Újgenerációs anonim böngészők

GULYÁS GÁBOR, SCHULCZ RÓBERT

Budapesti Műszaki és Gazdaságtudományi Egyetem, Híradástechnikai Tanszék
schulcz@hit.bme.hu

Kulcsszavak: web, böngészők, anonimitás, paradigma

A web már régóta felvet adatvédelmi kérdéseket a látogatók számára is: bizonyos szolgáltatók megfigyelik a felhasználók tevékenységeit, követik őket, adatbázist építenek ízlésvilágukról. Az anonim böngészők megoldást kínálnak a felhasználóknak, elrejtik őket a figyelő szemek elől. A cikkben bemutatunk néhány követésre használt módszert, illetve egy új, az anonimizáló szolgáltatásokra vonatkozó konstrukciós paradigmát, majd egy ez alapján értelmezett osztályozási rendszert is az anonim böngészők besorolásához.

1. Bevezető

A web böngészése során a látogatott weboldalak információszolgáltatás mellett adatokat is gyűjtenek; hálózati jelenlétünk, a használt böngésző, a böngészés folyamata olyan információkat árulnak el rólunk, amely tevékenységünket megfigyelhetővé, követhetővé teszi. Később az összegyűjtött információkat tartalmazó profil adatbázis direktmarketing célokra használható (célzott hirdetések, SPAM), kereskedni lehet vele, vagy akár dinamikus, személyre szabott árlista generálására használható webes boltokban. Ez az adatgyűjtés sokszor nem egyetlen weboldalra, vagy egy on-line tartalomszolgáltató hálózatára vonatkozik, hanem a szolgáltatók más partnerekkel együtt dolgozhatnak, így szélesebb skálájú profilt készítve a felhasználóról.

Bizonyos szituációkban valamilyen szolgáltató (vagy például egy cenzúrázó szerv) ki szeretné deríteni egy felhasználó személyét, az aktivitásáról készít naplót, vagy – a leggyakoribb esetben – blokkolná bizonyos tartalmak elérését.

Valamennyi felsorolt esetben megoldást kínálnak az anonim böngészők, garantálva a szolgáltatásban az anonimitást, és lehetőséget adva a cenzúra megkerülésére. Az anonim felhasználó tevékenységeit a tartalmak szűrésével összeköthetetlenné, titkosítással pedig a külső szemlélők számára megfigyelhetetlenné teszik. Továbbá biztosítják, hogy a felhasználónak az anonimitásból eredően nem fedhető fel valós személye, mivel tevékenységei sem illethetők pszeudonim azonosítóval.

A cikk bemutatja a külső-belső világ konstrukciós paradigmát, amelynek minden anonimizáló rendszernél szükséges feltétel és azt is körüljárjuk, milyen feltételeknek kell teljesülnie a paradigma megvalósításához a webes világban. Egy új, továbbfejlesztett osztályozási szempontrendszert is ismertetünk, amely a paradigma teljesítésének vizsgálatában játszik szerepet, így arra épül és felöleli [1]-ben olvasható attribútumokat is. Továbbá vizsgálunk olyan követési módszereket és technikákat, amelyek kiegészítő képet adnak [1]-hez képest.

2. Külső-belső világ konstrukciós paradigma

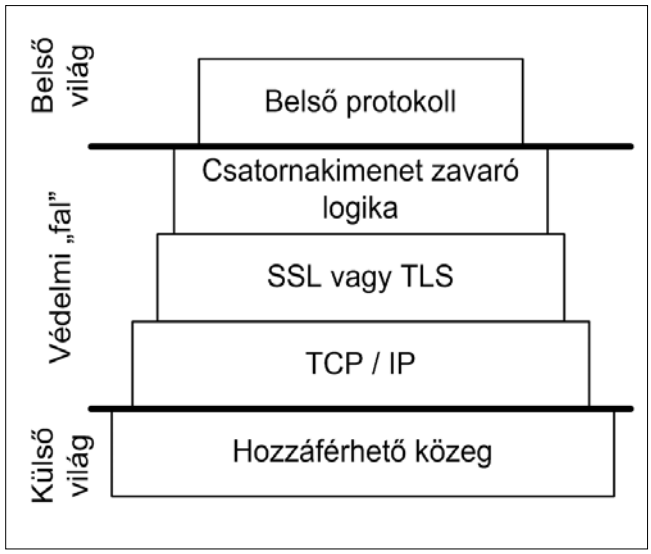
2.1. A paradigma általában: anonimitást nyújtó rendszerek

