02 Informační bezpečnost (2.5h)

tags: `#sss-základ, bezpečnost`

> Informační bezpečnost. Audit, řízení bezpečnosti, řízení rizik, protiopatření. Hodnocení bezpečnosti, hodnotící kritéria a procesy. Standardy v IT bezpečnosti a kryptografie, legislativa týkající se kryptologie. Digitální podpis - konstrukce, legislativa, správa veřejných klíčů, certifikační autority a infrastruktura veřejného klíče. Autentizace uživatelů v počítačových systémech - tajné informace, tokeny, biometrie. Identifikační systémy a správa identit. (PA018, PV079, PV157)

Základní pojmy

- **Anonymita** (Anonymity) - Anonymita je vlastnost systému, který zajišťuje možnost použití zdrojů nebo služeb bez zjištění identity uživatele tohoto systému.
- **Pseudonymita** (Pseudonymity) - Vlastnost systému, který zajišťuje možnost použití zdrojů nebo služeb bez zjištění identity uživatele tohoto systému tak, že uživatel je stále zodpovědný za toto použití. Určitá podobnost existuje s poštovními přihrádkami (PO Box).
  - Pseudonymita je např. přezdívka ve hře
- **Nespojitost** - 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.
- **Nepozorovatelnost** - Vlastnost systému, který zajišťuje možnost použití zdrojů nebo služeb tak, že ostatní nemohou zpozorovat používání daného zdroje nebo služeb.
- **Autentizace** - proces ověření (a tím i ustavení) identity (s požadovanou mírou záruky).
  - Autentizace probíhá např. při zadání jména a hesla
- **Autorizace** - udělení určitých práv a určení povolených aktivit.
  - Po autentizaci nastává autorizace - např. se přihlásíte jako admin a systém vám udělí práva.
- **Identifikace** - rozpoznání určité entity (systémem) v dané množině entit.
- **Integrita dat** - data nebyla neautorizovaně změněna (vložení dat, smazání dat, přeskupení dat…) od doby vytvoření, přenosu…
- **Autentizace původu dat** - potvrzujeme, že data pocházejí od určitého subjektu.
- **Aktiva** - data, fyzická zařízení, a další. Jsou to zdroje s hodnotou, něco, co má neopominutelnou hodnotu.
- **Škoda** - důsledek útoku na aktiva nebo na hodnotu aktiv.
  - může být zanedbatelná, akceptovatelná, významná, katastrofická…
- **Zranitelnost** - slabé místo v systému
  - Nezapatchovaný systém
  - Server veřejně přístupný z internetu se slabým heslem
- **Zranitelné místo** – slabina v návrhu, implementaci, provozu,… systému, který pracuje s aktivy
- **Hrozba** - akce/událost, která může ohrozit bezpečnost - potenciální využití zranitelnosti systému, který pracuje s aktivy, a díky existenci útočníků
  - **Zranitelnost** (systému) + **útočník** = **hrozba**
- **Riziko** - pravděpodobnost uplatnění hrozby
  - 2 aspekty - pravděpodobnost a výše škody: zanedbatelné, akceptovatelné, významné, katastrofické…
- **Útok** - realizace hrozby, akt využití zranitelnosti, může být úspěšný (dopad na hodnotu aktiv) či neúspěšný
- **Bezpečnost** – zamezení škodám eliminací zranitelných míst nebo útočníků pomocí bezpečnostních opatření
- **Opatření** – bezpečnostní služba (opatření) relevantní jisté hrozbě, která riziko dané existencí této hrozby odstraňuje nebo alespoň snižuje
  - Cena musí být menší než výše případné škody (např ISO 27002)
    - Pokud máme ve firmě 2 počítače a identifikujeme jako riziko například

ransomware a opatření by stálo 2 miliony, tak to nemá cenu, protože reinstalace 2 počítačů nás bude stát mnohem méně.
    - Technická, řídící, provozní
    - jiné dělení: preventivní (řízení přístupu), detekční (audit, detekce virů…)
- **Mechanismus** – metoda/technologie zajištění ochrany, například kryptografie, ACL, digitální podpisy apod., ale také procedury nebo chování

Zdroje: https://docs.google.com/document/d/1rXRimrxC-g0Wy-Awc5OZHRp14TO6Dk-IEGIMv6ZpEpM/ http://statnice.dqd.cz/mgr-szz:in-bit:7-bit

Audit, security management, risk management, countermeasures.

(Audit, řízení bezpečnosti, řízení rizik, protiopatření.)

Audit

Bezpečnostní audit je nezávislé posouzení stavu bezpečnosti v organizaci. Cíle a rozsah auditu mohou být různé. Audit posuzuje, zda procesy a opatření definované v bezpečnostní politice jsou správně implementovány a používány. Upozorňuje na možné zranitelnosti systému, které by mohly vést k ohrožení (= existence hrozeb). Také upozorňuje na nedostatečnost ochrany ve vztahu k novým poznatkům v oblasti bezpečnosti informačních a komunikačních technologií ve vztahu k uznávaným standardům. Audit bezpečnostních politik (opatření) má dvě části: 1. formální posouzení materiálů bezpečnostní politiky, 2. kontrola správnosti implementace stanovené bezpečnostní politikou.

Audit ISMS (Information Security Management System (ISMS) audits set the standard): * Např. podle ISO/IEC 27007 * Organizace by měla pravidelně kontrolovat a přezkoumávat zda má řádně instalovány a provozovány implementace bezpečnostních standardů, politik a předpisů formou auditu. * Metody: * Vyšetřování (analýza objektů, procesů, mechanismů) - cílené, všeobecné, detailní * Test(provoz testovaného objektu za daných cvičných podmínek) - např. test zálohování * Whitebox - znám vnitřní strukturu * Blackbox - neznám strukturu, test z venku * Greybox - kombinace * Interview (rozhovory s jednotlivci) - všeobecné, cílené, detailní * Příprava auditu - výsledky posledních auditů, seznámení se systémem, vyžádání materiálů od správců … * Vypracování plánu auditu - oblast zkoumání, jakou procedurou, jaké budou výstupy, * Výstup auditu - typicky rozděleno do závažností (např. velmi závažné = narušení bezpečnosti, doporučeno okamžitě odstranit)

Řízení bezpečnosti

Řízení bezpečnosti musí v organizaci fungovat jako součást celkového systému řízení organizace. Systém řízení bezpečnosti musí být přiměřený a šitý na míru konkrétní organizaci (politiky a procesy musí odrážet styl a kulturu organizace, přijaté politiky a procesy musí odrážet výsledky ohodnocení rizik). Technologie budování systému řízení bezpečnosti je definována standardy.

Ohodnocení rizik –> zvládnutí rizik –> implementace a prosazení politiky –> návrh a implementace ISMS (Information Security Management System).

ISO/IEC 27002 je standard, který dává cca 130 nástrojů (opatření) pro řízení bezpečnosti informací. Jako vstup k řízení bezpečnosti informací je vyžadováno následující: * vypracovaná BP (Bezp. Politika) * management na všech úrovních prosazuje BP * má být implementován měřící systém

ISMS je systém procesů, které zajišťují ustavení, zavádění, provozování/prosazování, monitorování, přezkoumávání, udržování a zlepšování bezpečnosti informací.

Řízení rizik

Jako **řízení rizik** jsou označovány procesy vedoucí k redukci rizik na akceptovatelnou úroveň. Cílem je ideálně plně eliminovat všechna rizika, racionálně pak snížit rizika na

přijatelnou úroveň. Toho je možné dosáhnout snížením pravděpodobnosti uplatnění hrozeb pomocí opatření, která omezují dostupnost zranitelných míst, snižují počet útočníků a podobně.

