PV080 - ochrana dát a informačného súkromia (by 395868)

Lekcia 1 – databázy dát

Agregácia dát = zoskupovanie osobných dát do rozsiahlych databáz – pre ľudí z marketingu, reklamy, poisťovníctva. *Inferencia* = odvodenie informácií s vyššou citlivosťou z informácií s nižšou citlivosťou. Získavame tak nepriamy prístup k informáciám bez prístupu k samotným dátam.

Štatistické databázy: obsahujú citlivé údaje o jednotlivcoch (vierovyznanie, zamestnanie...) *len* pre tvorbu vládnej politiky. Nesmie byť možné dostať sa k údajom konkrétnej osoby. Avšak v USA v 70. rokoch Dorothy Denning zistila z databázy sčítania ľudu zo série legitímnych otázok napr. plat svojho šéfa => *kritický dotaz* je sekvencia legitímnych otázok, ktoré ale databáza nesmie vyhodnotiť, lebo by došlo k získaniu informácií o jednotlivcovi.

Ochranné mechanizmy proti zneužitiu informácií z databáz: zákaz agregácie pri veľkých databázach, úmyselná zmena originálnych dát. Ďalšie protiopatrenia:

- *technika náhodného výberu* časti záznamov zo všetkých existujúcich
- *minimálny rozsah dotazu:* na vyhodnotenie dotazu nesmie byť použitých menej záznamov, než je stanovené minimum
- *perturbačné techniky:* pridanie pseudonáhodného šumu – k záznamom zahrnutým pre vyhodnotenie sa pridajú ďalšie podobné. Využíva tiež zaokrúhľovanie čísel.

Deanonymizácia užívateľov - experiment z r. 2008: Narayanan a Shmatikov vzali databázu hodnotenia filmov divákmi na škále 1-10. Pokiaľ vieme hodnotenie pre 5-8 filmov, vieme zistiť skutočnú identitu hodnotiteľa.

Bezpečnosť v zdravotníctve (vo význame security – ochrana IS proti stratám, nie safety – bezpečnosť zdravia). Dôveryhodnosť zabezpečuje rukopis, pečiatka, digitálny podpis. Dôvernosť je zabezpečená mlčanlivosťou lekára. Bezpečnosť v klinických informačných systémoch, *British Medical Association*:

- Prístup k záznamu má len ošetrujúci lekár a pacient
- Len jeden z lekárov je zodpovedný a môže záznam meniť
- Pacientovi musí byť oznámené, kto má prístup k jeho údajom
- Dáta nesmú byť zmazané skôr, ako uplynie predpísaná doba pre ich úschovu
- Všetky prístupy k údajom musia byť zaznamenané – kto a kedy s nimi pracoval
- Počítačové systémy, ktoré pracujú s takýmito dátami musia mať subsystém, ktorý presadzuje vyššie uvedené princípy. Jeho účinnosť musí byť nezávisle overená.

Lekcia 2 – súkromie

- *Súkromie* je právo a možnosť jedinca kontrolovať informácie o sebe a svojej činnosti; spolu s ochranou proti nežiadúcemu rušeniu (osobami).
- *Informačné súkromie* sa vzťahuje k prvej časti definície + zaistenie ochrany osobných informácií, pravidlá pre ich kontrolu a poskytovanie iným subjektom.
- *Osobné informácie* sú také, ktoré buď vôbec nechceme zdieľať, alebo chceme „kontrolovať ich pohyb“, čiže vyberať si, komu ich povieme.

Cena osobných dát: zdravotné údaje občana UK je možné získať za 150£, adresa: 20£, adresa podľa telefónneho čísla: 75£, výpis z registra trestov: 500£. Cenu osobných dát ovplyvňujú:

1.) Výška trestu tým, ktorí dáta neustrážili a spolupodieľali sa tak na ich úniku

2.) Výška trestu tým, ktorí s dátami neoprávnene manipulujú
3.) Úroveň ochranných mechanizmov

Podľa prieskumov je asi 20% občanov úplne ľahostajná k nakladaniu s ich osobnými údajmi, asi 20% je veľmi obozretených, zvyšok je ochotný časť svojich práv na súkromie nechať obmedziť za istú kompenzáciu - finančnú, alebo zlepšenie služieb: napr. vernostné karty pre zákazníkov obchodných reťazcov, ktoré na výmenu sledujú, čo daný človek často nakupuje a tak sú schopné vypracovať cielené ponuky. Avšak väčšina užívateľov online, aj tí, ktorí sa považujú za ľudí citlivých na svoje súkromie bez zábran zdeľujú svoje osobné údaje – či už v anketách, alebo na sociálnych sieťach.

Experiment v Cambridge pre študentov: na 28 dní budú mobilní operátori sledovať používanie telefónu – komu a *odkiaľ* (podľa najbližšej základňovej stanice) volajú a kde sa pohybujú. Študenti mali sami ohodnotiť, koľko chcú dostať zaplatené, ale s tým, že na experiment bol vyhradený obmedzený rozpočet, takže nemohli žiadať priveľa (zámerný tlak). Ak sa im povedalo, že výsledky budú využité len na akademické účely, priemer bol 27£ (max. 400£, min. 0). Ak sa im povedalo, že výsledky budú využité aj na komerčné účely, priemer stúpol na 32£. Ak si chceme byť istí, že nás nesledujú podľa mobilu, netreba ho nosiť so sebou alebo ho treba vypnúť ☺

Podobný experiment prebehol na jar 2006, zapojilo sa 2500 ľudí z Nemecka, Belgicka, Grécka, ČR a SR. Mohli si vybrať, koľko by chceli dostať za sledovanie na 1 mesiac alebo na 1 rok: 12-násobne dlhšie trvanie, ale sumy vzrástli len o dvojnásobok. Hypotéza: dlhodobé sledovanie nie je až také účinné, pretože za 1 mesiac sa dá zistiť už dosť veľa. Výsledok: 10% zúčastnených žiadalo menej ako 1€. Priemer bol okolo 40€, čo zhruba zodpovedalo výsledkom Cambridgského experimentu.

Lekcia 3 - relevantné bezpečnostné funkcie

1.) **Anonymita:** vlastnosť systému, ktorý umožňuje využívanie zdrojov alebo služieb bez zistenia identity používateľa.
2.) **Pseudonymita:** podobné, ale používateľ je stále zodpovedný za použitie zdrojov a v prípade neoprávneného použitia je možné jeho identitu zistiť (P.O. BOX poštové priehradky).
3.) **Nespojiteľnosť:** vlastnosť systému, ktorý umožňuje opakované využitie zdrojov alebo služieb tak, že ostatní si tieto použitia nebudú schopní spojiť v zmysle vzájomnej súvislosti. (Nezohľadňuje identitu používateľa, len rozsah služieb alebo zdrojov, ktoré využil.)
4.) **Nepozorovateľnosť:** vlastnosť systému, ktorý umožňuje využívať zdroje alebo služby tak, že ostatní používatelia nemôžu spozorovať toto použitie. Napr. ochrana proti *traffic analysis* – sledovanie, či šla správa z bodu A do bodu B (bez toho, že by sa čítal jej samotný obsah).

Je možné merať/hodnotiť informačné súkromie? Dva uhly pohľadu:

- **Spoločné kritériá (CC):** rozsiahly štandard pre *diskrétne hodnotenie* (áno/nie) bezpečnostných systémov. Hodnotený systém sa označuje ako TOE – Target of Evaluation.
- **Mixy -** systémy pre posielanie správ, obvykle s kamuflovanými správami + preposielanie medzi viacerými účastníkmi kvôli ťažšiemu vysledovaniu. Základ položil A. Pfitzmann a kol., definoval ich David Chaum. Sústredia sa len na prostredie, kde sa posielajú správy.

Anonymita (CC): ochrana identity užívateľov, nie ochrana identity subjektov v systéme. Identita užívateľov ostáva skrytá špecifickým subjektom pre špecifické operácie.
Pseudonymita (CC): identita užívateľa je skrytá, ale ak poruší isté chovanie, je možné tento stav zvrátiť => vybrané entity môžu vystopovať identitu užívateľa podľa aliasu.
Nepozorovateľnosť (CC): nijaký užívateľ systému nemôže pozorovať používanie daných služieb – špecifikované entity *nie sú* schopné pozorovať vykonávané operácie.
+ nespojiteľnosť. Nevýhoda CC: neriešia, ako sa daná vlastnosť dosahuje – len hodnotia.

