

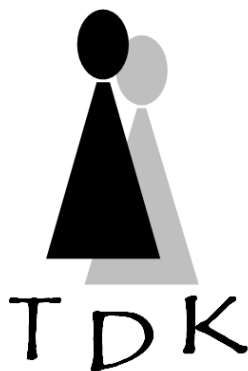


ÚJ SZÉCHENYI TERV

ANONIMITÁS AZ INTERNETEN

Tudományos Diákköri Dolgozat

Konzulens: Balogh Zoltán



Készítette: Oroszi Róbert
Gazdálkodástudományi kar
Mesterképzés
Gazdaságinformatikus szak
I. évfolyam

2012. március 26.

A BCE Közgáz Campus Tudományos Diákköri Konferenciáját a TÁMOP-4.2.2/B-10/1-2010- 0023 azonosítójú “A tudományos képzés műhelyeinek átfogó fejlesztése a Budapesti Corvinus Egyetemen” című projektje támogatja.



MAGYARORSZÁG MEGÚJUL



A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Tartalomjegyzék

1. Bevezetés	5
1.1. Anonimitás felhasználói oldalról	7
1.2. Anonimitás üzleti oldalról	7
1.3. A téma létjogosultsága, megéri vele foglalkozni?	7
2. Technológia	8
2.1. Mit lehet mérni?	9
2.2. Mit érdemes mérni?	13
3. Biztonsági	15
3.1. Anonimitás elleni kísérletek	16
3.2. Anonimitás biztonsági kérdései a böngészőben	16
3.3. Mire érdemes figyelni?	17
3.3.1. Inkognitó mód	19
4. Üzleti	20
4.1. A szereplők	21
5. Összefoglalás	23

Rövidítésjegyzék

ActiveX

ActiveX

Browser Detection

Br.Det.

Feature Detection

Feat. Detection

fehér kalapos hacker - white-hat hacker

white-hat hacker

HTML5

HTML5 egy webes szabványgyűjtemény, amelyet a webes fejlesztők, a böngészők készítői állítanak össze, és amely alapján adaptálják az új funkciókat

IndexedDB - Indexed Database API IndexedDB

ISP - Internet Service Provider

ISP

JavaScript

JavaScript no mi ez lurkó?

Proxy

Proxy

Pwn2Own konferencia

Pw2Own a CanSecWest biztonsági cég éves konferenciájának a részeként kerül megrendezésre.

Aki leggyorsabban át tudja venni az uralmat az internet böngészők aktuális verziója felett, pénzjutalomban részesül.

VPN - virtuális magánhálózat

webStorage

websztorázs

1. fejezet

Bevezetés

Az internet penetráció növekedése (TODO hivatkozás) és az információs társadalom fejlődése miatt a felhasználók egyre több szolgáltatásból választják az online verziót, egyre több időt töltenek (TODO hivatkozás erről?) az internetre csatlakozva.

Az online szolgáltatások széles választéka, és az azokat használó felhasználók adatainak eltulajdonításáról (banki adatok, számlaszámok) rengeteg cikk, tudományos munka készült már, ez a dolgozat azt szeretné bemutatni, hogy az interneten tevékenykedve milyen, szinte láthatatlan nyomokat hagynak maguk után a felhasználók, ezeket kik és hogyan használják ki.

A dolgozat bemutatja, mind felhasználói, mind szolgáltatói szemszögből mire kell odafigyelni (a felhasználóknak mit érdemes elrejtetni, a szolgáltatóknak mit érdemes monitorozni), hogy a lehető legkevesebb vagy éppen a legtöbb információhoz cseréljen gazdát.

A dolgozat végén pedig, egy, a felhasználói profil összeállítására alkalmas szoftver tervezését és megvalósítását ismerheti meg az olvasó.

1.1. Anonimitás felhasználói oldalról

Mivel az internet Magyarországon a rendszerváltás után jelent (TODO első szolgáltató), ezért a felhasználók tudása, és oktatása nem fejlődött az internet sebességével. Ezért sajnos az internetet böngésző felhasználók gyakran nincsenek tisztában, hogy milyen sok mindent elárulnak magukról egy-egy kattintással, elfogadnak olyan kéréseket, amelyeket el sem olvasnak, illetve megbíznak a weboldalakban.

Természetesen léteznek weboldalak, amelyek még a gyakorlott, az anonimitással teljesen tisztában lévő haladó felhasználókat is csapdába csalják.

A dolgozat megpróbál rámutatni, azokra biztonsági szempontokra, amelyeket szem előtt tartva a felhasználót sokkal kevesebbet fog elárulni magáról a böngészése során. Többek között a következő témákat érintve: privát böngészés, külső sütik, HTML5-, RIA veszélyei és lehetőségei.