A külső-belső világ paradigma szerint egy szolgáltatás akkor nyújthat anonimitási lehetőséget a belső felhasználók számára, ha a belső protokoll működése külvilágtól teljesen szeparált (a belső műveletek forgalomanalízistől, megtekintéstől és módosítástól védettek), valamint egy szolgáltatásbéli felhasználó nem képes kompromittálni más belső felhasználó anonimitását, kivéve, ha az adott művelet a belső működést leíró protokoll szerint szabályos (például, ha operátor tehet ilyet).

Szükséges az alábbi két feltétel teljesülése:

1. A külső világ a megfelelő anonimizáló protokoll által le van választva a belső világ működéséről, tehát egy olyan fél, amely a szolgáltatásnak nem résztvevője, képtelen megfigyelni a belső működést, valamint befolyásolni azt.

1. ábra Egy lehetséges protokollverem a külső világ szeparációjához



2. A belső protokollban a tervezése során biztosítani kell az anonimitás lehetőségét a belső világ felhasználói között (nem csak opció, kötelező is lehet).

Ennek egy lehetséges megvalósítása látható a *1. ábrán*. A védelmi fal funkciójában egy anonimizáló protokoll kell, hogy legyen, amely vagy külön hálózatra épül, vagy a kommunikációs protokollba van beépítve, mint az ábrán.

2.2. Szükséges kritériumok az anonimitás teljesüléséhez

Az anonimitás teljesüléséhez további kritériumoknak kell teljesülnie, amelyet a külső-belső világ paradigmában megfogalmazott szeparációs modellnek meg kell valósítania (1-2. kritérium), és a belső világ protokollnak is ki kell elégítenie (4. kritérium). A kritériumokat [11] a négy fő magánszféravédő és adatvédelmi kritérium alapján fogalmaztuk meg a webes világ értelmezésében.

A kritériumok értelmezésénél a *2. ábrán* látható viszony áll fenn: a felhasználó kéréseket küld B webes kiszolgálónak, ezt próbálja megfigyelni C külső megfigyelő. A kritériumok nem vonatkoznak a D anonimizáló szolgáltatásra, mivel az a működéséből fakadóan ismeri a forgalmazott tartalmat és a kommunikáló feleket is, így feltesszük, hogy az megbízható.

Az A felhasználó és a D anonimizáló hálózat között a kapcsolat titkosított, így a tartalomból a kommunikáció célja nem deríthető ki. Az anonimizáló szolgáltatás egyik célja annak a megvalósítása is, hogy az itt megfigyelhető üzeneteket a D-B szakaszon megjelenő üzenetekkel ne lehessen párba állítani.

1. *Összeköthetetlenség*:
   sem C külső megfigyelő, sem a B kiszolgáló nem képes eldönteni A felhasználó két üzenetéről, hogy azokat ugyanaz az A felhasználó küldte-e, sem pedig, hogy a két üzenetnek egyezik a feladója.
2. *Megfigyelhetetlenség*:
   a kommunikáció tartalmát csak A és B ismerhetik.
3. *Pszeudonim azonosítóval rendelkező felhasználó:*
   a felhasználó tevékenységei összeköthetőek, és egy fedőnévhez, vagy egyéb azonosítóhoz kapcsolhatóak, de ez alapján a valódi személyazonosság nem deríthető fel.
4. *Anonim azonosítóval rendelkező felhasználó:*
   a felhasználó cselekedetei viszony szinten sem köthetőek össze, így üzenetenként független pszeudonim azonosítóval rendelkezik (1 és 3. kritérium).

A kritériumok növekvő sorrendben erősödnek, és az anonimitás eléréséhez valamennyinek teljesülnie kell.

