

Új irányzatok a személyes adatok kezelésében és védelmében

Balogh Zsolt György

egyetemi docens

Budapesti Corvinus Egyetem

zsolt.balogh@uni-corvinus.hu

Az informatika fejlődési korszakai

Stand-alone számítógép

Adatbázis valós fizikai helyszínen
Adatbázis-kezelés klasszikus módszerei

Az adatvédelem klasszikus elvei

Networking (*Fix és mobile*)

Határokat átlépő adatáramlás
Adatbányászat

Személyiség-profil!
Ki férhet hozzá az adatokhoz?

Virtualizáció

Közösségi háló
Cloud computing

Hol vannak az adatok?
Bárki lehet adatkezelő

Megfigyelési technológia



WHEREVER YOU GO, WHATEVER YOU DO, WHOEVER YOU ARE,
YOU ARE UNDER SURVEILLANCE

BECAUSE YOU ARE A POTENTIAL CRIMINAL, PERHAPS YOU SECRETLY DOUBT THE SANCTITY OF CORPORATE PROPERTY, OR THE VALIDITY OF LAWS MADE BY THE RICH TO GOVERN THE POOR, OR THE SOUNDNESS OF CAPITALISM ITSELF—WE CAN'T AFFORD TO ASSUME YOU DON'T. THAT'S WHY THERE ARE VIDEO CAMERAS POINTED AT EVERY CASHIER AND POLICE CARS CIRCLING EVERY BLOCK. LEFT TO ITSELF, A STATE OF DISORDER AND INEQUITY RETURNS TO EQUILIBRIUM: OUR JOB IS TO PERPETRATE THIS ONE INDEFINITELY.

DEPARTMENT OF HOMELAND SECURITY
"in suspicion we trust!"
www.crimelibrary.com/surveillance



Adatvédelem garanciái

- **Célhoz kötöttség**
 - Személyes adat csak meghatározott célból kezelhető
- **Arányosság**
 - Csak a cél megvalósulásához elengedhetetlen adat kezelhető, a szükséges mértékben és ideig
- **Adatintegráció tilalma**
 - Tilos a különböző helyen, eltérő célra felvett adatkezelések összekapcsolása
- **Adattovábbítás korlátozottsága**
 - Az adattovábbítás az érintett hozzájárulásán vagy törvényi felhatalmazáson alapul.

Új elvek és eszközök

- Privacy Enhancing Technologies (PET)
- Privacy by Design (PbD)
- Privacy Impact Assessment (PIA)

PRIVACY ENHANCING TECHNOLOGIES

A PET célja az ÖNVÉDELEM

- Önrendelkezési képesség növelése (erősebb ellenőrzés a saját adatok felett)
- Adatminimalizálás
- Anonimitás szintjének megválasztása (álnév vagy teljes névtelenség)
- Összekapcsolhatóság, illetve összekapcsolhatatlanság szintjének megválasztása
 - Többszörös virtuális személyazonosság használata
- Tájékozott beleegyezés megvalósítása az on-line adatkereskedelemben is
- Privacy alku lehetősége
 - Adatkezelés feltételeinek és kapcsolódó kikötéseinek érdemi befolyásolása
 - Az adatkezelési feltételek betartásának technológiai kikényszerítése
 - Az adatkezelési feltételek érvényesülésének távfelügyelete
- Adatkövetés
 - Az adatalany naplózhatja, archiválhatja a tranzakciók meta-adatait
- Jogérvényesítés egyszerűsítése

Egyes PET eszközök

■ Kommunikációt anonimizáló eszközök

➤ Proxy szerverek

- Felhasználó bejelentkezik N.N. névvel, és a világ számára [USER!user@users.reverse.dns](#) néven látható
- Felhasználó bejelentkezik N.N. névvel, és a világ számára [USER!user@bnc.net](#) néven látható