1.2. Anonimitás üzleti oldalról

Az üzleti oldal természetesen teljesen más oldalról közelít az anonimitáshoz, egy weboldalnak tudnia kell monitorozni a felhasználóit, egy hírportál esetén releváns, célzott reklámokat kell tudni megjeleníteni, amelyhez szükséges egy minél pontosabb felhasználói profil felállítása.

A dolgozatban bemutatásra kerülnek azok a technikák, technológia lehetőségek, melyekkel a felhasználók minél könnyebben, pontosabban beazonosíthatók. Továbbá megvizsgálásra kerül a Facebook, melynek segítségével a felhasználói profil pontosítható.

1.3. A téma létjogosultsága, megéri vele foglalkozni?

Az anonimitás olyan webes alkalmazásoknál, ahol van regisztráció - és kötelező is regisztrálni (email alkalmazások, közösségi média) - természetesen nem kap komoly hangsúlyt, ugyanis tisztában vannak a felhasználóik adataival.

Azonban online hírportáloknál, keresőmotoroknál, ahol a tartalom ingyenesen elérhető és az elsődleges bevétel a reklámokból van, ott kimondottan fontosat szerepet kap a felhasználói profilok felépítése.

Az analitika rendkívül fontos ilyen weboldalak esetén, azonban nem képes arra, hogy megmondja az oldalra látogató felhasználókból, hogy volt-e már az oldalon, illetve mennyit töltött és milyen tartalmak érdeklik.

2. fejezet

Technológia

A felhasználó azonosítása hálózati kapcsolaton keresztül történő kommunikáció során figyelhető meg leginkább, ezért a technológia áttekintés a webes technológia lehetőségeire fog fókuszálni.

A webes technikák fejlődése egy inkább biztonságossá teszi a böngészést, amellet az új funkciók bevezetésével egyre több lehetőséget kínál a felhasználók azonosítására.

A modern böngészők egyre több mérési lehetőségeket kínálnak a következő pontban összefoglalásra kerül, hogy mik ezek, milyen adatokat tudhatunk meg ezek segítségével a felhasználóról. Ezután pedig a lehetőségeket kerülnek mérlegelésre technológia szempontból, hogy melyek azok az adatok, amelyek valóban információkat is tartalmaznak.

2.1. Mit lehet mérni?

Szerver oldali mérés A böngészők már a weboldal lekérések elküldésekor is számottevő mennyiségű adatot küldenek el a szervereknek. A 2.1 ábrán látható HTTP kérésből jól látható, hogy felhasználó milyen böngészőt használ (*User-Agent*), amely tartalmazza az operációs rendszer típusát (*Mac OS X*), a böngésző verziószámát (*Chrome 17*), a böngésző kompatibilitását (*Mozilla 5.0, AppleWebKit, Safari*). Továbbá fontos megemlíteni az fejlécben lévő sütiket (*Cookie*), amelynek segítségével, a webszerverek azonosítják a felhasználókat.

A 2.1 ábrán látható sütik kiválóan bemutatják a webes anonimitás/azonosítás fontosságát, ugyanis az `__utma` és az `__utms` sütiket a Google Analytics webanalitikai szoftver használja felhasználók azonosítására.

A kérés fejlécéből még megállapíthatóak, olyan adatok, mint a felhasználó operációs rendszerének/böngészőjének nyelvi beállítása (*Accept-Language*) vagy éppen a használt karakterkódolás (*Accept-Encoding*).

```

Accept:text/html,application/xhtml+xml,application/xml;q
    =0.9,*/*;q=0.8
Accept-Charset:UTF-8,*;q=0.5
Accept-Encoding:gzip,deflate,sdch
Accept-Language:en-US,en;q=0.8
Cache-Control:max-age=0
Connection:keep-alive
Cookie:__utma
    =176087398.927465515.1331063740.1331063740.1331063740.1;
    __utmz=176087398.1331063740.1.1.utmcsr=(direct)|utmccn=(
    direct)|utmcmd=(none);
Host:www.uni-corvinus.hu
User-Agent:Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_2)
    AppleWebKit/535.11 (KHTML, like Gecko) Chrome/17.0.963.79
    Safari/535.11

```

2.1. ábra. Egy HTTP kérés fejléce

Kliens oldali mérés Azonban, a legtöbb adatot a böngészők nem küldik el a kéréskor, hanem JavaScript segítségével lehet kinyerni a böngészőből. A HTML5 ajánlások bővülésével a JavaScript nyelv segítségével, egyre közelebb lehet kerülni az operációs szintű funkciókhoz, természetesen a megfelelő biztonsági korlátozások mellett.

A HTTP fejlécben látható adatok, mind elérhetőek JavaScript segítségével is (ez alól kivételt jelentenek a biztonságos címkével ellátott sütik). De milyen plusz adatok érhetőek kliensoldalról?