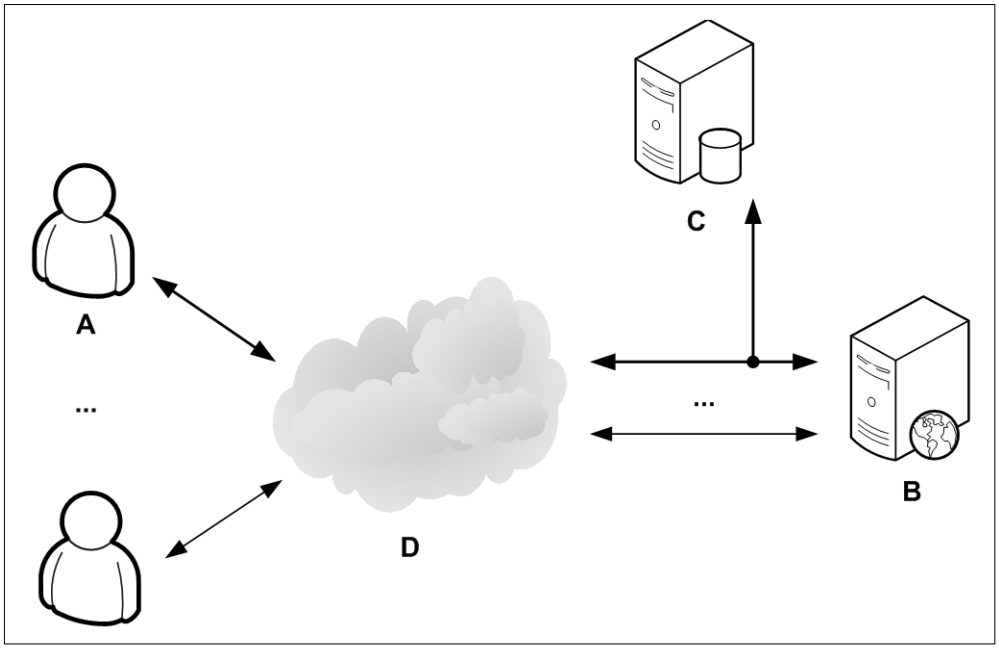
2.3. A paradigma és az anonim böngészők

A vizsgált szolgáltatások a külső világ szeparációját anonimizáló hálózattal oldják meg, amelyek általában TOR [9] hálózatot jelent, mint például a TorPark [10] szolgáltatása esetén. Fontos kiemelni, hogy a szolgáltatás célja nem a belső világ valamennyi szereplőjének az anonimizálása, hanem csak a felhasználóké, a többi résztvevő (például hirdetők) felé.

Anonim böngészők esetén a belső protokoll jól definiált és szabványosított, így ebben az esetben csak tartalomszűrésre van lehetőség. A tartalomszűrés igen sokrétű lehet, mert – amint az osztályozási szempontrendszerből és a következőkben bemutatott módszerekből is látható – számos elem és trükk használható a felhasználó kompromittálására, a szűrés megkerülésére is.

3. Szabotázs az anonimitás ellen – követési lehetőségek

Ezen módszerek közös jellemzője, hogy a felhasználót az első találkozás alkalmával megjelölik valamilyen módon, s ezt a – lehetőleg pszeudonim – azonosítót felhasználva a későbbiekben a felhasználó profilját adatbázisban tárolják.



2. ábra
Hálózati elrendezés a kritérium vizsgálatnál

3.1. Yahoo Web Beacons

A Yahoo Web Beacons egy jó példa arra, hogy megfigyelni nem csak titokban lehet, hanem nyilvános üzletet is lehet csinálni belőle. A Yahoo adatvédelmi szabályzatában található leírás szerint [3] az azonosítókat a saját oldalaikon a felhasználók azonosítására (például számlálóknál), a felület személyre szabására alkalmazzák, amellett névtelen információgyűjtésre a partnereiknél.

A szolgáltatás nyomkövetése OPT-OUT, de a [3] oldalon található linken keresztül lemondható. Ez csak a használt böngészőre érvényes, ráadásul az azonosító süti (cookie) megmarad, így a követés a sütik törlése után folytatódik.

