Szolgáltatások biztonsága

Dr. Fehér Gábor, PhD

Szolgáltatások biztonsága

- Vizsgálat több szemszögből
  - A felhasználó és a felhők
  - Felhasználó a felhők között
  - A felhők és a felhasználó

A felhő szolgáltatás biztonsága a felhasználó szemszögéből

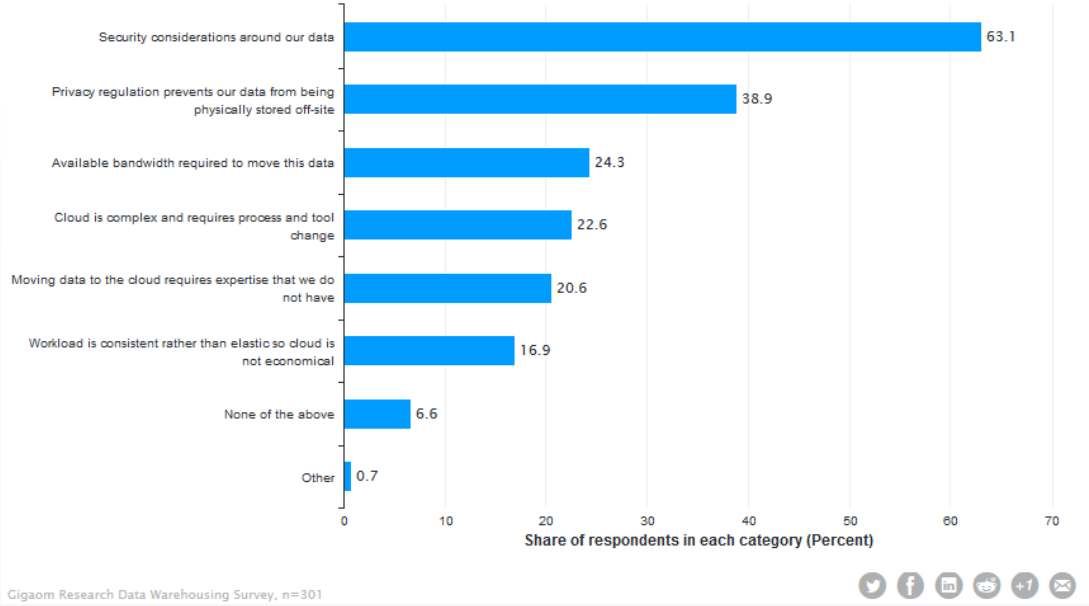
A felhasználó és a felhők

Felhő szolgáltatások biztonsága

- Biztonság, mint a felhő szolgáltatás terjedésének gátja
  - A biztonsággal kapcsolatos aggodalmak továbbra is vezető pozícióban a felhő megoldások elutasításánál
  - Szintén vezető indok, a biztonsághoz köthető bizalmasság (privacy) kérdése

SECURITY

PRIVACY



Felhő szolgáltatások biztonsága 2.

- Kik láthatják az adataimat?
- Hol van az adatom?
- Hihetek-e a felhőből származó adatoknak?

Felhő szolgáltatások fenyegetései

- CIA modell
  - A legkritikusabb 3 komponens
    - Confidentiality – Integrity – Availability

- Bizalmasság – confidentiality
  - A felhőben tárolt adat védelme
  - Adatszivárgások megelőzése
  - Védelem a felhő szolgáltatóval szemben

- Adathelyesség – Integrity
  - A felhőben lévő számítások helyessége
  - A felhőben tárolt adatok helyessége

- Elérhetőség – Availability
  - Védelem a felhő támadása esetén
  - Védelem a szolgáltatás kiesése/megszűnése esetén

Felhő szolgáltatások további fenyegetései

- Megnövekedett támadási felület
  - A felhő maga is támadható
    - Támadások a felhő szolgáltató alkalmazottain keresztül
  - A felhő hálózati kapcsolata is támadható
    - Az adatok az interneten mennek a felhőbe
  - Az erőforrásokon másokkal is osztozunk

- Nehéz/lehetetlen audit és nyomozás

Védelem a felhő szolgáltatóval szemben

- Támadó
  - A felhő szolgáltatás gonosz alkalmazottja
  - A felhő szolgáltató maga