Böngészőképessegek A felhasználó böngészője által implementált képességek, amelyből kinyerhető, hogy a felhasználó milyen a böngészők használ. Természetesen mind ezt elárulja a HTTP fejlécben található *User-Agent* is, azonban a HTTP fejléc a legtöbb böngészőben kézzel is módosítható, tehát az ilyen detektálásból (*Browser Detection*) gyakran fals-pozitív vagy fals-negatív azonosítás születhet, míg a JavaScript alapú megoldásból (*Feature Detection*) mindig pontos születik.

Bővítmények Olyan fontos - és hosszútávon állandó - adatok is kiolvashatók a böngészőkből, mint például a felhasználó által telepített bővítmények (pluginek). Ebben a

kategóriában a következő elemek fordulhatnak elő:

- **Adobe Flash**

Az Adobe Flash bővítmény pontos neve, és verziószáma, videók lejátszásához, streameléshez, animációkhoz használják.

- **Java**

A böngészőbe telepített Java bővítmény verziószáma, komplex hálózati adatfolyamok kezelésére, magas biztonsági szintet megkívánó alkalmazások (például internet-bankok) futtatására használják.

- **Silverlight**

A Microsoft Silverlight bővítménye, videók lejátszásához, és adat streameléshez használatos.

- **PDF olvasó**

Böngészőbe épített PDF olvasó, ez lehet alapértelmezett böngésző része, vagy külső beépülő bővítmény is lehet (például Adobe Reader).

Képernyőadatok A kliensoldalon hasznos adatok érhetőek JavaScript és CSS segítségével, a felhasználó által használt monitor felbontásáról, színmélységéről.

Sütik A webes alkalmazások sütikben (cookie) tárolják a felhasználókhoz kapcsolódó információkat, ilyenek lehetnek például a bejelentkezéshez, a legutóbbi látogatáshoz tartozó adatok. Ezek böngészőkhöz vannak kötve, tehát ha a felhasználó egy másik böngészőt indít el az internetezésre használt eszközén, vagy másik eszközről éri el az oldalt akkor nem lesznek elérhetőek.

A már említett és a 2.1 ábrán látható módon a sütikben az analitikai szoftverek egyéb, a felhasználói azonosítást megkönnyítendő adatot is elhelyeznek.

A HTML5-ben már nem csak sütikben van lehetőség adatok tárolására (a sütik mérete négy kilóbájtra van limitálva (*Number and size limits of a cookie in Internet Explorer* 2007)), hanem *webStorage*-ban is, amely már strukturáltabb, és nagyobb adathalmaz tárolását teszi lehetővé (Hickson, 2011) illetve az *IndexedDB*, amely *webStorage* méretbeli lehetőségeivel bír, viszont növelési lehetőséggel (bármeddig növelhető méret (*IndexedDB* 2012)), és még komplexebb adatformátumok tárolására is fel van készítve.

Lokalizációs adatok A felhasználó földrajzi pozíciójának meghatározása nem egyszerű dolog, a HTML5 lokalizációs interfészének bevezetése előtt, mindössze az ún. *fordított helymeghatározás* (reverse geocoding) létezett, amely a felhasználó IP címe alapján próbálta megállapítani a kliens pozícióját.

Azonban, míg az Egyesült Államokban az IP cím tartományok kiosztása régióként történt, addig Magyarországon nem volt ilyen szabályozás, tehát ezzel a módszer Magyarországon nem lehetséges pontosan meghatározni a felhasználó tartózkodási helyét.

Viszont az említett HTML5 lokalizációs interfésze (geoLocation) lehetővé teszi, a felhasználó pozíciójának pontosabb meghatározását, amely következőképpen történhet:

- **A környező vezeték nélküli hálózatok segítségével**

Ebben az esetben (Google Chrome és Firefox böngésző esetén) elküldésre kerül a Google térkép és lokalizációs szervereinek a felhasználó készüléke körül elhelyezkedő privát, és publikus vezeték nélküli hálózatok azonosítója (SSID), egyéni fizikai címe (MAC cím) illetve a jel erőssége. A válaszüzenetben visszaküldésre kerülnek a szélességi és a hosszúsági fokok.

- **Mobiltelefon tornyok**

Amennyiben a felhasználó készüléke képes mobiltelefon tornyokhoz kapcsolódni (mobiltelefon, táblagép, 3G modem), akkor a tornyok pozíciója is pontosítja a pozíciót.

- **GPS**

A specifikáció lehetőséget ad arra is, hogy ha felhasználó készülékében található GPS eszköz (mobiltelefon, táblagép, de akár laptop is), akkor a kért pozíció pontosságától függően ez is használatra kerül.

