Előházi János
PhD hallgató
elohazi.janos@gmail.com

ANONIMITÁS AZ INTERNETEN

Abstract

A cikk célja, hogy bemutassa az anonimitás biztosításának formáit és a rendelkezésre álló technikai eszközöket, amellyel a felhasználók megvédhetik személyes adataikat illetéktelenek előtt. A megoldások nem csak jóindulatú célt szolgálnak, segítenek annak is, aki szándékosan rejti el kilétét a külső megfigyelők (személyek vagy technikai eszközök) elől.

The aim of this paper is to introduce the realisation methods of anonymity on public networks including the existing technical tools and infrastructures. Using these techniques users are able to hide their personal data from third parties. These solutions are available for malicious use as well, for communicating parties who are to hide their real identity from outside persons and technical instruments.

***Kulcsszavak**: anonim kommunikáció, internet, chaum-mix, onion-routing*

1. Bevezetés

Az internet mára egy komplex szolgáltatásokkal rendelkező, univerzális szolgáltató csatornává vált. Ez azt jelenti, hogy információkeresésen túl vásárlásra, banki ügyekre, személyes ügyek intézésére, e-mailezésre, telefonálásra stb. használható. A sokszínűség viszont nem párosul biztonsággal. Ha egy védtelen számítógép ma kikerül az Internetre, pár percen belül (aktív használat nélkül is) számos rosszindulatú támadás áldozatává válik. Ez úgy lehetséges, hogy szemben a 90-es évek vírusaival, a kártevők nem passzív módon várakoznak, hogy egy fájl elindításával megfertőzhessenek más gépeket is, hanem aktív módon, az Internet segítségével újabb prédát keresnek a felhasználó tudta nélkül. Az ellenük való védekezésre rengeteg típusú tűzfal és vírusírtó áll a felhasználók rendelkezésére.
A támadás azonban úgy is érhet minket, hogy a számítógépünk nem fertőződik meg. Az interneten, hogy bizonyos műveleteket elvégezzünk, számos internetes oldalt látogatunk meg, sokszor meg kell adni valamilyen személyes azonosítót stb. A felhasználó minden tevékenységét egy oldal nyomon követheti un. cookie-k (sütik) segítségével. Ezek kisméretű szöveges információt tárolnak, melyek automatikusan elküldésre kerülnek, ha a felhasználó egy linkre ráklikkel. Ilyen módszerrel eltárolhatóak azok az áruk, melyeket a felhasználó egy on-line boltban a kosarába tett, vagy rögzíthető milyen dolgokat nézett meg, és az így nyert információ alapján más árura is felhívható a figyelme automatikusan.
Sok esetben a szokásainkat figyelő módszerek hasznosak, de előfordulhat olyan eset, amikor a felhasználó nem szeretné, ha azonosítaná őt a másik fél. Főleg nem, ha esetleg olyan tevékenységet végez on-line, melyről nem szeretné, ha bárki hozzá kötné. De az ilyen szélsőséges esetek figyelmen kívül hagyása esetén is előfordulhat, hogy valaki nem szeretné, ha telefonszámla adatait, az egészségi állapotára való adatait, a pénzügyi helyzetét és adatait (hitelkártya szám) stb. egy harmadik fél összekapcsolhassa.
Legtöbb esetben nem tudhatjuk, hogy mi is történik a háttérben. A törvények ugyan előírják, hogy a személyes adatokkal foglalkozó oldalak jogi nyilatkozatot tegyenek, ahol leírják

pontosan, hogy milyen célból és hogyan dolgozzák fel az általunk kiadott személyes adatokat, a felhasználónak a gyakorlatban azonban nincsen semmi lehetősége, hogy ezt ellenőrizni is tudja. Nem is említve az olyan eseteket, amikor a szolgáltató akaratán kívül, a rendszerébe való betörés révén jutnak illetéktelenek kezébe személyes adataink. Előfordulhat olyan eset is, amikor az on-line kommunikációt harmadik, rossz szándékú fél lehallgatja, és így jut illetéktelen adatokhoz.

2. Az anonimitás típusai

Ahhoz, hogy megfelelő módszert tudjunk alkalmazni identitásunk elrejtésére, meg kell határozni, hogy mit is szeretnénk a másik fél elől elrejteni. Egy on-line kapcsolatnak három olyan attribútuma van, amely a kommunikáló felek anonimitását határozza meg: a küldő kiléte, a fogadó kiléte és a kettőjük között lévő kapcsolat. A küldő kilétének elrejtésekor, a támadó nem tudja megállapítani, ki az üzenet forrása. A fogadó kilétének elrejtése esetén, a támadó azt nem tudja megállapítani, hogy ki az, akinek az üzenet szól. A harmadik esetben a támadó látja a küldőt és a fogadót, de nem képes arra, hogy a köztük lévő kapcsolatot felfedje.

