pet portál

Anonimizáló rendszerek elméletben és gyakorlatban

Szili Dávid
szili@pet-portal.eu

Hacktivity 2008
Budai Fonó Zeneház, 2008. szeptember 21.

Miről lesz szó?

- **Bevezetés, alapfogalmak**
- **Anonimizáló technikák csoportosítása**
- **Konkrét példák**
- **Demó**
- **Összefoglalás**

Anonimizáló rendszerek elméletben és gyakorlatban

BEVEZETÉS

Bevezetés: Alapfogalmak

- **PET: Privacy Enhancing Technologies** (tehát nem a pozitron-emissziós tomográfia ☺)
- **Miért kell?**
- **Anonimizáló technikák, protokollok**
- **Elvárások**
  - Anonimitás
  - Erőforrások
  - Harmadik felek

Bevezetés : Rendszerjellemzők 1.

- **Anonimitás**
  - Fogadó félnek
  - Küldő félek
- **Megfigyelhetetlenség**
  - kettő vagy több kommunikáló fél közötti információátvitel
- **Összeköthetetlenség**
  - Külső megfigyelővel szemben

Bevezetés : Rendszerjellemzők 2.

- **Hálózati terhelés**
  - Jelentős hálózati késleltetés, megnövekedett sávszélesség-igény
- **Skálázhatóság**
  - Az erőforrások számát növelve a rendszer mennyivel több terhelést képes elbírni
- **Bizalmasság**
  - Csak az arra jogosultak és csak az előírt módokon rendelkezhetnek az adatokról

Bevezetés: Rendszer által biztosított anonimitás

- **Levine-Shields-féle taxonómia**
  - Az anonimitás egy 0 és 1 közé eső érték
  - Szintek:
    - *Abszolút anonimitás*
    - *Gyanú felett*
    - *Lehetséges ártatlanság*
    - *Leleplezve*
    - *Bizonyítottan leleplezve*

Bevezetés :
Néhány ismertebb támadás

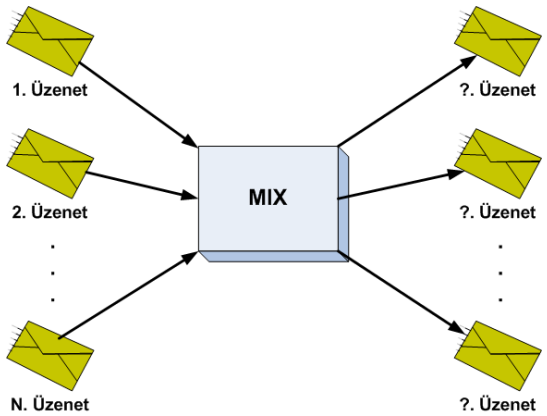
- **Lokális lehallgatás**
- **Predecessor támadás**
- **Sybil támadás**
- **Szolgáltatás-megtagadás (Denial of Service, DoS)**

