# PV080 – Ochrana dat a informačního soukromí

Vašek Matyáš

Konzultační hodiny – Po & Út 12:30 – 13:30

B415

Email: matyas@fi.muni.cz

# Průběh kurzu

- Přednášky v D1 Út 10:00-11:xx
- Doplňkové čtení
  - Materiály (vč. slajdů) na IS
  - Na IS2 a e-mailem diskuze, podněty, upozornění
- Aktivita v diskuzích, dobré odpovědi na otázky atd. průběžně hodnoceny (bonus až 10 %!!!)
- Polosemestrální písemná zkouška 35 %
- Závěrečná písemná zkouška 65 %
  - Je zájem o předtermín 20.12.?

# Hodnocení

A: 90 % (bodů) a více,

B: 80 % a více, ale méně než 90 %,

C: 70 % a více, ale méně než 80 %

D: 60 % a více, ale méně než 70 %

E: 50 % a více, ale méně než 60 %

F = neprospěl(a), za méně než 50 %.

- Kolokvium nebo zápočet alespoň 50 %.

# Témata kurzu – I.

- Informační soukromí – úvod, pojmy atd.
- Ochrana osobních dat a legislativa.
- Etika, profesionalita a práce s informacemi.
- Úvod do informační bezpečnosti.
- Potřeba ochrany dat ve vybraných oborech lidské činnosti
- Úvod do kryptografie, digitální podpis.

# Témata kurzu – II.

- Systémy podporující ochranu soukromí.
- Bezpečnostní politika při ochraně dat.
- Ochrana dat a management.
- Kontrola ochranných opatření.
- Internet a bezpečnost, ochrana soukromí.

# V přípravě dvě zvláštní přednášky

- **Karel Neuwirt** – bývalý předseda Úřadu pro ochranu osobních údajů
- **Jozef Vyskoč** – bezp. expert a auditor IS podle požadavků slovenského zákona na ochranu osobních údajů

# Soukromí (angl. *Privacy*)

- *Je v obecném pojetí charakteristikou života jedince a jeho práva a možnosti kontroly informací o sobě a o své činnosti, spolu s ochranou proti nežádoucímu rušení.*

- Informační soukromí se vztahuje především na zmíněnou možnost kontroly informací osobních dat a jiných relevantních citlivých informací. Tento termín se váže na jiná práva jedince, a tak je přesná definice obtížná.

# Informační soukromí

- Termín spíše pro neformální motivaci k zajištění ochrany osobních informací, pravidel pro jejich kontrolu a poskytování jiným subjektům atd.

- Příklady relevantních bezpečnostních funkcí:
  - anonymita,
  - pseudonymita,
  - nespojitelnost,
  - nepozorovatelnost.

# Soukromé informace

*Soukromé informace jsou informace, které nechceme sdílet s jinými, nebo u kterých chceme osobně kontrolovat jejich pohyb (tzn. sdílíme je s někým, ale ne s „ostatními“).*

[KC Laudon, Communications of ACM 9/96].

# Úroveň ochrany osobních dat

- *Rozhodujícím ukazatelem úrovně ochrany je cena osobních dat „na ulici“ – na černém či šedém trhu*. (Roger Needham, Cambridge U.)
  - Zdravotní data „běžné“ osoby v Anglii lze získat za cca 150-200 liber (7-10000 Kč)
  - V kanadské provincii Quebec podle některých „inzerátů“ 20-60 liber.
  - Podle Needhama by měla cena být výrazně nad 500 liber.

# Cenu osobních dat ovlivňují

1. Výše trestu těm, kdo data jiných řádně neohlídali a spolupodíleli se tak na jejich úniku.
2. Výše trestu těm, kdo s nimi neoprávněně manipulují.
3. Úroveň ochranných mechanismů.

# Postoj občanů k zacházení s osobními daty (Anglie, 90. léta)

- Necelých 20 % občanů totálně lhostejných,
- Stejný počet velmi obezřetných až paranoidních
- Asi 60 % je ochotno část svých práv nechat omezit za “přiměřenou úhradu” - finanční, věcnou či nejčastěji v podobě výrazného zlepšení služeb.