Anonymita (A.P.): subjekt je neidentifikovateľný v rámci danej množiny subjektov (tzv. anonymitná množina - obvyklí podozriví) => subjekt má minimálnu preukázateľnú zodpovednosť.
Nezáleží na chovaní užívateľov. Anonymita je silnejšia, ak je anonymitná množina väčšia (ale nemusí to tak byť vždy). Pre zistenie jej veľkosti sa používa *entropia.*
Pseudonym (A.P.): pomenovanie – reťazec bitov, ktorý je unikátny (ako ID). Je použiteľný pre autentizáciu jeho vlastníka. Ak sa opakovane používa jeden pseudonym, užívateľ získava istú reputáciu. Častejšie sa používa väčší počet pseudonymov.
Nespojiteľnosť (A.P.): nespojiteľnosť dvoch prvkov (subjektov, udalostí) znamená, že prvky nie sú ani viac, ani menej vo vzájomnom vzťahu s ohľadom na predchádzajúcu znalosť o systéme.
Nepozorovateľnosť (A.P.): stav *predmetov záujmu*, kedy nie sú odlíšiteľné od iných predmetov záujmu (pri správach v mixe napr. neodlíšiteľnosť skutočných správ od „šumu“).

Pseudonym môže byť:

- Verejný: napr. v zozname osôb, telefónne číslo v Zlatých stránkach
- Pôvodne neverejný: číslo účtu (nie je známe, ale banka ho má priradené k osobe)
- Pôvodne nespojený: prezývka v chate (zo začiatku ju nepozná nikto okrem jej vlastníka)

- **Identita (A.P.):** ľubovoľná podmnožina atribútov istého jedinca, ktorá tohto jedinca jednoznačne určuje v akejkoľvek množine jedincov. Identít môže mať jedinec viac.
- *Čiastočná* identita sa vzťahuje k istému kontextu alebo k istej role (XXXXXX je moje UČO v IS MUNI, ale v inom kontexte toto číslo nemusí nič znamenať).
- IMS (Identity Management Systems) sú systémy riadenia identity. Stavajú často na využití *Single sign-on* (jednoduché prihlasovanie) a *public key infrastructure* (spoľahlivé spojenie kľúča a osoby).

- **Pseudonym osoby** = reprezentácia danej osoby (napr. telefónne číslo).
- **Pseudonym role** = jedna osoba využíva pre rôzne role rôzne pseudonymy (login do IB).
- **Pseudonym vzťahu** = jedna osoba využíva rôzne nicky pre komunikáciu s rôznymi partnermi.
- **Pseudonym role - vzťahu** = komunikačný parter sa nedozvie, že dva pseudonymy použité v rôznych rolách patria v skutočnosti jednému človeku.
- **Pseudonym transakcie** = nie je možné zistiť, že dve rôzne transakcie vykonal v skutočnosti jeden subjekt. Je unikátny pre každú transakciu.

Lekcia 4 – ochrana osobných dát, legislatíva, etika

- Rada Európy (1950) – Konvencia o ochrane ľudských práv a základných slobôd – dva články (8 a 10) zaoberajúce sa nakladaním s informáciami
- Prvé „informačné zákony“ v Švédsku (1973), SRN (1977) a Rakúsku (1978)
- Rada Európy (1981) – Dohoda na ochranu osôb so zreteľom na automatizované spracovanie osobných údajov: záväzné pre verejný a súkromný sektor
- Smernica č. 95/46/EC EP o ochrane jednotlivcov vo vzťahu k spracovaniu osobných dát
- Upresňuje ju smernica 2002/58/EC o súkromí a elektronickej komunikácii
- Lisabonská zmluva („Ústava pre Európu“), články II-67 a II-68

Zákony v ČR:

- Listina základných práv a slobôd (2/1993) – nedotknuteľnosť osoby a jej súkromia, ochrana ľudskej dôstojnosti, osobnej cti, dobrej povesti a mena, súkromného a rodinného života + *ochrana pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním*

údajov o svojej osobe – je to právo, ktorého sa nemôžeme vzdať, tak ako právo na život (nemôžeme sa nechať zabiť nejakou firmou, aj keď im to podpíšeme)
- Občiansky zákonník – ochrana písomností osobnej povahy, obrazových snímkov, obrazových a zvukových záznamov
- Zákon o ochrane osobných údajov v informačných systémoch (1992) mal niekoľko problémov: nešpecifikoval, čo presne osobné údaje sú, ani aké sú sankčné opatrenia; ale obsahoval právo získať vyrozumenie o informáciách o osobe uchovávaných raz ročne bezplatne – v zmysle okruhu, nie obsahu (platné aj dnes)
- Lepší Zákon o ochrane osobných údajov (2000) – spracovateľ osobných údajov sa musí registrovať na Úrade pre ochranu osobných údajov => práva a povinnosti pri spracovávaní týchto údajov a tiež ich pohybe do zahraničia. Vzťahuje sa na **každé spracovávanie údajov** fyzickými a právnickými osobami, aj štátnymi orgánmi. Nevzťahuje sa len na zhromažďovanie údajov fyzickou osobou výlučne pre vlastnú potrebu, ktoré nie sú ďalej spracovávané.

Osobný údaj je údaj týkajúci sa určeného alebo určiteľného subjektu => identita je známa alebo je možné ju určiť na základe týchto údajov. O osobný údaj sa *nejedná*, pokiaľ je treba k zisteniu identity subjektu údajov neprimerané množstvo času, úsilia či materiálnych prostriedkov.
Citlivý osobný údaj vypovedá o národnostnom, rasovom alebo etnickom pôvode, odsúdení za trestný čin, politických postojoch, náboženstve, filozofickom presvedčení alebo sexuálnom živote.

Povinnosti správcu:

- Stanoviť účel, pre ktorý majú byť osobné údaje spracovávané
- Stanoviť prostriedky a spôsob spracovania osobných údajov
- Spracovávať LEN pravdivé a presné osobné údaje, ktoré boli získané v súlade so zákonom
- Overovať, či sú osobné údaje pravdivé a presné a pokiaľ tak nemôže učiniť, musí ich blokovať
- Zhromažďovať údaje odpovedajúce len stanovenému účelu a v rozsahu nevyhnutnom pre naplnenie stanoveného účelu
- Uchovávať údaje len po dobu, ktorá je nevyhnutná k účelu ich spracovania (výnimka: štatistika, veda, archívy). Po uplynutí tejto doby sa vykonáva deidentifikácia
- Nevyhnutný je *súhlas subjektu údajov* písomnou zmluvou (výnimky pre štátne inštitúcie) – napr. pri rušení bankového účtu neznamená, že tento súhlas automaticky zaniká
- Musí zdeliť subjektu, odkiaľ získal jeho osobné údaje a na aký účel ich bude používať

Pri porušení týchto povinností musí správca či spracovateľ napraviť chybný stav alebo poskynúť na vlastné náklady náhradu škody, ak subjekt utrpel osobnú ujmu. Subjekt môže byť pokutovaný, ak odmietne spolupracovať s Úradom pre ochranu osobných údajov.

POČÍTAČOVÁ ETIKA – systém morálnych princípov a pravidiel chovania v rámci IT: aké chovanie je správne? + Zodpovednosť jedinca pri používaní IT. Motivácie chovania:

1.) Úroveň zákonov a predpisov – strach z trestu a vynucovania sankcií
2.) Úroveň konvencií – profesné kódy (napr. lekári)
3.) Úroveň morálky – zvyky, skúsenosti

Ako sa morálke učí (už od detsva)? Keď niečo robím, je v poriadku, keby to niekto urobil mne? Aký dopad budú mať moje činy na ľudí, ktorých sa týkaju?

V IT: *vlastník* – ja rozhodujem o využití; *užívateľ* – používam cudzí majetok; *hacker* – informácie patria všetkým (tento postoj vznikol, keď počítače používali len vládne organizácie a občania ako daňoví poplatníci by mali mať právo na informácie, ktoré sú o nich spracovávané).

Veci – kopírovanie je obyvkle netriviálne, originál je možné rozoznať.
Informácie – kopírovanie je triviálne a originál je rovnaký ako kópia.

- **ACM** (Association for Computing Machinery): Code of Ethics and Professional Conduct
- **IEEE** – Software Engineering Code of Ethics and Professional Practice – okrem iného hovorí, že SW inžinier musí vykonávať svoju prácu v súlade s verejným záujmom a musí zaistiť čestnosť a nezávislosť vo svojich odborných odhadoch
- **Computer Ethics Institute:** Ten Commanments of Computer Ethics – dobrá myšlienka, ale náročné uplatnenie v praxi

Lekcia 5 – úvod do informačnej bezpečnosti

Bezpečnost (angl. Security) je *vlastnosť prvku* (napr. IS), ktorý je na určitej úrovni chránený proti stratám alebo tiež *stav* ochrany proti stratám.

Informačná dominancia = mať správne informácie na správnom mieste v správny čas (normálne) + zamedziť nepriateľskej strane v dosiahnutí informačnej dominancie (agresívne, používa napr. armáda). Pre minimalizáciu nepriateľskej informačnej dominancie je dôležité zveriť pracovníkom len najpotrebnejšie informácie a tiež týchto pracovníkov vopred aj priebežne preverovať.