Anonimizáló rendszerek elméletben és gyakorlatban

AZ ANONIMIZÁLÓ RENDSZEREK KATEGORIZÁLÁSA

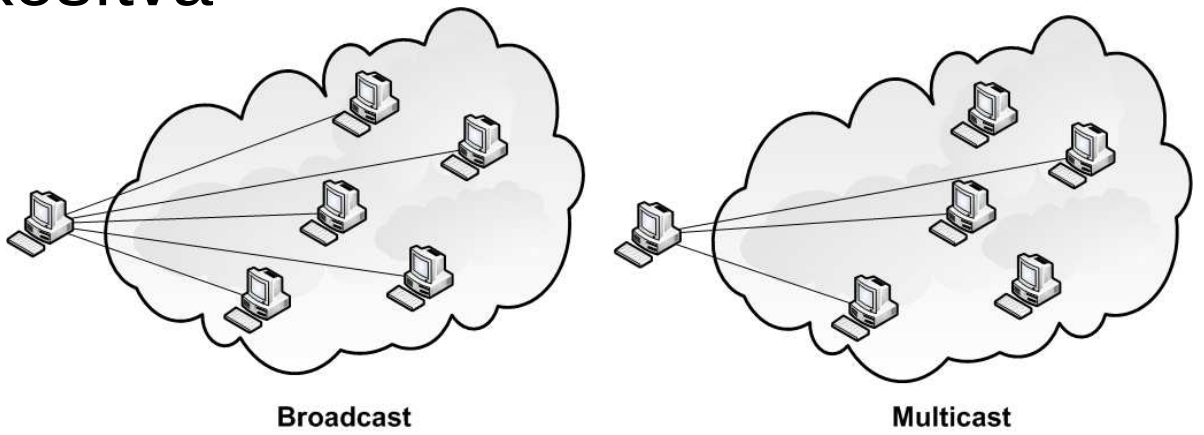
Kategórizálás: MIX-Net

- **David Chaum-féle MIX-ek**
  - A legelterjedtebb
  - Azonos hosszúságú üzenetek
  - Kimenet a bemenetitől eltérő, véletlen sorrendben



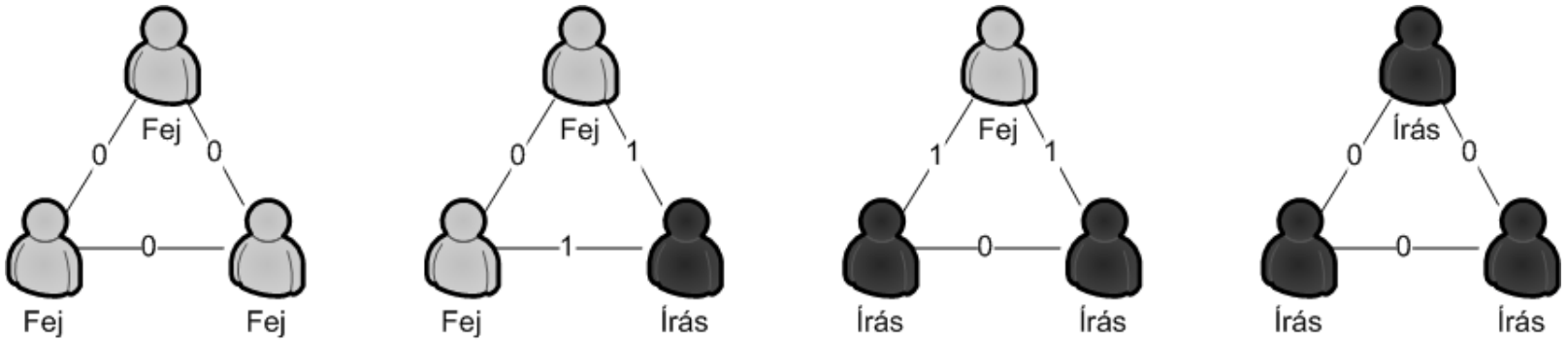
Kategórizálás: Broadcast, multicast

- **Broadcast vagy multicast**
  - Minden részvevő fix méretű csomagokat küld
  - Ha nincs küldendő csomag, akkor zajt küld
  - Csomagok a fogadó fél nyilvános kulcsával titkosítva



Kategórizálás: DC-net

- **Dining Cryptographer Network** (szintén David Chaum-tól)
- A Dining Cryptographers' Problem általánosítása



Kategórizálás: Egyéb megoldások

- **Léteznek különlegesebb megoldások is, amelyek nem illenek bele egyik fenti csoportok egyikébe sem**
  - Például:
    - Anonim Proxy
    - Buses protokoll

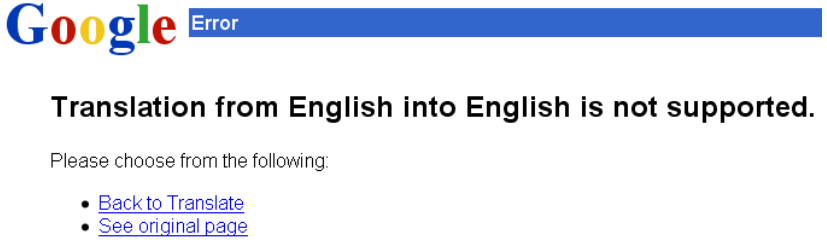
Anonimizáló rendszerek elméletben és gyakorlatban

GYAKORLATI PÉDÁK

Példák:
Web-es Proxy-k

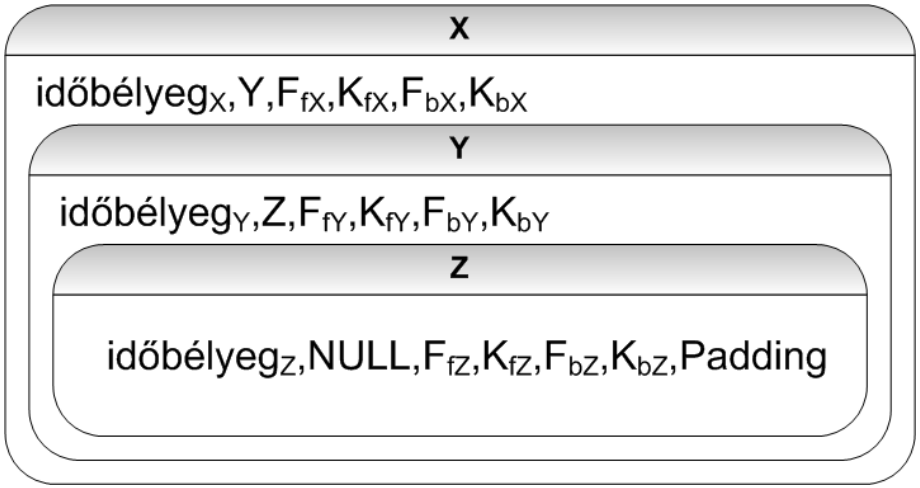
- **Pl. Anonymouse**
  - WWW
  - E-mail
  - Newsgroup

- **Anonymizerek (Pl. http://anonymity.com/)**
- **Régebben még:**
  - google translate ☺
  - ma már nem működik



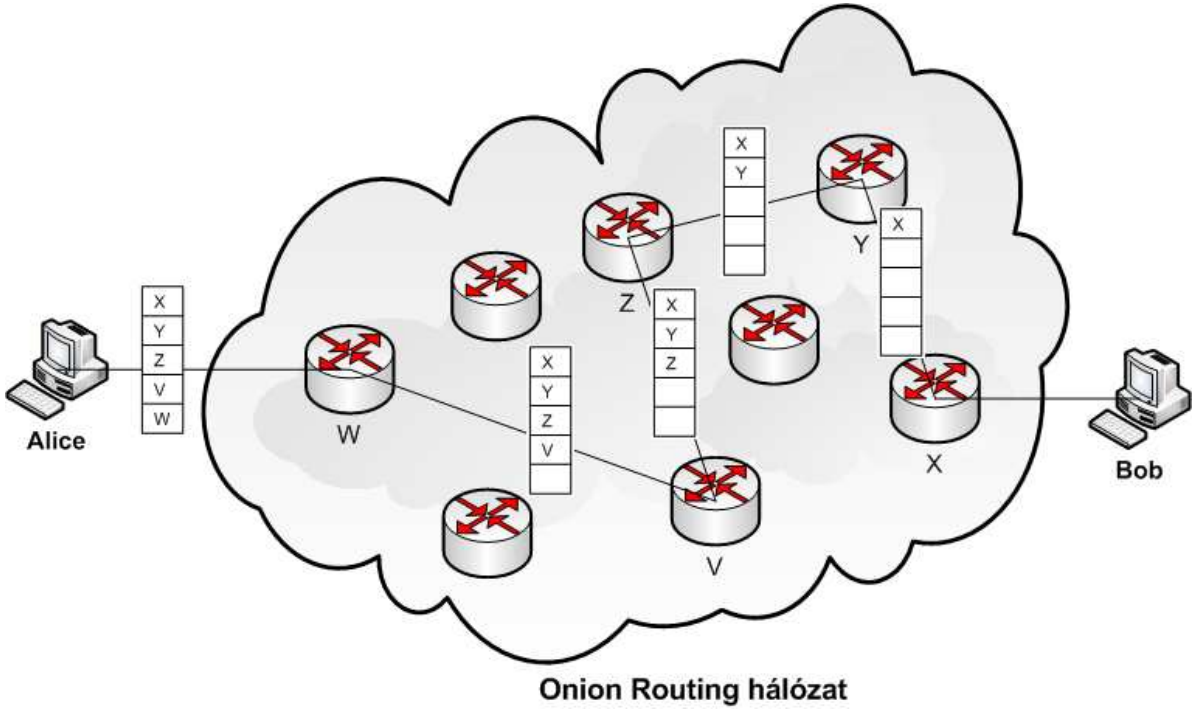
Példák: TOR 1.

- **Onion routing**
  - Cél a routing információk elrejtése
  - Onion: Egymásba ágyazott rétegek



Példák: TOR 1.

- **Onion routing**
  - Routing példa

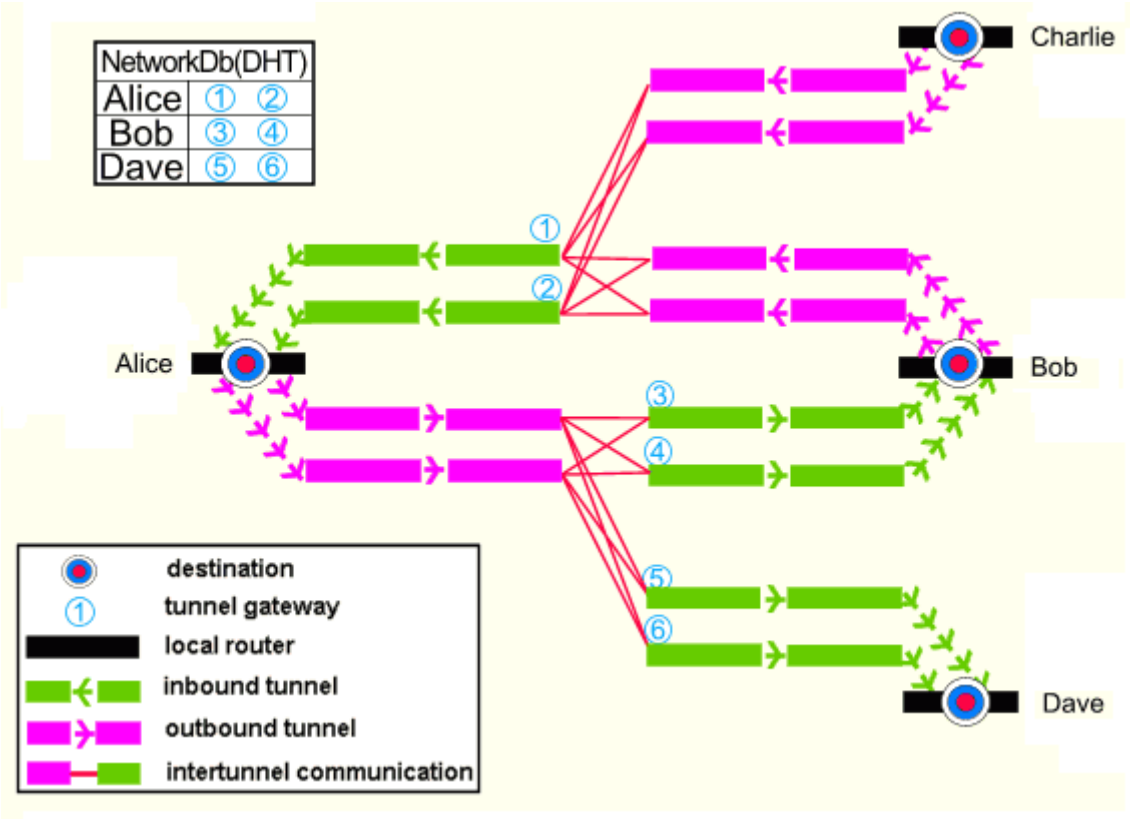


Példák:
I2P (Invisible Internet Project) 1.

