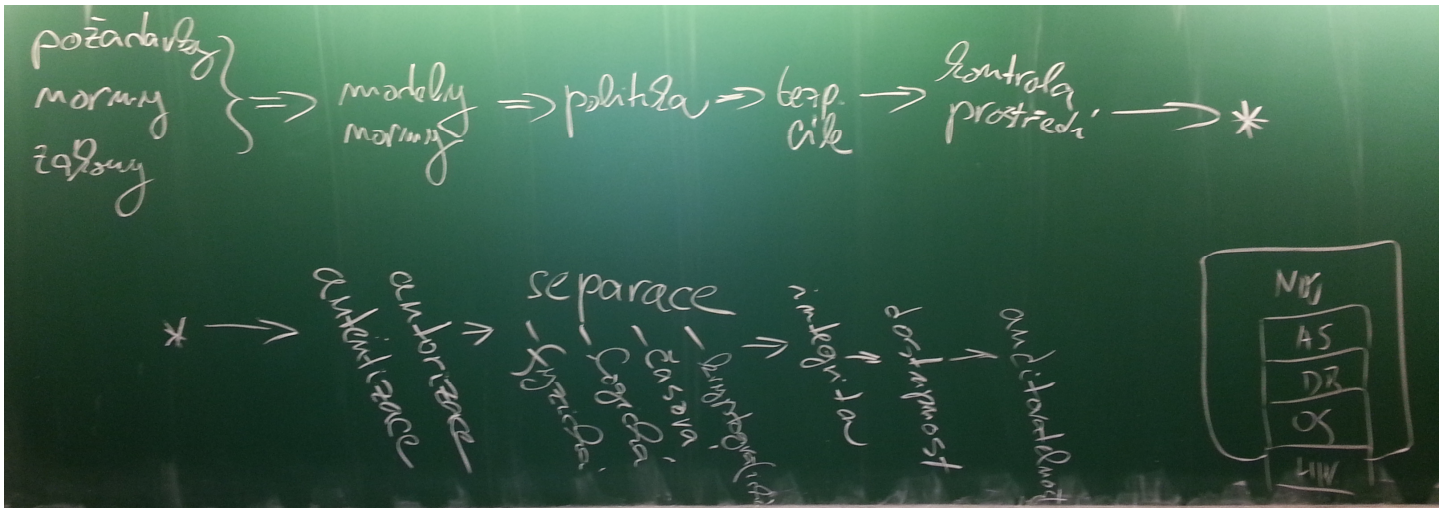
Bezpečnost

Hlavní komponenty bezpečnosti lze rozdělit takto:

- kontrola prostředí
- autentizace / identita
- autorizace
- separace
  - fyzická
  - časová
  - logická
  - kryptografická
- integrita
- dostupnost
- auditabilita

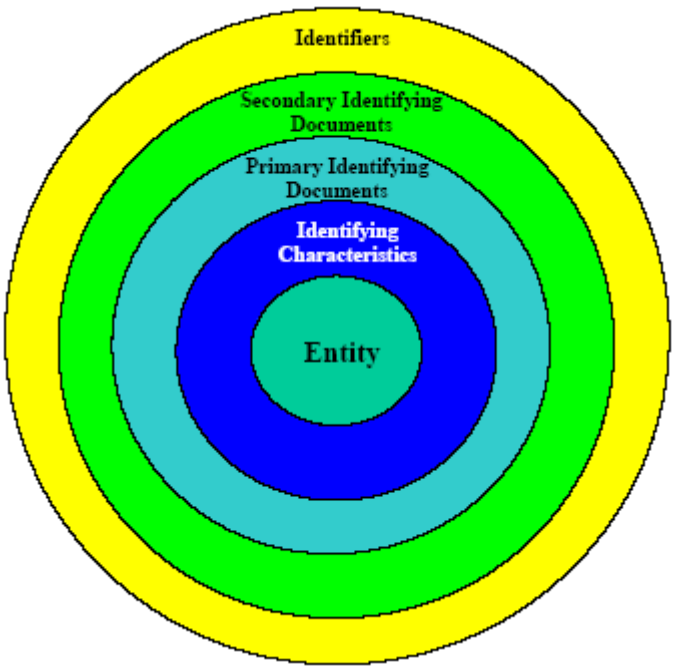


Autentizace

jde o proces (mechanismus) zjištění/ověření identity subjektu

zásadní význam pro možnost aplikace bezpečnostních mechanismů

asociace subjektu/identity s příslušnou sadou autorizací



Správa identity

Identifikátory: jméno, userID, rodné číslo

Sekundární identifikující dokumenty: směnka, výplatní páska, permanentka, ...
Primární identifikující dokumentu: občanský průkaz, pas, dokumenty svázané přímo s identifikující charakteristikou (např fotografií, otiskem prstu)
Identifikující charakteristika: biometrika, fotografie, další prostředky rozpoznání jednotlivce
Entita: bytost, místo, věc

Registrace (enrollment)

… iniciální přiřazení identifikačních dokumentů entitě
Zásadní důležitost pro spolehlivost a vlastnosti autentizace

Identita uživatele

Rostou nároky na informace udržované o uživateli, prostou identifikaci nahrazuje komplikovaná struktura označovaná jako ***profil***

- userID, heslo
- jméno, příjmení, tituly, ...
- bydliště
- kontaktní informace
- příslušenství ke skupinám, organizačním jednotkám, ...
- certifikáty, klíče
- personalizace
- oprávnění
-
- ...

Další příbuzné pojmy:

- alias
- anonymita
- pseudonymita

Autentizace protistrany

systémy pro správu informací musí zajistit dodání těchto informací autorizovaným uživatelům
navíc autentizace je nutná i při zajišťování např. fyzické bezpečnosti
Mechanismus autentizace může být založen na některém z následujících faktů:

- Co ví (pouze) dotyčná osoba - heslo, pass-phrase, šifrovací klíč

- Co vlastní - token, schopnost, znalost
- Schopnost provést operaci
- Cosi charakteristického - biometriky

Hesla

Charakteristika dobrého hesla:

- Obsahuje kromě velkých a malých písmen též číslice a další na klávesnici se vyskytující značky
- Dostatečná délka
- Nejde o obvyklé slovo nebo známou frázi
- Nepravděpodobné - nelze jej odvodit ze znalosti osoby vlastníka
- Často obměňované
- Není nikde po okolí poznamenáno

Passphrase

velmi dlouhá "hesla" – třeba citát z knihy, říkanka, ...
lze i na biometriky

Skupinová hesla

z různých důvodů občas systémy připouštějí hesla společná skupinám uživatelů - tato hesla jsou málo bezpečná, bývají často vyzrazena

Piny

(personal identification number)
jsou číselné řetězce standardní délky, sloužící k podobným účelům jako hesla
v souvislosti s platebními a kreditními kartami často používány 4-místné piny

Challenge-Response systémy

heslo může být zachyceno v průběhu vkládání, nebo při přenosu cílovému uzlu
časté změny hesla jsou pro uživatele zatěžující
vhodnější je, pokud systém zašle výzvu v podobě náhodné zprávy a uživatel jako heslo vrátí správnou reakci na tuto zprávu - např. její zašifrování tajným klíčem apod.

Jednorázová hesla

implementováno pomocí tokenů

Vícefaktorová autentizace

kombinace několika autentizačních postupů, např. pin + smart karta
vyšší úroveň bezpečnosti

- několik nezávislých bezpečnostních mechanismů aplikovaných paralelně, nebo
- aktivace silnějšího mechanismu a následná autentizace za použití tohoto mechanismu

Výměna tajností

protokol pro případ, že komunikující strany příliš nedůvěřují svému okolí a nechtějí vyzradit svoji identitu
pokud sdílejí tajný klíč *e*:

1. *A* zašle *B* zprávu **E**(*m, e*)
2. *B* vrátí *A* zprávu **E**(*m* + <*heslo*>, *e*)

pokud tajný klíč nesdílejí, neobejdou se bez centrální autority *C*:

1. *A* zašle *C* zprávu {*B, m*} e_A
2. *C* vytvoří transakční klíč *k*
3. *C* zašle **E**(<*B, m, k,* **E**(<*A, m, k*>, e_B)>, e_A) zpět *A*
4. Dešifrováním zprávy *A* získá *m, k* a **E**(<*A, m, k*>, e_B)
5. *A* zašle **E**(<*A, m, k*>, e_B) uzlu *B*

pro zajištění ochrany proti znovupoužití starých zpráv *m* musí obsahovat timestamp

Asymetrické klíče

Schopnost provádět operace tajným klíčem jednoznačně identifikuje držitele (dokazovatel) tohoto klíče:

1. ověřovatel zašle dokazovateli náhodně volený řetězec
2. dokazovatel jej transformuje za použití tajného klíče
3. ověřovatel pomocí odpovídajícího veřejného klíče ověří správnost

Symetrické klíče

protokol běží stejným způsobem jako v případě asymetrických klíčů, pouze v tomto případě může ověřovatel napodobovat (impersonation) dokazovatele

Passphrases

jde vlastně o dlouhá hesla, mohou to být části písní, básniček, části citátů …
pokud použijeme vhodný kompresní algoritmus, lze passphrázi transformovat ve velmi kvalitní heslo

navíc je možné aplikovat různé další měření - např. rytmus stisku jednotlivých kláves, jež bývá pro každého charakteristický

Tokeny, smart cards

token je obecné označení pro předmět, který autentizuje svého vlastníka
musí být jedinečný a nepadělatelný
obvyklá implementace jsou nejrůznější magnetické nebo čipové karty
pokud karta umí reagovat na vnější podněty, má např. vlastní výpočetní kapacitu, paměť, hovoříme o tzv. *smart card*
předložení tokenu bývá často kombinováno s nutností zadat odpovídající heslo

Tokeny pouze s pamětí

bjsou obdobou mechanických klíčů, paměť může obsahovat jednoznačný identifikační řetězec

Tokeny udržující hesla

token po zadání jednoduchého uživatelského hesla vydá určený kvalitní klíč, který udržuje

Tokeny s logikou

umí zpracovávat jednoduché podněty typu vydej následující klíč, vydej cyklickou sekvenci klíčů, může mít omezen počet použití
pomocí těchto tokenů lze realizovat systém s one-time hesly
každý klíč cyklické sekvence může zpřístupňovat jistou část výpočetního systému
tyto tokeny lze používat též k ochraně programů, přístupům k nejrůznějším placeným službám apod.

Inteligentní tokeny (smart cards)

jsou ideálním doplňkem chalenge-response systémů, mohou mít vlastní vstupní zařízení pro komunikaci s uživatelem, vlastní časovou základnu, mohou zajišťovat např. šifrování, generovat náhodná čísla apod.

Biometriky

jde o techniky identifikace lidí na základě jejich osobních charakteristik
navzájem se odlišují různou mírou spolehlivosti, ceny a v neposlední řadě i společenské přijatelnosti

hledáme charakteristiky mající dostatečnou mezi-osobní variabilitu při zachování vnitro-osobní reproducibility
kvalitu biometrik lze charakterizovat:

- četnost nesprávných odmítnutí - autorizovaného subjektu
- četnost nesprávných přijetí - útočníka
- kvalitou senzorů (!)

Verifikace hlasu

testovaný subjekt přečte systémem náhodně zvolenou frázi, sejmutá zvuková stopa je kmitočtově omezena (nejčastěji na 3kHz) a je proveden rozbor zvuku na základě původu jednotlivých složek zvuku v činnosti hlasového aparátu - fonace, frikace.
Výsledek je vhodným způsobem komprimován na vzorek velikosti 1 až 2 kB a porovnán se srovnávacím vzorkem
Výhodou je přirozenost a možnost provádět verifikaci např. prostřednictvím telefonu.

Verifikace dynamiky podpisu

Sledují se změny tlaku, zrychlení v jednotlivých částech, celkový průběh zrychlení, zarovnání jednotlivých částí podpisu, celková rychlost, celková dráha a doba pohybu pera na a nad papírem apod.
Ze získaných hodnot je opět vytvořen vzorek, který je porovnán se srovnávacím vzorkem.
Výhodou opět přirozenost a sociální akceptovatelnost, nevýhodou malá mechanická odolnost snímačů, a značná variabilita podpisu u některých lidí.

Verifikace otisků prstů

Systém provádí statistický rozbor výskytu tzv. markant - hrbolků, smyček a spirál v otisku prstu a jejich vzájemné polohy
často se provádí testování uživetelem zvoleného výběru několika prstů
Výhodou je vynikající mezi/vnitro-osobní variabilita, a dobrá zpracovatelnost vstupních dat, nevýhodou jsou možné negativní asociace uživatelů, a mnohdy sporná spolehlivost snímačů

Geometrie ruky

Metoda zkoumá délku a šířku dlaně a jednotlivých prstů, boční profil ruky apod.
Výsledkem je velmi malý vzorek - cca 18 bytů. Metoda je poměrně spolehlivá avšak poněkud dražší. Možnost podstrčení odlitku ruky.

Obrazy sítnice

Zařízení pořídí obraz struktury sítnice v okolí slepé skvrny, tento obraz je digitalizován a převeden na vzorek délky přibližne 40 bytů (!)
Obrázky sítnice mají stejné charakterizační vlastnosti jako otisky prstů
Výhodnou metody je značná spolehlivost a velmi obtížná napodobitelnost. Proto jde o metodu vhodnou k nasazení v prostředí nejvyššího utajení. Nevýhodou jistá subjektivní nepříjemnost, opět jde o velmi drahou technologii.

Další biometriky

rysy obličeje, Bertillonovy míry, rytmus psaní na klávesnici, EEG, EKG, otisky dlaní a chodidel, otisky chrupu, genetické rozbory, …