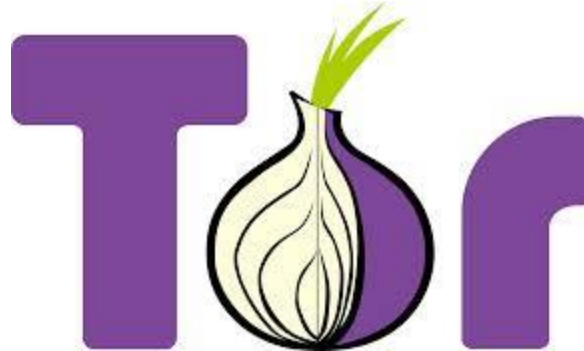
➤ Egyes gyakran alkalmazott anonimizáló szoftverek

- *Bip IRC Proxy*
- *bnc*
- *ezbounces*
- *JBouncer*
- *muh bnc*
- *psyBNC*
- *shroudBNC*
- *SimpleBouncer*
- *dirproxy*

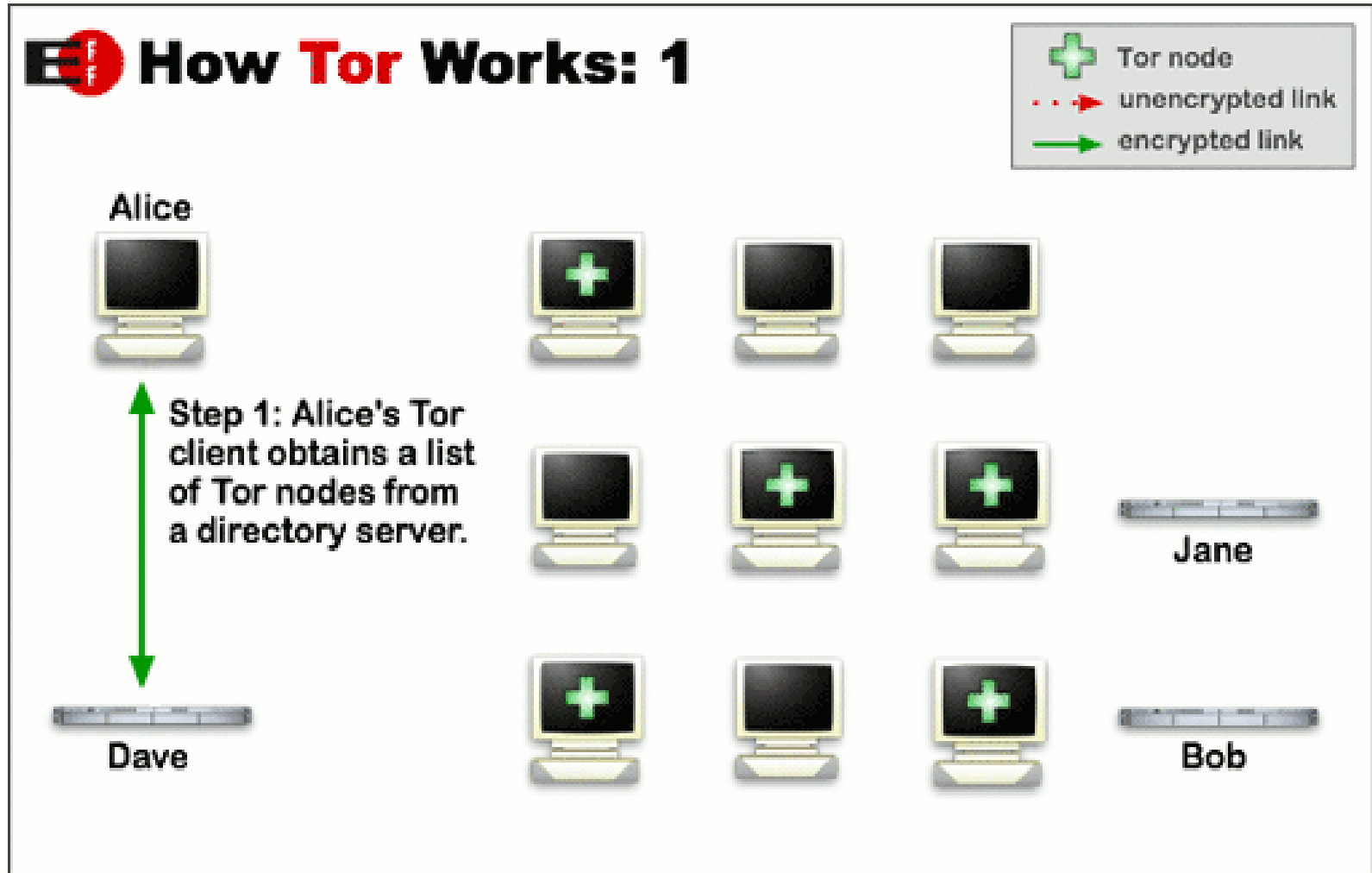
Egyes PET eszközök

- Megosztott hamis online személyazonosítók
 - Valaki készít a Skype-on, MSN-en, Facebook-on egy hamis személyiséget
 - Név
 - Lakcím
 - Telefonszám
 - Életmód adatok
 - A személyiség account adatait nyilvánosságra hozza az Interneten
 - Innentől kezdve bárki kényelmesen használhatja ezt a kreált hamis személyiséget saját célú kommunikációra
- Többszörös virtuális személyiség
 - Az összekapcsolás lehetősége nélkül