- **Garlic routing**
  - több üzenetet összefogva
  - gerezdek plusz opciókat tartalmazhatnak
  - a garlic paddinget tartalmaz
- **Tunnel routing**

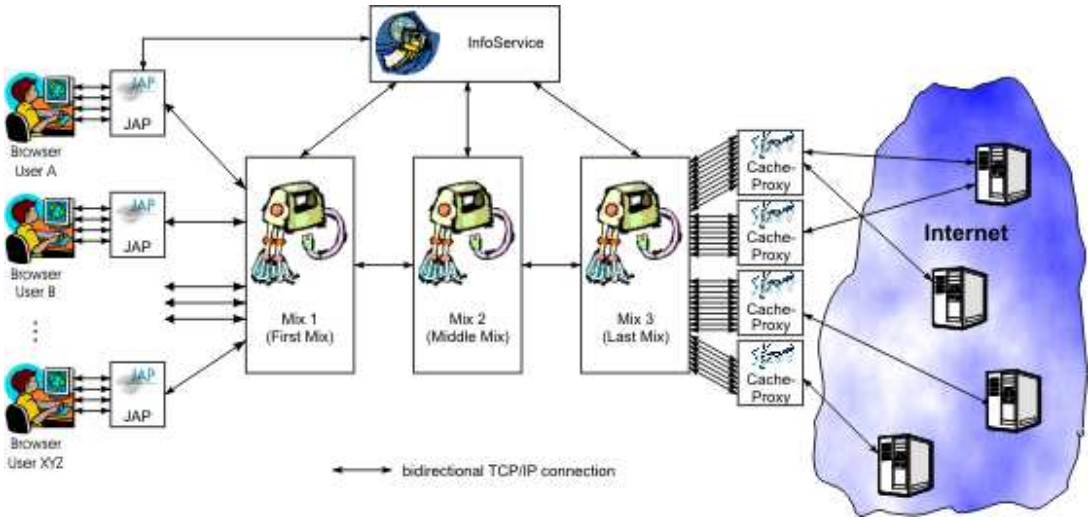
Példák:
I2P (Invisible Internet Project) 2.

- **I2P routing**
  - Routing péld



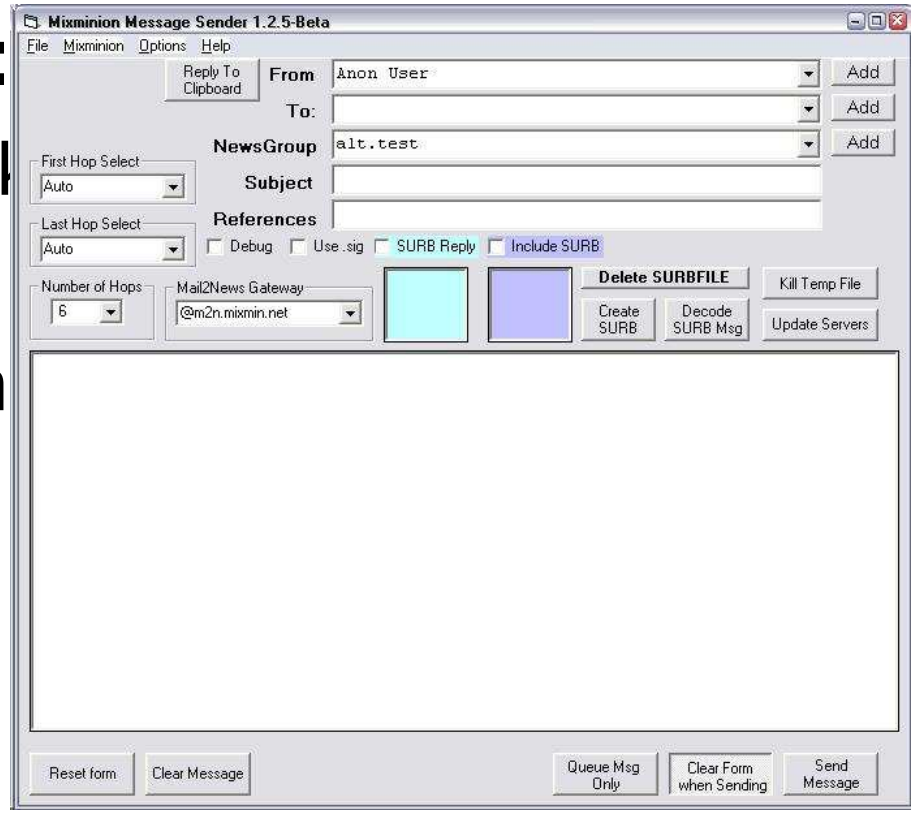
Példák: JAP

- **MIX alapú hálózat**
  - JonDo/JAP
  - MIX / MIX Cascade
  - InfoService



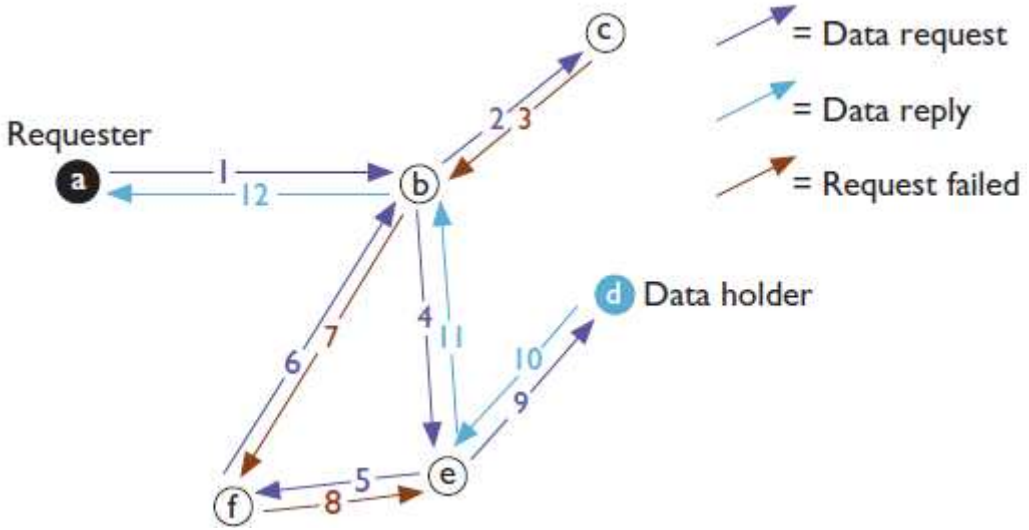
Példák: Cypherpunk, Mixmaster, Mixminion

- **E-mail anonimitás: remailer!**
- **Remailer típusok:**
  - Type I: Cypherpunk
  - Type II: Mixmaster
  - Type III: Mixminion



Példák: Freenet

- **P2P hálózat**
  - Decentralizált
  - Anonim
  - Speciális kulcsok
    - CHK, SSK, USK,
  - Routing



Anonimizáló rendszerek elméletben és gyakorlatban

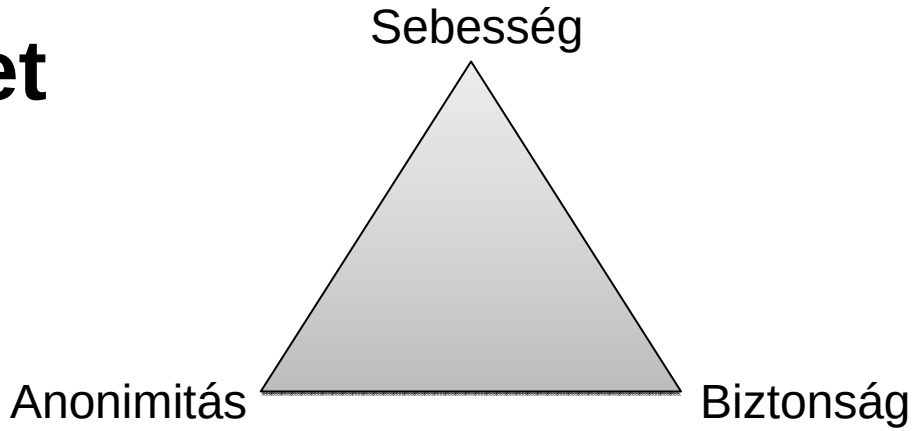
DEMO, DEMO…

Anonimizáló rendszerek elméletben és gyakorlatban

ÖSSZEFOGLALÁS

Összefoglalás

- **Komplex probléma, sokféle megoldás**
- **Kompromisszumok**
- **A jelenlegi helyzet**
- **Mit hoz a jövő?**



pet portál

Köszönöm a figyelmet!

Kerdesek?

Szili Dávid
szili@pet-portal.eu

Hacktivity 2008
Budai Fonó Zeneház, 2008. szeptember 21.