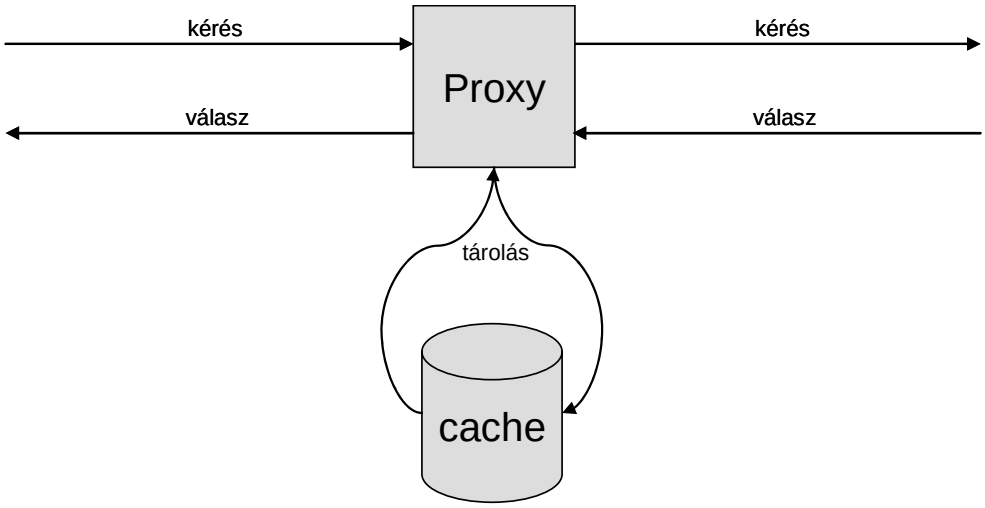
A megfelelő védelemhez meg kell határozni azt is, hogy ki az a harmadik fél, a „támadó”, aki elől a fenti információkat el akarjuk rejteni. Különösen kényes szituációban lehet akár a kommunikáló fél is, aki előtt a kilétünket nem szeretnénk felfedni, de legtöbb esetben a külső támadók és a belső kompromittálódott egységek elől szeretnénk a fenti információkat elrejteni. A külső támadó egy olyan entitás, ami képes arra, hogy a teljes kommunikációs utat, vagy annak egy részét felügyelje, és a felügyelt részen áthaladó üzenetek mindegyikét lehallgassa. A belső eszközök pedig lehetnek kompromittálódott routerek, melyek a támadó befolyása alatt, számára (is) továbbítják a rajtuk áthaladó információt [5].

3. Technikai megoldások

Ahhoz, hogy a fenti célokat elérjük, számos gyakorlatban alkalmazható megoldás létezik.

Anonim proxy-k

A proxy szerver egy adott alkalmazásra (HTTP, e-mail stb.) kiépített gyorsító tár általában. Fogadja a klienstől érkező kéréseket, és ha nem szerepel a gyorsító tárjában továbbküldi azokat a címzettnek, majd a megkapott információt amellett, hogy továbbítják a küldőnek, el is tárolják azt a gyorsítótárukban (ld. 1. ábra). Ebben az esetben viszont a címzett számára a proxy fog a kommunikációs félnek tűnni, tehát a küldő személye elrejthető a fogadó (és a proxy-n túli hálózatot figyelő támadó) elől [5][7].

