoliv)

Ukládání hesel

- V otevřeném tvaru
- V nečitelné podobě
    - *šifrovaná* - využíváme v situaci, kdy chceme mít přístup k otevřenému tvaru hesla
    - *hašovaná* - ukládáme pouze výsledek hašovací funkce

„Solení“

- haš není jen funkcí hesla, ale ještě dodatečné náhodné informace (soli)
- v tabulce hesel musíme ukládat i sůl: userid, sůl, f(sůl, heslo)
- delší efektivní heslo
- řešení pro stejná hesla (stejná hesla s různou solí budou mít různé haše)

PIN (Personal Identification Number)

- Levnější klávesnice
- Obtížněji zapamatovatelné než hesla
- Obvykle používány s fyzickým předmětem
- Někdy lze změnit podle přání zákazníka
- Obvykle 4-8 znaků dlouhé
- Procedurální omezení proti útokům hrubou silou
    - Zabavení karty při několika (3) nesprávných PINech
    - Nutnost re-aktivace záložním (delším) PINem po několika nesprávných PINech

Tokeny (co kdo má)

Nejčastější tokeny v IT/IS:

- Karty
    - Čipové (bankomatová, SIM, USB token)
        - Paměťové (chipcard), Paměťové se speciální logikou, Procesorové (smartcard)
        - Kontaktní, Bezkontaktní (Autentizace bývá obvykle založena pouze na ověření sériového čísla karty)
    - S magnetickým proužkem - 3stopý proužek ~ 250 B (spolehlivě), poměrně jednoduše se kopírují.
- Autentizační kalkulátory (s tajnou informací, s hodinami, způsob vstupu/výstupu)

Čipová karta jako aktivní prvek

- Čipové karty mají i nezanedbatelnou výpočetní sílu.
- Na čipové kartě je možné implementovat kryptografické algoritmy i protokoly.
- Je možné na kartě provádět operace s citlivými daty tak, že tato data nemusí opustit čipovou kartu (např. vytváření digitálního podpisu).
- Symetrické šifrovací algoritmy běží v prostředí čipové karty bez problémů (často též speciální HW akcelerátory - např. DES, 3DES, AES).
- Asymetrické kryptografické algoritmy jsou řádově náročnější, proto vyžadují specifické koprocesory.

Bezpečnost čipových karet

- Fyzická bezpečnost (physical security) – překážka umístěná kolem počítačového systému za účelem ztížení neautorizovaného fyzického přístupu k tomuto počítačovému systému.
- Odolnost vůči narušení (tamper resistance) – vlastnost části systému, která je chráněna proti neautorizované modifikaci způsobem zajišťujícím podstatně vyšší úroveň ochrany než ostatní části systému.
- Zjistitelnost narušení: systém, u kterého jakákoliv neautorizovaná modifikace zanechává zjistitelné stopy.
- Detekce narušení: automatické zjištění pokusu o narušení fyzické bezpečnosti.
- Odpověď na narušení: automatická akce provedená chráněnou částí při zjištění pokusu o narušení.

Biometriky (co kdo je)

Biometriky – „automatizované metody identifikace nebo ověření identity na základě měřitelných fyziologických nebo behaviorálních vlastností člověka“.
Biometrická data nejsou nikdy 100% shodná, musíme povolit určitou variabilitu mezi registračním vzorkem a později získanými biometrickými daty

Model biometrické autentizace

- Fáze registrace
    - prvotní získání biometrických dat (kvalita je velmi důležitá)
    - vytvoření registračního vzorku (získání důležitých charakteristik)
    - uložení registračního vzorku (karta, snímač, pracovní stanice, server)
- Fáze identifikace / autentizace
    - získání biometrických dat
    - vytvoření charakteristik (jeden vzorek k dispozici)
    - srovnání charakteristik (míra shody registračního vzorku s aktuálními daty)
    - finální rozhodnutí ano/ne

Chybovost biometrických systémů závisí na řadě faktorů:

- typ snímače, používání různých typů snímačů
- prostředí ((ne)možnost přizpůsobit prostředí, vnitřní, venkovní prostory, zdroje světla…)
- nastavení (počet pokusů, omezení kvality vzorků,…)
- uživatelé

Fyziologické charakteristiky

- Ruka
    - Otisk prstu
    - Otisk dlaně
    - Geometrie (tvaru) ruky
    - Žíly ruky (geometrie)
- Oko
    - Duhovka
    - Sítnice
- Tvář
- Hlas

- DNA
- Lůžka nehtů
- Vůně/pot
- Tvar ucha…

Charakteristiky chování

- Dynamika podpisu
- Hlas (dle podnětu)
- Pohyby tváře
- Dynamika chůze
- Dynamika psaní na klávesnici

5. Kerberos, bezpečnost v prostředí Internetu.

Kerberos
Je síťový autentizační protokol umožňující komukoli komunikujícímu v nezabezpečené síti prokázat bezpečně svoji identitu někomu dalšímu prostřednictvím důvěryhodné třetí strany. Kerberos zabraňuje odposlechnutí nebo zopakování takovéto komunikace a zaručuje integritu dat. Byl vytvořen primárně pro model klient-server a poskytuje vzájemnou autentizaci – klient i server si ověří identitu své protistrany.

Autentizace proběhne ve čtyřech krocích:
Krok 1

- Klient požádá autentizační server (AS) o Ticket Granting Ticket (TGT).
- AS vyhledá klienta ve své databázi, vygeneruje klíč relace (session key) SK1, který bude použit pro komunikaci mezi klientem a Ticket Granting Serverem (TGS). AS zašifruje klíč SK1 za použití tajného klíče (secret key) klienta (uživatelského hesla) a pošle jej klientu.
- AS dále vytvoří TGT zašifrovaný pomocí tajného klíče TGS a také jej pošle klientu.

Krok 2

- Klient dešifruje přijatý SK1 pomocí svého tajného klíče.
- Klient vytvoří authenticator obsahující uživatelské jméno, IP klienta a časové razítko. Pošle authenticator spolu s TGT službě TGS spolu s požadavkem na službu, kterou chce použít.
- TGS dešifruje TGT zaslaný klientem pomocí svého tajného klíče a získá z něj klíč relace SK1. Pomocí SK1 dešifruje authenticator. Ověří informace z authenticatoru.
- TGS vytvoří klíč relace SK2 pro komunikaci mezi klientem a cílovým serverem (službou). Zašifruje SK2 pomocí SK1 a pošle jej klientu. TGS vytvoří tiket pro použití cílové služby obsahující jméno klienta, jeho IP adresu, časové razítko, čas expirace tiketu a SK2. Tiket zašifruje pomocí tajného klíče a jména cílového serveru a pošle jej klientu.

Krok 3

- Klient dešifruje SK2 pomocí SK1.
- Klient vytvoří nový authenticator, zašifruje jej pomocí SK2 a spolu s tiketem jej zašle cílovému serveru.
- Cílový server dešifruje tiket pomocí svého tajného klíče a ověří jej.
- U služeb, kde je vyžadováno, aby se server prokázal klientu, zašle cílový server klientu časové razítko zvětšené o 1 zašifrované pomocí SK2.

Krok 4

- Nyní cílový server i klient mají jistotu o totožnosti komunikačního partnera.
- Vzájemný síťový provoz šifrují pomocí SK2.

Závěr

http://statnice.dqd.cz/mgr-szz:in-ins:7-ins

Slidy k PV080 a PV157