# Nedávný výzkum v Německu – I.

- *Privacy in e-commerce: stated preferences vs. actual behavior (Berendt a kol.), ACM Communications, April 2005*
- Soukromí si chránící – 30 %
- (Téměř) lhostejní – 24 %
- Citliví na profilování – 26 %
- Citliví na identitu – 20 %

# Nedávný výzkum v Německu – II.

- Za určitých okolností je ovšem většina uživatelů online ochotna zapomenout na zábrany a sdělit osobní informace i bez skutečně závažných důvodů (takto učinit)
- I uživatelé, kteří podle vlastního názoru jsou citliví na ochranu osobních dat, tak při online interakci nekontrolují v tomto směru své chování

# Experiment v Cambridge

- *How Much is Location Privacy Worth? (Danezis a kol.)*
- Info studentům 1. ročníku o placeném výzkumu se sběrem informací o jejich pohybu (mobil – 28 dnů, 24 hodin denně)
  - Aukce!!!
- £10 medián, £27.4 průměr (max. £400, min. 0)
- Se zvážením prodeje pro komerční účely pak £20 medián, £32.8 průměr (max. £300, min. 0)

# Anonymita

Anonymita je vlastnost systému, který zajišťuje možnost použití zdrojů nebo služeb bez zjištění identity uživatele tohoto systému.

# Pseudonymita

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).

# Nespojitelnost (angl. *unlinkability*)

Vlastnost systému, který zajišťuje možnost *opakovaného* použití zdrojů nebo služeb s tím, že ostatní si tato použití nebudou schopni spojit.

- Spojení ve smyslu vzájemné souvislosti.
- Může se jednat o postupně i současně poskytované stejné i různé služby.
- Nezohledňuje identitu uživatele, ale rozsah služeb a zdrojů, které byly použity stejným uživatelem.

# Nepozorovatelnost (angl. *unobservability*)

Vlastnost systému, který zajišťuje možnost použití zdrojů nebo služeb tak, že ostatní nemohou zpozorovat používání daného zdroje nebo služeb.

- Ochraňovanými hodnotami nejsou informace o uživatelích, ale o použití zdrojů nebo služeb.
- Příkladem aplikace může být ochrana proti tzv. analýze provozu (angl. *traffic analysis*).

# K zamyšlení...

- Je e-mailová adresa ve tvaru `Jmeno.Prijmeni@NejakaFirma.cz` osobním údajem nebo nikoliv?

- Může zaměstnavatel sledovat e-mailovou komunikaci svého zaměstnance, který při nástupu na nové místo stvrdil písemně svůj souhlas s tím, že nebude používat e-mail pro soukromé účely?