Pri utajení dát zvažujeme:

- či tieto dáta majú vôbec byť utajované – rozmyslieť si, ktoré informácie sú naozaj kľúčové a ich zverejnenie by spôsobilo napr. pád firmy
- či samotná existencia týchto dát je utajovaná => **STEGANOGRAFIA** je vedná disciplína (podobor kryptografie) zaoberajúca sa utajením komunikácie prostredníctvom ukrytia správy tak, aby si pozorovateľ neuvedomil, že komunikácia *vôbec prebieha*. (Príkladom je ukrytá správa v obrázku.) Sila tejto komunikácie stojí a padá na jej utajení, a preto zachytenie skrytej správy znamená jej prelomenie. Preto sa spravidla kombinuje s ďalšími metódami šifrovania.
- či je dokonca dôvod utajenia týchto dat utajovaný

Pojmy:

- **aktíva** = dáta, hodnoty, ktoré chránime
- **zraniteľnosť systému** = problematické („slabé“) miesto v systéme => prípadná **hrozba**
- **riziko** = je pravdepodobnosť uplatnenia hrozby (zvažuje sa aj možná výška škody)
- **útok** = realizácia hrozby; môže byť úspešný (znižuje hodnotu aktív) alebo neúspešný

Bezpečnostné opatrenia:

1.) Prevencia = obmedzujeme riziko: zariadime, aby bol útok málo pravdepodobný, alebo veľmi drahý => tak vytvárame **bezpečnostné opatrenia,** ktoré sú implementované **bezpečnostnými mechanizmami.**
2.) Detekcia
3.) Reakcia

Kde môže zlyhať bezpečnosť?

- Samotný algoritmus je navrhnutý nesprávne – málo pravdepodobné, ale slabé bezpečnostné opatrenia pri jeho návrhu môže byť zámerné – aby bolo napr. možné sledovať ľudí používajúcich GPS, alebo odpočúvať hovory (GSM)
- Systém - jeho naprogramovanie je nesprávne – čo sa stáva pri neskúsených programátoroch
- Chyby pri implementácii systému – sú časté – spôsobené snahou firiem ušetriť
- 95% bezpečnostných zlyhaní nastáva úmyselným jednaním užívateľov, zvolením nesprávneho hesla (PIN 1234), alebo použitím programov, ktoré heslo zverejňujú nezašifrovanou komunikáciou na Internete (trojany pre nemeckú vládu na odchytávanie skype hovorov)

Štatistika - incidenty sú spôsobované najčastejšie chybami (neúmyselne): 50 - 70%, ďalej škodlivým softwarom: 5 - 10%; zámerné *sabotáže zamestnancov* (aj bývalých): 10 - 20% - pomsta šéfovi alebo kolegom, snaha obohatiť sa, alebo skorumpovaný zamestnanec (napr. upratovačka má prístup do všetkých kancelárií a zároveň je slabo platená, takže jej nezáleží na firme). Vonkajší útok len 1 - 5% !

Absolútne bezpečné systémy neexistujú!

Nad čím sa treba zamyslieť, keď zvažujeme bezpečnostné opatrenia:

- Čo útočník (príp. útočníci) získa napadnutím daného systému?
- Koľko peňazí, času, ľudí a strojov musí nasadiť na útok?
- Oplatí sa mu to?

Klasifikácia útočníkov:

- **Trieda 0** (script kiddies) – nedisponujú dostatočnými znalosťami o systéme a využívajú na útok akékoľvek dostupné prostriedky (hackovacie programy z Internetu, skúšanie hesiel)
- **Trieda 1** (inteligentní nezasvätení útočníci) – nemajú dostatok znalostí o systéme, ale využívajú známe bezpečnostné slabiny; nehľadajú nové
- **Trieda 1.5** – majú znalosti o systéme, okrem zneužívania známych bezpečnostných chýb aj hľadajú nové
- **Trieda 2** (zasvätení insideri) – pracovali v danom systéme a majú o ňom špecializované znalosti, disponujú sofistikovaným vybavením, sú schopní vykonať analýzu systému v reálnom čase + majú možný prístup do niektorých častí systému
- **Trieda 3** (organizácie) – vládne organizácie (NSA), spravodajské služby - majú unikátne zariadenia, ktoré nie sú bežne dostupné + majú veľké finančné zabezpečenie

Na **ochranu komunikácie a dát** používame *fyzickú ochranu*: čipové karty, záloha dát do rôznych počítačov, Faradayova klietka – v jej vnútri nie je možný žiadny príjem elektromagnetických vĺn (napr. rádiových); a menej nákladnú *kryptografiu* (viz Lekcia 6).

Dôvernosť: zabránenie zistenia sémantického obsahu dát nepovolanými (neautorizovanými) osobami, a to utajením existencie informácie, maskovaním medzi inými dátami, kontrolou prístupu k miestam, kde sa dáta nachádzajú, alebo *šifrovaním* (zmenou dát do inej podoby pomocou kľúča).

Dôvernostný bezpečnostný model Bell – LaPadula:

- Procesy nesmú čítať dáta na vyššej úrovni („môžeš čítať Normal a Secret, ale nie Top Secret“)
- Procesy nesmú zapisovať dáta do nižšej úrovne

Integrita: k dátam môžu pristupovať len oprávnené osoby => bez jej súhlasu dáta nesmú svoj stav zmeniť vôbec (tzv. silná integrita), alebo ho nemôžu zmeniť nepozorovane (slabá integrita).

Integritný bezpečnostný model Biba: (je inverzný k modelu Bell - LaPadula)

- Procesy nesmú čítať dáta na nižšej úrovni – no read down
- Procesy nesmú zapisovať dáta do vyššej úrovne – no write up

Dostupnosť: *autorizovaní* užívatelia majú mať prístup k dátam a službám čo najmenej komplikovaný. Spolu s dôvernosťou a integritou tvorí **CIA** – Confidentiality, Integrity, Availability. K nim sa často pridáva 4. prvok: **preukázateľná zodpovednosť** (accountability) – za aktivity v systéme sú užívatelia zodpovední voči majiteľovi dát – preto k dátam pristupujú len autentizovaní užívatelia a vytvárajú sa záznamy, kto pracoval s akými dátami => **nepopierateľnosť** – vykonanú aktivitu nemožno poprieť.

Autenticita: dáta sú chránené na integritu (vieme, že neboli zmenené) a zároveň vieme, od koho pochádzajú. **Autentizácia entít:** vieme presne, s kým komunikujeme.

Zásadné kroky pre zaistenie bezpečnosti:

1.) Analýza hrozieb – dôležitá, pretože ak zle zhodnotíme, čo treba chrániť a aké sú možné hrozby, takmer vždy navrhneme nesprávne bezpečnostné opatrenia
2.) Špecifikácia bezpečnostnej politiky a architektúry – politika = požiadavky, pravidlá, postupy, ktoré určujú, čo majú dosiahnuť a zaistiť ochranné opatrenia; architektúra = popisuje štruktúru komplexu opatrení a jednotlivým častiam priradí bezpečnostné funkcie
3.) Popis bezpečnostných mechanizmov – techniky pre implementáciu bezpečnostných funkcií

Nevhodnosť doplnkovej bezpečnosti (add-on security): najprv je pracne vybudovaný nejaký systém, a až na konci sa príde na to, že treba zaistiť ochranu spravovaných informácií. Vedie k dodatočnému vybudovaniu ochrany na nižšej úrovni + vyšším nákladom.

Elektronická bezpečnosť zahŕňa obmedzenie rizík pri používaní elektronického zariadenia – počítače, mobilné telefóny, platobné karty, Internet banking. Riziká = neoprávnené použitie našich financií, odpočúvanie hovoru, zneužitie identity. Cieľ = zamedziť zneužívaniu týchto zariadení + nájsť osobu pokúšajúcu sa o zneužitie + minimalizovať škody.

Iné úrovne bezpečnosti: *fyzická* (prístup osôb k systému – aby sa nestalo, že z počítača so skvelým bezpečnostným systémom niekto vymontuje pevný disk; prírodné katastrofy), *personálna* (akí zamestnanci pristupujú k chráneným dátam?)

Zaistenie bezpečnosti je dlhodobý a opakovaný proces, pretože systémy sa menia!

Lekcia 6 – úvod do kryptografie, digitálny podpis

- **autentizácia:** preukazujem svoju totožnosť na základe niečoho, čo *mám* (občiansky preukaz), *viem* (login a heslo) alebo *som => biometrika* (fyziologické charakteristiky – hlas, odtlačky)
- **autorizácia:** na základe autentizácie dostanem prístup k nejakej službe
- **delegácia:** preukazujem, že môžem vystupovať za niekoho iného

Kryptografia je umenie ochrániť význam dát pomocou *šifrovania*, čo je proces transformovania informácií z normálne čitateľného stavu do zdanlivého nezmyslu. Snahou kryptografie je zaistiť, že konkrétnu správu si nemôže prečítať neoprávnená osoba.