- **Fordított helymeghatározás**

Abban az esetben, ha az adott készülék sem mobiltelefon tornyokra nem képes csatlakozni, vezeték nélküli hálózat sincs a környezetében és GPS eszközzel sem rendelkezik, a fordított helymeghatározás ilyenkor is használható, hiszen internetkapcsolattal rendelkeznie kell a webes tartalmak eléréséhez.

A HTML5 lokalizációnál fontos kiemelni, hogy a böngésző alapértelmezetten nem teszi elérhetővé a felhasználó pozícióját, hanem egy megerősítést kér, amelyet elfogadva lesz csak elérhető az adat.

Egyéb mérhető adatok Lehetőség van még a böngészőkben olyan egyéb adatok mérésére, melyek nincsenek benne a specifikációban illetve a beépülő bővítmények segítségével érhetőek el.

Ilyenek lehetnek például az Adobe Flash segítségével elérhető operációs rendszerre telepített betűtípusok vagy az adott készülékben megtalálható vagy készülékhez kapcsolt multimédiás eszközök, mint például a webkamera.

Továbbá a nem standard megoldások közé tartozik, az Internet Explorerben megtalálható ActiveX komponensek, melyekkel akár az operációs rendszer szintjén lehet futtatni nem webre fejlesztett szoftvereket, amelyek természetesen szinte mindent elérhetnek - az asztali programokhoz hasonlóan. Az ActiveX komponensek hátránya, hogy csak Internet Explorerben és Windows platformon érhetőek el.

2.2. Mit érdemes mérni?

A 2.1 pontban bemutatásra kerültek a legfontosabb mérhető adatok, azonban fontos kiemelni, hogy nem érdemes minden adattal foglalkozni, de vajon melyek azok az adatok, amelyek valójában információt is tartalmaznak?

A HTTP fejléc A HTTP fejléc módosítása nem tartalmaz elegendő információt ahhoz, hogy érdemben megérje vele foglalkozni, és az elküldött adatok legtöbbje módosítható, korlátozható illetve ki is egészíthető a telepített böngészőkben (ez történhet kézzel vagy a bővítmények, kiegészítők által).

A böngésző neve, verziója Mint említésre került a 2.1 bekezdéseiben a böngésző neve, kompatibilitása, verziószáma mind kliens-, mind szerveroldaltól elérhető, azonban ennek mérése hosszútávon nem profitábilis. Ennek oka, hogy 2010 júliusában a Google Chrome - szakítva a korábban megszokott böngészőverziók frissítési szokásaival - hatheti kiadási ütemtervre váltott (Laforge, 2010), majd őt követte a Mozilla is, amely pont egy évvel később hozta meg hasonló döntését (Nightingale, 2011).

Tehát az ilyen gyors ütemű verzióváltások mellett, ez az adat sem szolgálhat nagy segítséggel.

Sütik A sütik (és egyéb kliensoldali adattárolási formák) kihasználása rendkívül fontos dolog, ugyanis a felhasználóról korábban eltárolt információk, kliens és szerveroldali közötti megosztása ezeken keresztül történhet meg.

Lokalizációs információk A felhasználó pozíciójának elmentése is kiemelten fontos eleme a mérésnek. Természetesen, a minél pontosabb méréshez szükség van a felhasználó beleegyezésére, azonban ha az adott oldal képes rávenni a képernyő túloldalán helyet foglaló internetezőt, hogy erősítse meg megosztási szándékát (például nyereményjátékba való bekerülés lehetőségével), akkor mindenképpen az egyik legfontosabb információvá lép elő.

Bővítmények Érdemes monitorozni a bővítmények verzióit, illetve a különböző bővítmények jelenlétét a böngészőkben.

A 2.1 pontban megemlítsre került, hogy a bővítményekkel olyan adatok is elérhetőek, melyek a webes kliensoldali technológiákkal (JavaScript, CSS) nem, vagy csak részlegesen. Viszont ezek a bővítmények nincsenek jelen minden böngészőben, vagy éppen minden platformon, de akkor mégis miért szükséges velük foglalkozni?

Éppen az a plusz információ teszi őket fontossá, hiszen ezen apró pluszok segítségével válik lehetővé a felhasználók beazonosítása.

3. fejezet

Biztonsági

3.1. Anonimitás elleni kísérletek

Az internetes anonimitás már régóta vita tárgya. A Kaspersky biztonsági cég szerint az internet legnagyobb hibája az anonimitás (Goodin, 2009).

Az anonimitás ellen sok érv felhozható, mint ahogy meg is teszik évről évre. Ekkor az egyik legfontosabb érv (az anonimitás ellen) a kéretlen levelek, a gyermekpornográfia, és az internetes behatolások számának csökkentése, megszüntetése. Azonban, mint Bruce Schneier is megemlíti (Schneier, 2010) az anonimitás megszüntetésének hatására a felhasználók kerülőutat választanának vagy mások gépeire betörve - a vétlen személyazonosságával - hajtanák végre az illegális tevékenységeket.