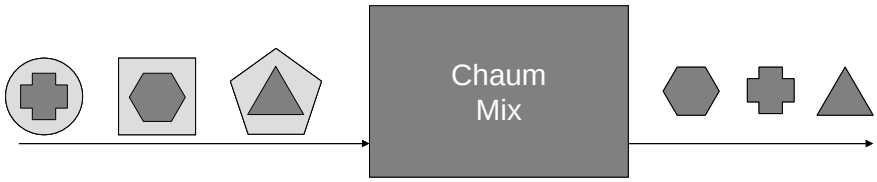


1. ábra A proxy működési elve

A gyakorlatban a proxy egy helyi hálózatból fogad kapcsolatot, és a célja, hogy a külső kommunikációt felgyorsítsa. Az anonim proxy-k viszont bárhonnan fogadnak kapcsolatot, és azt állítják magukról, hogy az általuk megszerzett információt (ki, kivel és mit kommunikált) nem adják át harmadik félnek. Az internetről letölthető ilyen anonim proxy-lista, melyet időről időre frissítenek, és a nyilvántartott proxy-k mindegyikét leellenőrzik, hogy tényleg nem adja-e ki az adatokat illetékteleneknek (akik akár a bűnüldözési szervek is lehetnek).
Az előnye ennek a megoldásnak, hogy ingyen igénybe vehető, és egyszerű esetben megfelelő védettséget nyújt; a hátránya, hogy meg kell bízni a proxy-ban, és csak egy bizonyos alkalmazási célból (pl.: HTTP) alkalmazható

A Chaum Mix

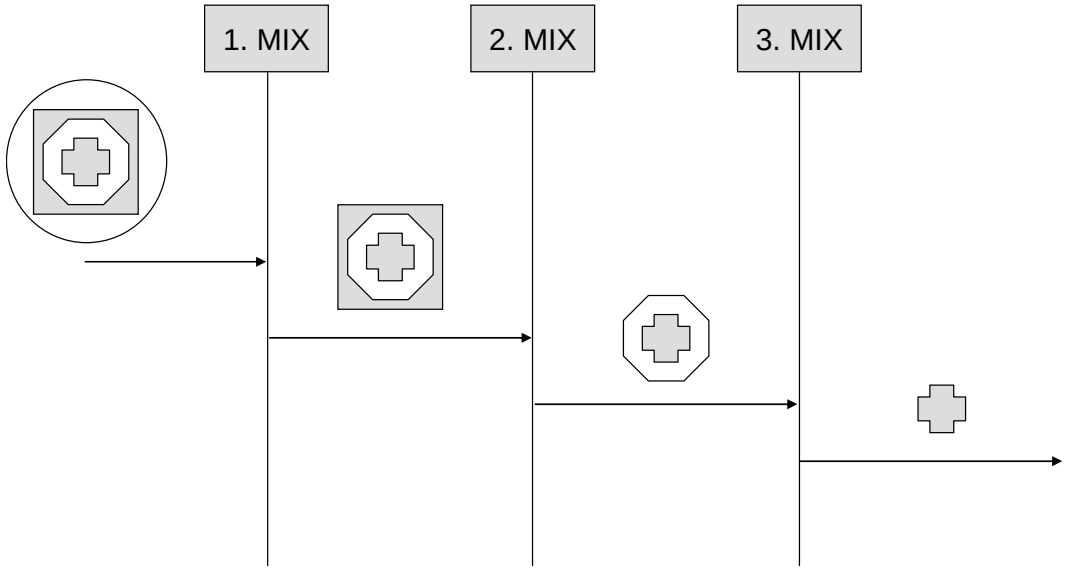
A Chaum Mix képes arra, hogy elrejtse a küldő személyét a kommunikációs partner előtt, illetve meggátolja, hogy a küldő és fogadó közötti kapcsolat harmadik fél számára felfedezhető legyen. Működési elve a 2. ábrán található [5].



2. ábra Chaum Mix

A küldendő üzenetet a Mix által ismert kulccsal titkosítják. A Mix, dekódolja az üzenetet, és továbbküldi a címzettnek. A Mix a feldolgozást kötegelt módban végzi, így meg tudja változtatni a kimenő üzenetek sorrendjét (pl.: ha egy üzenet a 2. volt a sorban, biztos, hogy a kimenő sorban nem a 2. lesz), megnehezítve így a Mix két oldalát figyelő számára, hogy összepárosítsa a kimenetet és a bemenetet. A Mix eldobja az üzenetismétléseket. (Ha a küldő fél úgy érzi, hogy az üzenet nem ért célba, újra elküldi azt. Ez a TCP/IP protokoll mechanizmusaiból következik.)
A fenti felállásban a küldőnek meg kell bíznia az általa használt Chaum Mix-ben, hiszen ő az aki, ismeri az elrejtendő információkat, viszont nem biztos, hogy a felhasználó felügyelni képes a működését. Ahhoz, hogy a megbízhatóságot növelni lehessen, több Chaum Mix-en is átküldhető az információ. Ebben az esetben, ha csak egy Mix is korrektül viselkedik, a kommunikációs partnerek kiléte nem fedhető fel a támadó által. A 3. ábra mutatja, hogy a

gyakorlatban ez hogyan is néz ki. Látható, hogy az egyes Mix-ek csak az ő kommunikációs partnereiket, és csak az ő általuk használt kódolási kulcsot ismerik. Így a 3. Mix csupán azt tudja, hogy a 2. Mix-től jövő csomagot a címzettnek kell eljuttatnia, és számára a forrás a 2. Mix. Ezt betartva érhető el, hogy ha legalább egy Mix nem kompromittálódott, az elért célkitűzés megvalósul, vagyis a küldő fél illetve a kommunikációs kapcsolat a küldő és fogadó között harmadik fél által nem felismerhető.