Řízení rizik např. (ISO/IEC 27005) zpravidla zahrnuje tyto procesy: * ohodnocení rizik (**risk assessment**) se skládá z: * analýza rizik (**risk analysis**) * vyhodnocení rizik (**risk evaluation**) * zvládání(zmírnění) rizik (**risk mitigation**) - výběr a implementace opatření snižující rizika * akceptace rizik (**risk acceptance**) – rozhodování o přijatelnosti rizik dle stanovených kritérií * informování o rizicích (**risk communication**) – sdělení informace všem, kdo mohou rizika ovlivnit nebo být jimi ovlivněni

Ohodnocení rizik je systematické zkoumání aktiv, hrozeb, možných útočníků. Jedná se o formální přesně definovaný proces. Existují nástroje pro vedení procesu ohodnocování rizik, například CRAMM. Cílem je dosáhnout vyrovnanosti časových a finančních nákladů na ochranu a provoz, potřebné přesnosti při odhadech rizik a potřebných vědomostí pro volbu opatření pro zvládnutí rizik. Výstupem bývá tabulka s aktivy, hrozbami a mírami rizika (malé, velké, střední,…).

Prvním krokem je orientační ohodnocení rizik. Typicky je to součástí tvorby Deklarace politiky. Výsledkem je rozhodnutí o volbě jedné z metodologií ohodnocení rizik (elementární, neformální, detailní):

- *Elementární* ohodnocení rizik je převzetí opatření na základě analogie podobných systémů a ze všeobecných standardů.
- *Neformální* ohodnocení rizik je ohodnocení rizik na základě znalostí jednotlivců – odborníků na bezpečnost (interních nebo externích) bez použití standardních strukturovaných metod a nástrojů.
- *Detailní* (formální) ohodnocení rizik je ohodnocení standardními strukturovanými metodami a nástroji ve všech fázích (identifikace aktiv, identifikace zranitelných míst, …).
- *Kombinované* ohodnocení rizik kombinace předchozích přístupů, jak kde je to nutné (včetně ekonomických hledisek).

Forma **analýzy rizik** je buď kvantitativní nebo kvalitativní. - **Kvantitativní analýza rizik** je založena na součinech pravděpodobností útoků a numerických výší škod. Výsledky jsou bezprostředně použitelné pro analýzu přínosů doporučených opatření. Znalosti pravděpodobností jsou vesměs nepřesné a hodnocení výše škod je často subjektivní. - **Kvalitativní analýza rizik** využívá škály odhadovaných potenciálních škod a odhadovaných frekvencí výskytů útoků. Nepoužívá numerické vyjádření pravděpodobností nebo výší škod, získají se tak hodnoty rizik, které určí oblasti, které by měly mít prioritu při řešení rizik. Výsledky jsou vesměs nepoužitelné pro analýzu přínosů doporučených opatření.

Základní kroky procesu ohodnocení rizik: 1. charakteristika systému 2. identifikace hrozeb 3. identifikace zranitelností 4. analýza opatření – sem patří bezpečnostní politika (definuje opatření) 5. určení pravděpodobnosti 6. analýza dopadů 7. vyhodnocení rizik 8. doporučení opatření, prohlášení o aplikovatelnosti 9. dokumentování výsledků ohodnocení rizik

Zvládání(zmírnění) rizik: usilování o dostatečné snížení rizik za nejmenší možnou cenu. Preventivní opatření se přijímají většinou pro velká rizika, pro menší rizika pouze nápravná opatření. U nejmenších rizik je možné riziko prostě akceptovat nebo se proti němu pojistit. Výstup je implementace opatření.

Protiopatření

Bezpečnostní politika (BP) je soubor pravidel specifikující účinný způsob uplatňování **opatření** (implementované adekvátními mechanismy) potřebných pro dosažení požadované úrovně akceptovatelných rizik.

BP říká: * co se chrání, proti čemu/komu – bezpečnostní cíle * jak se ochrana uplatňuje – způsob dosažení bezpečnostních cílů

Detailnost BP závisí na cílové oblasti, ve které je politika uplatňovaná. Bezpečnostní politika je důvěryhodná, pokud se jejím dodržováním prokazatelně dosáhne požadované úrovně ochrany aktiv. Důvěryhodná BP musí jednoznačně stanovovat/popisovat stavy systému a

správně zvládat reakce na bezpečnostní incidenty podle jednoznačně stanovených požadavků na bezpečnost.

Na úroveň důvěryhodnosti lze dát záruku (audit, certifikace). Ale jen jestli je dobře specifikována, navržena a implementována.

Jednoduchý příklad aplikace Bezpečnostní politiky *Politika*: Je zakázáno opisovat domácí úkoly ať s vědomím či nevědomím autora originálu. *Cíl*: Nikdo nevlastní kopii DÚ jiného studenta *Porušení politiky:* Alice si neochrání svůj DÚ na sdíleném disku ve škole. Bob úlohu opíše. Kdo se choval v rozporu s bezpečnostní politikou? Bob. Politika totiž nepožaduje, aby DÚ byly chráněny před opsáním, pouze vyžaduje, aby úkoly nebyly opisovány.

Stěžejním pojmem je **opatření**. Typické opatření je kombinací technologie, chování a procedury: - např.: antivirový program + pravidelné aktualizace + vyškolení personálu pro bezpečnou práci s emailovými přílohami - Nejlepší praktiky, pro volbu opatření je standard ISO 27002. Pokud je riziko nízké (zanedbatelná pravděpodobnost a dopad), tak se pravděpodobně pouze pojistíme. Při vysokém riziku (katastrofický dopad hraničící s jistotou) vytvoříme plán, abychom takové riziko eliminovali.

Perfektní bezpečnost je dosažena absolutní eliminací všech rizik. Často jsou známá teoretická řešení, která jsou prakticky nepoužitelná. BP lze dále zúžit. Jedním zúžením je **Politika bezpečnosti informací (ITSP - IT Security Policy)**, která se obvykle se zavádí v přirozeném jazyce a chrání informační aktiva. Stanovuje se obvykle na 5-10 let a je nezávislá na konkrétním IT vybavení. Zúžením ITSP je BP systému zpracování informací. Tu definuje **ISO/IEC 27000 - Plán zvládání rizik** a určuje způsob zabezpečení dat v dané organizaci.

Návrh a tvorba BP Návrh a tvorba BP je iterativní proces. Finální verze musí odrážet výsledek ohodnocení rizik. BP musí respektovat charakteristiky činností, lokalit a aktiv organizace a technologií pro zpracování informací. BP definuje systém stanovení cílů a strategií řízení organizace a rizik. Stanovuje kritéria pro evaluaci rizik a strukturu procesu hodnocení rizik. BP musí být schválena vedením organizace, pravidelně přezkoumávána, případně podle potřeby aktualizována.

Deklarace politiky je krátký dokument, který odpovídá na otázky: * pro koho je politika závazná * Jestli pro všechny zaměstance, nebo jen pro administrátory * vymezení oblasti působnosti politiky * co tato politika chrání * důvod, proč se zavádí (vyjádření podstaty hrozeb,…)

Následuje určení metodiky řízení rizik, kritérií pro hodnocení rizik, struktury procesu hodnocení rizik a stanovení zodpovědnosti.

- Dále musejí být identifikovány požadavky na soubory opatření, které zajišťují vyhovění politice:
  - plán reakcí na incidenty
  - plán zachování činností
  - plán zálohování dat
  - ochrana před viry
  - politika řízení přístupu, hlášení bezpečnostních incidentů,…

Odhad ceny vybudování systému pro řízení bezpečnosti (ISMS – Information Security Management System), hodnocení a kvantifikace potenciálních zisků, návrh plánu implementace a stanovení odpovědnosti za implementaci.