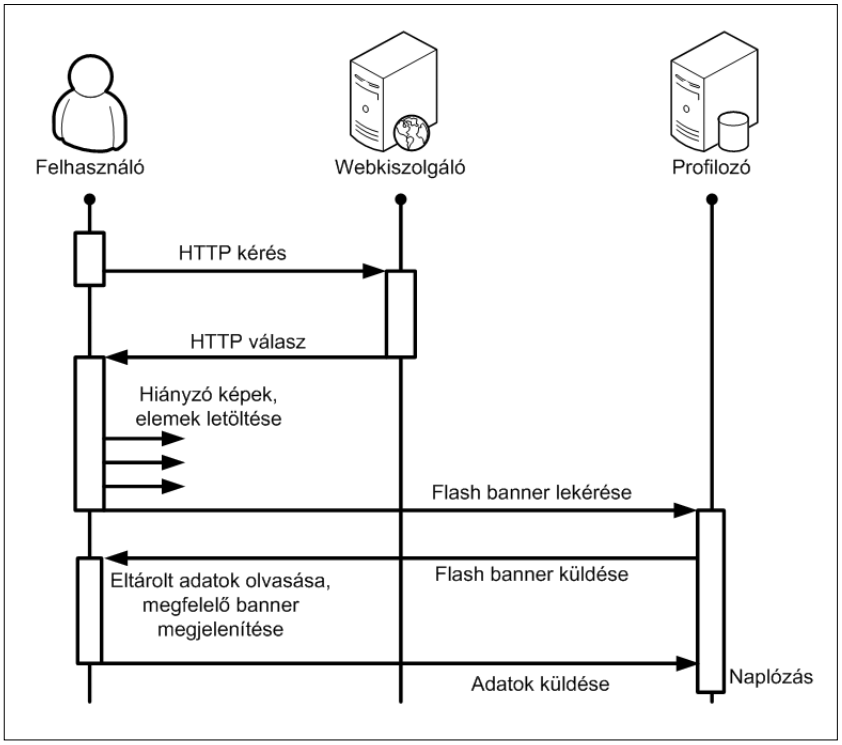
A web beacons a web poloskákhoz [2] hasonló megoldást alkalmaz. A weboldalakon olyan fájlokra mutató linkeket helyez el, amelyek letöltése után a böngészőt egy süti jelöli majd meg. A Yahoo rendszere ennek a sütinek a segítségével követi a felhasználót, és végzi későbbi tevékenységeit.

3.2. Flash PIE

A Flash PIE [4] (Persistent Identification Element, perzisztens azonosító elem) hasonló a web bugokhoz. Működésükben is hasonlítanak és az azonosító tárolása sütikhez hasonló elemek segítségével, az SO-kkal (Shared Object, megosztott objektumok) történik [7].

Az SO-k esetében több, összejátszó weboldalnak könnyebb dolga van, mint a sütiknél, ugyanis esetükben az elérhetőség csak opcionális paraméter. Ennek köszönhetően az oldalak kollaborációja, az egymás között megosztott információk cseréje rendkívül egyszerűvé válik, ugyanígy a felhasználók azonosítása (és a követése) is.

3. ábra
A flash PIE működése



Mivel az SO-k nem a böngésző sütijei között tárolódnak, így könnyen rejtve maradnak a felhasználó szeme elől. Az is előfordulhat, hogy a felhasználó által használt takarító szoftverek nem foglalkoznak ezekkel az objektumokkal, egyszerűen figyelmen kívül hagyják őket.

Egyszerű és általános védekezési megoldás lehet a SO-k tiltása, azonban ez bizonyos szolgáltatások használhatatlanná válásához vezethet, csak úgy, mint ahogy weboldalaknál a sütik mellőzése. A Flash-objektumok bináris formátumúak, így a tartalom szerinti szűrésük nem lehetséges anonim böngészők számára.

3.3. Követés gyorsítótárba mentett JavaScripttel

A JavaScript gyorsítótárazott fájljai alapján történő követés [5] hasonló a web poloskák módszeréhez: a weblaphoz egy JavaScript állományt csatolnak, amelyben egy változóban eltárolnak egy azonosító értéket. Ez az érték elérhető lesz a későbbi látogatások alkalmával, amíg a gyorsítótár nem frissül.

Ezt lehet használni az azonosítót tartalmazó süti pótlására, amelyből minden betöltéskor, ha a süti nincs jelen, újra létrejön és fordítva is: ha a süti létezik, a JavaScript állományba a kiszolgáló a süti értékét írja. Ezt a módszert szemlélteti a [8].

4. Taxonómia a külső-belső világ paradigma alapján

A taxonómia két fő csoportját a külső világ szeparációja, valamint a szűrési mechanizmusok alkotják. Ezen kívül egyéb kritériumokat is érdemes vizsgálni, mert jelentősen befolyásolják a böngésző értékét.