The Onion Routing project




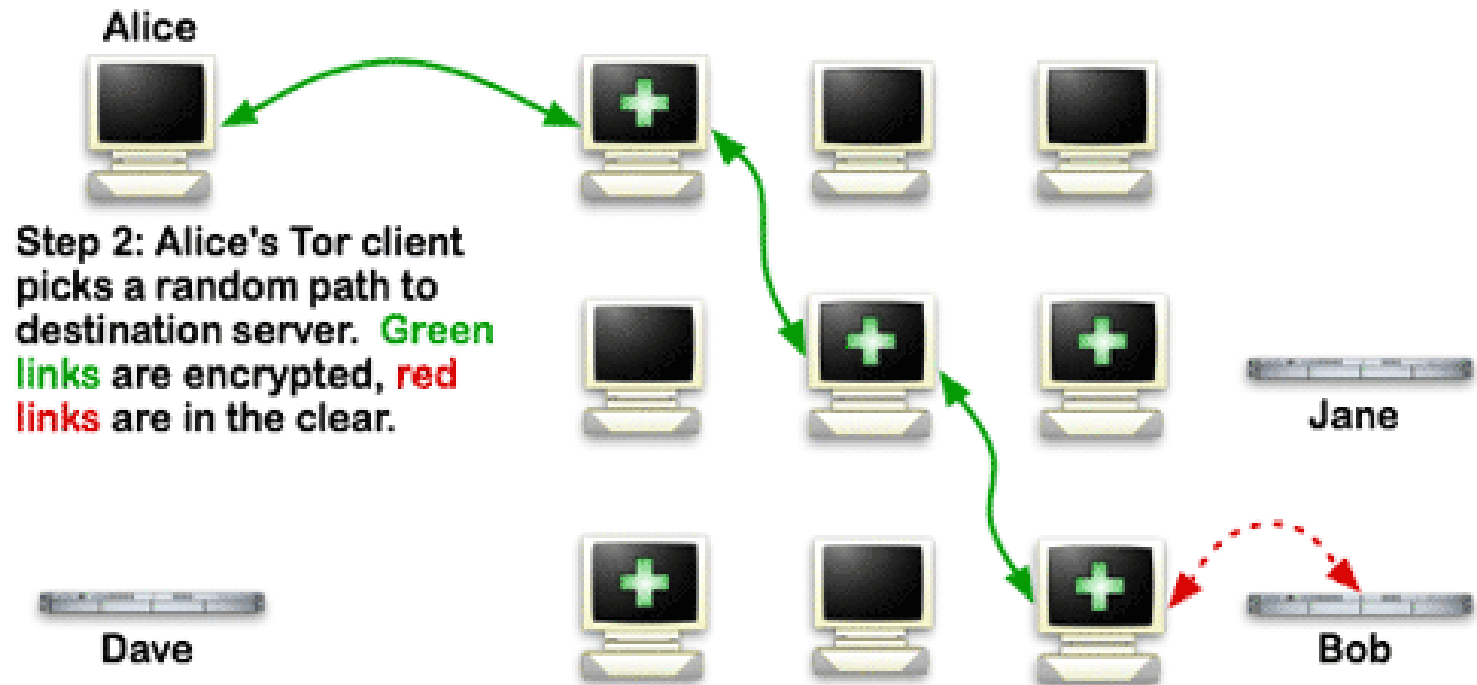
The TOR project



The TOR project

How Tor Works: 2

 Tor node
 unencrypted link