Prosazování BP Prosazování bezpečnostní politiky je cyklický proces, který se skládá z následujících kroků: 1. posouzení vstupních vlivů, vypracování Deklarace politiky 2. provedení ohodnocení rizik – analýza rizik a vyhodnocení rizik s cílem dosažení: * vyrovnanosti časových a finančních nákladů na ochrany a provoz * potřebné přesnosti při odhadech rizik * potřebných vědomostí pro volbu opatření pro zvládnutí rizik, to je pro vypracování Prohlášení o aplikovatelnosti opatření 3. vypracování projektu politiky – zvládnutí rizik rozhodnutím o použitých opatřeních, připravení Plánu zvládnutí rizik (detailní politika bezpečnosti systému) 4. implementace a prosazení politiky, návrh a implementace ISMS 5. plnění činnosti organizace pod kuratelou prosazené politiky a ISMS 6. vyhodnocování adekvátnosti politiky 7. ohodnocení rizik (bod 2) a běží nové kolo životního cyklu péče o bezpečnost (informací)

Role V rámci řízení bezpečnosti v organizaci jsou chápány následující role: * Správní rada * nejvyšší management * výkonný management * řídící výbor (pokud není ustaven, tak samostatný bezpečnostní architekt) * CISO (Chief of Information Security Officer) * lokální správci, administrátoři systémů, auditoři

Správní rada požaduje soulad strategií organizace (pomocí auditní zprávy)

Výkonný management definuje procesy nutné k propojení bezpečnosti informací a cílů organizace, zajišťuje odpovědnosti při řízení rizik.

Řídící výbor je ustanovený nejvyšším managementem organizace z členů napříč funkční strukturou organizace. Řídící výbor přezkoumává a podporuje strategie bezpečnosti informací a usiluje o integraci, zajišťuje, aby management podporoval integraci bezpečnosti do strategií organizace. Stanovuje cíle bezpečnosti informací, posuzuje a schvaluje bezpečnostní politiku, vymezuje oblast působení ISMS. V podstatě je to dohlížecí orgán.

CISO je většinou jmenován řídícím výborem. Vytváří bezpečnostní politiku (společně s řídícím výborem), určuje její cíle a strategie a stanovuje oblast působení. Instruuje řídící výbor o aktuálních hrozbách, zranitelnostech a adekvátních krocích k jejich eliminaci. Provádí iniciální posouzení rizik, identifikuje změny rizik a zajišťuje odpovídající reakce. Zajišťuje, že vrcholový management a řídící výbor odsouhlasuje rizika a přístup organizace k řízení rizik, plán zvládání rizik a nutnou úroveň záruky za bezpečnost. Pro jednotlivé cíle vybírá opatření a kontroluje, aby tyto cíle byly implementací opatření dosaženy. Vypracovává zprávy o bezpečnostních incidentech a řídí reakce na ně, včetně prokázání jejich příčin a určení a zajištění adekvátních opravných a/nebo preventivních akcí. Informuje řídící výbor o postupu implementace ISMS, o incidentech, problémech a bezpečnostních záležitostech.

Lokální správci odpovídají za identifikaci hrozeb a hodnocení rizik v systémech, které spravují, například systémy, sítě, areály,… Odpovídají za implementaci vybraných opatření, testování plánů zachování činností (obnova sítě, udržování činnosti v areálu,…).

Uživatelé IT musí znát a dodržovat politiku bezpečnosti informací v organizaci.

Zdroje: https://docs.google.com/document/d/1rXRimrxC-g0Wy-Awc5OZHRp14TO6Dk-IEGIMv6ZpEpM/ http://statnice.dqd.cz/mgr-szz:in-bit:7-bit

Safety evaluation, evaluation criteria and processes.

(Hodnocení bezpečnosti, hodnotící kritéria a procesy)

Hodnocení bezpečnosti se provádí, aby se zjistila dosažená úroveň bezpečnosti. K hodnocení bezpečnosti je využíván standard Common Criteria (ISO/IEC 15408) a kritéria OWASP (Open Web Application Security Project).

Hodnotící kritéria podporují vyslovení záruky, že následující procesy byly vedené přísným a standardním způsobem * specifikace informační bezpečnosti TOE (target of evaluation = produkt/systém), * implementace informační bezpečnosti TOE * vlastní hodnocení informační bezpečnosti TOE

Hodnotící kritéria - seznam podmínek, které vyvíjený/kupovaný produkt nebo systém má být schopný (musí) splnit, resp. kterým musí vyhovět.

Metodologie hodnocení - způsob provedení hodnocení zda hodnocený produkt/systém vyhovuje stanoveným kritériím. Určuje ji autorita (např. EU, stát).

Kdo standard hodnotících kritérií IT bezpečnosti využívá? * **Zákazník** - může udat požadavky na informační bezpečnost požadovaného produktu/systému a žádanou sílu záruky za jejich validnost. Výsledky hodnocení jsou mu sděleny. * **Výrobce** - může specifikovat bezpečnostní vlastnosti nabízeného produktu/systému, má nějaký bezpečnostní cíl, který může vyhovovat zákazníkovým představám. * **Hodnotitel** může hodnotit, zda daný TOE má deklarované vlastnosti, zda vyhovuje požadavkům zákazníka, hodnocení se vesměs řeší jako zakázková činnost, může mít **certifikát** potvrzený **autoritou pro hodnocení informační bezpečnosti**, na základě hodnotitelské zprávy TOE

může vydat certifikát potvrzující záruku bezpečnosti TOE **certifikační autorita**.

Vyslovení záruky bezpečnosti informací v TOE (produktu/systému)

Cíl hodnocení z pohledu bezpečnosti informací: * vyslovení úrovně záruky, s jakou lze garantovat, že TOE zajišťuje (deklarovanou) informační bezpečnost * použitá hodnotící kritéria proto musí definovat míru záruky * Security Assurance Requirements (SAR) - vyjadřují míru jistoty, že produkt/systém splňuje funkční požadavky * míra záruky musí být vyjádřena vhodnými stupni (úrovněmi) * Obecně: nízká, střední, vysoká * Podle CC (Common criteria) EAL1 až EAL7 (Evaluation Assurance Level), kde EAL1 je nejnižší úroveň. * EALi = úroveň záruky za dosaženou kvalitu informační bezpečnosti * Každá úroveň definuje množinu SARs, které mají být naplněny

Pro dosažení cíle hodnocení - tj. pro vyslovení záruky za dosaženou kvalitu informační bezpečnosti se musí prokázat, že zavedená bezpečnostní opatření * mají správnou funkčnost - poskytují ochranu proti všem relevantním hrozbám * jsou efektivní - účinně zabraňují hrozbám, kvůli kterým byly zavedeny * hloubka a důkladnost procedur ověření obou těchto vlastností jsou dané požadovanou úrovní záruky * EAL1 - ověření na základě uživatelské dokumentace * EAL7 - na precizních algebraicko-logických modelech

Produkt, systém, předmět hodnocení (TOE) * Hodnocení produktu * obtížně se posuzuje efektivnost bezpečnostních rysů (není známé prostředí, ve kterém bude produkt provozovaný, není jasné, co bude konkrétní uživatel od produktu vyžadovat) * Hodnocení systému * požadavky na efektivnost bezpečnostních rysů systému bývají zřejmé * jejich vyslovení je ale složitý a technický proces

Přínosy a problémy hodnocení * Provedení hodnocení může produktu otevřít cestu na nové trhy * Bývá to dobrý reklamní nástroj * Hodnocení může odstranit starost, zda výrobek obstojí na trhu * Jakákoliv změna TOE hodnocení znehodnocuje až anuluje * Pokud nějak pozměním TOE (samotný produkt) * Uživatel, který není expertem v hodnocení bezpečnosti nemusí plně rozumět zárukám z výsledků hodnocení a nemusí být schopen zadat požadavky na hodnocení.

Kdo hradí hodnocení? * Hradí sponzor hodnocení - výrobce produktu, vlastník systému * Pokud se jedná o produkt, náklady lze rozptýlit mezi zákazníky

Metodologie hodnocení * hodnocení provádí hodnotitel, který má být dozorovaný autoritou pro hodnocení informační bezpečnosti * pro sponzora je hodnotitel důvěryhodnou 3. stranou, uzavírají smluvní vztah * hodnotitel vypracovává hodnotící zprávu, ve které píše o úrovni bezpečnosti TOE * certifikát dosažené úrovně záruky odvozené při hodnocení vydává uznávaná certifikační autorita na základě hodnotící zprávy hodnotitele * autoritou má být národní/mezinárodní instituce. Certifikační autority bývají vládní agentury (NIST) nebo licencované komerční organizace (tak se to dělá v EU).