Kryptoanalýza sa zase snaží šifry prekonávať. Jej spojením s kryptografiou vzniká **kryptológia**.

Šifra je dvojica algoritmov, ktorá umožňuje *šifrovať* (nie „kryptovať“ – nespisovné!) a následne *dešifrovať*. Činnosť a výstup daného algoritmu sú bližšie špecifikované **kľúčom,** čo je „parameter“, ktorý by mal byť známy len zúčastneným stranám.

História kryptografie:

- Scytale (vyslov skɪtəli) sa používal v starovekom Grécku. Je to drevená palička, na ktorú sa namotal papierik, ktorý sa popísal textom. Po rozvinutí papiera text nedával zmysel. Príjemca musel mať na prečítanie správy paličku rovnakého priemeru. Takáto šifra sa nazýva *transpozičná,* pretože mení usporiadanie písmen v texte.
- Caesarova šifra je *substitučná,* pretože nahradzuje písmená inými písmenami (napr. a -> d).

S príchodom počítačovej éry vznikali omnoho komplexnejšie šifry, ktoré dokážu pracovať so všetkými binárnymi údajmi (teda nie len s písaným textom). Mnoho počítačových šifier pracuje s dátami po bitoch alebo skupinách (blokoch) bitov, narozdiel od klasických šifier, ktoré priamo menili konkrétne písmená a číslice. Extenzívne štúdie kryptografie začali v 70. rokoch. Významné kryptologické konferencie: americké Crypto spolu s Eurocryptom a Asiacryptom, ktoré pomáha usporadúvať IACR.

Okrem šifrovania máme ďalšie požiadavky na podávané správy:

- integrita: správa došla nezmenená
- autenticita: správu poslal naozaj ten, kto je uvedený ako odosielateľ
- nepopierateľnosť: keď ja pošlem správu, tak mám istotu, že príjemca ju dostal (aby sa nemohol vyhovoriť, že som mu niečo neoznámil)

Napr. mail ani jednu z týchto požiadaviek nespĺňa.

Tri dimenzie kryptografie (jej rozdelenie):

1.) Druhy použitých operácií: substitúcia, permutácia, ...
2.) Druhy a parametre kľúčov: symetrické, asymetrické, bez kľúčov
3.) Spôsob spracovania dát: v blokoch, v súvislom prúde, ...

Kľúče sú rozsiahle reťazce bitov (náhodné čísla, prvočísla...). S rastúcou výpočetnou silou počítačov a teda väčším počtom útokov hrubou silou sa ich dĺžka zväčšovala, aj keď samotná dĺžka kľúča nie je jediným dôležitým faktorom. Závisí hlavne na kvalite šifrovacieho algoritmu, výpočetných kapacitách dostupných útočníkovi a iných faktoroch.

Symetrické šifrovanie: do roku 1976 jediný druh šifrovania: odosielateľ a príjemca sa dohodnú na jednom *spoločnom* algoritme a kľúči => rovnaký kľúč pre šifrovanie a dešifrovanie (napr. čísla značiace stránky, riadky a slová v knihe). Ak je kľúč dlhší ako správa, v podstate ho nie je možné prelomiť. Väčšinou je ale správa omnoho dlhšia ako kľúč, teda isté prvky kľúča sa opakujú a tak je možné v ňom nájsť systém. Problém: zdieľanie kľúča.

Staršie algoritmy, ako DES, DES3 sú už dnes veľmi ľahko prelomiteľné. Aktuálne najpoužívanejší: Advanced Encryption Standard (Rijndael). Bol vyrobený pre americkú NSA pre posielanie správ na úrovni top secret. Využíva kľúče dlhé 128 - 256 bitov (dĺžka kľúča určuje počet kôl).

Na kratšiu dobu komunikácie (niekoľko dní, týždňov) stačí 80-bitový kľúč. V minulosti sa používal 56-bitový => 2^{56} možných kľúčov, ktoré je ale dnes možné vyskúšať a prelomiť za cca 10 hodín.

Použitie v autentizácii: *Challenge-Response authentication:* Dve strany majú dohodnuté heslo (kľúč). Jedna strana pošle správu zašifrovanú týmto kľúčom, druhá ju príjme, dešifruje, odpovie, znovu zašifruje a pošle späť. Tak sa zároveň navzájom autentizujú, pokiaľ predpokladajú, že jedine oni dvaja poznajú toto heslo. Problém je pri komunikácii viacerých strán naraz.

Asymetrické šifrovanie využíva dva kľúče: súkromný – má ho majiteľ kľúča (používajú sa pre tvorbu podpisu, dešifrovanie) + verejný – je voľne dostupný (používa sa pre overenie podpisu, šifrovanie). Tieto kľúče sú jednosmerné, teda z jedného sa nedá zistiť druhý (neexistuje k nim inverzná funkcia). Kľúče sú najčastejšie dlhé 2048-4096 bitov => zložitejšie algoritmy, náročná implementácia.

Použitie v autentizácii: A zašifruje správu verejným kľúčom B a odošle. B ju dešifruje svojim súkromným, vykoná dohodnutú operáciu a zašifruje odpoveď verejným kľúčom A. A ju príjme a dešifruje svojim súkromným kľúčom. Takto sa ale autentizuje len A, nie B (napr. my sa preukážeme serveru, ale je potrebné, aby sa aj server preukázal nám).

Hash je jedinečný číselný odtlačok správy, z ktorého nie je možné rekonštruovať pôvodnú správu => vlastnosť *jednosmernosti* (pretože hash má napr. 256 bitov a správa 20 KB). Hashovacie funkcie MD5, SHA-0 a -1 majú problémy, preto sú dočasne doporučené dlhšie varianty SHA.

Ak má hashovacia funkcia vlastnosť *slabej bezkolíznosti,* je výpočetne nemožné nájsť k **danému vstupu** iný odlišný vstup tak, aby boli výsledné hashe rovnaké. *Silnej* = pre ľubovoľnú dvojicu.

Digitálny podpis zaisťuje nepopierateľnosť pôvodu. Vznikne tak, že A vytvorí hash správy a zašifruje ho svojim *súkromným* kľúčom. B ho po prijatí dešifruje verejným kľúčom A a tak overí jeho autenticitu, pretože svoj súkromný kľúč má mať len A. Tento podpis zároveň potvrdzuje integritu, pretože ak by niekto zmenil obsah správy, mala by iný hash. Nezaisťuje šifrovanie – len podpisuje dokument. Najznámejší podpisový algoritmus **RSA** sa používa tiež na asymetrické šifrovanie.

Z*aručený elektronický podpis* je jednoznačne spojený s konkrétnou osobou. Technologicky rovnaká je *elektronická značka,* ktorú ale môžu používať aj právnické osoby. Podpis a značka sa líšia v úrovni ochrany súkromného kľúča. Použitie podpisu: autentizácia dát / počítačov / osôb.

Problém autenticity verejných kľúčov – patrí verejný kľúč naozaj konkrétnej entite?
PKI (Public Key Infrastructure) 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.

Certifikačná autorita – štruktúra:

- 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 (ak je náš počítač napadnutý trojanom a kľúč môže byť zneužitý)
- Vrchol stromu certifikačných autorít predstavuje VeriSign
- Podobu certifikátov špecifikuje štandard X.509

Kontrola verejného kľúča:

- Konzervatívna: kľúč / certifikát je *neplatný*, pokiaľ nie sme spoľahlivo informovaní o opaku
- Liberálna: kľúč / certifikát je *platný,* pokiaľ táto informácia nie je spochybnená

Verejný kľúč sa používa na šifrovanie komunikácie medzi dvoma stranami, obvykle po pripojení na webstránku, ktorá implementuje HTTPS. Napríklad klient banky chce mať prístup k svojmu Internet bankingu a pripojí sa na stránku www.bank.example. Keď sa načíta táto stránka, spolu s dátami, ktoré zobrazí prehliadač užívateľ dostane verejný kľúč banky. Keď užívateľ zadá na stránke nejaké informácie a odošle ich banke, jeho webový prehliadač ich zašifruje použitím verejného kľúča vydaného bankou www.bank.example. Jedine privátny kľúč banky môže dešifrovať tieto informácie. Preto aj keby niekto odchytil (zašifrované) dáta, ktoré klient odoslal, čitateľné (dešifrované) dáta, môžu byť prečítané len bankou, pretože vlastní privátny kľúč.