- Képességek
  - Elérhető tárolt adatok
    - Teljes másolat készítése
    - Észrevétlen próbálkozás a másolaton
    - Fájlrendszer közvetlen elérése
  - Elérhető futó kódok
    - Teljes memóriatartalom elérése
    - Programkönyvtárak cseréje
  - Elérhető hálózati kapcsolatok
    - Hálózati adatok tükrözése

Untrusted third party

Védelem a felhő szolgáltatóval szemben

- Motiváció
  - Adatok megismerése
    - Adatok manipulálása
  - Az ügyfelek megismerése
    - Jövedelmezőbb árazás
    - Szolgáltatás fejlesztése
  - Információ saját használatra / eladásra

Támadó ✓ Képesség ✓ Motiváció ✓

Védelem? Bizalom?

Host proof védelem

- A „confidentilaity” problémák megoldása a titkosítás
  - A megfelelően titkosított adatok nem visszafejthetőek a kulcs ismerete nékül
    - A megfelelő titkosító kellő hosszúságú kulccsal rendelkezik a nyers erő támadások kivédésére
  - A kulcs ismerete/tárolása/használata nagyon fontos kérdés

- Felhő tárolók esetén a „host proof” módszer nyújthat megoldást
  - Az adatokat a felhő titkosított fromában tárolja
  - A titkosítást még az ügyfél végzi, a csak számára ismert kulccsal
  - Nincs szükség a bizalomra

  - A titkosítva tárolt adat a felhőben nem visszafejthető
  - A titkosítva tárolt adat a felhőben nem kereshető/megosztható/szerkeszthető/...

Host proof védelem 2.

- A kliens oldalon történő titkosítás
  - JavaScript segítségével (legtöbbször webes elérés esetén)
    - A feltöltés/letöltés támogatása egyelőre nem kellően megoldott
    - A scriptek integritásának ellenőrzése nem egyszerű
  - Böngésző bővítménnyel
  - Natív kóddal
  - Az ellenőrzés nem egyszerű, a kód lehet összezavart, nehezen elemezhető
  - A kód legtöbbször a felhő szolgáltatótól származik (zárt APIk)
    - Nyílt kód esetén sem egyszerű – általában szakember végzi és tanúsítványt csatol
- Sokszor a tárolás más felhő szolgáltatónál történik

Host proof szolgáltatások (példák)

- Host proof / zero knowledge

Teljesen homomorfikus titkosítás

- A műveletet a titkosított adatokon végezzük, de az eredmény a titkosítás feloldása után is helyes
  - A kriptográfia szent grálja

- Sajnos egyelőre csak elméletben létezik, a gyakorlatban
  - Lassú futás
  - Rövid kulcs
  - Kis adat
  - De van remény!
- A teljesen homomorf titkosítás segítségével a számítási felhő szolgáltató számára a titkosított adatok elérhetetlenné válnak

Felhő erőforrások megosztása

- A felhő természete révén a felhasználó sok más felhasználóval közösen veszi igénybe az aktuális gép erőforrásait
  - Lehetőség nyílik hibák kihasználására és a gépek közötti átjárásra
  - Cross VM / Inter VM támadások

- Szoftverhibák kihasználása – VM escape
  - Cloudburst, VMWare (2009)
    - Emulált 3D gyorsítóban lévő hiba kihasználása
  - VENOM, QEMU, Xen, KVM (2015)
    - Virtuális floppy meghajtóban lévő hina kihasználása
    - Alapból engedélyezve még akkor is, ha a rendszer nem használja

Felhő erőforrások megosztása 2.

- „Sidechannel” támadások
  - Pontosan megfigyelt működési idők és ebből következtetések
    - Kriptográfia műveletek sokszor nagyon időigényesek
    - Az idő igény függ a a használt kulcstól is
    - A kulcs mefgejthető ha ismerjük a művelet időigényét
  - Általában a cahce mehanizmusok mértékének és idejének mérése
  - Nagyon „zajos” mérések
    - Nem életszerű a fenyegetés, de létezik „proof-of-concept”

Nincs védekezés?

- Leállított gépek támadása
  - A gép nem elérhető kikapcsolt állapotban, de ez nem jelenti, hogy valóban nem támadható!