Metody hodnocení * **investigativní hodnocení** (produktově/systémově orientované) - zkoumá se a testuje se hotový produkt/systém a jeho vlastnosti - obtížně opakovatelné * **auditní přístup** (procesně orientované) - hodnotí se dokumentace a procesy návrhu, vývoje, pořizování a provozování TOE - snadněji opakovatelné

Common Criteria (CC) K hodnocením se využívá **hodnotících kritérií** což je obecně seznam podmínek které vyvíjený/kupovaný produkt nebo systém má být schopný (musí) plnit. Common Criteria poskytují framework, který umožňuje, aby uživatel specifikoval požadavky na bezpečnost produktu, výrobce specifikoval vlastnosti produktu a nezávislý hodnotitel posoudil zda výrobek odpovídá požadavkům. Historicky se namísto Common Criteria v Evropě používali ITSEC (IT Security Evaluation Criteria) a v USA TCSEC (Trusted Computer Security Evaluation Criteria).

Tento standard se dělí do 3 částí: * Part 1: Introduction and general model * Part 2: Security functional requirements * Part 3: Security assurance requirements

CC: standard (rozsáhlý) pro hodnocení bezpečnosti systémů, umožňuje lepší srovnávání systémů i specifikaci požadované funkčnosti * s tím souvisí funkčnosti systémů pro ochranu inf. soukromí * anonymita, pseudonymita, nepozorovatelnost a nespojitelnost * existenciální pohled - vlastnost buď je, nebo není * kritéria neřeší, jak je vlastnosti dosaženo * kritéria neumožňují jiné než diskrétní (ano/ne) ohodnocení * zájem uživatelů, výrobců, hodnotitelů * profil bezpečnosti (čipové karty, biometriky atd.) * mini-

kritéria - katalogovány jako samostatný hodnotitelský dokument * popisy bezpečnostních potřeb jsou často různorodé * security target (ST) - teoretický koncept/cíl * hodnocení TOE - odpovídá realita teorii (ST)? * požadavky na funkčnost a záruky * konkrétní TOE je hodnocený proti konkrétnímu ST do určité úrovně prověření (EAL) - od 0 (nevyhovující) po 7 (formálně navržený s formálně ověřeným návrhem a testovaný TOE) * **vyšší EAL neznamená lepší bezpečnost, pouze vyšší míru prověření**

Specifikační dokument Common Criteria (CC) * **profil ochran** (protection profile, PP) * dokument typicky vytvářený uživatelem nebo nějakou uživatelskou komunitou * identifikuje požadavky na bezpečnost pro jisté prostředí (použití čipových karet pro nepopíratelnost u podepisování, síťové firewally pro řízení přístupu) * PP lze použít jako šablonu pro definici bezpečnostního cíle * **bezpečnostní cíl** (security target, ST) * dokument definující bezpečnostní vlastnosti produktu/systému, tzv. Security Functional Requirements (SFRs) * specifikace bezpečnostních funkcí poskytovaných produktem * součástí CC je standardní katalog těchto funkcí * SFR může definovat, jak se má konkrétní role autentizovat * produkt/systém se hodnotí, jak splňuje zadaný ST * lze rovněž hodnotit ST, zda vyhovuje zadanému PP * obsahuje popisy bezpečnostních problémů řešených pomocí TOE a provozního prostředí TOE

Common Criteria, hodnocení produktu a PP * **Hodnocení TOE** typicky sestává ze 2 kroků * hodnocení ST, o kterém TOE sděluje, že ho splňuje, zda problém řešený produktem je problémem, který je potřeba řešit * vlastní hodnocení TOE proti tomuto ST, zda TOE splňuje úroveň zaručitelnosti definované v ST * **Hodnocení PP** * probíhá před formální deklarací PP relevantní autoritou odpovědnou za bezpečnost IT * cílem hodnocení je získat jistoty, že PP správně identifikuje požadavky na bezpečnost

Jak CC používají … * **Zadavatelé vývoje:** Jako specifikace bezpečnostních požadavků na TOE (Target of Evaluation - produkt) PP. Tedy generické požadavky na bezpečnostní rysy produktu. * **Vývojáři:** Pomocí dokumentu ST definují bezpečnostní vlastnosti produktu * **Hodnotitelé:** Používají PP a ST jako měřítko míry, jestli TOE vyhovuje dané bezpečnosti * **Zákazníci:** (při vypsání výběrového řízení, VŘ) - vyhledá/vypracuje profil ochrany, který splňuje jeho požadavky a použije ho při specifikaci objednávky, vypsání VŘ * **Uživatelská sdružení, resorty:** (zdravotnictví, státní správa) - definují pomocí CC profily ochran, které specifikují společné požadavky na bezpečnost

Následují další poznatky z PV080 (mozno nepotrebne)

Pojmy * **Akreditace** - oficiální souhlas (pověření) s prováděním určité činnosti * **Certifikace** - vydání daného osvědčení na základě provedeného hodnocení * **Hodnocení** (evaluace) - ověření shody deklarovaných vlastností (dle kritérií) * **Validace** - ověření platnosti/souladu, v US terminologii "hodnocení", viz výše

Důležité pojmy z CC * **Předmět hodnocení** (TOE - target of evaluation) - produkt nebo systém (nebo jeho část), který je předmětem hodnocení * Např. smartcard a implementace šifrovacích protokolů * **Specifikace bezpečnosti** (ST - security target) - cílová kombinace komponent spojených s konkrétním produktem nebo systémem * Např. že smartcard je tamper-resistant * **Profil bezpečnosti** (PP - protection profile) - implementačně nezávislá skupina bezpečnostních požadavků určité skupiny TOE * Např. použití čipových karet pro nepopíratelnost u podepisování

Význam a výhody kritérií * usnadňují nasazení a používání bezpečných systémů – jednodušší srovnávání a výběr podle skutečných potřeb * usnadňují specifikaci požadavků * ujasňují požadavky na návrh a vývoj

Organizační bezpečnostní kritéria * jednoznačné přiřazení odpovědnosti * průběžná podpora * schopnost reakce na incidenty * periodické prověrky bezpečnostních kontrol * prověřování zaměstnanců * analýza rizik * bezpečnostní a technická školení * rozdělení pravomocí a odpovědností * systém schvalování a autorizací * bezpečnostní plán

Provozní bezpečnostní kritéria (aktivity, které se týkají běhu firmy) * kontrola možného znečištění vzduchu (kouř, prach, chemické látky) * kontroly zajišťující stabilitu dodávky elektrické energie * přístup k datovým médiím a metody jejich likvidace * externí distribuce dat a jejich označování * fyzická ochrana objektů (např. výpočetního střediska, kanceláří) * kontroly vlhkosti * kontroly teploty * zabezpečení pracovních stanic, notebooků a počítačů

Technická bezpečnostní kritéria * ochrana komunikací (např. vzdálený přístup, propojení systémů, routery) * šifrování * kontrola přístupu * identifikace a autentizace * detekce průniku * systémový audit

OWASP The Open Web Application Security Project má být nástrojem pro měření úrovně bezpečnosti webových aplikací. Bezpečnostní kritéria podle OWASP se dělí na základní kritéria a rozšiřující kritéria (která zaručují vyšší stupeň úroveň ochrany). Dále se každé kritérium ohodnocuje podle úroveň záruk za bezpečnost a to do těchto kategorií: * Vysoká záruka - dané bezpečnostní opatření byly prokázané manuální kontrolou zdrojového kódu aplikace * Střední záruka - dané bezpečnostní opatření byly prokázané manuální kontrolou funkcionality dané aplikace * Nízká záruka - dané bezpečnostní opatření byly prokázané automatizovaným testováním kódu nebo aplikace * Velmi nízká záruka - dané bezpečnostní opatření byly prokázané analýzou návrhu aplikace * Žádná - aplikace nebyla nijak analyzována

Zdroje: https://docs.google.com/document/d/1rXRimrxC-g0Wy-Awc5OZHRp14TO6Dk-IEGIMv6ZpEpM/ http://statnice.dqd.cz/mgr-szz:in-bit:8-bit

Standards in IT security and cryptography, legislation related to cryptology.