Tento mechanizmus je bezpečný jedine vtedy, ak si je klient istý, že to, čo vidí vo svojom prehliadači je skutočne stránka banky. Ak do prehliadača zadá www.bank.example, ale jeho pripojenie je presmerované na falošnú webstránku, tá predstiera, že je stránkou banky a dá mu falošný verejný kľúč. Užívateľ vyplní osobné údaje, odošle ich a zašifrujú sa falošným (útočníkovým) verejným kľúčom. Útočník si ich tak v kľude môže prečítať, pretože vlastní odpovedajúci privátny kľúč.

Keďže certifikačná autorita spája verejný kľúč s jeho vlastníkom, pri podozrení ju môže používateľ kontaktovať a spýtať sa, či tento verejný kľúč naozaj patrí www.bank.example.

PGP (Pretty Good Privacy) využíva všetky princípy asymetrického šifrovania, ale neuznáva certifikačné autority, ale Web of trust.

Kombinácia prístupov symetrického a asymetrického šifrovania – hybridné kryptosystémy:

- dlhú správu zašifrujeme symetrickým kľúčom (je to rýchlejšie)
- tento kľúč doručíme druhej strane využitím asymetrickej kryptografie – zašifrujeme ho verejným kľúčom druhej strany a priložíme ku správe

Kerckhoffsov princíp hovorí, že kryptografický algoritmus by mal byť verejne známy a kontrolovaný, tajný je len kľúč. Algoritmy, ktoré tento princíp neuznávajú nazývame *proprietárne* =>
Security through obscurity – viera, že len dobre utajený algoritmus je bezpečný.

Lekcia 7 – elektronická bezpečnosť (viz. 5) – kreditné karty, mobily, IB

Elektronické zariadenia musia navzájom *preukazovať svoju identitu* – napr. kreditná karta preukazuje svoju identitu bankomatu, mobil (SIMka) preukazuje svoju identitu rádiostanici mobilného operátora.

Metódy autentizácie:

- niečo, čo viem = znalosť nejakého tajomstva (PIN, heslo)
- niečo, čo som = fyzická vlastnosť (biometrika – hlas, odtlačok prsta, sken sietnice oka)
- niečo, čo mám = vlastnosť nejakého predmetu - *tokenu* (kľúč k dverám, kreditná karta)
- + kombinácie týchto metód (občiansky preukaz = token, fotka = biometrika)

Dôležitým aspektom autentizácie je, že sa pri nej musíme chovať tak, aby naše chovanie niekto nemohol zopakovať - napr. odpozerať PIN ku karte + prečítať dáta (údaje o karte a majiteľovi) z magnetického prúžku a následne replikovať kartu. Treba rátať s tým, že naša činnosť môže byť pozorovaná, odpočúvaná atď.

Aj ten, voči komu sa autentizujeme môže ukradnúť našu identitu. Dôkaz nulového rozšírenia znalosti (zero-knowledge) = osoba preukazuje, že pozná riešenie nejakého problému. Overovateľ sa nemôže dozvedieť tajomstvo, ktoré pozná preukazujúca sa strana a tak sa za ňu nebude môcť vydávať.

Krádež **mobilného telefónu** – ukradnutý telefón je možné jednoducho odblokovať. Zneužitie údajov uložených v mobile – telefónny zoznam, osobný plán, záznamy o transakciách, audio, video, fotky. Pre zlodeja je nevýhodné, že mobilný telefón s ukradnutou SIM kartou je možné identifikovať, lokalizovať a následne zamerať.

Zneužitie **bezdrôtového prenosu** – šifrovanie v GSM má veľmi nízku bezpečnosť. O chybách v tomto štandarde sa vedelo už počas jeho vývoja, preto sa tvrdí, že tam boli zavedené zámerne. V mnohých krajinách sa šifrovanie nepoužíva vôbec. Aj napriek relatívnej jednoduchosti sú na odpočúvanie nutné isté technické znalosti a zariadenia. Nový štandard **3GSM** sa považuje za bezpečnejší.

Operátor môže taktiež sledovať všetky hovory. Záznam zvuku je ale relatívne náročný na kapacitu úložných zariadení a ťažko sa automatizuje jeho spracovanie => vyhodnocovanie podľa kľúčového slova. Naproti tomu SMS správy zaberú málo miesta a ľahko sa automaticky vyhodnocujú.

Zneužitie prídavných zariadení: **Bluetooth** má veľmi slabú bezpečnosť – mnoho ľudí ho má stále zapnutý bez toho, že by ho používali. Má prakticky vyšší dosah ako udávaných niekoľko metrov.

EÚ nariaďuje po dobu 2 rokov ukladať parametre *každej* elektronickej komunikácie – **data retention.** Zber údajov je často potrebný – pri vyšetrovaní trestnej činnosti, alebo zaznamenávanie dĺžky hovorov pre potreby operátora – no zároveň sa zneužíva.

Platobné karty – princíp uloženia údajov:

- Magnetický prúžok: upravená čítačka ju môže prečítať a vytvoriť kópiu dát – *nebezpečné*
- Karty s čipom: čip neposkytuje čítaciemu zariadeniu (bankomatu) svoje kompletné údaje a môže sa autentizovať pokročilými kryptografickými technikami. Vyrobiť kópiu čipu je veľmi náročné, pretože je nutné ho rozobrať a analyzovať, no rada útokov vôbec nevyžaduje vytvárať kópiu čipu. Kvôli kompatibilite s bankomatmi v iných krajinách tieto karty stále obsahujú klasický magnetický prúžok.

PIN je možné odpozorovať (pomáha ochranný kryt na PINpade, zakrývanie prstov a zároveň minimálny pohyb ruky) alebo použiť kameru nad bankomatom, rafinovanejším riešením je kamera citlivá na tepelné žiarenie, ktorá sníma teplotu kláves. Útočníkova najlepšia pozícia je priamo za alebo priamo pred pozorovanou osobou. Čiastočné protiopatrenie pri platbe v obchode: použitie PINu a zároveň autentizácia podpisom, rôzne PINy pre rôzne transakcie (v závislosti na čiastke).

Niektoré kreditné karty je možné použiť na **platby po Internete**. Zadáva sa obvykle číslo karty, meno vlastníka, dátum platnosti a bezpečnostný kód z druhej strany karty. Tieto zadané údaje si obchodníci ukladajú a tak ich tiež môžu použiť k platbe na Internete, alebo môžu byť ukradnuté z ich serveru. Navyše, zákazníkovi nie je zaručená väzba medzi zobrazovanou a potvrdzovanou transakciou.

Internet Banking – autentizácia len pomocou hesla nestačí – minimálne SMS autorizácia. Používa sa aj *osobný kľúč*, ktorý využíva asymetrickú kryptografiu. Je uložený na CD, USB, SD-karte, alebo čipovej karte (najbezpečnejšie). Najmenej bezpečný bod: keď sa prehliadač pripája na stránku banky a sťahuje verejný kľúč banky a aplikáciu, s ktorou bude užívateľ pracovať. Možné riešenie: klient dostane túto aplikáciu na médiu priamo od banky.

Využíva sa aj *autentizačná kalkulačka:* vzdialený počítač pošle klientovi výzvu – tú klient zadá do svojej „kalkulačky" a na displeji sa objaví odpoveď, ktorú zadá do počítača. Celá komunikácia je takmer na úrovni zero-knowledge. Bezpečnosť je porovnateľná s čipovými kartami.

Lekcia 8 – biometrika a ochrana súkromia

Biometrika je metóda autentizácie *osôb*. Režimy použitia: **verifikácia** (identita osoby je známa) a **identifikácia** (identita osoby nie je známa – je nutné prejsť celú databázu možných záznamov na overenie danej osoby).

Biometrika zahŕňa *biologické charakteristiky,* ktoré sú merateľné automatizovane:

- **fyziologické** (statické) charakteristiky:
  - ruka – odtlačok prsta, dlane, geometria ruky, žily ruky
  - oko – vzor dúhovky (iris; aj na vzdialenosť 1m), sietnica (bezprostredne pri skeneri)
  - tvár, čiastočne hlas, DNA
- **behaviorálne** (dynamické) charakteristiky:
  - dynamika podpisu / písania na klávesnici
  - hlas
  - chôdza, pohyby tváre

Proces použitia biometrík:

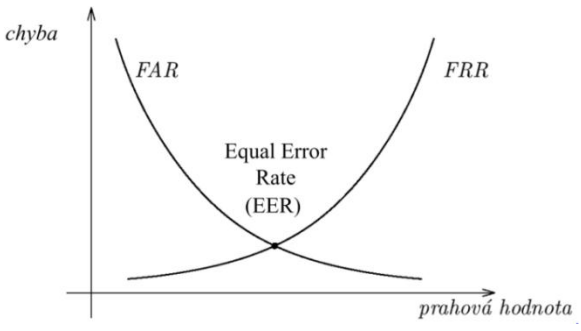
- registrácia = prvotné snímanie biometrických dát, vytvorenie vzorky a jej uloženie do databáze (registráciu je potrebné urobiť dôkladne)
- verifikácia/identifikácia = následné snímanie biometrických dát a ich porovnanie so vzorkou