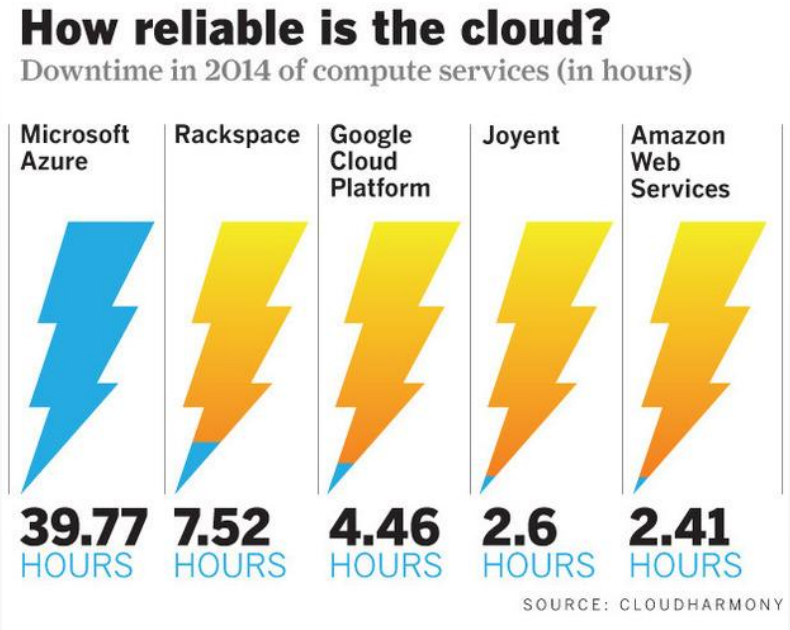
Felhő erőforrások megosztása 2.

- A támadónak azonos gépre kell kerülnie az áldozattal
  - Ha nincs közösködés, az biztonságos, de a szolgáltató számára nem hatékony -> lesz szomszéd
  - Az áldozat gépe bemérhető
    - Hálózati felderítő toolok (traceroute, ping, TTL, …)
    - Kisérletezés az adott gépről indulva (időmérés)
  - Elosztó algoritmus vizsgálata
    - Hansonló feladat, hasonló terhelések eredményezhetnek közös gépet
    - Azonos indulási idővel is kerülhetnek gépek egymás mellé

Felhők elérhetősége

- Felhő SLA
  - Legtöbb esetben IaaS felhő elérhetőségi garanciája
    - 99% - 99.99% (99%: 3.65 nap kiesés / év - vagy - 7 óra / hónap)
    - Sokszor aggregrált érték az összes példányra vonatkozóan
  - Válaszidő, hibaelhárítási idő
  - Nem teljesítés esetén jóváírás a felhasználónak

- A felhőben tárolt adatok, szolgáltatások szétszórása növelheti a rendelkezésre állást
  - Védelem a hálózati hibák ellen
  - Szoftveres hibák esetén ritkán véd



Pl. Amazon CloudFront

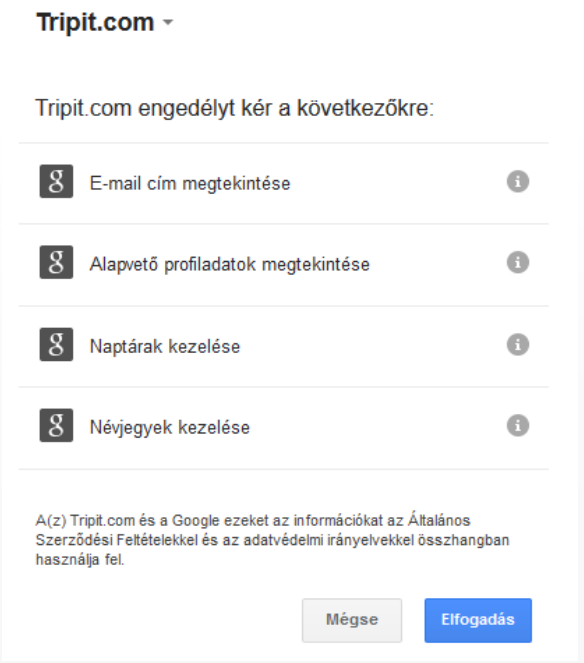
Jogosultságkezelés felhő szolgáltatásokkal

Felhasználó a felhők között

Szolgáltatások jogosultságkezelése

- Több felhő szolgáltatás esetén a felhasználó összekapcsolhatja a szolgáltatásokat a bővebb funkcionalitás végett
  - Pl.: kapcsolatok, naptárak tárolása (google) + utazást segítő szolgáltatás (tripit)