(Standardy v IT bezpečnosti a kryptografie, legislativa týkající se kryptologie.)

Standard (neboli norma, doporučení) je úmluva o technické specifikaci, nebo o jiném podobně přesně stanoveném kritériu. Standardy se dělí na de iure (schválena uznávanou institucí) na de facto (v rámci jisté komunity, např.: RFC) a firemní (proprietární) standardy.

V různých oblastech technického života existují známé standardizační de iure organizace. Zde je výčet několika z nich: * Standardizace čehokoliv: ISO - International Organization for Standardization * Oblast elektrotechniky: IEC - International Electrotechnical Commision * Komunikace: ITU - International Telecommunications Union * V oblasti IT: ISO/IEC JTC1 - tzv. Joint Technical Committee. JTC1 zřídilo společně ISO a IEC, proto ISO/IEC :-) * V oblasti bezpečnosti IT: podvýbor SC 2 výboru ISO TC 68 * V oblasti IT komunikace: ITU-T (úzce spolupracuje s ISO/IEC JTC1)

Dále existují speciální, evropské, standardizační organizace (opět de iure): CEN (obdoba ISO), CENELEC (obdoba IEC), ETSI (obdoba ITU). Na národní úrovni existují také de iure organizace (např. ČSNI). Nicméně v IT hrají důležitou roli především ty z USA: IEEE (elektronika, elektrotechnika), NIST, ANSI (zástupce USA v organizaci ISO, věnuje se bezpečnosti v IT a především v bankovnictví).

Co se týče De Facto standardů tak nejznámější jsou organizace ISOC (internet society) a IAB (internet activities board - rada pro internetové činnosti). Dobrým příkladem De Facto standardů jsou RFC, které zpracovává IETF (internet engineering task force). IETF byla pověřena IABem. Posledním zajímavou De Facto standardizační komunitou je OWASP (Open Web Application Security Project). Jak název napovídá vydává standardy vývoje bezpečných webových aplikací.

Konkrétních standardů je samozřejmě velké množství. Nejdůležitější asi je ISMS (Information Security Management System) standard (ISO/IEC 27001:2005).

Kromě výše uvedených standardů jsou důležité i ty z kategorie firemních, příkladem je PKCS (public key cryptography standards), který je publikovaný firmou RSA Labs. * Classification of standards by publisher * Worldwide – ISO, ISO/IEC, CCITT/ITU * US – ANSI, NIST * EU – CEN, CENELEC, ETSI, ECMA * Groups – IETF-RFC, IEEE * Industrial – RSA – PKCS * Basic cryptography standards * Symmetric crypto – DES, AES * Asymmetric crypto – encryption, signatures, key exchange and transfer * IEEE P1363 – Factoring-based, Discrete log based, Elliptic curve * NIST FIPS 186-3 – Digital Signature Standard * Hash functions – SHA-1, RIPEMD, (MD5), SHA-512 * Applied/Functional cryptography standards * Digital certificates – X.509, * PKCS – RSA, D-H, Certificate, Message, Private-Key, Attributes, Certificate Request, Crypto Token Interface &

Information, ECC * Security/Crypto protocols * Low level – basic standards (entity auth.) * ISO/IEC – Key Management 11770, Non-rep. 13888 * IETF (Internet Engineering Task Force) – PKIX, IPSEC, S/MIME * PKCS - norma vyvinutá formou RSA Security pro snadné používání kryptografie s veřejnými klíči (často definovány i v RFC) * PKCS#1 - RSA šifra * PKCS#3 - Diffie Hellman * PKCS#5 - symetrické šifry * PKCS#7 - syntaxe kryptografických zpráv - CMS, S/MIME apod. * PKCS#8 - formát soukromých klíčů * PKCS#10 - formát žádosti o certifikát * PKCS#11 - obecné API pro práci s crypto-tokeny * PKCS#12 - ukládání soukromých klíčů i s certifikátem, chráněno heslem * PKCS#13 - kryptografie nad eliptickými křivkami * ISO 27k – BS7799 * Code of Practice for Information Security Management – 1995 * Specification for Information Security Management Systems – 1998 * Update of both in 1999 * ISO/IEC standard 17799 * ISO/IEC 27000 series * ISO/IEC 27001 replaces ISO/IEC 17799 * ISO/IEC 9798-1:2010 Information technology – Security techniques – Entity authentication * Part 3: * Unilateral auth. * One-pass – signed sequence number or timestamp * Two-pass – challenge-response (random number) * Mutual auth. * Two-pass – signed sequence numbers or timestamps * Three-pass – challenge-response (random number) * Two-pass parallel – two unilateral two-pass protocols * ISO/IEC 11770-1:2010 Information technology – Security techniques – Key management * Part 1: Key management framework * Part 2: Mechanisms using symmetric techniques * Part 3: Mechanisms using asymmetric techniques * Secret key agreement (7 mechanisms) * Secret key transport (6 mechanisms) * Public key transport * Without a TTP (2 mechanisms) * Using a CA (1 mechanism) * https://is.muni.cz/auth/el/1433/podzim2012/PV181/um/std/Cryptographic_standards.pdf * MDx hashe v RFC * SHA hashe v NIST FIPS 180

Zdroj: http://statnice.dqd.cz/mgr-szz:in-bit:8-bit

Digital signature - construction, legislation, public key management, certification authorities and public key infrastructure.

(Digitální podpis - konstrukce, legislativa, správa veřejných klíčů, certifikační autority a infrastruktura veřejného klíče)

<ins>Digitální podpis</ins>

- **Prvek, potvrzující původ podepsaného dokumentu**
  - autenticita = integrita + prokázání původu
- je to "kus dat" - **bitová reprezentace**
- stvrzení lze prokázat i později (nepopíratelnost)
  - majitel podpisu nemůže popřít zaslání zprávy
- každý subjekt má 2 klíče:
  - **privátní (soukromý) klíč pro vytváření podpisu**
  - **veřejný klíč pro ověření podpisu**
- 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

Digitální podpis - co podepisujeme? * Algoritmy digitálního podpisu založené na asymetrické kryptografii jsou relativně pomalé. * V praxi **nepodepisujeme celý dokument** (velikosti v kB, MB i GB) ale pouze hash (kontrolní součet) (fixní délky řádově stovky bitů). * Není bezpečné rozdělit dokument na několik částí a ty podepsat separátně. * **Při kombinaci šifrování veřejným klíčem a podpisu je nutné dokument nejprve podepsat (privátním klíčem) a pak teprve zašifrovat (veřejným klíčem).**

Digitální podpis – bezpečnost * pro bezpečnou funkčnost digitálního podpisu je nezbytně nutné * **udržovat privátní klíč v tajnosti** – každý, kdo má přístup k privátnímu klíči má možnost vytvářet platné podpisy * **zajistit integritu veřejného klíče** – pokud bychom ověřovali platnost podpisu pomocí nesprávného klíče můžeme dojít k nesprávným závěrům

Digitální podpis – integrita veřejného klíče * **Jak zajistit integritu veřejného klíče?** * **Pomocí certifikátu veřejného klíče!** * Certifikát váže veřejný klíč k subjektu (spíše k

nějakému identifikátoru subjektu). * Tato vazba je digitálně podepsána důvěryhodnou třetí stranou (certifikační autoritou). * Jak zajistit integritu veřejného klíče certifikační autority? * Nezaměňovat s elektronickým podpisem! Digitální podpis je “podmnožinou” elektronického podpisu.

Pod elektronický podpis spadá například i oskenovaný ruční podpis, písmena na konci mailu napsaná na klávesnici, a pod.

Požadavky na digitální podpis * integrita * silná - data nesmí bez povolení majitele změnit svůj stav * slabá - data nesmí bez povolení majitele nepozorovaně změnit svůj stav * prokázání původu dat * ověření data/času podpisu * nepopíratelnost - pravost lze prokázat i později

Rozdíl digitálního podpisu od ručního:

Digitální podpis	Ruční podpis
vždy prováděn počítačem, nebo jiným zařízením	vždy prováděn rukou (až na padělky)
závislý na podepisovaných datech (zaručuje integritu)	nezávislý na podepisovaných datech(nezaručuje integritu)
může být vytvářen i bez vědomí uživatele (trojské koně, podepisující dokumenty bez vědomí uživatele)	

Digitální podpis (tak jako ruční podpis) nezaručuje důvěrnost - přenášená data může přečíst kdokoliv.