Variabilita:

- biometrická dáta nedávajú jednoduché odpovede typu áno/nie – heslo je buď 1234 alebo nie, ale napr. podpis človeka je zakaždým mierne odlišný => biometrické dáta **nikdy nie sú na 100% zhodné** a dobrý systém sa s tým musí vysporiadať. (100% zhoda nastáva často pri útokoch na systém). Zavádza sa *prahová hodnota* („aké % zhody je ešte prijateľné?“)
- presnosť samotného snímacieho zariadenia
- faktory prostredia (teplota, svetlo)

Chyby:

- nesprávne prijatie neoprávnenej osoby **(False Acceptance Rate)**
- nesprávne odmietnutie správnej osoby **(False Rejection Rate)**
- *Failure to Enroll* (nemožnosť zaregistrovať užívateľov – napr. ťažko pracujúci človek má zodraté ruky)
- *Failure to Acquire* (nemožnosť získať dáta)



Problémy:

1.) Problém živosti: Je skenovaná vzorka od živej osoby?
(napr. kontrola, či skenovaným prstom prechádza krv)
2.) Je vzorka skutočne od osoby, ktorá je práve pri vstupnom zariadení? (kontroluje strážnik)
3.) Nebol napichnutý komunikačný kanál medzi zariadením a riadiacim počítačom?
4.) Nízke požiadavky na bezpečnosť = vysoké FAR; vysoké požiadavky na bezpečnosť = vysoké FRR

5.) Odtlačky osôb je možné jednoducho získať, takisto vlasy, kúsky kože atď.
6.) Užívatelia s poškodenými alebo chýbajúcimi orgánmi
7.) V biometrických systémoch sa nachádzajú **osobné údaje** – identitu človeka určujú relatívne presne a tak je možné spojovať jeho jednotlivé činy => citlivá administrácia
8.) Vzorku narozdiel od hesla nie je možné príliš meniť, takže ak sa používa vo viacerých systémoch, je možné ľahko ju získať (jediné riešenie: overovanie hlasu vždy na nejakej unikátnej vete, ktorú sme pravdepodobne nikdy nehovorili)
9.) Legislatíva

Biometrické dáta nie sú tajné! Systém na tom nesmie byť založený.

Lekcia 9 – bezpečnosť: kontroly, bezpečnostná politika, štandardy

Pripomenutie pojmov:

- **aktíva** = dáta, hodnoty, ktoré chránime
- **zraniteľnosť systému** = problematické („slabé“) miesto v systéme =>
- prípadná **hrozba** (akcia, ktorá môže ohroziť bezpečnosť; potenciálne využitie zraniteľnosti)
- **riziko** = je pravdepodobnosť uplatnenia hrozby (zvažuje sa aj možná výška škody)
- **útok** = realizácia hrozby; môže byť úspešný (znižuje hodnotu aktív) alebo neúspešný

Kontroly:

- Čo vlastne robiť? (analýza rizík)
- Ako to robiť? (bezpečnostná politika)
- Aký systém použiť? (kritériá hodnotenia bezpečnosti)
- Robíme to dobre? (interný audit – kontrolné oddelenie nezávislé na IT oddelení!)
- Robia to nesprávne? (externý audit – dôraz je kladený na dokumentáciu, nie technológiu! Auditor otestuje vybrané časti systému a testuje, či je dokumentácia správna)

Analýza rizík v IT obecne: podľa štandardu pre riadenie bezpečnosti ISO/IEC 27002. Používa sa len pre veľké spoločnosti, ktoré sú kriticky závislé na IT (napr. e-shopy). Pre malé firmy a živnostníkov stačia úplne iné kontroly.

Zásadné kroky pre zaistenie bezpečnosti:

1.) Analýza hrozieb – zvažujeme, čo treba chrániť a aké sú možné hrozby. Často sa vychádza z analýzy skúseností iných spoločností, ktoré chránili podobné hodnoty a boli napadnuté.

- Skôr *odhad* rizík, menej formálny než skutočná analýza
    - **Kvantitatívna**: náročnejší postup, ale zrozumiteľný výstup v $$$
    - **Kvalitatívna**: automatizovateľná, ale výstup: ťažšie zrozumiteľná diskrétna stupnica
- Metóda **ALE** (Annual Loss Expectancy) = SLE x ARO
  (Single Loss Exposure x Annualized Rate of Occurence)
- Metóda **BPA** (Business Process Analysis) = širšie poňatie rizík, nie len IT. Výstupy: mapa procesov a ich popisy, tabuľka rizík (kvalitatívna), doporučenia
- **CRAMM** (Risk Analysis and Management Method) postupuje v 3 štruktúrovaných krokoch: i) identifikácia a ocenenie hodnôt – ii) odhad hrozieb – iii) výber protiopatrení

Analýza sa vykonáva zberom informácií – dotazníky, pohovory so zamestnancami.

2.) Špecifikácia bezpečnostnej politiky a architektúry:

- **politika** = požiadavky, pravidlá, postupy, ktoré určujú, čo majú dosiahnuť a zaistiť ochranné opatrenia (t.j. formálna stratégia, ako dosiahnuť cieľ – minimalizáciu rizík)
- celková BP je všeobecná, nezávislá od IT; konkretizuje ju systémová BP
- používajú sa *štandardy* (viz. nižšie)
- **architektúra** = popisuje štruktúru komplexu opatrení a jednotlivým častiam priradí bezpečnostné funkcie

3.) Popis bezpečnostných mechanizmov – techniky pre implementáciu bezpečnostných funkcií

Štandardy sústredia zásadné poznatky o rôznych protokoloch:

- ISO/IEC 27002 sa venuje zásadám budovania a využívania systému riadenia bezpečnosti (model PDCA: Plan – Do – Check – Act)
- Medzinárodné organizácie: ISO, IEC, ITU
- Európske organizácie: CEN, CENELEC, ETSI
- Národné organizácie: ANSI, BS, DIN, ČSNI
- ČSNI = *Český normalizační institut* – vydáva technické normy, ktoré ale nie sú záväzné
- ISO – štandardy musia vyhovovať požiadavkám daného odvetvia po celom svete => berie do úvahy názory všetkých zainteresovaných strán (výrobci, dodávatelia, užívatelia, vláda, testovacie laboratóriá, výskumné pracoviská)
- Štandardy **NIST** – Special Publications (využívané často v USA),
  Napr. dokument 800-27: Engineering Principles for Information Technology Security hovorí:
  - predpokladajte, že externé zdroje nie sú bezpečné
  - usilujte o jednoduchosť
  - fyzicky alebo logicky odďeľte kritické zdroje
  - minimalizujte časti systému, ktoré musia byť vysoko bezpečné
  - neimplementujte nadbytočné bezpečnostné mechanizmy

Organizačné bezpečnostné kritériá: jednoznačné priradenie zodpovednosti, schopnosť reakcie na incidenty, preverovanie zamestnancov, analýza rizík, bezpečnostné školenia
Prevádzkové bezpečnostné kritériá: kontrola zaisťujúca stabilitu dodávky elektrickej energie, fyzická ochrana objektov, kontrola možného znečistenia vzduchu, kontrola vlhkosti, teploty...
Technické bezpečnostné kritériá: ochrana komunikácie, šifrovanie, kontrola prístupu, autentizácia

Kritériá hodnotenia bezpečnosti umožňujú jednoduchšie porovnanie rôznych bezpečných systémov. Klient (firma) si tak môže vybrať podľa svojich skutočných potrieb.

- Napr. Trusted Computer System Evaluation Criteria („oranžová kniha“): hodnotenie systémov od A1 (najvyššia bezpečnosť) po D (žiadna)
- *Hodnotenie* = overenie zhody deklarovaných vlastností
- **Common Criteria:**
  - TOE = Target of Evaluation – produkt alebo systém, ktorý je predmetom hodnotenia
  - ST = Security Target – špecifikácia bezpečnosti
  - PP = Protection Profile – implementačne nezávislá skupina bezpečnostných požiadavkov určitej skupiny predmetu hodnotenia

Krypto-štandardy:

- Symetrická kryptografia: AES (od r. 2001) – algoritmus **Rijndael** – kľúč 128 bit (10 rund), 192 bit (12 rund) alebo 256 bit (14 rund); spracováva dáta po bajtoch
- Asymetrická kryptografia: IEEE P1363, NIST FIPS 186-3 (Digital Signature Standard)
- Hashovacie funkcie: SHA-1, -2, -3
- Digitálne certifikáty: X.509

Hodnotenie kryptografických modulov: štandard **FIPS** 140-1, -2, -3, ktorý hodnotí napr. fyzickú bezpečnosť, bezpečnosť OS, rozhranie modulu, služby a autentizáciu, správu kľúčov alebo metódy pre zmiernenie iných útokov.