 encrypted link



The TOR project

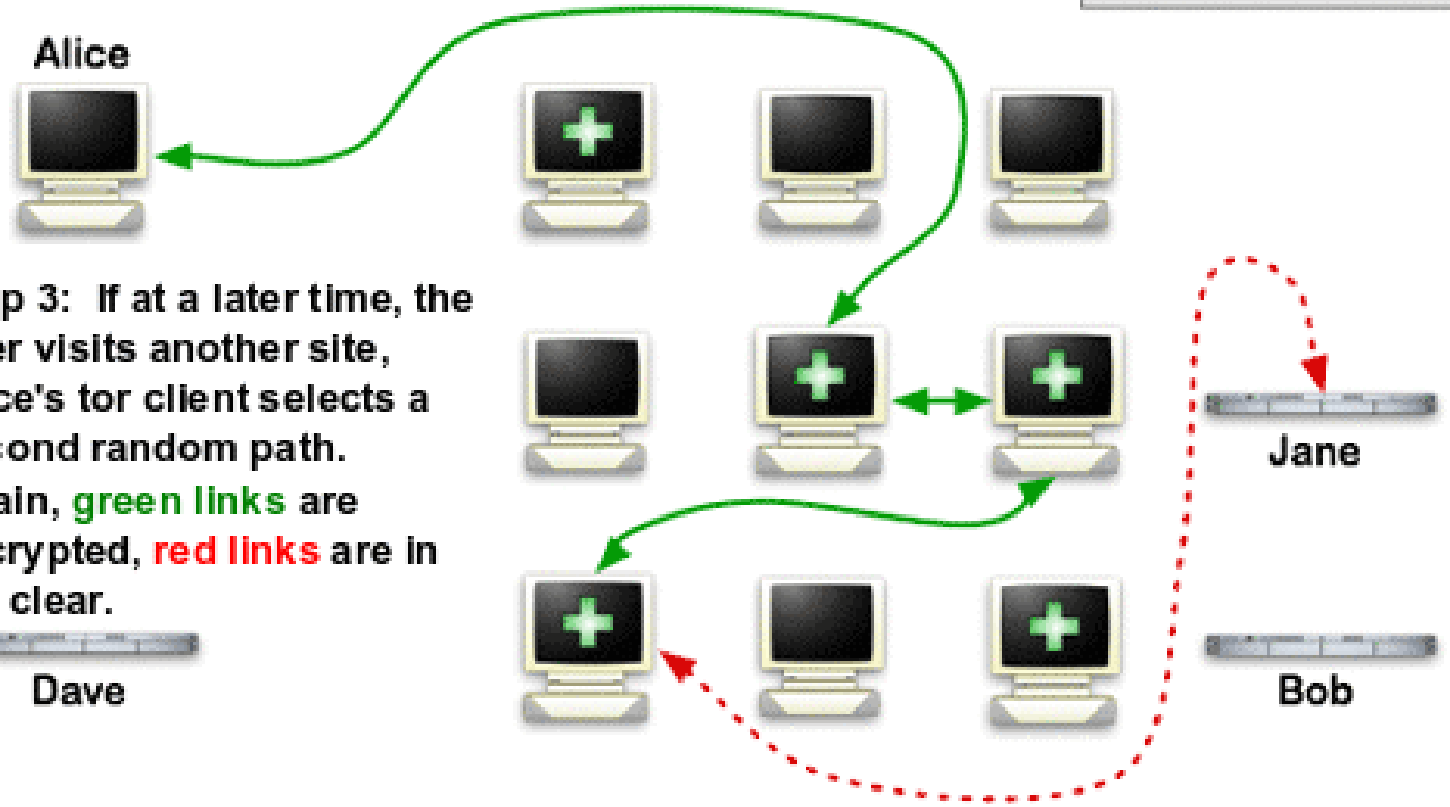
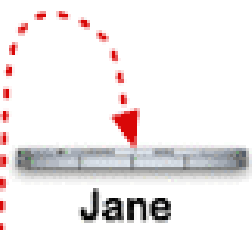
How Tor Works: 3