Az internetes anonimitás megakadályozása illetve megszüntetése ellen irányuló jogszabályok és törvények a 2011-es és 2012-es években nagy félzúdulást váltottak a közösségben. Ezek közül a legfontosabbak az Egyesült Államokban bevezetni kívánt **SOPA**, és ennek az európai verziója az **ACTA**.

SOPA és az ACTA háttere

Mind a SOPA, mind az ACTA a szerzői jogok védelme, a szellemi tulajdonok hamisítása ellen létrehozott regulák gyűjteménye, azonban bekerültek olyan cikkelyek is a javaslatokba, melyek a felhasználók szólásszabadságát is erősen korlátozták volna.

De milyen kapcsolatban áll az internetes anonimitás a SOPA, ACTA törvényjavaslatokkal?

A dolgozat alapvetően a felhasználók azonosításának technikai lehetőségét tűzte ki célul, azonban az említett törvényjavaslatok mellett, igazából a téma létjogosultsága rengeteget csökkenne. A SOPA, és ACTA elfogadásával az amerikai, és európai internetezők anonimitása megszűnne, az ISP számára kötelező válna a forgalom monitorozása, az adatok kiadása az illetékes hatóságoknak. *Tor anonymity will become illegal with SOPA acts?*
2011

3.2. Anonimitás biztonsági kérdései a böngészőben

Mielőtt a webes alkalmazások biztonsági kockázatairól, és az azok ellen való védekezésről esne szó, érdemes megvizsgálni maguknak a böngészőknek a veszélyeit.

Az böngészők biztonsága rendkívül fontossá vált az internetes elvégezhető feladatok

gyarapodásával. Hiszen a felhasználók most már nem csak híreket olvasnak, hanem böngészőn keresztül fizetik be a havi áramszámlát, adják le az adóbevallást vagy éppen videóhívás formájában beszélgetnek családjukkal.

Mivel a legtöbb felhasználónak az internet magát a böngészőt jelenti, ezért a legtöbb felhasználókat érintő internetes támadás a böngészőből érkezik. Mivel a böngészők a felhasználó számítógépen szinte mindenhez hozzáfér (szoftverhez és hardverhez), ezért ha egy támadó megszerzi a böngésző feletti uralmat, akkor az a számítógép feletti uralmat is jelenti.

A kanadai *Pwn2Own* nevű évente megrendezésre kerülő biztonsági konferencián a biztonsági szakemberek ún. fehér kalapos hackerek, próbálják meg megkerülni a böngészők biztonsági mechanizmusát. A versenyen 2009-ben (Buherátor, 2009), 2010-ben a Google Chrome termékének kivételével az összes böngésző a hackerekkel szemben (Buherátor, 2010), 2011-ben a Mozilla Firefox és a Google Chrome felett sem sikerült átvenni az uralmat (Buherátor, 2011), viszont 2012-ben már minden böngészőben sikerült hibát találni a kíváncsiskodó szakembereknek (Buherátor, 2012).

3.3. Mire érdemes figyelni?

A 2.1 és a 2.2 pontokban felsorolásra kerültek olyan adatok, melyeket lehet, illetve érdemes mérni a felhasználó böngészőjében. Ebben a fejezetben, megvizsgálásra kerülnek az adatok olyan oldalról, hogy hogyan lehet védekezni ellenük.

Sütik Maguk a sütik nem érdemes védekezni, azonban van egy speciális formájuk, mely a felhasználók azonosításának leginkább kedvelt formája, ez pedig nem más, mint a külső féltől származó süti (*third party cookie*). Mint már a előző fejezetben említésre került a süti alapvetően a felhasználói azonosítást segítik, teszik lehetővé a webes alkalmazásoknál, tehát az egy doménen működő oldalaknál nincs szükség minden megnyitás alkalmával a felhasználó nevét, és jelszavát elkérni, hanem a sütiben eltárolt munkamenet azonosító (*session id*) alapján képesek autentikálni.

Alapértelmezetten azonban a webes alkalmazások nem csak arra a doménre képesek sütik beállítani, amelyeken látszólag nem működnek. Szerencsére a külső sütik tiltása már minden böngészőben lehetséges és ajánlott beállítás minden internethasználó számára. Viszont fontos arra felhívni a figyelmet, hogy a külső sütik tiltása nem tiltja le a `localStorage` használatát, tehát az továbbra is elérhető lehetőség a weboldalak számára, hogy a külső adataikat ott helyezték el.

Lokalizációs információk A fordított helymeghatározás ellen érdemben nem lehet fellépni, mert elrejtteni nem lehet a felhasználó IP címét, persze vannak megoldások, hogy a weboldalak megtévesztésére.