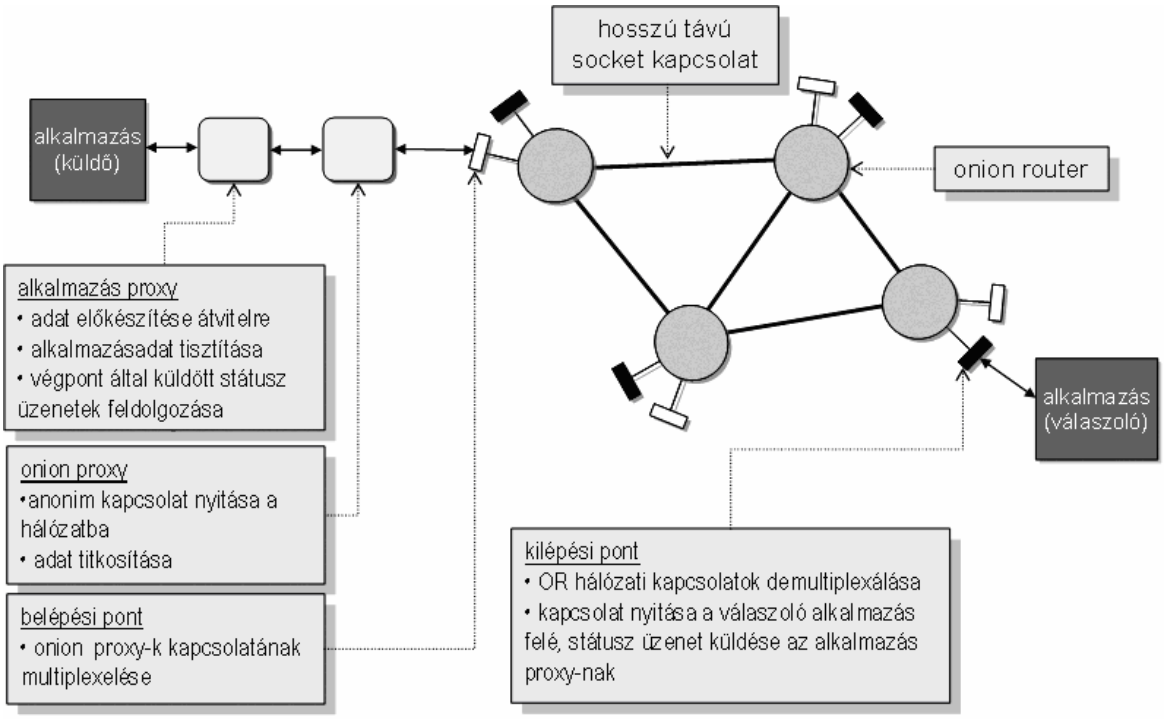


3. ábra Chaum Mix-ek lánca

A Chaum Mix-ek előnye, hogy megfelelő biztonságot nyújtanak, hátránya, hogy az egyes Mix-eket különböző (távoli) hálózati szegmensben célszerű elhelyezni.

Onion routing

Az Onion routing Chaum Mix-ek valós idejű hálózata; egy általános célú infrastruktúra anonim kommunikációs célokra nyílt hálózatokon, mint az internet. Alkalmazás specifikus proxy szerverek használatával bármilyen célra fel lehet használni [4][5].
A működés úgynevezett Onion Routerek logikai hálózatán alapszik. Minden egyes Onion router egy valós idejű Chaum Mix. Az üzenetek közel valós időben továbbítódnak ezeken a hálózati elemeken. Az egyes routereket különböző hálózati szegmensekbe kell telepíteni. Az anonim kapcsolat az egyes Onion routerek között dinamikusan épül fel. Ld. 4. ábra.
Az ilyen megoldás előnye, hogy elosztott, hibatűrő és biztonságos.