Alice



Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.



PRIVACY BY DESIGN

A PbD jelentősége

- A személyiségvédelem alapvető konfliktusa...
 - Absztrakt elvek és jogi követelmények
 - Valódi, ténylegesen működő adatkezelő rendszer
- ... és a feloldási lehetőségek.
 - Jogi megfelelési vizsgálat (Legal compliance checking)
 - Audit
 - PIA
 - PbD

A PbD jelentősége

- Az adatvédelem alapelvei
 - Információs önrendelkezés
 - Az adatalany tájékozott beleegyezése
 - Nyílt és törvényes adatkezelési cél
 - Arányosság
 - Jogcím a személyes adatok kezelésére
 - Az adatok integritása és minősége
 - Mentességek és kivételek
 - Adatbiztonság
 - Jogorvoslatok (ex-post)
 - Adatvédelmi biztos / Adatvédelmi hatóság
 - Polgári per
 - Büntetőeljárás

A PbD jelentősége

- A PbD egy lehetséges módja a személyes adatok releváns, hatékony, eredményes és proaktív védelmének
 - Beruházás az adatkezelő rendszer felépítésébe
 - Adatkezelő
 - A PbD ex-ante jogvédelmet jelent

PRIVACY IMPACT ASSESSMENT – (PIA)
ELŐZETES HATÁSVIZSGÁLAT

Mi a PIA?

- PIA > Compliance checking
- PIA > Adatvédelmi audit



A PIA szakaszolása

1. Előzetes intézkedések
 1. Probléma felismerés
 2. Megállapodások
2. Előkészítő szakasz
 1. Szervezet és folyamatok feltérképezése
 2. Áttekintő tanulmányok
3. Konzultatív és elemző szakasz
4. Dokumentáció elkészítése
5. Ellenőrzés
 1. Intézkedések hatásosságának felmérése
 2. Visszacsatolás / Javítás
6. Tanúsítás, auditálás

A PIA kockázatelemzési ismérvei

- Magánszférába tolokodó technológia alkalmazása
 - (Privacy intrusive technology)
- Újszerű azonosító technológiák és módszerek
- Anonimitás és pszeudonimitás kizárása
- Outsourcing alkalmazása???
- Többszintű adatkezelő/feldolgozó intézményrendszer
- Jelentős mennyiségű személyes adat újszerű feldolgozása
- Adatintegráció → Személyiségprofil kialakítása
 - Adattisztítás
 - Összefűzés
 - Kereszthivatkozások
- Vannak-e releváns mentességek vagy kivételek?
 - Nemzetbiztonsági, közbiztonsági érdekből
 - Személyes adatok rendszeres és törvényes közzététele
 - Üvegseb

That's all Folks!