Általános megoldás a szerzői jogok védelme érdekében, hogy adott tartalmak, bizonyos országokból nem tesznek elérhetővé, ekkor az azonosítás IP cím alapján történik. Ennek megkerülésére használhatóak a proxyk, illetve VPN megoldások. Ebben az esetben a szerverek nem a felhasználó IP címét veszik alapul, hanem a proxy vagy éppen a VPN szolgáltató címét.

A HTML5 lokalizáció alapján történő helymeghatározás - az alapértelmezett beállítások szerint - engedélyt kér a felhasználótól a pozíció megosztására, tehát ez az információ teljesen kontroll alatt tartható.

Böngészőképességek A böngésző képességeinek módosítása nem lehetséges, mindössze a böngésző neve módosítható. A böngésző nevének módosítása viszont csak a böngésző detektálásra hagyatkozó adatgyűjtők ellen nyújthat védelmet, a képesség alapú detektálással szemben nem.

Bővítmények A böngészők, így a felhasználók biztonsági szintjét nagy mértékben rontják a bővítmények, melyek hibásan implementálnak képességeket, vagy éppen olyan lehetőségeket engednek, melyek segítségével a felhasználó egyértelműen azonosítható. A böngészők gyártói megtesznek mindent, hogy a bővítmények minél kevésbé legyenek veszélyesek a felhasználóra, erre kiváló példa a Google Chrome-ban működő ún. sandbox mód, amely bizonyos korlátozások között engedi csak a bővítmények futását (nem írhatnak a lemezre, nem nyithatnak új ablakot). *Sandbox*

Emellett azonban, a monitorozó weboldalak továbbra is értékes információkat szerezhetnek a bővítményekről, ennek meggátolására a legjobb módszer, ha minden bővítmény futását a felhasználó engedélyezi. Ennek a megoldásnak körülményessége miatt, ezt a lehetőséget a csak a Google Chrome implementálta és mindössze csak a Java bővítményekre. *Blocked plug-ins* 2011

Viszont szerencsére az egyedileg engedélyezett futást a felhasználók könnyen megoldhatják egyénileg telepített böngésző kiegészítőkkel.

3.3.1. Inkognitó mód

Az inkognitó vagy csak gyakran pornó módként emlegetett képesség az Apple Safari böngészőben mutatkozott be 2005-ben (Trapani, 2004), mára az összes fontosabb böngészőben elérhető (Google Chrome - 2008, Mozilla Firefox 2009, Internet Explorer - 2009, Opera - 2010). Segítségével bármikor indítható egy új, teljesen üres böngésző, amely nem tartalmazza, és nem is tárolja az előzményeket, a személyes beállításokat.

Mit tud az inkognitó mód?

2006-ban Jeremiah Grossman bemutatott egy sebezhetőséget, amelyben mindössze CSS segítségével képes volt megállapítani, hogy felhasználó milyen oldalakat látogat (Grossman, 2006). Ez a hiba az összes böngészőt érintette, kivéve a Safari inkognitó módját. Természetesen mára ezt a hibát már javították, és már normál módban sem okoz problémát.

Viszont a probléma rávilágított arra a tényre, hogy böngészőknek szükségük van egy olyan módra, amelyet bezárva a felhasználók számítógépén nem marad semmi nyoma (előzmények, sütik) a tevékenységnek. Azonban az inkognitó mód nem csak a nem felhasználó által elrejteni kívánt dolgoktól véd meg, hanem az felhasználók azonosítását végző weboldalaknak komoly bosszúságot okoz, ugyanis a böngészőben elhelyezett sütik, a localStorage-ba írt bejegyzések, a tárolt felhasználónevek, jelszavak is mind eltűnnek az ablak bezárása után.

Természetesen időről időre megjelennek megoldások, melyek a frissen felfedezett hibák segítségével mégis képesek azonosítani a felhasználókat, azonban a böngészők gyakori verzióváltásának, és hibajavítások kiadásának köszönhetően gyorsan orvosolják a problémákat.

4. fejezet

Üzleti

4.1. A szereplők

Az üzleti szempontoknál érdemes megvizsgálni, hogy egyáltalán kik azok a szereplők a piacon akik szeretnék a felhasználókat azonosítani. Az elsődleges célja a felhasználók azonosításának, hogy az érdeklődésnek megfelelő tartalmat tudjon nyújtani a szolgáltató, ennek a legfontosabb, és üzletileg a legjelentősebb formája a reklámok.

Persze felmerül a kérdés, hogy a felhasználók hol találkozhatnak reklámokkal a weben, a válasz tulajdonképpen az, hogy mindenhol, a dolgozat azonban következő - jelenleg a legfontosabb - területekre koncentrál: közösségi oldalak, hír- és hírgyűjtő oldalak illetve keresők.