Lekcia 10 – bezpečnosť v praxi prostredia Internetu

PGP – autor Phil Zimmermann – chcel vytvoriť program dostupný ľuďom po celom svete, aby mohli šifrovať svoju komunikáciu po Internete. Využíva kombináciu symetrickej a asymetrickej kryptografie (verejným kľúčom príjemcu sa šifruje vždy novo generovaný kľúč pre symetrickú šifru; súkromný kľúč slúži na podpis hashu správy). Dnes výraznejší vývoj ako **GPG** – Gnu Privacy Guard.

PGP kľúč využíva najčastejšie algoritmy RSA a DSS. Je spojený s:

- *UserID*, ktoré môže byť úplne ľubovoľné, preto sa naňho netreba spoliehať
- *KeyID*, čo je relatívne malé číslo, preto je možné uhádnuť KeyID niekoho iného
- Odtlačkom (fingerprint) – unikátny

Pre konkrétny verejný kľúč sa nastavuje *úroveň dôvery* – znamená to, že vyjadrujeme dôveru v pôvod dát podpísaných vlastníkom odpovedajúceho privátneho kľúča. **Tranzitivita dôvery:** napr. verím kľúču tohoto človeka + všetkým ďalším, ktoré podpísal. Je dôležité podpísať si vlastný verejný kľúč privátnym pre zaistenie *integrity*. Od ľudí, ktorým verejný kľúč poskytujeme by sme mali požadovať, aby ho podpísali tiež. Predanie kľúča mailom alebo cez web link nie je dôveryhodné!

TLS - Transport Layer Security, predtým SSL (Secure Sockets Layer) je protokol firmy Netscape pre autentizáciu entít (klient, server). Zaisťuje kontrolu integrity, dôvernosť komunikácie. Kombinuje symetrickú a asymetrickú kryptografiu. Využívajú ho eshopy, IS...

- TLS/SSL Record Protocol = základná vrstva
- TLS/SSL Handshake Protocol = pre úvodnú autentizáciu (digitálnymi certifikátmi) servera voči klientovi (autentizácia klienta voči serveru na vyžiadanie). Klient dostáva certifikát serveru (ak je niekto v strede a odchytí pravý certifikát, klient dostane upozornenie, že prijatý certifikát sa nezhoduje so serverom). Nastáva výmena kľúčov, určenie šifry a ďalej bezpečná komunikácia.

IPSec – bezpečnostný protokol pre IPv4; v IPv6 šifrovanie priamo.

Tieto protokoly samy o sebe fungujú relatívne dobre, problém je často na strane užívateľa (navštevovanie pochybných stránok, malware a následne prihlásenie do Internet bankingu) + pozri nastavenia prehliadača, koľko certifikačných autorít je nastavených ako dôveryhodných.

Firewall chráni proti útokom zvonka – komunikáciu môže **povoliť** / **zakázať** / **preložiť**, čiže analyzovať a rozhodnúť, či povoliť alebo zakázať. Napr. cez port 80 môžu byť vedené rôzne typy komunikácie – web, mail atď. Je nutné, aby firewall zistil, o akú komunikáciu ide a aplikoval pravidlá, ktoré má priradené danému typu komunikácie.

V takom prípade sa firewall správa ako aplikačný proxy server, ktorý analyzuje obsah komunikácie. Často je napadnutý útokmi **denial of service:** zahltenie webového serveru komunikáciou z množstva strojov a jeho následná nedostupnosť pre užívateľov.

Systémy detekcie prieniku (IDS, Intrusion Detection Systems) fungujú podobne ako antivíry – je nastavené štandardné chovanie a kontroluje sa, či nenastala *atypická komunikácia*, alebo sa kontroluje *databáza* možných útokov. Je možné použiť ich v sieti aj na počítači.

Ďalšia možnosť zistenia podozrivého chovania v sieti: **honeypot.**

Steganografické súborové systémy:

- Máme zašifrovanú (encrypted) správu M kľúčom K: $E_k(M) = M'$
- Správa M' dešifrovaná kľúčom K vráti spätne správu M: $D_k(M') = M$
- Pre osobu, ktorá nepozná K je M nečitateľná
- Ak majiteľ prezradí K, dôjde k odhaleniu M
- Majiteľ M nemôže poprieť existenciu utajovanej informácie a môže byť k odhaleniu kľúča K donútený
- Preto sa používajú systémy **vierohodnej popierateľnosti** (plausible deniability, PD):
- M = „zabijupapouska“
- K = „jkhgxzileqwpov“
- M' = „ikiogtxlteqhyv“
- A pri vymáhaní kľúča je možné vierohodne tvrdiť:
- K = „wcxuxzileqwpov“
- M = „milujupapouska“

Kryptografický súborový systém (FS) šifruje obsah súborov. Šifrované dáta = prúd náhodných bitov, a preto budia na disku pozornosť (bežné súbory nemajú takú úroveň náhodnosti). Preto sa používa FS poskytujúci PD (vtedy už nie je kryptografický, ale *steganografický*). Ten šifruje obsah **všetkých** súborov a voľné miesto zapĺňa náhodnými bitmi => FS obsahuje súbory, ktoré vyzerajú dôverne, ale ich odhalenie nespôsobí problémy. Majiteľ pod nátlakom odhalí kľúč k nejakému voľnému miestu.

Cieľom projektu **ETERNITY SERVER** je vytvoriť trvalé uloženie dát, pričom zmazať ich nemôže ani pôvodca, pretože sa kopírujú na množstvo spolupracujúcich serverov + odolnosť voči výpadku.

Lekcia 11 – anonymná komunikácia na Internete

Anonymnú komunikáciu používame, keď chceme chrániť osobné údaje. Typy anonymity: užívateľa, lokácie, transakcie. Anonymita tiež patrí medzi relevantné bezpečnostné funkcie (viz. lekcia 3). Nutnosť zaistiť anonymitu napr.:

- Pri ochrane informácii o zdravotnom stave (anonymita – lekár má informácie o zdravotnom stave bez väzby na identitu pacienta *vs.* pseudonymita – lekár pozná len nejaké ID pacienta, ktoré je v záznamoch spojené s osobou, ale lekárovi na určenie diagnózy stačí poznať len ID)
- Pri elektronických voľbách
- Ak komunikujeme v prostredí, kde nie je sloboda slova
- Pri udaní trestnej činnosti

Anonymita (C.C.): užívateľ môže využiť zdroj alebo službu bez odhalenia svojej identity.
Anonymita (mixy): subjekt je neidentifikovateľný v rámci danej množiny subjektov (tzv. anonymitná množina - obvyklí podozriví).

Anonymitu vyjadrujeme z ohľadom na **model útočnika:**

- *pasívny* – analyzuje aktivitu užívateľov v sieti / *aktívny* – vstupuje do komunikácie, môže označiť konkrétne správy a neskôr ich vystopovať
- *lokálny* – vidí len časť siete / *globálny*

Charakteristiky anonymity: (mixy)

- Kvantitatívna – závislá na veľkosti anonymitnej množiny, ale nie je to jediný rozhodujúci faktor – je potrebné zohľadniť aj chovanie subjektu. Môžeme mať napr. anonymitnú množinu veľkosti 100, ale len 5 užívateľov z nich posiela správy hromadne a pravidelne
- Kvalitatívna – odolnosť voči útokom

Cena za anonymnú komunikáciu = zvyšovanie latencie. V prípade mixov veľmi výrazné, v prípade Onion routingu (kde nastáva voľba ciest tak, aby sa prešlo čo najmenej uzlov) menej výrazné.

Anonymitné systémy sú náchylné na **útoky typu traffic analysis**: pasívny útok, útočník sa snaží zistiť, kto s kým komunikuje (tzn. medzi ktorými dvoma uzlami prechádzajú správy). Podľa toho profiluje účastníkov. Ochrana: posielanie falošných správ v sieti, ktoré sú neodlíšiteľné od skutočných.

Keďže Internetová komuikácia je vysledovateľná a dáta sú zviazané s ich odosielateľom, je vhodné používať **mixy** – menia tok a výskyt dát na komunikačnom kanáli. Vstupy nie je možné jednoducho spojiť s výstupmi. Obsah správ je šifrovaný, ale nie kvôli tomu, že odosielateľ chce skryť obsah správy, ale aby bola daná správa nerozlíšiteľná od ostatných.