# Lze měřit/hodnotit informační soukromí?

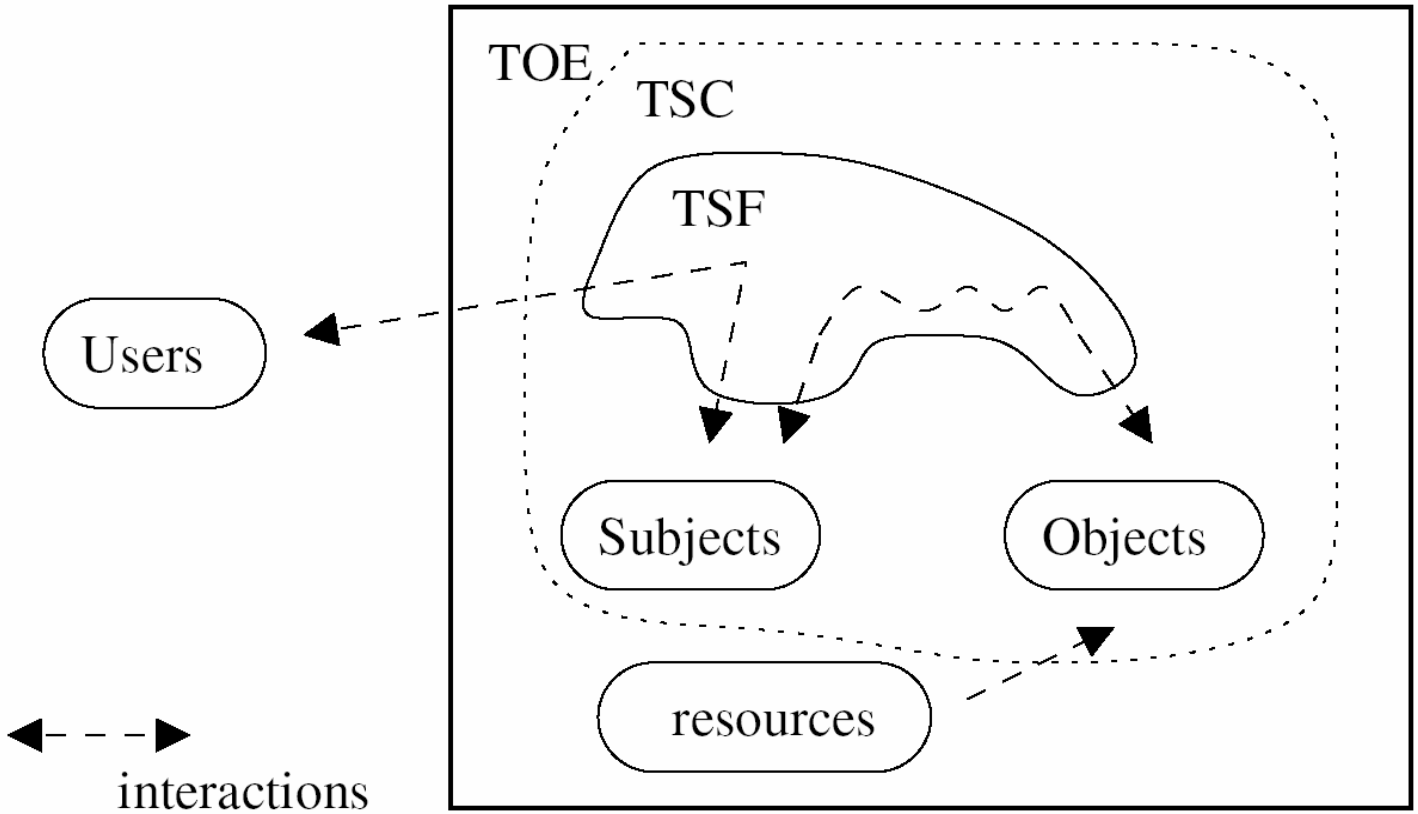
- Na jaké úrovni jsou data spojitelná s určitou osobou?
- Jakou míru jistoty máme při spojení různých datových položek?
- Na jaké úrovni je něco pozorovatelné?

# Dva hlavní směry/pohledy

- *Mixy* – systémy pro posílání zpráv, obvykle s klamavými (kamuflovacími) zprávami, přeposílání mezi více účastníky (než je nejkratší/nejoptimálnější cesta)
  - Příklad systému později v semestru
- *Společná kritéria (systémy)* – standard (rozsáhlý) pro hodnocení bezpečnosti systémů, umožňuje lepší srovnávání systémů i specifikaci požadované funkčnosti
  - Více informací také později v semestru

# Model Společných kritérií

TOE: Target of Evaluation – celý (hodnocený) systém
TSF: TOE Security Functions – HW, SW, FW který TOE využívá
TSC: TSF Scope of Control – interakce podléhající bezp. politice TOE
security polic



# Nepozorovatelnost (CC)

- Uživatel může použít zdroj nebo službu bez toho, aby ostatní byli schopni zjistit, že je daný zdroj nebo služba používán
- Úrovně:
  - specifikované entity nejsou schopny pozorovat specifikované operace prováděné specifikovanými entitami na specifikovaných objektech
    - a s podmínkami pro práci s relevantními informacemi
  - nebo specifikované subjekty poskytují specifikované služby bez vyžadování informací (TSF)
  - nebo specifikovaní uživatelé mohou pozorovat použití specifikovaných zdrojů nebo služeb

# Anonymita (CC)

- Uživatel může využít zdroj nebo službu bez odhalení své identity
  - Jedná se o ochranu identity uživatelů, nikoliv ochranu identity subjektů v systému
- Úrovně:
  - specifikované entity nejsou schopny určit skutečné uživatelské jméno spojené se specifikovanými subjekty, operacemi, objekty
    - a specifikované subjekty získají specifikované služby bez vyžadování informací (TSF)

# Pseudonymita (CC)

- Uživatel může použít zdroj nebo službu bez odhalení své uživatelské identity, ale je stále zodpovědný za toto použití
- Úrovně:
  - [Anonymita 1.1] s přidělením aliasů pod kontrolou TSF a specifikovanou metrikou aliasů
    - a s právy zvrácení pro specifikované entity za specifikovaných podmínek
    - nebo se znovuvyužitím aliasu za specifikovaných podmínek

# Nespojitelnost (CC)

- Uživatel může opakovaně využít zdroje nebo služby bez toho, aby ostatní byli schopni vzájemně spojit tato užití
- Další členění/úrovně nejsou

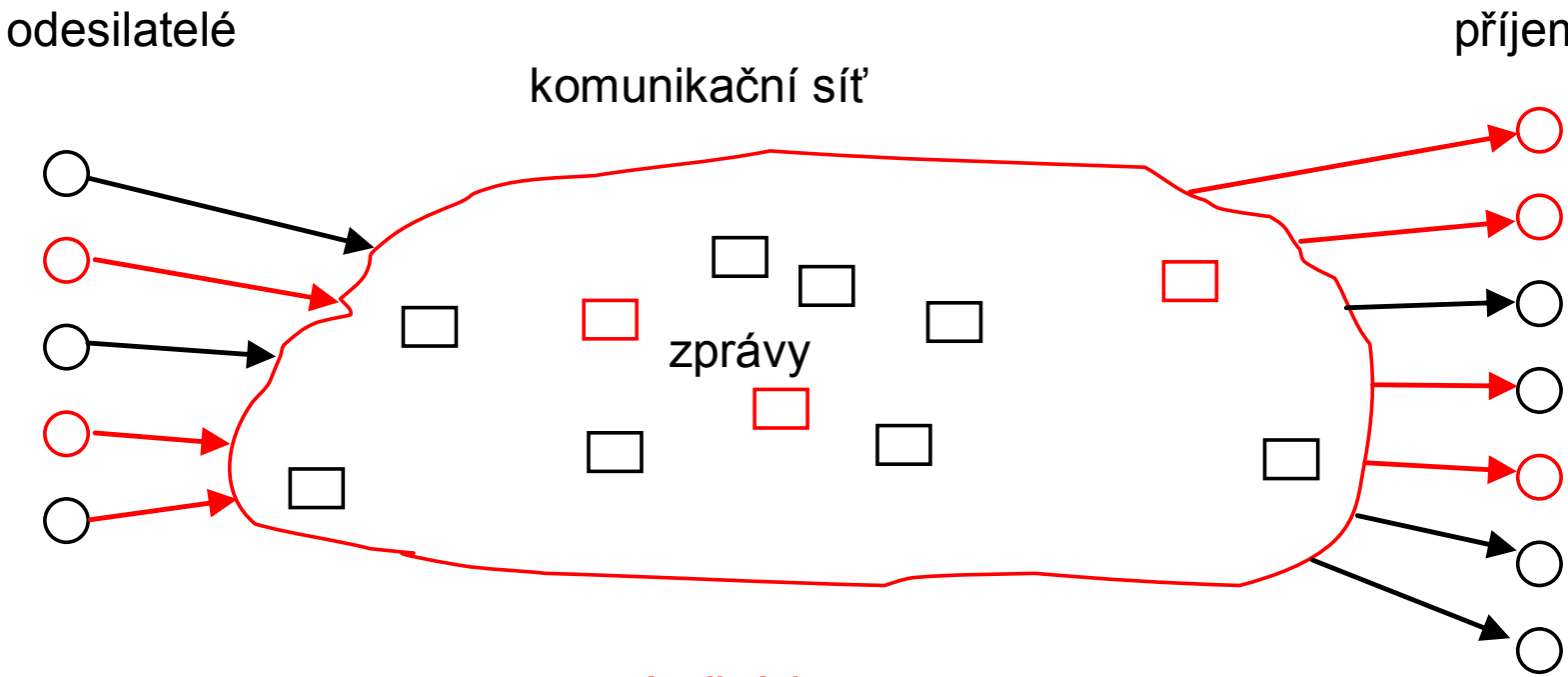
# Pohled Společných kritérií

- Existenciální pohled – vlastnost buď je, nebo není
  - Kritéria neřeší (a ani to nemají za cíl) jak je vlastnosti dosaženo
  - Kritéria neumožňují jiné než diskrétní (Y/N) ohodnocení

# A. Pfitzmann a kol. - terminologie

- Anonymity, Unobservability, Pseudonymity, and Identity Management - A Proposal for Terminology
- Soustředí se pouze na prostředí, kde se posílají zprávy od odesilatelů k příjemcům
  - Specifickou (a nejvýznamnější) podmnožinou jsou tzv. mixy (sítě mixů zadefinoval David Chaum v roce 1981)

# Takže obvyklé prostředí...




útočníci
(příklad jejich domény červenou barvou)

(Zdroj: A. Pfitzmann)

# Anonymita subjektu (A.P.)

- Stav bytí neidentifikovatelným v rámci dané množiny subjektů, tzv. anonymitní množině.
- Anonymitní množina je množinou všech možných subjektů (obvyklí podezřelí ☺)
  - s ohledem na odesilatele možných odesilatelů
  - s ohledem na příjemce možných příjemců atd.
- Anonymita subjektu je tedy vždy spojena s touto množinou!
  - Lze vnímat tak, že anonymita je silnější pro větší anonymitní množinu
    - Otázkou je někdy přínos tohoto pohledu – získáte více, když při stejné pravděpodobnosti víte, že pravděpodobnost spojení s nějakou identitou je pro daný subjekt různá pro různě velké množiny?

# Nespojitelnost (A.P.)

- Nespojitelnost dvou nebo více prvků (např. subjektů, zpráv, událostí...) znamená, že v takovém systému nejsou prvky ani více, ani méně ve vzájemném vztahu s ohledem na předchozí znalost o systému
  - tzn. že pravděpodobnost spojení těchto prvků je stejná před a po (prů)běhu nějaké posloupnosti událostí v systému

# Předmět zájmu

- Terminologie Pfitzmanna a kol. definuje *předmět zájmu* (item of interest) jako označení pro případ, že cílem zájmu není subjekt (jako např. u anonymity)
  - Pak lze definici anonymity subjektu rozšířit...

# Nepozorovatelnost (A.P.)

- Stav (daných) předmětů zájmu, kdy nejsou odlišitelné od jiných předmětů zájmu.
  - U zpráv v mixech např. neodlišitelnost „skutečných“ zpráv od šumu
  - S ohledem na stejného útočníka pak lze říct: Nepozorovatelnost => anonymita
- Pro nepozorovatelnost a anonymitu u systémů pro posílání zpráv se používají mixy, příklad systému později v semestru na zvláštní přednášce

# Pseudonym (A.P.)

- Z řeckého *pseudonumon* – falešně pojmenovaný
  - tzn. používající jiné než „skutečné jméno“
- Pozor – „skutečné jméno“ (např. dané oficiálními státními dokumenty) se během života mění
  - Jako pseudonym lze pak označit každé pojmenování (identifikátor)

# Pseudonymita (A.P.)

- Bytí pseudonymním je stav používání pseudonymu jako identifikátoru (ID).