Közösségi oldalak

A közösségi oldalak a reklámok szempontjából egy speciális területnek számítanak, ugyanis a felhasználók nem anonim módon (értsd bejelentkezés nélkül) böngésznek az oldalon, hanem egy bejelentkezés után. Továbbá az közösségi oldalakon a felhasználók már regisztrációkor megosztják az alapvető információkat magukról (név, születési dátum, lakhely, foglalkozás), illetve az oldalon történő tevékenységeikkel további adatokat adnak ki magukról. Összességében elmondható, hogy az oldalak itt nem kell az anonim felhasználókból megépíteni a felhasználói profilokat, hiszen a tagok önként megteszik, amelynek megbízhatósága, pontossága sokkal jobb minőségű, mint az anonim azonosítás.

A Facebook, mint a legnagyobb közösségi oldal (2011. decemberi adatok közel 845 millió havi aktív felhasználói aktivitást jeleztek (*Facebook Statistics* 2011)), nagyon szigorú specifikációban köti ki a megjeleníthető reklámok kinézetét, formátumát, szövegezését, cserébe viszont a nagyszámú profilnak köszönhetően a hirdetéseket lehető legpontosabban képes célozni (targetálni). ThinkDigital és Facebook, 2011

Hír- és hírgyűjtő oldalak

A pusztán internetes híroldalaknál az legfontosabb bevétel a reklámokból származik, ezért rendkívül fontos szerepet kap a felhasználói profilok felállítása, és a célzott reklámok megjelenítése. A profilok felállítására létezik sok kutatóintézet és internetes piackutató cég, akik kész megoldásokat kínálnak a portáloknak.

A Közép-Európai régióban a legnagyobb ilyen jellegű felméréseket, monitorozást végző szervezete a Gemius (<http://gemius.hu>), illetve fontos kiemelni, a jelenleg egyre több elismerést elnyerő magyarországi feltörekvő céget, a Playertise szolgáltatás (<http://playertise.com>), amely a hírportálon (és egyéb, akár személyesen oldalakon)

megjelenő videók tartalma, és a felhasználói profil képes a hirdetéseket megjeleníteni.

Fontos kiemelni, hogy a közösségi oldalak egyre több problémát okoznak a hírportáloknak, mivel a sokkal pontosabb felhasználó profilok, és nagyobb számú célzott reklámok száma a hirdetőköt elcsábítják. *EU newspapers record worst-ever drop in ad revenue* 2009

Ennek köszönhetően egyre több hírportál kezdi bevezetni - a reklámok mellett - a fizetési modelljét, amellyel próbálják pótolni a hirdetésekből csökkenéséből származó veszteségeiket. Edmonds, 2011

Keresők

A legnagyobb webes kereső oldalak rendelkeznek saját megoldással reklámok, és a hirdetések kiszolgálására (Google - AdWords, Yahoo - Advertising, Bing - AdCenter). Természetesen a közösségi oldalak által egyre nagyobb szelet a keresőket is megviseli, ezért próbálnak a keresők is minél pontosabb profilokat összeállítani, illetve a lehető információt kinyerni a felhasználók böngészőiből, akár a megoldásaikkal már a szűrke zónában ténykedve. Schubarth, 2012

Mivel lehet még tökéletesebb profil összeállítani?

Természetesen a regisztrációval. A Google rengeteg egyéb szolgáltatással rendelkezik a keresőjén kívül (email, blog olvasó, mobil- és asztali operációs rendszer, fordító, stb.), amelyekkel megpróbálja rábírní a felhasználót a regisztrálásra, majd a kumulált adatokból már egy olyan profilhoz jut, amelynek segítségével a hirdetések átkattintási aránya (clickthrough rate) magasabb lesz. Továbbá a Google a regisztrált felhasználók részére, olyan plusz szolgáltatások érhetőek el, mint a személyre szabottabb keresési lehetőség, amely a Google+ közösségi oldalon folytatott tevékenység alapján rendezí sorrendbe a találatokat. Andrey, 2012

5. fejezet

Összefoglalás

Összesítve elmondható, hogy webes anonimitás talán minden korábbi szintjénél komolyabb szerepet kaphat az egyre bővülő online szolgáltatások széles palettája és lehetőségei miatt. De ami talán a legfontosabb, hogy a felhasználóknak meg kell tanulniuk, hogy milyen módszerekkel tudják magukat nagyobb biztonságba helyezni, ugyanis olyan cégek sem riadnak vissza a szürke zónától, mint a Google, ha van lehetőségük a felhasználóról információkat gyűjteni. Továbbá a törvényhozók is elkövetnek mindent, hogy felhasználók monitorozása a hatóságok szeme elől sem lehessen rejtve.

Továbbá fontos kiemelni a közösségi oldalakat, amelyekre a felhasználók önkéntesen feltöltik az adataikat, nem törődve azzal, hogy az oldalak üzemeltetői továbbadják-e harmadik félnek, illetve mit tesznek az adataikkal. Sajnos az internetes-biztonság tudás és oktatás alanya szintje miatt, a weboldalak könnyen kihasználhatják a felhasználók jóhiszeműségét, amellyel fontos információkhoz juthatnak a profilok felépítését illetően.