- OAuth
  - Jogosultságkezelés a felhőszolgáltatások adatai között



OAuth jogosultságkezelő protokoll

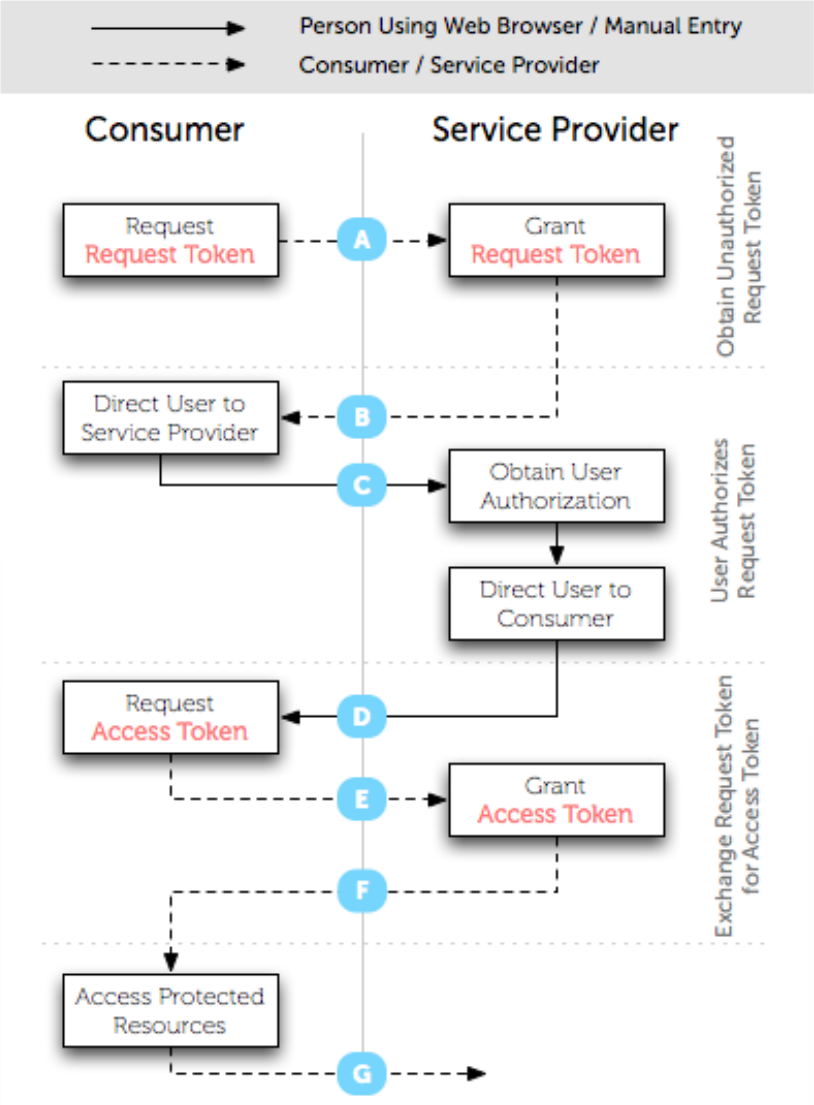
- Jogosultság delegáció a felhasználó hitelesítési adatai nélkül

Ilyen esettel remélhetőleg már nem találkozunk!