Technické řešení digitálního podpisu * spolehlivý asymetrický kryptografický algoritmus * nejznámějšími používanými algoritmy jsou RSA a DSA. * dvojice klíčů z nichž jeden je veřejný a druhý soukromý (utajený) * infrastruktura certifikačních autorit ověřujících pravost veřejných klíčů (PKI - Public Key Infrastructure)

Digitální podpis může být obecně * s obnovou zprávy * obsahuje v sobě přímo podepisovaný dokument * v praxi se spíše nepoužívá - asymetrické kryptografické algoritmy jsou příliš pomalé a neefektivní při použití na rozsáhlé vstupní dokumenty * bez obnovy zprávy * neobsahuje podepisovaný dokument * podepisuje se pouze hash dokumentu (standardní metoda) * digitální podpis se pak připojí ke zprávě

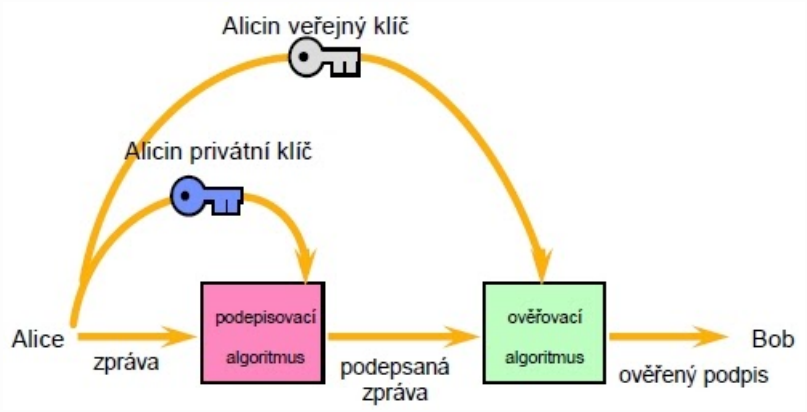
Aby Bob mohl úspěšně ověřit pravost podpisu (autenticitu - integritu + původ) musí znát veřejný klíč Alice. Aby nemohlo dojít k situaci, že Eva podstrčí Bobovi svůj vlastní veřejný klíč, musí být veřejný klíč Alice opatřen certifikátem certifikační autority (viz. PKI).

Při ověření podpisu je nejprve znovu vypočten hash zprávy. Poté je pomocí veřejného klíče autora podpisu dešifrován obsah digitálního podpisu a výsledek je porovnán s vypočteným hashem zprávy. Pokud jsou obě hodnoty hashe stejné, je podpis z matematického hlediska platný. 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.

Problémy * kompromitace soukromého klíče * je nutno okamžitě revokovat certifikát veřejného klíče u CA (CRL - certificate revocation list) * důvěryhodnost certifikační autority * co když byla kompromitována databáze CA? * co když nevěříme nikomu na světě? * časová souslednost podepsání a kompromitace soukromého klíče * pokud nastala souslednost Kompromitace -> Podepsání -> verifikace, pak si nemůžeme být jisti * pokud nastala souslednost Podepsání -> Kompromitace -> verifikace, pak by mělo být ověření podpisu ještě v pořádku * jak ale zjistíme časovou souslednost? * řeší se opět pomocí CA - při podepisování přidá CA do digitálního podpisu svou časovou značku. Lze tedy porovnat, jestli byl klíč revokován před, nebo po podepisování * viry a trojské koně můžou v případě napadení autorova systému podepisovat dokumenty bez vědomí autora (lze předcházet použitím čipových karet), a nebo autorovi podstrčit k podepsání jiný dokument, než který autor vidí na obrazovce

Digitální podpis - konstrukce

Schéma digitálního podpisu:



Každý subjekt má 2 klíče: * privátní (soukromý) klíč pro vytváření podpisu; * veřejný klíč pro ověření podpisu.

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.

V praxi se digitální podpis vytváří následujícím způsobem (protože aplikace asymetrického algoritmu na rozsáhlé datové soubory je časově značně náročná): * vytvoří se hash (kontrolní součet datového souboru), který je vlastně přesnou reprezentací (charakteristikou) dat, * hash sa 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 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. 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

Digitální podpis - legislativa

Česká legislativa (zákon 227/2000 Sb.) definuje pojmy:

Elektronický podpis * "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.

Zaručený elektronický podpis * ověřuje integritu zprávy ale ne identitu podepsané osoby (certifikát může být vydaný kýmkoliv - např. si vygeneruju vlastní klíče), je teda dost nahovno i když to z názvu není vůbec jasné. zdroj: https://www.earchiv.cz/b12/b0209001.php3 * 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

Uznávaný elektronický podpis * je zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahujícím údaje, které umožňují jednoznačnou identifikaci podepisující osoby * zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem certifikačních služeb, který je usazen mimo území České republiky, byl-li kvalifikovaný certifikát vydán v rámci služby vedené v seznamu důvěryhodných certifikačních služeb jako služba, pro jejíž poskytování je poskytovatel certifikačních služeb akreditován, nebo

jako služba, nad jejímž poskytováním je vykonáván dohled podle předpisu Evropské unie

Kvalifikovaný elektronický podpis * Je definován nařízením Evropského parlametu eIDAS * Také založen na kvalifikovaném certifikátu * Jedná se o nejvyšší úroveň elektronického podpisu * Umožňuje autentizovanou komunikaci s úřady v rámci celé EU

Elektronická pečeť * stejné jako zaručený elektronický podpis, ale podepisujícím je právnická osoba, organizační složka státu, atd., která drží prostředek pro vytváření elektronických značek a označuje datovou zprávu elektronickou značkou * pro ověření podpisu je vydáván systémový certifikát (veřejného klíče) * certifikátu k takovému podpisu se říká "systémový certifikát" * zaručený elektronický podpis a elektronická pečeť jsou technologicky totéž, jen úroveň ochrany soukromého klíče je jiná

Elektronický podpis vs. pečeť * 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). * Zákon říká, že se automaticky předpokládá, že podepisující četl, co podepsal * Elektronická pečeť * 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 správa soukromého klíče a jeho použití je jiné. Podpisem podepisující stvrzuje, že četl obsah zprávy, pečeť tuto záruku nedává.

Kvalifikovaný certifikát * Má povinná pole podle vypsaná v §12 jako například * Jméno, příjmení podepisujícího, * Jméno, příjmení nebo firma podepsaného * Unikátní číslo certifikátu. * Platnost * Omezení

Kvalifikovaný poskytovatel certifikačních služeb - Plní určité podmínky a je hlášen na ministerstvu

Akreditovaný poskytovatel certifikačních služeb * Plní podmínky a navíc získá akreditaci ministerstva * Může vydávat Zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb , který jako jediný je uznáván v komunikaci s úřady v ČR

Algoritmy pro podpisy Jaké algoritmy s jakými parametry lze používat bylo řízeno vyhláškou ÚOOÚ. Později se od toho upustilo a nyní se pouze odvolává na ETSI standardy. Např. nemohou od 2010 používat SHA-1.

Public key management

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 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 Explorerech, Navigatorech atd.).

Otázkou často je, zda ono certifikování svěříme nějaké "důvěryhodné" instituci - tzv. třetí straně, nebo zda jej provádíme přímo sami. Oba postupy mají své výhody a 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 WWW - 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 milionu.

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 prohlížeče od Microsoftu nebo Netscape.