4. ábra Onion router architektúra

A szomszédos routerek között hosszú távú kapcsolat áll fent, a kapcsolatok közötti kommunikáció DES[1] titkosítással kódolt. Mind a fogadó mind a küldő irány külön kulccsal titkosított. A kapcsolaton az anonim kéréseket multiplexált módon szolgálják ki. Az anonim kommunikációs csatornák mindegyike egyedi azonosítóval rendelkezik (ACI – Anonymous Connection Indicator). Egy ACI egyedi azonosítója a kommunikációnak két onion router között, de az egész hálózaton ez már nem igaz. Minden üzenet azonos, 48 bájt hosszúra tördelt. Az egyes üzenettöredékek szintén DES-sel kódoltak. Különböző kérések üzenettöredékei keverednek, de az egy üzeneten belüli üzenettöredék-sorrend nem változik.
Ahhoz, hogy egy alkalmazás az ily módon létrehozott anonimitást biztosító hálózaton keresztül kommunikáljon be kell állítani, hogy az egyik onoin router belépési proxy-ját használja, amikor az internetes kommunikációt végzi. Az első kérés az onoion routerek hálózatán véletlenszerűen bolyong, majd véletlenszerű az is, melyik router kilépési pontján távozik a kérés az eredeti címzett felé. Ha a kilépési pont el tudja érni a kívánt cél, akkor létrejön egy logikai útvonal az onion routerek hálózatán, és a kommunikáció minden további csomagja az első által bejárt utat foglya megtenni.
A routerek közötti kérések a Chaum Mixek struktúrájához hasonlóan hagymahéj szerkezetűek, innen a megoldás elnevezése. Minden réteg az adott oinoin router nyilvános kulcsával kódolt. A kezdeti router állítja elő a teljes hagymahéj szerkezetű üzenetet, az első kérés által begyűjtött nyilvános kulcsok alapján. Ahogy a kérés továbbítódik a hálózaton minden egyes router lebont egy réteget (a sajátját). Ellentétes irányban a művelet is megfordul, és minden router hozzáad egy réteget a csomaghoz.
A kapcsolat bontását a kommunikáció két végpontja kezdeményezheti, melyet a kommunikációban részt vevő routerek továbbítanak egymásnak.

[1] DES: Data Encryption Standard – Titkosítási szabvány 1976-tól, szimmetrikus kulcsú blokk kódoló.

Anonym crowds

Az onion router megoldás megköveteli egy állandó hálózat meglétét, ami drága megoldás. Az olcsóbb megoldás az anonim tömeg használata. A „tömeg” felhasználók egy dinamikusan kialakított csoportja. Minden felhasználó futtat egy „jondo” nevű processzt. Ha egy felhasználó elindít egy jondo-t, akkor az kapcsolódik egy kiszolgálóhoz, amit „blender”-nek hívnak. Ez ellátja az új klienst a megfelelő információkkal, hogy csatlakozhasson a hálózathoz (titkosítási kulcsok, stb.), és jelenti az új kliens megérkezését a tömeg többi tagjának.

Ha a felhasználó anonim módon szeretne kommunikálni, akkor a Web-böngészőjét úgy kell beállítania, hogy mint egy proxy-t használja a saját jondo processzét. Ha ez a jondo fogad egy kérést, akkor azt továbbítja a tömegben szereplő másik jondonak (vagy akár rögtön küldheti a cél felé is!). Ez eldönti, hogy a kérést továbbítsa a cél felé, vagy továbbküldje a tömegen belül. Az első csomagot követő kérések, az első által kijárt utat követik. A válasz üzenetek is ezt az utat követik, természetesen fordított irányban. A jondo-k közötti kommunikáció titkosított.

A megoldás elrejti a küldő személyét, hiszen a támadó látja ugyan az üzenetet, de nem tudja megmondani, hogy a tömeg mely tagja küldhette azt. A küldő nem különböztethető meg a többi nem küldőtől. Egy helyi támadó meg tudja figyelni a tömegben lévő egy kliens kommunikációját, így tudja a küldő kilétét, de a célt nem ismeri, mert a hálózaton belüli kommunikáció titkosított, kivéve abban az esetben, ha a kérés a cél felé lett továbbítva. A tömeg szereplői viszont összejátszhatnak, és eltérhetnek a protokolltól, kiadva az általuk továbbított (kódolatlan) információt egy támadó számára.

Az anonim tömegek hátrányai, hogy a kérés tartalma a tömegen belüli jondo-k előtt ismert. A protokoll kijátszható Java appletekkel és ActiveX komponensekkel, mert ezek használata közvetlen kapcsolatot követel. A jondo-k használata jelentős költséget jelentenek. A megoldás nincs védve DoS[2] támadások elől.