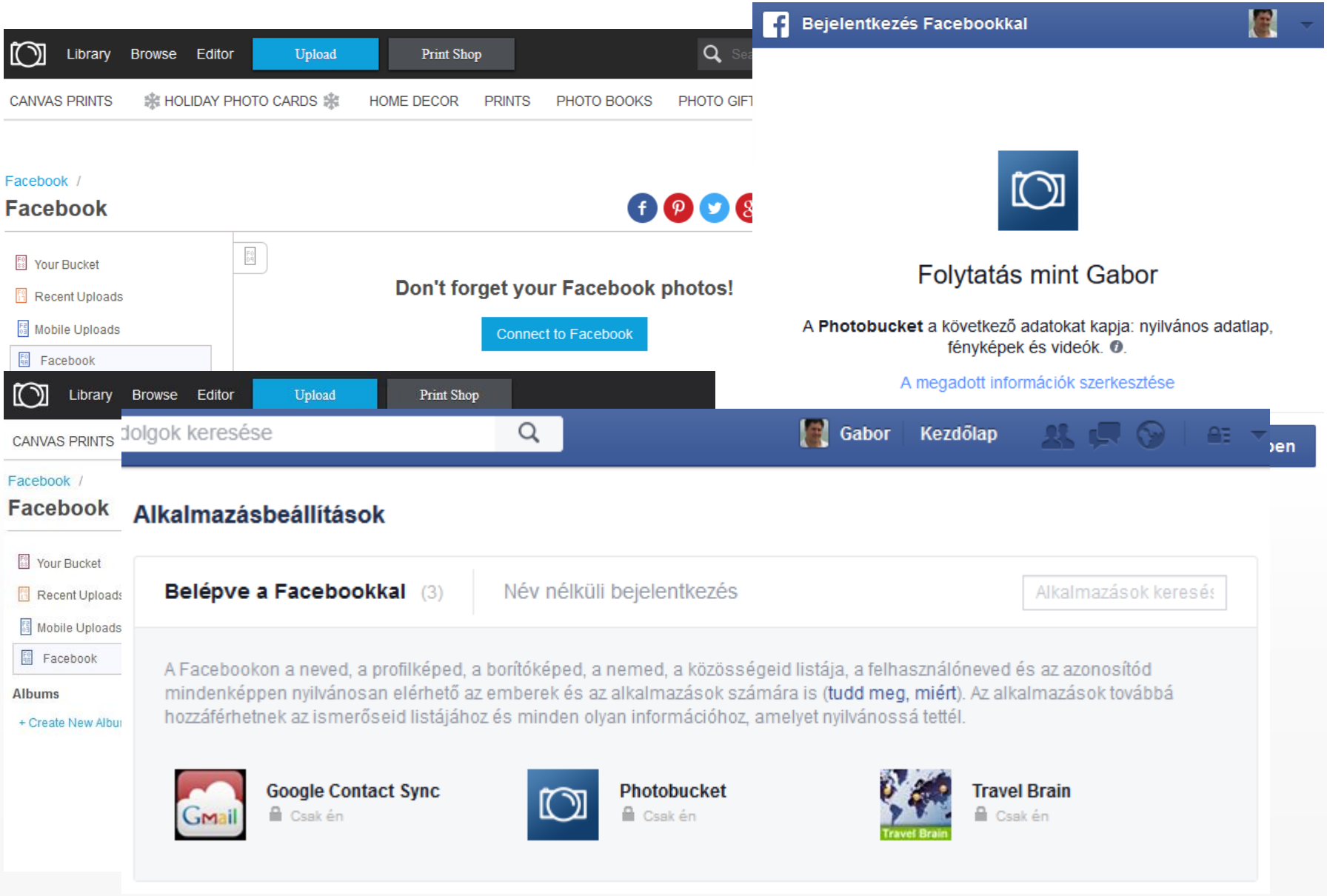
- A hitelesítés nem delegálódik, csak a jogosultságok kerülnek beállításra!

OAuth jogosultságkezelő protokoll 2.

- Consumer
  - Szolgáltatás, aki a felhasználó adatait használja
  - Regisztrálnia kell a kívánt adat szolgáltatónál
  - A kérésben megnevezi, mely adatokat szeretné elérni
- Servcie Provider
  - Szolgáltatás, aki a felhasználó adatait szolgáltatja
  - Tokenek a szolgáltatásoknak
- Request Token
  - Token az azonosításhoz
- Access Token
  - Token az információhoz
  - Frissíteni kell



OAuth példa


Library
Browse
Editor
Upload
Print Shop
CANVAS PRINTS
HOLIDAY PHOTO CARDS
HOME DECOR
PRINTS
PHOTO BOOKS
Facebook /
Facebook
Your Bucket
Recent Uploads
Mobile Uploads
Facebook
Albums
Don't forget your Facebook photos!
Connect to Facebook
Bejelentkezés Facebookkal
Folytatás mint Gabor
A Photobucket a következő adatokat kapja: nyilvános adatlap, fényképek és videók.
A megadott információk szerkesztése
Gabor
Kezdőlap
Alkalmazásbeállítások
Belépve a Facebookkal (3)
Név nélküli bejelentkezés
Alkalmazások keresés
A Facebookon a neved, a profilképed, a borítóképed, a nemed, a közösségeid listája, a felhasználóneved és az azonosítód mindenképpen nyilvánosan elérhető az emberek és az alkalmazások számára is (tudd meg, miért). Az alkalmazások továbbá hozzáférhetnek az ismerőseid listájához és minden olyan információhoz, amelyet nyilvánossá tettél.
Google Contact Sync
Csak én
Photobucket
Csak én
Travel Brain
Csak én

OAuth 2.0

- OAuth 2.0 biztonság
  - Túlságosan bonyolult és és nem feltétlenül biztonságos
  - A megfelelő implementációval biztonságos lehet
    - Google és Facebook implementációk biztonságosak

A felhasználó nyomonkövetése a felhőben

A felhő és a felhasználó

Privacy-enhancing technologies (PET)

- A felhasználók privát szférájának védelme
  - Rendelkezés a felhasználó saját adatairól, irányítás
  - Harmadik fél adatgyűjtésének minimalizálása
  - Anonimitás, összekapcsolhatatlanság
  - Ellenőrzés a szabályok betartásával kapcsolatban

- Eszközök
  - Titkosítás
  - Házirendek (policy)
  - Szűrések
  - Anonimitás

Titkosítás

- Védelem az adatok számára
  - Ki ellen véd és hol?

- Új titkosítási módszerek megjelenése
  - Identity Based Encryption (IBE)
  - Attribute Based Encryption (ABE)
    - Az adatok attribútumok alapján titkosítottak. A felhasználó a megfelelő jogosultságokkal hozzáférhet a számára elérhető adatokhoz.
    - Titkosítás + jogosultságkezelés
    - Szenzor adatok titkosítása, felhő tárolás

- Szükséges alap, de magában még nem elégséges
- Ritkán automatikus, legtöbbször a felhasználó maga intézi
  - De pl. HTTPS enforcer

Házirendek

- Védelem web böngészés közben
  - World Wide Web Consortium (W3C)
  - Pl.: TRUSTe

- Utasítások/házirendek a böngészők, web szerverek számára
  - A felhasználó meghatározza saját preferenciáit
  - A web szerverek betartják a házirendet figyelembe véve a felhasználó kéréseit
  - A web szervereket automatikusa megfigyelik/tesztelik
  - Tanúsítványok kiállítása

Tracking Preference Expression (W3C)

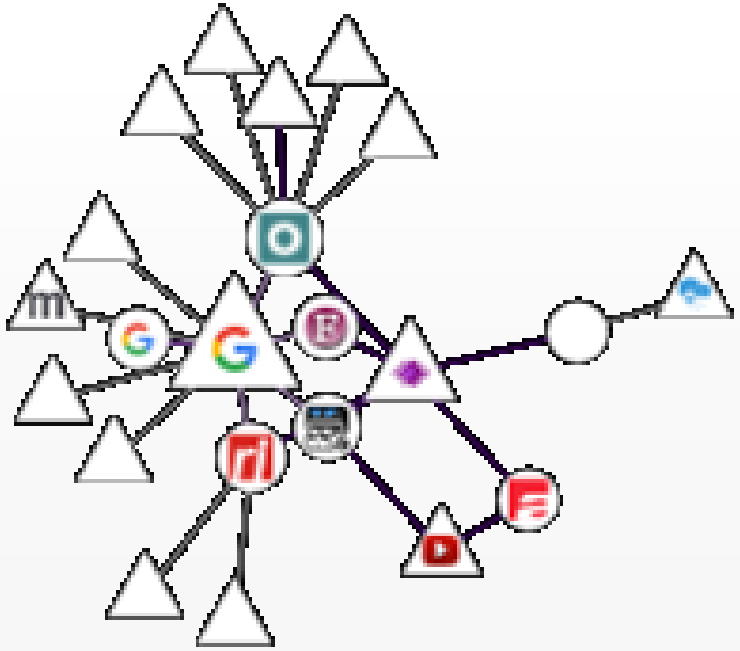
- Do Not Track (DNT) mező
  - Felhasználó preferenciája a követéssel szemben
  - Scriptek számára feldolgozható
  - API a kivételek kezeléséhez
  - Információs és státusz a felhasználó számára

```
GET /something/here HTTP/1.1
Host: example.com
DNT: 1
```

Felhasználók nyomonkövetése / Tracker

- Felhasználók felismerése
  - Megfigyelés több látogatott oldalon keresztül is
  - Látogatások kapcsolata
    - Keresés az egyik oldalon – reklám egy másik oldalon
  - Relámok pontosabb eljuttatása