Certifikační autorita (CA)

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 vydává certifikáty na základě požadavku od registrační autority * RA (registrační autorita) ověřuje identitu žadatele, posílá požadavek na vystavení certifikátu * Revokace – umožňuje předčasné zrušení platnosti certifikátu (pokud je náš počítač napadnutý trojanem a klíč může být zneužitý) * Vrchol stromu certifikačních autorit představuje VeriSign (pozor, těch vrcholů může být spousta. Např. česká pošta má kořenové CA atd…) * Podobu certifikátů specifikuje standard X.509

Certifikační proces probíhá v následujících krocích: * Odesílatel podepisovaného dokumentu žádá CA o digitální certifikát pro svůj veřejný klíč * CA ověřuje identitu žadatele (prostřednictvím RA) a certifikát vydává * CA ukládá certifikát do veřejně přístupného on-line repozitáře * Odesílatel podepisuje dokument svým privátním klíče a odesílá jej s připojeným certifikátem (nebo celým řetězem CA až ke kořenovému CA…) * Příjemce ověřuje digitální podpis veřejným klíčem odesílatele a požaduje ověření digitálního certifikátu v repozitáři příslušné CA (případně lokálně na disku) * Repozitář vrací zprávu o stavu odesílatelova certifikátu

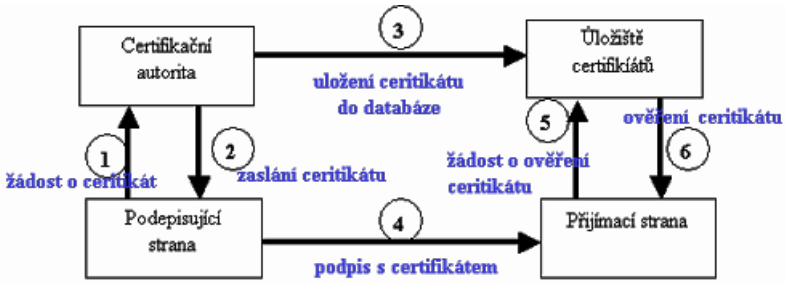
Chain of trust: https://www.youtube.com/watch?v=LPxeYtMDxl0 Asymetrická kryptografie jak z pohledu digitálního podpisu tak z pohledu šifrování: https://www.youtube.com/watch?v=GSIDS_lvRv4

Subjekt, který vydává digitální certifikáty (digitálně podepsané veřejné šifrovací klíče), čímž usnadňuje využívání PKI tak, že svojí autoritou potvrzuje pravdivost údajů, které jsou ve volně dostupném veřejném klíči uvedeny. * registrace uživatelů certifikátů * vydávání certifikátů k veřejným klíčům * odvolávání platnosti certifikátů * vytváření a zveřejňování seznamu certifikátů * vytváření a zveřejňování zneplatněných certifikátů CRL (Certificate Revocation List) * správa klíčů po dobu jejich platnosti (životního cyklu) * dodatkové služby – např. poskytování časových razítek (time-stamping)

Registrační autorita (RA) * nepovinná složka * vytváří vazbu mezi klientem a CA v souladu s popisem postupů při poskytování certifikačních služeb * přijímá žádosti o certifikace * ověřuje pravdivost uvedených údajů * předává certifikát CA k podpisu * podepsaný certifikát předá klientovi

Adresářová služba * obvykle minimálně 2 adresáře * privátní – zálohování platných klíčů a pro archivování klíčů, kterým uplynula doba platnosti (provozovanou pod bezpečnostní ochranou zajišťovanou CA) * veřejný – uchovávání a distribuce certifikátů a CRL, sklad certifikačních informací * požadavky * rozšiřitelné schéma * replikovatelnost * vysoký vyhledávací výkon

Proces vystavení certifikátu * **generování klíčových dat** – pomocí dostupného SW vybavení uživatelem, případně u poskytovatele certifikačních služeb (PCS) * **příprava identifikačních údajů** – doložení dokladů * **předání klíčových dat a identifikačních údajů PCS/RA** – žadatel předá PCS data a doklady o jejich pravosti (ne nutně ve stejný čas a stejným způsobem) * **ověření informací** – PCS si ověří, že lze vydat certifikát * **tvorba certifikátu** – CA vytvoří potřebná data, ta podepíše * **předání certifikátu** – certifikát je předán žadateli a zveřejněn

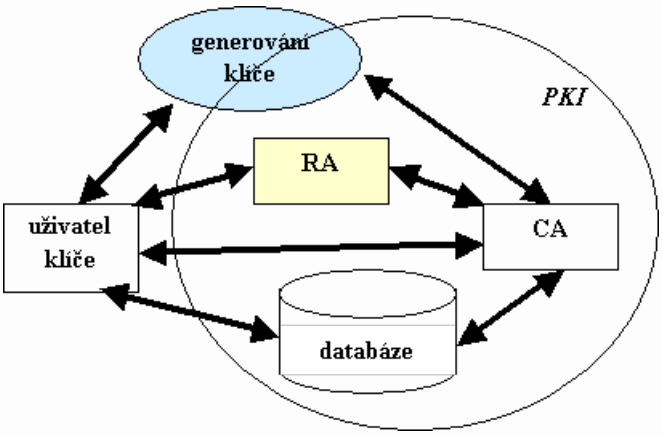


<ins>Public key infrastructure</ins>

Pomocná infrastruktura pro správu veřejných klíčů 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

PKI spojuje veřejný klíč se subjekte prostředníctvím vydání certifikátu certifikační autoritou. Její hlavní úlohou je digitálně podepsat veřejný klíč patřící danému člověku – a to pomocí vlastního privátního klíče samotné CA, takže závisí na důvěryhodnosti konkrétní autority. Tento podpis potvrzuje - certifikuje vlastnictví daného veřejného klíče.

Komponenty PKI 1. **Certifikační autorita** (CA) – poskytovatel certifikační služby, vydavatel certifikátu 2. **Registrační autorita** (RA) – registruje žadatele o vydání certifikátu a prověřuje jejich identitu 3. **Adresářová služba** – prostředek pro uchovávání a distribuci platných klíčů a seznam zneplatněných certifikátů (CRL)



Zdroje: https://docs.google.com/document/d/1rXRimrxC-g0Wy-Awc5OZHRp14TO6Dk-IEGIMv6ZpEpM/ http://statnice.dqd.cz/mgr-szz:in-bit:4-bit

User authentication in computer systems - secret information, tokens, biometrics.

(Autentizace uživatelů v počítačových systémech - tajné informace, tokeny, biometrie.)

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.

Cílem autentizace je ověřit proklamovanou identitu uživatele. Autentizační metody v zásadě dělíme do tří, resp. čtyř skupin: 1. **Na základě výlučné znalosti** (co kdo zná) * např. tajné

hesla, PIN, algoritmy atd. 2. **Podle vlastnictví specifických předmětů** (co kdo má) * např. token, magnetické a inteligentní 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(autentizace) 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.

Identifikace vs. autentizace * *Identifikace* * Určení totožnosti osoby (1:N) * "Pozitivní autentizace" * Hůře dosažitelné (malá skupina uživatelů, nízká přesnost, výjimka: sken duhovky) * *Autentizace* * Verifikace (ověření) tvrzení osoby o její totožnosti (1:1) * Jednodušší než identifikace

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“ * hash 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) * zabraňuje použití rainbow tables: * Předpočítané hashe hesel

PIN (Personal Identification Number) * 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)

„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

- „něco, co uživatel je“ (a ostatní ne)
- měřitelné biologické charakteristiky člověka - uživatele
- fyzické parametry orgánů
- chování (behaviorální) – parametry činnosti
- míra tolerance – prahová hodnota
- nesprávné odmítnutí/přijetí

Příklady biometrik * otisk prstu * vzor duhovky * vzor sítnice * srovnání obličeje * geometrie ruky * verifikace hlasu * dynamika podpisu * dynamika psaní na klávesnici * žíly na zápěstí

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: * trénovaní/nováčci * Jakou mají zkušenost s používáním biometrických systémů * úředníci/dělníci/horníci… * jejich motivace

Fyziologické charakteristiky (statické) * 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 (behaviorální charakteristiky: dynamické) * Dynamika podpisu * Hlas (dle podnětu) * Pohyby tváře * Dynamika chůze * Dynamika psaní na klávesnici

Charakteristiky * **Genotypické** – geneticky založené (např. DNA) * **Fenotypické** – ovlivněné prostředím, vývojem (např. otisk prstu)

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 stádiu vývoje (např. analýza pachů či rozmístění žil na zápěstí), avšak mnohé technologie jsou již relativně vyzrálé a komerčně dostupné (např. otisky prstů nebo systémy porovnávající 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 (psychickým stavem) jako např.

stres nebo nemoc.