Onion routers	Anonym Crowds
a küldő és a fogadó nem kapcsolható össze	a küldő anonimitását biztosítja
védelem a kommunikációt globálisan lehallgatni képes támadótól	a kommunikációt teljes mértékben lehallgatni képes támadóval szemben nem nyújt védelmet
nyilvános kulcsú titkosítást használ (legalább a kommunikációs csatorna felállítása idején – első csomag küldésekor)	szimmetrikus titkosítást használ

1. táblázat Az Onion routerek és anonim tömegek összehasonlítása

Anonym.OS

Ma már ingyenes operációs rendszer is készült az anonimitás biztosítására, az Anonym.OS[1]. Ez az operációs rendszer az anonim tömeg megoldását használja fel. Az operációs rendszer egy úgynevezett live CD, vagyis CD-ről működik, és minden futás közben generált adatot a memóriában tárol, így a gép újraindítása illetve kikapcsolása után

[2] DoS – Denial of Service: Olyan támadási mód, ahol a cél a hálózat megbénítása nagy számú kérés küldésével.

semmilyen árulkodó adat nem marad a kliens számítógépén [2]. A rendszer a Tor anonim hálózatot használja, és egy megfigyelő számára Windows XP-nek tűnik, hogy ne tűnjön fel különcsége. A Tor rendszerben a felhasználók közötti kommunikáció titkosított, második generációs onion routing-nak is nevezik, mert egyszerre valósítja meg az onion ruterek által követett megoldást, és az anonim tömeg által nyújtott dinamikusan változó hálózatokat [3]. Az operációs rendszer rendelkezik e-mail klienssel, böngészővel és azonnali üzenetküldő programmal, így az internet által nyújtott összes népszerű szolgáltatást ki tudja elégíteni.

Összegzés

A fent vázolt módszerek mindegyike kétélű: használhatnak helyes célt, illetve árthatnak is. Segíthetik az átlagos felhasználót abban, hogy megvédje személyes adatait illetéktelenektől, viszont nagyszerű segítség azoknak, akik az interneten illegális vagy megkérdőjelezhető dolgot végeznek.
A módszerek felsorolása követi erősségüket, kivéve az utolsó két megoldást. A TOR és az Onion routing rendszerek egymásnak alternatívái. A TOR az Onion routing un. light-weight, pehelysúlyú megoldása. Az Onion routing igényel egy előre kiépített, robosztus, karbantartott rendszert, melyet felhasználva elrejthető a két kommunikáló fél közötti kapcsolat. A TOR rendszerek önszerveződő, önkéntes „aktivistákból" állnak, akik egymást segítve, saját kapcsolatuk sebességének és számítási kapacitásuk egy részét feláldozva végzik el ugyanazt a feladatot, amelyet az Onion routing rendszerek is megvalósítanak amellett, hogy saját kéréseiket is kezelik.
A közelmúltig az anonim proxy-k jelentették az egyetlen elérhető megoldást, amellyel kétes mélységű, de egy bizonyos szintű anonimitási fok elérhető volt. Az Onion routing megoldás drága, a dedikált hálózat miatt, viszont nagy hatásfokú módszer. Az elmúlt egy évben a TOR rendszerek elterjedése lehetővé teszi, hogy az átlagos felhasználó is az Onion routing által nyújtott szolgáltatást vehessen igénybe. Az egyre gyorsabb végfelhasználói internet-kapcsolatoknak köszönhetően a TOR rendszerek használata nem okoz észrevehető felhasználói-élménybeli különbséget. Emellett számos közelmúltban megjelent ingyenes alkalmazás támogatja, úgy, mint a fentebb említett Anonym.OS vagy a hetekben megjelent TorPark névre keresztelt, a Firefox böngésző alapjait használó, TOR rendszereket igénybe vevő anonimitást biztosító böngésző program [8][9].

Felhasznált irodalom

[1]. http://www.sg.hu/cikkek/42045
[2]. http://sourceforge.net/project/showfiles.php?group_id=136357&package_id=176062
[3]. http://tor.eff.org/
[4]. http://www.onion-router.net/
[5]. http://www.hit.bme.hu/~buttyan/
[6]. http://www.whatthehack.org/
[7]. http://www.anonymizer.com/
[8]. http://www.sg.hu/cikkek/47355/nevtelen_bongeszes_modositott_firefox_szal
[9]. http://www.torrify.com/