- Módszerek
  - Sütik (Cookies)
    - Flash / hagyományos sütik
  - Javascript
  - Etags
    - Cache bejegyzés
  - Tracker Beacons
    - Apró képecskékbe rejtve



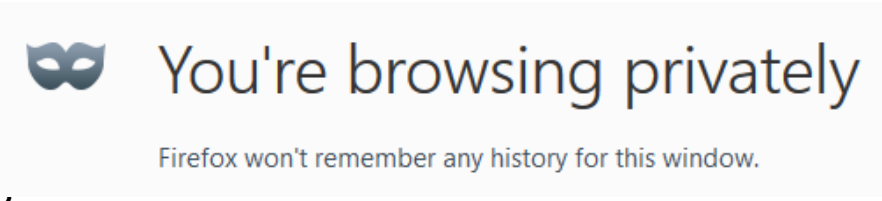
Szűrések

- A trackinghez módszerek szűrése
  - Nehezen működő megoldások, legtöbbször a böngészési élmény rovására megy
  - Csak az ismert minták szűrése
    - Fehér listák készítése
    - Minták bővítése közösségi alapon

Anonimitás, pszeudo-anonimitás

- Segítségével a nyomonkövetők elvesztik a kapcsolódási információkat
  - Minden kapcsolat tiszta lappal indul

- Bongésző anonimitása
  - Private mode
    - Böngésző zárása után minden
    - JavaScript? Tracker beacons?



- Hálózati anonimitás
  - A hálózati kapcsolat anonimitása
    - „Anonim” IP címek használata

- Pszeudo-anonimitás
  - Különböző „anonim” identitások váltogatása

Anonim hálózatok

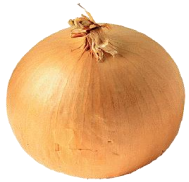
- VPN, proxy megoldások
  - A felhasználó a VPN szerver IP címén látszik
  - Választható végződések
  - Ígéret szerint, a felhasználó forgalmát nem figyelik
  - BitCoin fizetési lehetőség

- A forgalmat sokszor mégis figyelik
- Nem teljesen anonim, inkább egy másik identitás
  - Pl.: útvonaltervezés hazáig?

- Legális / illegális proxy listák
  - SOCKS5

TOR – The Onion Router

- Hálózati anonimitás
  - Hálózati kapcsolat a résztvevő állomásokon keresztül
  - Minden egyes kapcsolat titkosítva van
    - Az állomások nem ismerik a rajtuk átmenő forgalmat
      - Minden állomás csak a saját rétegét hámozza le (hagyma) az igazi adat legbelül van
    - Az utolsó állomás kivétel
      - Az utolsó állomás identitását vesszük fel
      - Az utolsó állomásnál már az eredeti forgalom jelenik meg
  - A hálózati kapcsolatok (hurok) szabadon alakítható
    - Választható kimementi pontok



TOR – The Onion Router 2.

- Hidak
  - A tor végpontok ismertek, így az ISP tilthatja ezeket. A hidak nem publikus végpontok , rajtuk keresztül csatlakozhat a blokkolt végpont is
- „pluggable transport”
  - Saját hálózati protokoll a blokkolás kivédésére
- TOR szolgáltatások
  - A TOR hálózatban szolgáltatások is lehetnek
    - A szolgáltatás helye ismeretlen!
    - Csak a TOR hálózatban érhető el egy randevú ponton keresztül
- TOR Browser
  - Anonim, védett böngésző + TOR hálózat
    - Még így sem teljes a védelem. Bizonyos forgalmak a böngészőn kívül is mehetnek!

Tökéletesebb anonimitás

- TOR + VPN
  - VPN elérés TOR hálózaton keresztül
    - Kliens -> VPN kliens -> TOR -> VPN szerver -> szerver
    - A VPN nem ismeri a felhasználó belépési pontját
    - A TOR hálózat utolsó elem nem ismeri a valódi forgalmat és célállomást
    - Egyelőre korlátozott támogatás

- TAILS - **t**he**a**mnesic**i**ncognito**l**ive**s**ystem
  - „Live” virtuális gép a tor köré építve
  - Ami a gépből kimegy, biztosan titkosítva van, nincs megkerülés
  - Kikapcsolás után minden adat elvész
  - Kriptográfiai alkalmazások az anonim használathoz
    - USB, Email tikosítás, HTTPS kikényszerítés, biztonságos törlés, ...