- Digitální pseudonym – řetězec bitů, který je
  - unikátní jako ID (s velmi velkou pravděpodobností) a
  - použitelný pro autentizaci jeho vlastníka a předmětů zájmu (např. odeslaných zpráv)

# Poznámky k pseudonymitě

- Anonymita a prokazatelná zodpovědnost (accountability) jsou dva extrémy
- V praxi obvykle vhodná pseudonymita
  - Ovlivňuje spojitelnost mezi předměty zájmu a uživateli
- Opakované použití pseudonymu může uživateli umožnit ustavení reputace (důvěryhodnosti)
- Uživatelé používají větší počet pseudonymů
  - Odhalují spojitost mezi nimi jen v případě potřeby (zisku výhod, času, peněz...)

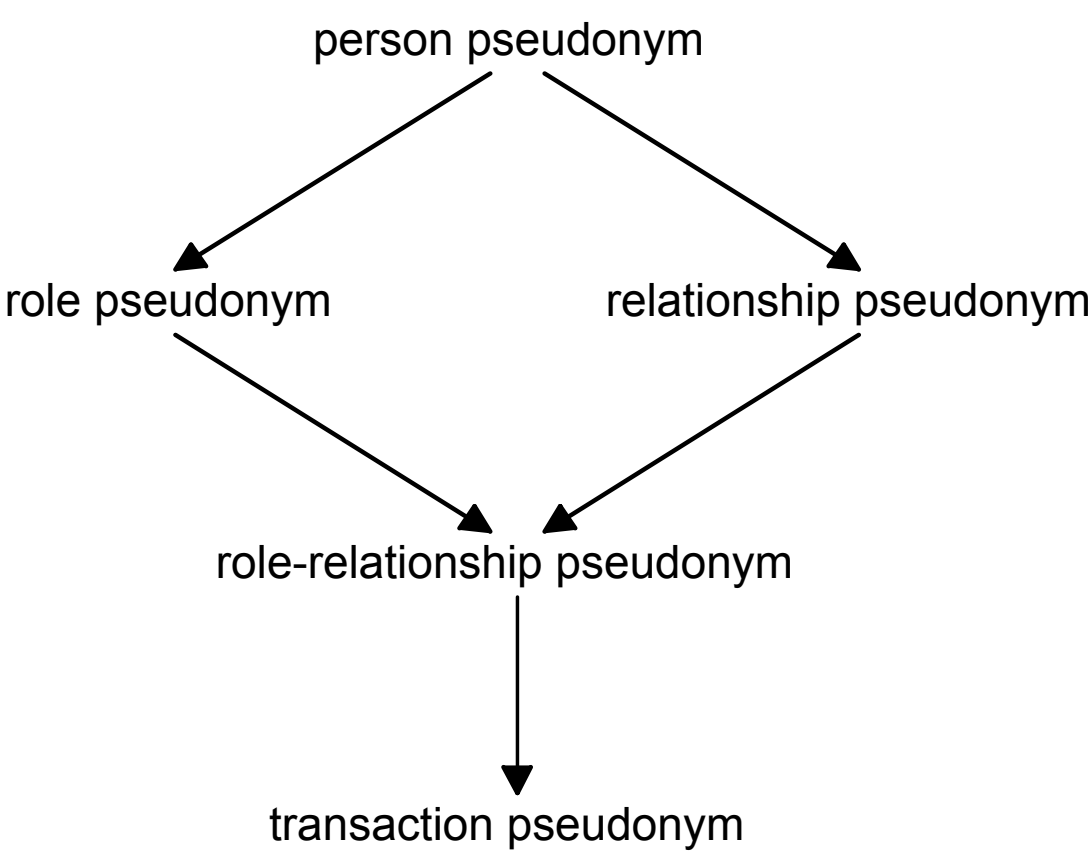
# Vztah mezi pseudonymem a vlastníkem (A.P.)

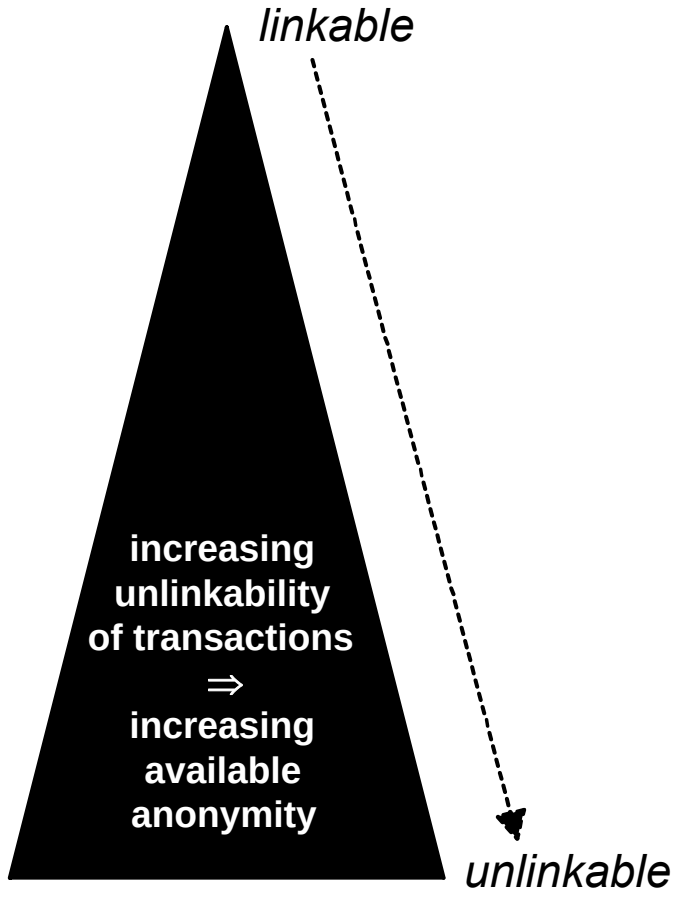
- *Veřejný pseudonym* – veřejně znám od počátku, např. v seznamu osob
- *Původně neveřejný pseudonym* – není od počátku znám veřejně, např. číslo účtu, pseudonymní certifikát veřejného klíče (podpisový certifikát)
- *Původně nespojený pseudonym* – není od počátku znám nikomu mimo jeho vlastníka, např. ID v chatu

# Spojitelnost s ohledem na použití pseudonymu v různých kontextech (A.P.)

- Pseudonym *osoby* – vnímán jako reprezentace dané osoby
- Pseudonym *role* – osoba používá různé pro různé role (může někdy i stejné)
- Pseudonym *vztahu* – pro každého partnera je použito jiné jméno
  - může být stejné pro komunikaci se stejným partnerem v různých rolích
- Pseudonym *role-vztahu* – unikátní pro roli a vztah (partnera)
- Pseudonym *transakce* – unikátní pro transakci

# Úroveň anonymity/nespojitelnosti transakcí podle druhu pseud. (A.P.)



# Identita (A.P.)

- Libovolná podmnožina atributů určitého jedince, která tohoto jedince jednoznačně určuje v jakékoliv množině jedinců.
  - Tzn. není jedna identita, ale několik.
  - Částečná identita se pak vztahuje k určitému kontextu či roli, tzn. i k omezené množině jedinců.
    - Pak může být i pseudonym za určitých okolností identifikátorem pro částečnou identitu.

# Systémy řízení identity

- Angl. *Identity Management System – IMS*
- Využívají technologie pro návrh a správu atributů (popisů) identity
- V jednodušší podobě známy dříve jako
  - Single sign-on (systémy jednoduchého přihlašování)
  - Public-key infrastructures (infrastruktury veřejných klíčů – nejčastěji pro spolehlivé spojení klíče a informací o osobě)