Az osztályozási szempontrendszer célja az anonim böngészők funkcionalitási vizsgálatának lehetővé tétele, a különböző attribútumokba sorolás segítségével. Az alábbiakban az osztályozási szempontrendszer látható.

Külső világ szeparációs megoldásai
- HTTPS
- Alkalmazott anonimizáló protokollok

Belső világ védelme
- Tartalomszűrés helye
  - Kliensoldalon
  - Szerveroldalon
- Szűrt tartalmi elemek, információk
  - Kiszolgálótól érkező
  - JavaScript
  - Java
  - Flash
  - Klienstől távozó
  - Böngésző, operációs rendszer információk
  - URL referer
- „Rosszindulatú” elemek szűrése
  - Reklámok

  - – Felugró ablakok
- Sütikezelési szintek
  - – Szerveroldali tárolás
  - – Bizonyos sütik szűrése
  - – Blokkolás (mind)
- Egyéb helyi nyomok törlése
  - – Gyorsítótár
  - – Előzmények
- HTTPS átjátszása (és szűrése)

Hordozhatóság

- Alternatív csatlakozási pont
  - – Klienseken keresztül
  - – Dedikált átjátszók
- Szolgáltatás típusa
  - – Telepített proxy alkalmazás
  - – Webes proxy
  - – Hagyományos proxy (csak be kell állítani)
  - – Hordozható alkalmazás (pl. USB meghajtón)
- Operációsrendszer-, böngészőfüggetlenség

Egyéb kritériumok

- Saját reklámok a szolgáltatásban
- Kezelőfelület alkalmassága (szolgáltatás elhagyása figyelmetlenségből, vagy túl zavaró, sok helyet foglal)
- Forgalomkorlátozás
- Sebességkorlátozás
- Naplózási feltételek

5. Összefoglalás

Webes privátszférát érintő kérdésekkel egyre többen ismerkednek meg, és egyre többen használnak anonim böngészőket. A felhasználók és kutatók számára is fontos, hogy ezeket a szolgáltatásokat objektíven, az elvárt tudásuk alapján értékelni tudják. Ehhez nyújt segítséget a cikkben bemutatott osztályozási szempontrendszer, valamint a kritériumok, amely a szolgáltatás architektúrájának ellenőrzésében nyújtanak segítséget.

Jelenleg kevés szolgáltatás van, amely teljes megoldást kíván nyújtani a felsorolt problémákra, de nagyobb problémát jelent, hogy a jó szolgáltatások fizetősek. Például a TorPark-ot e cikk írásakor fizetőssé alakítják át, miközben az ingyenes, mindenki számára elérhető változat egyszerűen használhatatlan a rendelkezésre bocsátott túl kicsi sávszélesség miatt.

A szerzők remélik, hogy a jövőben a privátszférához való jog nem csak egy szlogen lesz, hanem tény, és nem azon fog múlni a jog teljesülése, hogy valakinek van-e rá pénze, vagy sem.

Irodalom

[1] Gulyás G.:
Anonim-e az anonim böngésző?
Technológiák és szolgáltatások elemzése.
Alma Mater sorozat.
BME GTK ITM, Budapest, 2006. március.

[2] Hullám G.:
A web bug technológia – barát vagy ellenség?
Székely Iván–Szabó Máté Dániel (szerk.):
Szabad adatok, védett adatok.
Alma Mater sorozat.
BME GTK ITM, Budapest, 2005. március.

[3] Yahoo Web Beacons
http://info.yahoo.com/privacy/us/yahoo/webbeacons/details.html

[4] Flash PIE
http://www.mistered.us/tips/flash/settings.shtml

[5] JavaScript alapú követés gyorsítótárral
http://www.mukund.org/blog/101/

[6] Electronic Privacy Information Center
http://www.epic.org

[7] Flash: SO-k (megosztott objektumok)
http://www.adobe.com/cfusion/knowledgebase/index.cfm?id=tn_16194

[8] JavaScript gyorsítótárazást használó követési módszer
http://www.mukund.org/files/archive/2006/09/14/tracking-using-cache.html

[9] TOR anonimizáló hálózat
http://tor.eff.org/

[10] TorPark
http://www.torrify.com/

[11] Gulyás G.:
Az anonimitás és a privacy kérdései a csevegő szolgáltatásokban.
Tanulmányok az információ- és tudásfolyamatokról 11.
BME GTK ITM, Budapest, 2007. május.