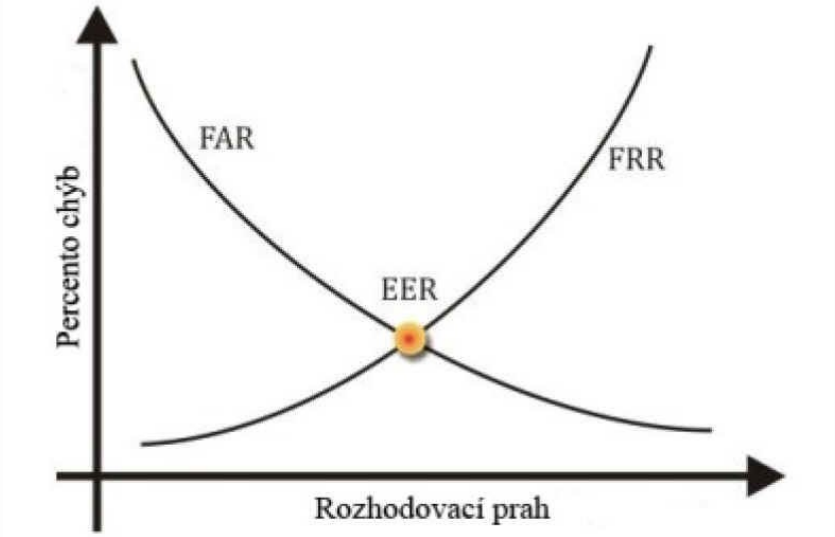
Nejvýznamnější rozdíl mezi biometrickými a tradičními technologiemi je odpověď systému na autentizační požadavek. Biometrické systémy nedávají jednoduché odpovědi typu ano/ne. Heslo buďto je 'abcd' nebo ne, magnetická karta s číslem účtu 1234 jednoduše je nebo není platná. Podpis člověka však není vždycky 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. Základní požadavek na kvalitní biometrický systém - ověření živosti (teplota, pocení, odpor, krevní tlak, absorbce světelných vln, a pod.).

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. 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) * řešením je více vstupů, když neprojde sken sítnice žádáme PIN * **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) * řešením je více-fázové ověření

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.



Čím vyšší je rozhodovací práh (nakolik musí nastat shoda), tím se snižuje **FAR**, ale zároveň zvyšuje **FRR**. Jinak řečeno, pokud budu vyžadovat 100% shodu, je mizivá šance, že neoprávněnému uživateli udělím přístup a zároveň že ho oprávněnému nepřidělím. Chceme dosáhnout **Equal Error Rate (EER)**.

Zdroje: https://docs.google.com/document/d/1rXRimrxC-g0Wy-Awc5OZHRp14TO6Dk-IEGIMv6ZpEpM/ http://statnice.dqd.cz/mgr-szz:in-bit:11-bit

Identification systems and identity management.

(Identifikační systémy a správa identit.)

(!! FYI, vypracovanim tejto podotazky si niesom vobec isty, mozno by sa to hodilo prekontrolovat. Aj ked vela veci je spomenutych uz v predoslej podotazke)

Identifikace: * 1:n * identita není známa (nutné projít celou databázi registrovaných osob) * identifikace je náročnější proces * dělení databáze (clustering)

Otisky prstů * Jedna z nejstarších metod * Získání otisku prstu: * za použití inkoustu * bez použití inkoustu * Snímače otisků prstů: * Optické * Silikonové (kapacitní) * Elektrooptické * Ultrazvukové * Tepelné * Tlakové

Geometrie ruky * Snímá se tvar ruky, Ten ovšem není jedinečný (např. ve srovnání s otisky prstů) * Snímače snímají 3D * Rychlost: verifikace asi během 1 s * Přesnost: málo přesné, tvar ruky není jedinečný, nevhodné pro identifikaci * Pouze omezeně vhodné pro verifikaci * FAR i FRR kolem 3 - 5 % * **Dynamika podpisu** * Důležitý je nejen výsledný podpis, ale i způsob (dynamika) jeho psaní * Vstupní zařízení: tablet/speciální snímač * Verifikace behem 1s * Malá přesnost, nedostatečná pro většinu aplikací * často důraz pouze na dynamickou komponentu psaní bez ohledu na výsledný podpis

Verifikace hlasu * Snímání: běžný mikrofon, telefon * Docela rychlé * Reálné výsledky ovlivněny šumem linky a šumem z okolí

Dynamika psaní na klávesnici * Založeno na způsobu psaní na klávesnici * měří se čas stlačení klávesy a čas mezi stisky kláves * algoritmy pracují na principu srovnávání vzorů (pattern matching) nebo neuronových sítí (neural networks – problém přidání dalšího uživatele) * možnost kontinuální autentizace uživatele

Oční duhovka * Srovnává se jedinečný vzor oční duhovky * Rychlost – miliony srovnání za sekundu * velmi přesné, vhodné i pro identifikaci * Černobílá kamera

Oční sítnice * Srovnává se vzor cév na oční sítnici * Pro snímání se používá infračervený

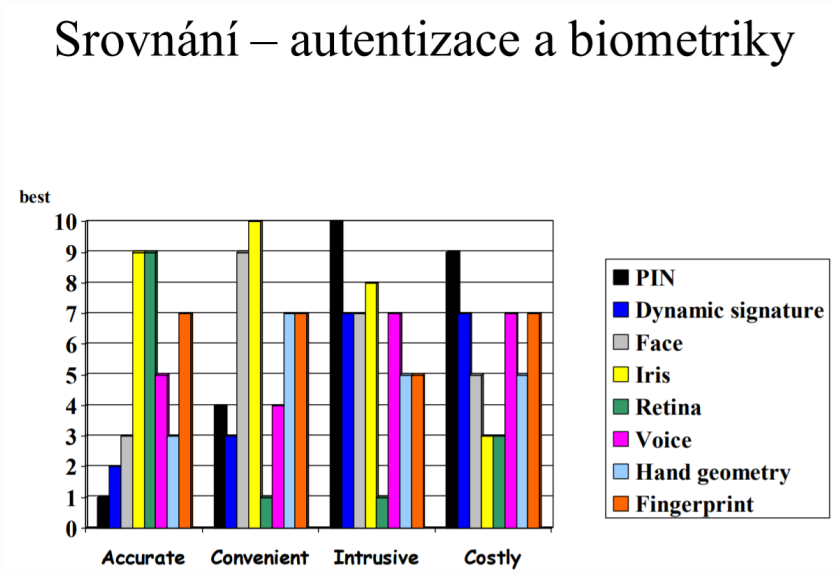
zdroj světla * Velmi přesné, ale snímání není uživatelsky příjemné

Rozpoznání obličeje * Rychlost: Velice výpočetně náročné, verifikace až několik sekund * Přesnost se výrazně zlepšila v posledních 5 letech * Obličej člověka se mění v čase * Účes, brýle, náušnice * Problém osvětlení a pozadí

Nejslibnější technologie: Otisk prstu, Duhovka, Ověření mluvčího

Praktické problémy * Správa charakteristik * Omezení při použití charakteristik: jedna charakteristika může být použita ve více systémech! * Zveřejnění nesmí ohrozit bezpečnost! * Záležitosti s ochranou soukromí a uživatelskou přívětivostí pro uživatele. * Legislativa a omezení.

TLDR: * Biometriky mohou být velmi citlivé informace * Biometriky nejsou tajné * Kopírování nemusí být triviální, ale není obtížné * Spolehlivost: nemohou být zapomenuty * Nová ochranná opatření mají za následek nové druhy útoků – bezpečnostní „klasika“



Zdroje: PV157: prednáška “Biometrická autentizace uživatelů” (+ http://statnice.dqd.cz/mgr-szz:in-bit:11-bit)