Felhasznált irodalom

Andrey (2012). *Google+ Search Personalisation*.

Letöltve: 2012. február 25.

URL: <http://www.firstrate.co.nz/blog/google-plus-search-personalisation/>.

Blocked plug-ins (2011).

Letöltve: 2012. március 16.

URL: <http://support.google.com/chrome/bin/answer.py?hl=en&answer=1247383>.

Buherátor (2009). *Pwn2Own: Mindenki elhasalt*.

Letöltve: 2012. március 12.

URL: http://buhera.blog.hu/2009/03/19/pwn2own_mindenki_elhasalt.

— (2010). *Pwn2Own 2010*.

Letöltve: 2012. március 12.

URL: http://buhera.blog.hu/2010/03/25/pwn2own_2010.

— (2011). *Pwn2Own 2011. összefoglaló*.

Letöltve: 2012. március 12.

URL: http://buhera.blog.hu/2011/03/12/pwn2own_osszefoglalo_2011.

— (2012). *Pwn2Own és Pwnium*.

Letöltve: 2012. március 12.

URL: http://buhera.blog.hu/2012/03/08/pwn2own_es_pwnium.

Edmonds Rick (2011). *9 reasons newspapers are suddenly asking print subscribers to pay for full Web access*.

Letöltve: 2012. február 23.

URL: <http://www.poynter.org/latest-news/business-news/the-biz-blog/141628/9-reasons-newspapers-are-suddenly-asking-print-subscribers-to-pay-for-full-web-access/>.

EU newspapers record worst-ever drop in ad revenue (2009).

Letöltve: 2012. március 2.

- URL: <http://www.euractiv.com/innovation/eu-newspapers-record-worst-drop-ad-revenue/article-185349>.
- Facebook Statistics* (2011).
- Letöltve: 2012. március 20.
- URL: <http://newsroom.fb.com/content/default.aspx?NewsAreaId=22>.
- Goodin Dan (2009). *Security boss calls for end to net anonymity*.
- Letöltve: 2012. március 20.
- URL: http://www.theregister.co.uk/2009/10/16/kaspersky_rebukes_net_anonymity/.
- Grossman Jeremiah (2006). *I know where you've been*.
- Letöltve: 2012. február 22.
- URL: <http://jeremiahgrossman.blogspot.com/2006/08/i-know-where-youve-been.html>.
- Hickson Ian (2011). *Web Storage*.
- Letöltve: 2012. március 16.
- URL: <http://www.w3.org/TR/webstorage/>.
- IndexedDB* (2012).
- Letöltve: 2012. március 24.
- URL: <https://developer.mozilla.org/en/IndexedDB>.
- Laforge Anthony (2010). *Release Early, Release Often*.
- Letöltve: 2012. március 1.
- URL: <http://blog.chromium.org/2010/07/release-early-release-often.html>.
- Nightingale Johnathan (2011). *Every Six Weeks*.
- Letöltve: 2012. március 5.
- URL: <https://blog.mozilla.com/futurereleases/2011/07/19/every-six-weeks/>.
- Number and size limits of a cookie in Internet Explorer* (2007).
- Letöltve: 2012. március 21.
- URL: <http://support.microsoft.com/kb/306070>.
- Sandbox*.
- Letöltve: 2012. március 21.
- URL: <http://dev.chromium.org/developers/design-documents/sandbox>.
- Schneier Bruce (2010). *Anonymity and the Internet*.
- Letöltve: 2012. március 20.
- URL: http://www.schneier.com/blog/archives/2010/02/anonymity_and_t_3.html.

Schubarth Cromwell (2012). *Google, others spy on Apple Safari users.*

Letöltve: 2012. február 20.

URL: <http://www.bizjournals.com/sanjose/news/2012/02/17/google-facebook-others-spy-on-apple.html>.

ThinkDigital, Facebook (2011). *HIRDETÉSI FELÜLETEK TECHNIKAI SPECIFIKÁCIÓJA.*

Letöltve: 2012. február 22.

URL: http://thinkdigital.hu/web/files/richteditor/filemanager/Specifikacio_2011-Q2_-_FACEBOOK.pdf.

Tor anonymity will become illegal with SOPA acts? (2011).

Letöltve: 2012. március 6.

URL: <http://thehackernews.com/2011/12/tor-anonymity-will-become-illegal-with.html>.

Trapani Gina (2004). *Safari's private (porn) browsing mode.*

Letöltve: 2012. február 27.

URL: <http://lifehacker.com/102146/safaris-private-porn-browsing-mode?tag=softwaremacosx>.