- **Anonymný email** využíva remailer alebo *broadcast* – zašifrovaná správa sa pošle všetkým na sieti, ale len pravý príjemca má kľúč na dešifrovanie
- Prvý návrh mixovacích systémov: David Chaum – threshold mix (1981)
- **Pool mix** má vnútornú pamäť – správy spracováva v dávkach. Každá má nastavený nejaký príznak, ktorý keď klesne na 0, správa bude uvoľnená z pamäte a odoslaná príjemcovi
- **Continuous (stop – and - go) mix** – správy sú po istý čas pozastavené v mixe pred ich ďalším odoslaním

Mixy sa často spájajú do *mixovacích sietí*:

- Zapojenie ako **sieť mixov** = nereštriktívne smerovanie (užívateľ sám volí cestu)
- Zapojenie ako **kaskáda mixov** = reštriktívne smerovanie (užívateľ si nemôže vyberať cestu)
- Hybridné zapojenie

Iný systém: **PRIME projekt** – cieľom je navrhnúť prostredie, kde užívatelia majú kontrolu nad šírením informácií o sebe. Keď si objednávame niečo z eshopu, nemôžeme si byť istí, ako je zabezpečená komunikácia s obchodníkom, na čo bude ďalej využívať osobné dáta, komu ich ďalej poskytne atď.

Používa PRIME toolbox – tvorba a použitie rôznych digitálnych identít, kde každá má pridružené atribúty (na túto emailovú adresu nechcem dostávať reklamy, požadujem len jedného overovateľa transakcie kreditnou kartou atď.) – užívateľ sám definuje, s čím súhlasí – zabraňuje sa tomu, že len odklikne nezmyslené obchodné podmienky, ktoré si ani neprečíta.

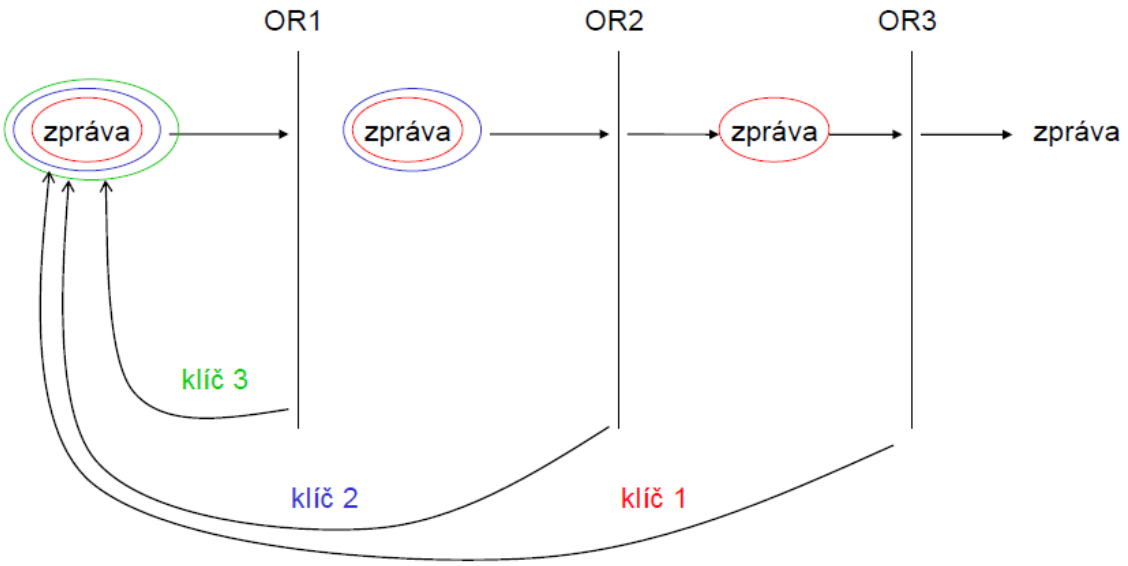
Podporuje tiež *private credentials* – hlavný „certifikát“ subjektu, ktorý obsahuje osobné informácie a funguje ako napr. občiansky preukaz. Pri nákupe tovaru, na ktorý je nutné mať viac ako 18 rokov poskytuje potvrdenie obchodníkovi, pričom nemusí vedieť presný vek. PRIME projekt má tiež snahu minimalizovať množstvo poskytovaných dát.

Ochrana realizácie bezhotovostných platieb: **3D-secure system** – validitu platobnej karty overuje priamo banka, nie obchodník – ten je len informovaný o úspešne vykonanej transakcii.

Lekcia 12 – anonymitná komunikácia v praxi

Mixminion (www.mixminion.net) – mixovacia sieť pre odosielanie anonymných emailových správ (remailer). Užívateľ *má možnosť špecifikovať cestu v sieti*. Aby bolo možné na anonymnú správu odpovedať, používa sa SURB – Single Use Reply Block – zašifrovaná dátová štruktúra, ktorá obsahuje informácie o spiatočnej ceste a je pripojená k správe (je to vlastne jednorázový „odpovedný lístok“, ktorého platnosť je časovo obmedzená). Odpoveď je v sieti nerozlíšiteľná od normálnej správy.

Onion Routing je súhrnný názov pre systémy, ktoré poskytujú anonymnú komunikáciu vo verejnej sieti. Poskytuje obojsmerné anonymné spojenie pre rôzne služby/protokoly (www, ssh, ftp, ...), pričom tieto služby nie je nutné modifikovať – pracuje ako proxy. Ďalšia výhoda oproti mixom: Onion Routing pracuje takmer real-time, takže latencia je minimálna.



Dáta sú spracované cez sériu *Onion Routerov* namiesto priameho spojenia klient/server. Onion Routre komunikujú cez **symetricky** zašifrované spojenie. Samotné dáta sú šifrované **asymetricky** (onion routre sťahujú verejný kľúče z InfoService – adresárový server), pričom každý OR odstráni vrstvu paketov dešifrovaním. Dáta sú dôsledkom dešifrovania na každom OR „zmenené“.

Každý OR pozná len svojho predchodcu a nasledovníka a ukladá si zoznam preposlaných paketov. K OR sieti sa pristupuje cez proxy, ktoré transformuje dáta do podoby zrozumiteľnej pre OR sieť.

TOR – **The Onion Routing** je Onion Routing systém druhej generácie. Prináša tieto vylepšenia:

- Perfect forward secrecy – session kľúče nie sú ohrozené, pokiaľ by došlo k vyzradeniu hlavného kľúča
- Nie je nutné vyvíjať špecializované aplikačné proxy (podpora väčšiny TCP-based aplikácií bez modifikácie) a nevyžaduje zmeny v jadre OS

- Dáta môžu opustiť sieť v ľubovoľnom mieste (v OR boli len niektoré uzly „exit nodes“)
- Testovanie **integrity** prenesených dát (ochrana proti tagging útokom)
- **Skryté služby** – server je anonymný - *skrytý* za niekoľkými OR a môže *riadiť prichádzajúci dátový tok* tým, že bude akceptovať komunikáciu len z istých OR (ochrana voči útokom DoS). Príklad: server XY komunikuje len s OR 1, 2, 3. Potom na InfoService je povedané, že XY je prístupný len cez tieto vybrané onion routre.
- Podpora adresárových serverov – info o sieti
- Voľne dostupný systém

Možné ohrozenie útokom *traffic analysis* (viz. George Danezis & Steven J. Murdoch)

Projekt AN.ON – anonymity online – poskytuje anonymitu pomocou spojenia zo serverom cez *kaskádu* mixov (resp. správnejšie **Onion Routerov**). Mixy využíva viac užívateľov naraz, niektoré sú spoplatnené. Podporuje služby HTTP, HTTPS, FTP. Použitie: cez klientskú aplikáciu JonDo – funguje ako proxy, cez ktorú sa pripája browser.

Anonymný proxy server umožňuje nepriame pripojenie na www stránku. Požiadavku od klienta spracuje proxy, predá ju serveru a následne vráti klientovi výsledok. Cieľový server spravidla vidí len komunikáciu s proxy serverom. Používa sa, keď nechceme zverejniť svoju IP adresu, ale keďže takýto anonymitný systém obsahuje len jeden prvok, môže byť ľahko kompromitovaný a anonymita nie je zaručená.

DC Net je teoretický koncept systému, ktorý zaisťuje anonymitu odosielateľa aj príjemcu. Definoval ho David Chaum. Je postavený na **probléme večeriacich kryptografov:**

Traja kryptografi sedia na večeri. Čašník im oznámi, že za večeru už niekto zaplatil. Mohol zaplatiť buď jeden z nich, alebo NSA, čo zistia nasledovne:

Každá dvojica (kryptograf a kolega vpravo) si hodí mincou tak, aby ten tretí nevidel výsledok. Potom každý vyhlási, či dve mince, ktoré vidí (jeho a kolegova vľavo) padli na rovnakú stranu alebo nie.

Ak platil kryptograf, bude klamať a povie opak toho, čo vidí. Párny počet rozdielov značí, že platila NSA, nepárny počet rozdielov značí, že platil jeden z kryptografov, pričom neplatiaci sa nemá šancu dozvedieť, ktorý zo zvyšných dvoch to bol.

Inak vyjadrené: