TANULMÁNYOK AZ INFORMÁCIÓ- ÉS TUDÁSFOLYAMATOKRÓL 11.; 2006/2; 137-157. O.

Az anonimitás és a privacy kérdései a csevegő szolgáltatásokban

Gulyás Gábor György*

Budapesti Műszaki és Gazdaságtudományi Egyetem
Gazdaság- és Társadalomtudományi Kar
Információ- és Tudásmenedzsment Tanszék
1111 Budapest, Sztoczek u. 2. St. ép. I. em. 117.
Telefon: (36 1) 463-1832, Fax: (36 1) 463-4035
e-mail: gaborgulyas@gmail.com

Absztrakt

A csevegő szolgáltatások reneszánszukat élik — a százmilliós felhasználótáborral rendelkező szolgáltatásokat már nem csak magánemberek veszik igénybe, hanem vállalatok is alkalmazzák belső kommunikációra, ügyfélszolgálatok üzemeltetéséhez is. Kutatásaink során[1] megvizsgáltuk a szolgáltatások egy halmazát, s ezek alapján felállítottunk egy taxonómiát, melynek segítségével, a négy fő magánélet-védő kritérium figyelembe vételével értékeltük őket. Megállapítottuk, hogy a létező szolgáltatások változó színvonalú megoldásokat nyújtanak, és összességében egyikük sem alkalmas e kritériumok maradéktalan teljesítésére. Vizsgálatunk során két elterjedt szolgáltatásban magánszféra-védelmi rést fedeztünk fel. Tanulmányunk végén javaslatot teszünk kutatási eredményeink továbbhasznosítására.

Kulcsszavak: anonimitás, csevegő szolgáltatások, privacy

1. Privacy, Internet, szolgáltatók

A csevegő szolgáltatások jelen vannak, mióta az Internet — mai értelmében — megalakult, kereskedelmi, nyílt hálózattá vált. Ahogy terjedt az Internet, úgy a hagyományosnak tekinthető e–mail használatán túl felmerült az igény a gyorsabb, és közvetlenebb kapcsolatot biztosító csevegő szolgáltatások iránt. Azóta a szolgáltatások sokat fejlődtek, s a

* Gulyás Gábor György, V. évfolyamos Műszaki Informatika szakos hallgató, BME Információ– és Tudásmenedzsment Tanszék

[1] A szerző köszönettel tartozik Szili Dávid III. évfolyamos műszaki informatikus hallgatónak az empirikus vizsgálatokban nyújtott közreműködéséért, valamint a kutatás későbbi fázisaiban Póka Balázs V. évfolyamos műszaki informatikus hallgatónak értékes észrevételeiért.

fejlődésnek köszönhetően a korai, chat jellegű szolgáltatások[2] új generációjaként megjelentek már a 90-es évek közepén a mindenki számára elérhető, ingyenes ún. azonnali üzenetküldő szolgáltatások[3]. Manapság a szolgáltatások reneszánszukat élik, és felhasználók százmillióinak nyújtanak közvetlen beszélgetési közeget.

1.1. A privacy kérdése csevegő szolgáltatásokban

Az azonnali üzenetküldő szolgáltatások létrejötte után a két szolgáltatástípus útja különvált, s ez utóbbiak terjedtek el leginkább, amelyekhez ma számos ingyenes hálózat és kliensprogram áll rendelkezésre. A növekedés minden elképzelést felülmúlt, alkalmazásuk az élet több területén utat tört magának. Ma már százmilliós felhasználótábora van az azonnali üzenetküldő szolgáltatásoknak[4] [1], s ezek a hálózatok hatalmas, több milliárd üzenetből álló forgalmat bonyolítanak le naponta[5] [2].

Az azonnali üzenetküldő szolgáltatások egyre inkább a mindennapi élet részévé válnak, mind a privát, mind a munkahelyi használatot tekintve. A közeljövőben elképzelhető, hogy a szolgáltatások kilépnek eddigi környezetükből, hogy a mobil platformokon is domináns helyzetbe kerüljenek, ezzel még jobban integrálódva a mindennapi használatba[6] [3] [4]. Minél jobban az élet részévé válik a szolgáltatások használata, a magánszférát érintő kérdések annál fontosabbá válnak, és a precíz magánszféra–védelem alapvető igénnyé formálódik. Ennek a kérdéskörnek az általános megoldására törekvő EU konzorciumi projekt a PRIME [5].

Az üzenetküldő szolgáltatások már manapság sem csak a magánélet részesei, számos munkahelyen használják őket a kollégákkal, főnökkel való kapcsolattartásra, de ügyfélszolgálat is működhet (részben) azonnali üzenetküldő szolgáltatásra alapozva[7]. Mivel a vállalati használatban értékes információk utazhatnak át a rendszeren, több szolgáltatás speciális biztonsági lehetőségeket kínál vállalatok részére.

---

[2] A chat jellegű szolgáltatásokra tipikusan jellemző, hogy a felhasználók szobákban barangolhatnak, így tartva a kapcsolatot a többi felhasználóval.

[3] Az azonnali üzenetküldő szolgáltatásokban központi helyet foglal el a partnerlista, s a felhasználó ezen keresztül tartja a kapcsolatot az ide felvett partnereivel. Az angol elnevezése "Instant Messenger", rövid formájában IM.

[4] 2006 februárjában Európában 82 millióan, Észak Amerikában 69 millióan használtak azonnali üzenetküldő szolgáltatásokat a ComScore áprilisi cikke szerint.

[5] 2005-ben naponta átlagosan majdnem 14 milliárd üzenet volt az azonnali üzenetküldő hálózatok forgalma a ComputerWorld weboldal egy cikke szerint.

[6] Több szolgáltatásnak létezik olyan kliens programja, ami kézi készülékre letölthető, s így a szolgáltatás azokról is igénybevehető.

[7] Ilyen ügyfélszolgálattal például a neves cég, a Hewlett-Packard is rendelkezik.

Más alkalmazások is lehetségesek: könyvtárakban is működtetnek olyan ügyfélszolgálatokat, amelyek azonnali üzenetküldő szolgáltatásokon érhetőek el[8] [6], de a könyvtárakon és a munkahelyi alkalmazáson túl az azonnali üzenetküldő szolgáltatásoknak széles alkalmazási köre is elképzelhető.

Az elterjedtségnek köszönhetően többen felfigyeltek a szolgáltatásokban rejlő gyengeségekre: egyre több vírus és féreg kering az azonnali üzenetküldő szolgáltatások hálózataiban, főleg a közkedveltebbekben. Bár a legtöbb szolgáltatásban már bevezettek védelmi megoldásokat, de a szűrési, védelmi kérdésekre nem létezik egyelőre átfogó, egyértelmű válasz.

1.2. Hol az anonimitás?

A legnagyobb penetrációnak örvendő azonnali üzenetküldő szolgáltatások alapja az ún. jelenlétjelzés, azaz a kliens oldal központi elemén, a partnerlistán a felhasználók nyomon követhetik mások tevékenységeit, hogy mikor érnek rá, mikor nem, és néha azt is, hogy mikor ülnek le a számítógépük elé. Véleményünk szerint ez a helyzet a közeljövőben tovább fog súlyosbodni a modern mobil eszközök térnyerésével és a rájuktölthető azonnali üzenetküldők elterjedése miatt.

Mindemellett a jelenlétjelzés technológiának köszönhetően a partnereknek sűrűbben nyílik alkalma arra, hogy felkeressék egymást, hogy spontán kezdeményezzenek beszélgetéseket, és előfordulhat, hogy ennek egyetlen motivációja a másik jelenléte. Az ilyen jellegű viselkedés érvként állhat a magánszféra-védelem és az anonimitás bevezetése mellett.

Korábbi chat jellegű rendszerekben a felhasználók úgy is használhatták a szolgáltatást, hogy egy új identitást választva léptek be, így az anonimitás elviekben lehetőség volt. A jelenlegi azonnali üzenetküldő rendszerekben ez már nem lehetséges, ugyanis a felhasználókat egyértelműen azonosítja a partnerlistán a pszeudonim regisztrációs azonosítójuk[9]. A jelenlét és a látható állapot kezelése tipikusan a letiltás és rejtőzködés műveletekre korlátozódik.

---

[8] . Egy létező könyvtári alkalmazása azonnali üzenetküldő szolgáltatásoknak: http://www.umuc.edu/library/help/instantmessage.shtml

[9] Angol nyelven az ún. „screen name”.

2. A létező csevegő szolgáltatások vizsgálata

Vizsgálataink célja a sokak által használt, valamint a privacy, anonimitás, illetve biztonság szempontjából érdekesnek tekinthető csevegő szolgáltatások elemzése volt egy a célnak megfelelő, saját szempontrendszer felállításával.

2.1. Vizsgálati módszerek és a kiválasztott szolgáltatások

A szolgáltatások egy részét az EPIC [7] ajánlásából válogattuk össze. A kiválasztott szolgáltatásokat úgy választottuk ki, hogy a csevegő szolgáltatások minél szélesebb körét lefedjék. Fontos tény, hogy vizsgálatainkat 2006. február és júniusa között végeztük, azóta több új, az alábbi listába sorolható szolgáltatással ismerkedtünk meg, illetve több vizsgált szolgáltatáshoz új kliens jelent meg. A kiválasztott szolgáltatások az alábbiak voltak:

1. táblázat: A vizsgált szolgáltatások

Szolgáltatás neve	A szolgáltatás weboldala
MSN Messenger	http://messenger.msn.com
ICQ	http://www.icq.com/
Skype	http://www.skype.com
Yahoo Messenger	http://messenger.yahoo.com/
BitWise Instant Messenger	http://www.bitwiseim.com/
AOL Instant Messenger (AIM)	http://www.aim.com/
Softros LAN Messenger	http://messenger.softros.com/
PSST	http://psst.sourceforge.net/
mIRC és UnrealIRCd	http://www.mirc.com/ http://unrealircd.org

Az MSN, Yahoo Messenger és ICQ szolgáltatások kiválasztásukat elterjedtségüknek és felhasználóbarát alkatuknak köszönhetik — bőségesen nyújtanak olyan kiegészítéseket a kliensprogramjaik, amelyekkel mások nyugalmát könnyen meg lehet zavarni. Az ICQ esetében döntésünket segítette, hogy hálózata igen régi és régóta elterjedt — SPAM–bot-ok[10] és hirdetők először ezekben a rendszerekben kezdtek tevékenykedni, s teszik azt ma is, éppen ezért kíváncsiak voltunk védelmi és szűrőrendszerére.

[10] Azonnali üzenetküldők esetében következetesebb lehetne a „spim” szó használata, ugyanis a „spim” kifejezés a „spam” és IM (Instant Messenger) szavak összevonásából származik (precízen „spIM”-nek szokás irni). Nem jelent azonban fogalmi zavart a „spam” szó sem, így e két kifejezést a továbbiakban egyenértékűnek tekintjük.

A Skype szolgáltatása sokak számára a biztonságos beszélgetés szinonimája, ugyanis nem csak a szöveges beszélgetéseket, hanem a VoIP hívásokat is titkosított csatornán továbbítja (a szolgáltatás elsősorban a VoIP hívások köré épül). A szolgáltatás a másik háromhoz képest kevés zavarásra felhasználható funkcióval rendelkezik és hirdetők ellen is kevésbé védett (a hirdetőket egyszerűen ki is lehet zárni a partnerlistán kívüli felhasználók letiltásával).

A BitWise még inkább eltérő filozófiájú, mint az eddigi kliensek. A Skype-hoz hasonlóan kódoltak a kommunikációs csatornák, ezért döntöttünk — mint alternatíva — vizsgálata mellett.

További programokat, szolgáltatásokat is kiválasztottunk vizsgálatra. A programokat azonban csak részben kívántuk tesztelni, mivel a teljes körű tesztelés eredményei egyébként sem mutattak volna lényeges eltéréseket. Ilyen volt az AIM, amely szintén elterjedt és „nagy" azonnali üzenetküldő, mint az MSN és Yahoo Messenger.

A Softros Lan Messenger specialitása, hogy biztonságos kommunikációt ígér egyenrangú kliensekkel (peer–to–peer hálózat formájában) a helyi hálózatra, amely elgondolás egész filozófiájában eltér az eddig megismert azonnali üzenetküldőkkel szemben. A PSST még ennél is egyszerűbb szolgáltatás: erős titkosítást ígér végpont-végpont összeköttetésre. Két változata volt elérhető, mindkettőt teszteltük.

A chat jellegű szolgáltatások világából a legelterjedtebb és az egyik legrégebbi szabványosított megoldást, az IRC (Internet Relay Chat) választottuk. Sok IRC szerver és kliens implementáció létezik. Elsősorban szerveroldali megoldást kívántunk tesztelni, mivel már a mIRC klienshez rengeteg (ténylegesen több száz, ezer) kiegészítés található, amelyek között akadhatnak a kutatáshoz illők is, de ezek kiszűrése és végigpróbálása felemésztette volna a kutatás erejét. Szervernek az UnrealIRCd kiszolgálót választottuk, mivel sok magánszféra óvó szolgáltatása van, ingyenes és támogatja az SSL-t a kliens-szerver szakaszon. Mindemellett saját SPAM szűrő rendszerrel rendelkezik.

A kiválasztott szolgáltatások elsődleges vizsgálata alapján felállítottunk egy osztályozási szempontrendszert, amely segítségével utána a szolgáltatásokat empirikus módon megvizsgáltuk, majd értékeltük. Az így létrehozott eredmények alapján további kutatásokat végeztünk, s megvizsgáltuk a felfedezett gyengeségeket.

2.2. Osztályozási szempontrendszer

A taxonómia felállítását a listába tartozó programok segítségével végeztük, hogy segítségével a különböző szolgáltatások objektív összehasonlítása egyszerűbbé váljék. Az osztályozási szempontrendszer egy részét kiválasztottuk, mint elsődleges szempontokat, s az empirikus vizsgálatokat ezekkel végeztük el[11].

A következő fejezetekben a fontosabb kritériumokat ismertetjük a négy fő attribútum csoport szerint bontva.

2.2.1. Általános szolgáltatási attribútumok

Az itt említett attribútumok a csevegő szolgáltatások tipizálásában nyújtanak segítséget, illetve a különböző típusok tulajdonságainak szétválasztásában.

A csevegő szolgáltatásokat első sorban típus szerint különböztetjük meg, amely a következők valamelyike lehet: azonnali üzenetküldő, chat jellegű és peer–to–peer. Megemlítjük a hibrid szolgáltatás típust, azonban mivel ilyen rendszert nem találtunk, nem vettük bele a taxonómiába.

A hálózati modellek szorosan kapcsolatban állnak az előbbi fogalmakkal. Megkülönböztetünk központi szerverre, az elosztott szerverhálózatra épülő szolgáltatásokat, illetve a peer–to–peer jellegűeket.

Vizsgáltuk, hogy a felhasználók milyen fedőnévvel jelenhetnek meg a csevegő szolgáltatásban. Itt is két fő kategória különböztethető meg: a felhasználók vagy tetszőleges fedőnevet választhatnak, vagy regisztrálniuk kell. Egyes speciális esetek előfordulnak, amikor a program például a számítógépre bejelentkezett felhasználó nevét alkalmazza (vagy véletlen sorsol), de ez a megoldás nem jellemző.

A kommunikáció során igénybe vehető médiumok alapvetően meghatározzák a sikerességét, elterjedtségét egy csevegő szolgáltatásnak, és az is nagyon fontos szempont, hogy elsődlegesen milyen médiumhoz készítették a szolgáltatást. Ennek megfelelően megvizsgáljuk, hogy egy adott rendszerben mely médiumok használhatóak a szöveges, VoIP és videó átvitel lehetőségek közül.

[11] A szűkítés oka a kutatás terjedelmének racionális korlátozása volt.

Érdekes kérdés a szolgáltatások esetében, hogy a kommunikáció többszereplős formái engedélyezettek-e a párbeszéd, vagy konferencia lehetőségekből. Egyes rendszerekben a konferencia alternatívája a szoba, vagy más nevén a csatorna. Fontos megjelölni, hogy a szöveges beszéd mellett VoIP beszélgetésre is van-e lehetőség, vagy webkamera használatára a többszemélyes beszélgetésekben.

A keresésnek, felhasználók felfedezésének jellegzetesen három módja van. Rá lehet keresni[12] az attribútumok valamilyen minta szerinti megadásával a felhasználókra, vagy ellenőrizni lehet valahogy a névnek az érvényességét, azaz aktuális jelenlétét a rendszerben. Lehet, hogy a név a partnerlistán rajta van, így automatikusan kiderül az állapota (jelenlétjelzés), de lehet, hogy külön lehet csak ellenőrizni. Ezen szempontok közül az első kettő több esetben egyszerre teljesülhet.

2.2.2. A négy fő magánéletvédő, adatvédelmi és egy kiegészítő kritérium

A négy fő magánéletvédő, adatvédelmi kritérium definícióját és értelmezését csevegő szolgáltatásokra vonatkozóan az alábbiakban adjuk meg. Ez a négy kritérium a következő (egy kiegészítő kritériumot is értelmeztünk):

- *Anonimitás*: először feltételezzük, hogy a felhasználó személye nem határozható meg akkor sem, ha ismerjük a szolgáltatást igénybe vevő összes felhasználót, vagy valamilyen egyedi azonosítójukat. A felhasználó azonosítója nem köthető másik, a rendszerben használt azonosítóhoz. Ez a kitétel a korábban használt azonosítókra is vonatkozik, azaz összegezve a mindenkori azonosítókra.
- *Pszeudonimitás*: a felhasználó személye ekkor sem derülhet ki, de megengedjük, hogy az összeköthetetlenség sérüljön — a felhasználó azonosítója köthető más rendszerbeli, vagy korábbi azonosítókhoz (tehát az azonosító előtörténettel rendelkezik, vagy azonosítókkal csoportba vonható).
- *Megfigyelhetetlenség*: olyan tulajdonság, mely megköveteli, hogy két vagy több kommunikáló fél közötti információátvitel tartalmát harmadik félnek nem lehetséges megismerni, csak az átvitel tényét tudja megállapítani.
- *Összeköthetetlenség*: a PRIME és a Common Criteria V3.1. értelmezését egyesítettük; külső megfigyelő ne legyen képes megállapítani, hogy a rendszeren belüli eseményekért ugyanazon felhasználó felelős-e, vagy sem. Két felhasználó esetében ez azt jelenti, hogy a kommunikáló felek közti üzenetváltások időben nem összeköthetőek. Az összeköthetetlenséget értelmezzük csoportokra is, a

[12] Keresés, ellenőrzés az — angol nevén — „user directory”-ban.

csoportos beszélgetési viszonyok összefűzéséből ne legyen kivehető annak az életfolyamata.

- *Összekapcsolhatatlanság*: a felhasználók összekapcsolhatóságával foglalkozunk ennél a kritériumnál, azaz a fennálló kapcsolatok felderíthetőségével. Ez megfelel a Common Criteria szerinti megfigyelhetetlenségnek, amely szerint a kommunikációban résztvevő felek kiléte rejtett a külső megfigyelő elől. Ha az *összekapcsolhatóság* teljesül, akkor bizonyos esetekben sérülhet az *összeköthetetlenség* tulajdonság, mivel a felhasználók jelenléte összekapcsolhatóvá teszi egy szobának, vagy konferenciának a különálló viszonyait. Az anonimitást is kompromittálhatja, hiszen ha egy felhasználó beszélget valakikkel, és utána kilép, vagy kiesik a rendszerből, majd másik névvel (az előzőtől függetlennel) visszatér, akkor a kapcsolatok kirajzolódásából következtetni lehet a korábbi névre, mert a partnerek neve nem változott.

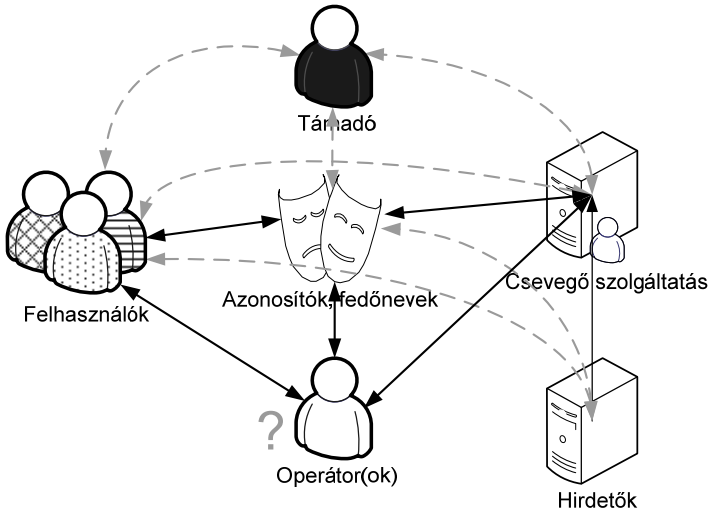
A rendszer következő szereplőit különböztetjük meg:

- átlagos felhasználók
- kiemelt felhasználók: operátorok
- csevegés–szolgáltató
- felhasználói csoportok tagjai (szoba, csatorna, konferencia) és azon kívül esők
- hirdetők
- támadó, rendszeren kívül eső, külső szemlélők (például közbenső szolgáltatók)

A felsorolt szereplők viszonyát vizsgáltuk átlagos felhasználókkal és felhasználói csoportokkal.

2.2.2.1. A szereplők kapcsolatrendszere

Kutatásunkban a felsorolt szereplőket egy kapcsolati ábrán vonjuk össze. Az ábrán a felhasználói csoportokat nem foglaltuk össze, ellentétben a többi szereplővel. A fekete nyilak jelzik, hogy mely entitások melyekkel vannak kapcsolatban. Az operátor mellett egy kérdőjelet tüntettünk fel, hiszen az operátor alkalmasint a rendszer egészét láthatja, így a kompromittálása veszélyes lehet a rendszer egészére. A nem kívánatos kapcsolatokat a szaggatott, szürke színű nyilak jelzik.



1. ábra: Szereplők és kapcsolataik

Mindemellett az ábrába néhány egyszerűsítést is bevittünk. A szolgáltatás ugyan mindig ismeri a felhasználók és fedőnevek halmazát, és így párosítást is képes végezni, de feltesszük, hogy ilyet nem tesz, mert megbízható. Így elképzelhető az az eset is, hogy problémás, ha a szolgáltatást kompromittálja a támadó fél (ezekkel a lehetőségekkel itt nem foglalkozunk, mert a technikai megvalósítás függvénye).

2.2.2.2. Az anonimitás és a pszeudonimitás kiemelt fontossága a szereplők szemszögéből

Megjegyezzük, hogy bár megfigyeljük az anonimitás lehetőségét a különféle rendszerekben, de a vizsgált rendszerek egyike sem tűzi ki célként az anonimitás lehetőségét.

Egy felhasználó akkor anonim a többi felhasználó számára, ha az adott pillanatban fellelhető információk alapján nem tudják valós személyhez kötni, vagy korábbi felhasználóhoz. Ha ismerhető a rendszert használó összes felhasználó IP címe, akkor se lehessen IP cím – felhasználó név párosokat létrehozni. Ha a felhasználó neve kötött, például egy pszeudonim fedőnévhez, akkor ez a kritérium nem teljesülhet. A kritérium teljesülése azért fontos, hogy a többi felhasználó elől bármikor el lehessen tűnni, és ez csak ebben az esetben teljesülhet.

Operátorok számára fontos, hogy a felhasználó megfigyelhető és azonosítható legyen. Ez ellentmond az anonimitás követelményének, sokszor számukra a felhasználók nem anonimek, és a felhasználókat könnyen IP címekhez kapcsolhatják. Ez csak akkor nem jelent különösebb fenyegetést az anonimitásra, ha nem élnek vissza ezzel. Sajnos a legtöbb rendszerben az operátori működés nem ismert, s az azonnali üzenetküldő szolgáltatásokban feltételezhetően nincsenek is ilyen értelemben vett operátorok.

Hirdetők, szolgáltató. A szolgáltató ismeri, hogy a felhasználói honnan kapcsolódnak, milyen azonosítókat használnak. A szolgáltató részéről akkor biztosan nem tekinthetünk anonimnek egy felhasználót, ha a külső világ felé köthető információkat naplózzák. Ha legfeljebb a belső tevékenységeket, akkor a felhasználó fedőnevét pszeudonimnek tekinthetjük. Ha ezek sem kerülnek naplózásra és a felhasználó tevékenységei, különböző használt azonosítói, nevei nem összeköthetőek, akkor anonimnek tekintjük.

A hirdetők számára a felhasználói azonosító és valamilyen egyedi azonosító, mint például az IP cím, valószínűleg a szolgáltató segítsége nélkül nem összeköthető, viszont megfigyelhetik a felhasználók IP címét és további adatokhoz, profilhoz köthetik azokat, ezért fontos, hogy a szolgáltatás reklámjai megbízhatóak legyenek, és kizárólag a szolgáltatástól töltődjenek fel a felhasználókhoz.

Külső szemlélők, közbenső szolgáltatók. A külső szemlélők számára minden felhasználóra teljesülnie kell az anonimitásnak, hiszen ha ez a kritérium nem teljesül, az kompromittálja a többi szereplőre felírt kritériumokat.

A többi kritérium teljesülése az anonimitás szempontjából fontos és elengedhetetlen.

2.2.3. Egyéb magánszféra- és adatvédelmi szempontok

Az alábbi kritériumok elvárhatóak egy csevegő szolgáltatásban, hiszen meghatározzák, hogy a felhasználó hogyan védekezhet a különböző zavaró hatások ellen, illetve hogyan dönthet az őt érintő adatok láthatóságáról.

2.2.3.1. Megjelenési módok és rejtőzködési lehetőségek

Sokat számít, hogy a felhasználó eldöntheti-e, milyen néven akar megjelenni a rendszerben. Egyes rendszerekben ez tetszőleges lehet, de általában a regisztrációs azonosító köti a felhasználókat, speciális esetben ez csak a belépéshez kell, s tud egy független azonosítót választani.

A rejtőzködési lehetőségek általában alapvető szolgáltatásként értelmezhetőek minden csevegő szolgáltatás esetében. Ezért külön megvizsgáljuk a szabályozás módját (például tiltás, láthatóság engedélyezése). A legtöbb szolgáltatásban lehetőség a láthatatlan mód (egyes esetekben így be is lehet jelentkezni), így a felhasználó eltűnhet a teljes partnerlistája elől. Kapcsolódó kérdés, hogy a felhasználó kérhet-e listát arról, hogy mely felhasználóknak szerepel a partnerlistáján. Így a felhasználó felfedezheti és kizárhatja a láthatatlan megfigyelőket az életéből.

Bizonyos esetekben egy felhasználó nem feltétlenül akarja az állapotát elrejteni valaki elől, lehetséges, hogy csak valakitől nem szeretne üzeneteket fogadni. Ekkor a mellőzés[13] műveletről beszélhetünk.

Továbbá megvizsgáljuk minden rendszerben, hogy a felhasználó hogyan szabályozhatja azt, hogy megjelenjen-e a keresőrendszerben, illetve, hogy ki adhatja hozzá a partnerlistájához (és milyen feltételek mellett láthatja az állapotát).

2.2.3.2. Rendelkezés a profilról és a felhasználó adatairól

A profil létrejöhet a regisztráció során, és később is létrehozhatják. Vannak szolgáltatások, ahol az előbbi automatikus, ezért vizsgáljuk, hogy rendelkezhet-e erről a felhasználó, illetve milyen rendelkezések vannak róla. A profil kezelése tipikusan történhet a kliensprogramon belül és webes adatlapon. Fontos kérdés a láthatóság kérdésének kezelése.

A webkamerával, vagy mikrofonnal rendelkező tulajdonos nem feltétlenül kívánja mindenkivel megosztani a tényt, hogy ilyen eszközzel rendelkezik — az esetleges „zaklatások” elkerülése végett. Ezért ennek az információnak az elrejtése kívánatos lehet.

A belépési adatokat a legtöbb rendszer rögzíti, ha kérik. Ez kényelmes lehet, de a számítógép egyszerű használatával a felhasználó megszemélyesíthető. Ezért fontos, hogy pontosan szabályozható legyen, hogy a belépési adatok mely része maradjon meg a program emlékezetében, és tetszés szerint törölhető legyen.

2.2.3.3. Tevékenységek automatikus felfedése

Ide sorolunk minden olyan tevékenységet, amelyek a felhasználó a gépén végez (vagy ha nem használja, akkor azt), illetve például a webkamera képének hirdetését. Hasonló funkció

[13] Angolul „ignore”.

lehet az éppen hallgatott zene előadójának és címének a kiírása a név mellé, vagy az épp nézett filmé, de ha ilyen funkciókat támogat a program, akkor annak szabályozhatónak kell lennie.

2.2.3.4. Audiovizuális magánszféra védelme

Az audiovizuális magánszféra védelmére leginkább azoknak a rendszereknek kell felkészülniük, amelyek sok erre tekintve sértő szolgáltatást nyújtanak. Ide tartoznak a beszélgetésben szereplő különféle animációk, rajzok, képek, hangok, hangfelvételek, stb. Ide soroltuk a kellemetlen kifejezések szűrését is. Hangok esetében különösen zavaró lehet az automatikus lejátszás, a hangerő megfelelő szabályozhatóságának hiánya.

2.2.3.5. SPIM védelem

A reklámüzenetek és a reklámozó felek elleni védelmet vizsgáljuk teljes körűen SPIM védelem címszó alatt, a szolgáltatások terjedésével ez a kérdéskör fontossá vált.

2.2.3.6. Kapcsolódó szolgáltatások és reklámok

Egyes programok hirdető, spyware, időjárás jelentő kisméretű programokat telepítenek maguk mellett, netán más programokhoz kínálnak fel kiegészítéseket. Egyes esetekben a telepítésük rejtett, néha opcionális, de előfordul, hogy kötelező.

2.2.4. Biztonsági funkcionalitás

A biztonsági funkcionalitás elemeit vizsgálva a négy fő kritérium beteljesítéséhez szükséges alapelemek létét ellenőrizzük, és megnézzük, hogy a biztonságosnak kikiáltott termékek valójában mennyire mondhatóak valójában annak.

A beléptetés védelme akkor érdekes címszó, ha a kapcsolat nem védett, csak a bejelentkezés idejére. Ha nem csak a beléptetés védett, hanem a teljes kapcsolat, illetve, ha lehet tudni a szerverekről és az azok közti kapcsolat védelméről, akkor azt is megvizsgáljuk. A szöveges beszélgetések védelme még elterjedtebb, de a hang és videó médiumoké kevésbé. Manapság ez egyre fontosabb kérdés, mivel már hallani lehetett olyan adathalászati módszerről, amikor VoIP csatornák lehallgatásával jutott információhoz az illető [10]. Innen már csak egy lépés eljutni a webkamerás beszélgetésekhez, amelyek valószínűleg ehhez hasonlóan egyre inkább elterjednek majd.

Egy korszerű kliensprogramtól elvárható, hogy figyelmeztesse a felhasználót, ha gyanús esemény következik be, például adathalászat–gyanús egy URL, vagy ha vírusgyanús fájlt szeretne neki küldeni. Az is előnyös lehet, ha a felhasználó a saját tapasztalatának megfelelően beállíthatja a programban szkeptikusságának szintjét, és hasonló módon menedzselheti a biztonsági beállításokat is.

2.3. Vizsgálati eredmények

A szolgáltatások vizsgálati eredményeit jegyzőkönyvben rögzítettük; legfontosabb megállapításainkat az alábbiakban foglaljuk össze.

2.3.1. Elhatárolható rendszertípusok

Az empirikus elemzések eredményeképpen két fő rendszertípust különíthetünk el, ami jól megfelel a definícióként megadott rendszertípusoknak, és a típus maga vonz bizonyos tulajdonságokat. A két típust az alábbi összehasonlító táblázatban vetjük össze:

2. táblázat: A két fő rendszertípus összehasonlítása.

Chat jellegű szolgáltatás	Azonnali üzenetküldő szolgáltatás
Szabadon választható fedőnév	Kötött azonosító (regisztrált)
Szobák	Konferenciák
Konkrét fedőnév jelenlétének lekérdezése	Jelenlét érzékelés partnerlista alapján
Felhasználók felfedezése (szobák, szerver oldali névlista)	Felhasználók keresése
Parancsvezérelt (kevés grafikus elem)	Grafikus felület (kevés parancs)
Mellőzés, identitásváltás	Tiltás, rejtett állapot
Központi szerver, elosztott szerverhálózat	Központi szerver, szerverfarm

A peer–to–peer rendszerekre tipikusan szabadon választható fedőnév, esetleg névlista használata jellemző. A felhasználók felderítése elosztott módon, automatikusan történik, vagy egy másik médiumon keresztül.

A három típuson túl létezhet — ahogy korábban említettük — egy olyan rendszertípus is, amely hibrid, azaz egyszerre tartalmaz chat jellegű és azonnali üzenetküldő szolgáltatásokra utaló jellegzetességeket is. Ilyen rendszerrel nem találkoztunk, de az ICQ szolgáltatását ilyen típusúnak is tekinthetnénk. Mint vizsgálataink során kiderült, az ICQ és az AIM közös hálózatot használ, a kliensek között olyan mértékű az átjárhatóság, hogy a felhasználók felvehetik egymást a partnerlistájukra. Továbbá kiderült számunkra, hogy az ICQ

szolgáltatásában a konferencia jellegű beszélgetések kiszolgálását egy integrált szolgáltatás végzi — egy UnrealIRCd szerverre kapcsolódik a kliens, ahol létrehoz egy szobát, amely otthont nyújt a beszélgetésnek. Ebbe a szobába a felhasználó meghívhatja a partnereit. A szerver szobái webes felületen listázhatóak, és meglátogathatóak az ICQ beépített IRC kliensprogramja segítségével.

Úgy látjuk, hogy az ICQ nem egy hibrid, hanem inkább egy több protokollt is átfogó szolgáltatás, amely ezt a tényt a felszín alá rejti. Ennek ellenére a szolgáltatást azonnali üzenetküldő szolgáltatásként értékeltük, hiszen ez a fő profilja.

2.3.2. Tipikus megoldások a magánszféra-védelemben

Az azonnali üzenetküldő szolgáltatások a felhasználó kezébe általában listák kezelésére adnak lehetőséget, amikor a felhasználók eldönthetik, hogy ki láthatja őket (akkor is, ha rejtett az állapotuk mindenki felé), s kik számára rejtettek. Ezek általában állandó listák, egyedül egy szolgáltatás (Yahoo Messenger) esetében találkoztunk ideiglenes listákkal — ilyenkor a felhasználó csak az adott belépési viszony erejéig szerepelt az adott listán. Az összes felhasználó elől a rejtett módra váltással lehet eltűnni. A láthatatlanság felhasználónkénti megadása a tiltás műveletet, a láthatóság pedig rejtett módban a felfedést jelenti.

A profilok szempontjából általánosan elmondhatjuk, hogy jól szabályozhatóak minden rendszer esetében. A profilokhoz kapcsoljuk a státusz webes megjelenítését ICQ és Skype esetén (kikapcsolható a webes státusz megjelenés). E két szolgáltatás és a BitWiseIM esetén a profil webes felületen nem jelenik meg, ilyen lehetőség nincs. A profilokat minden felhasználó megtekintheti, szabályozásuk egyszerű — a kitöltött mezők jelennek csupán meg, kitöltésük nem kötelező (például nem regisztrációhoz kötött). Az MSN és a Yahoo Messenger esetén létezik weboldalon megtekinthető profil (és csak ott), s mindkét esetben a webes profil célcsoportja jól megválasztható. Az utóbbi esetében ez teljesen ki is kapcsolható, vagy csak 18 éven felülieknek engedélyezhető.

A belépési adatok kezelése kritikus kérdés lehet egy nyilvános, vagy otthoni, de több felhasználós számítógépen. A legtöbb program nyújt erre megoldást, bizonyos kliensek esetén a jelszót elfelejti a program, ha bejelentkezéskor nem kérjük a megjegyzését (direkt törlés nincs). Egyedül az MSN Messenger ad lehetőséget az adatok direkt törlésére (a jelszó „elfelejtést” is támogatja).
Nagyon hasonló az alapvető tevékenységek automatikus felfedése minden rendszer esetén: mindegyik vizsgált azonnali üzenetküldő szolgáltatás lehetőséget nyújt a távollét automatikus beállítására (sok esetben állítható az addig várandó idő a kiírandó üzenettel

együtt). Néha további automatikus esemény-felfedés is értelmezett, mint például teljes képernyős programok futtatása, filmnézés, zenehallgatás, webkamera képe.

Az audiovizuális magánszféra védeleme programonként viszont igen eltérő képet mutat. Különösen változó aszerint, hogy a programok milyen ide kapcsolódó szolgáltatás elemeket nyújtanak. Az audiovizuális magánszférát zavaró elemek lehetnek:

- Hangklip: mikrofonnal rögzített felvétel
- Emotikonok: a szöveges emotikonok megjelenítése képekkel
- Felhasználói képek, animációk, emotikonok: különböző karaktersorozatokhoz hozzárendelhető saját képek, apró animációk, amelyek a beszélgetés szövegében jelennek meg
- Hangbetétek: bemutató jellegű, rövid zene, vagy dalrészletek (vagy egyéb)
- Animációk: a beszélgetés szövegéből kilógó, általában nagyméretű animációk
- Közös háttér, megjelenítési stílus: ez utóbbi a beszélgetés egész ablakára vonatkozik.

A felsoroltak tiltása, vagy korlátozása mellett az audiovizuális magánszféra védelmét szolgálhatja:

- Bizonyos üzemmódban a jelző–, (egyéb felhasználói–,) rendszerhangok tiltása.
- VoIP hívások automatikus elutasítása, vagy néma kicsöngés.
- Kellemetlen, vagy tiltott kifejezések szűrése: sok esetben például politikai kifejezések, trágárságok és hasonló kifejezések kerülnek automatikus kimoderálásra.

A SPIM védelem is sokféleképp jelenik meg a különböző programokban. Általában nincs konkrét védelemről szó, ilyen szűréssel egyedül az ICQ szolgáltatásban találkozhatunk. Az MSN Messenger szolgáltatásában ad–hoc módon fejlesztett, nem dokumentált szűrés van beépítve (amely mibenlétéről megkeresésünkre nem tudtak érdemi választ adni), a Yahoo Messenger esetében pedig szavak szűrésére specializálódott védelem található. Ezek egyike se mondható túl hatékonynak. A SPIM fenyegetettség az MSN Messenger (vagy Windows Messenger), illetve az ICQ és AIM közös hálózatában a legmagasabb [12], mindemellett érdekes kérdés, hogy a legfenyegetettebb rendszerben, az MSN Messenger-ben, miért nincs beépített védelem.

Ami külön pozitívumként jelenik meg a teszteltek esetében, hogy külső program használatát nem kényszerítik rá a felhasználóra. Ez valószínűleg a kevésbé elterjedt szolgáltatásokra, kliensprogramok forgalmazóira lehet jellemző.

2.3.3. Az anonimitás és a kapcsolódó kritériumok teljesülése

Az anonimitás lehetősége csevegő szolgáltatásokban kritikus lehet, ennek ellenére kevés rendszerben jelenik meg lehetőségként. Megvizsgáltuk a szükséges kritériumok teljesülését.

2.3.3.1. Anonim és pszeudonim megjelenés

Az anonimitás fogalmát a kritérium magyarázatánál értelmeztük csevegő szolgáltatások esetében. Ennek értelmében az empirikus vizsgálatok nyilvánvalóvá tették, hogy az azonnali üzenetküldő szolgáltatások esetén nem lehetséges jelen lenni anonim formában, mivel a regisztrációs azonosítóra a felhasználó mindig visszavezethető. Ez titkosítást nem alkalmazó rendszerekben a külső megfigyelő számára sem jelent gondot, ahol azonban titkosítás van, ott azonosítani kell tudni a felhasználó fedőnevét az összekapcsoláshoz. Ez már nem olyan egyszerű probléma, de megoldható lehet, éppen ezért is fontos a titkosított adatkapcsolat.

Az operátori, moderátori funkciók betöltéséről, az ilyen kiemelt jellegű felhasználók lehetőségeiről sajnos ismereteink korlátosak, véleményünk szerint ezekben a rendszerekben ilyen beosztású felhasználók nincsenek. Ezt alátámasztja az, hogy a felhasználók eleve nincsenek a szolgáltatás elemei miatt kiszolgáltatva másoknak, illetve tudnak védekezni a többi felhasználó zavaró viselkedése ellen (még ha nem is kifinomult módszerekkel). Többmilliós felhasználótábor esetén ilyen kiemelt felhasználókról nincs is értelme beszélni, inkább rendszeradminisztrátorokról. A rendszeradminisztrátorok ebből a szempontból inkább egyenlőnek tekinthetők magával a szolgáltatással.

Hirdetőket jelen esetben csak azonnali üzenetküldő szolgáltatásban tudunk értelmezni, mivel a vizsgált chat jellegű szolgáltatásban nincsenek hirdetésre alkalmas felületek.

Így egy felhasználó csak egy chat jellegű szolgáltatásban lehet anonim. A vizsgálati összeállítás esetén például akkor, ha minden adatot megváltoztat a felhasználó, és a host részben rejtett. Mivel ez opcionális, és ha ez a szerveren nem automatikus, a felhasználónak rögtön a fellépést követően fel kell vennie ezt a módot.

Egy ilyen szerveren (pontosabban a szerverláncon) lévő szolgáltatás-szintű[14] operátorok számára a felhasználó nem anonim. Ennek az az oka, hogy ők akkor is láthatják az igazi

[14] IRCOP elnevezésű szerveroperátorok.

host-ját a felhasználónak, ha az titkosított módban van, és az IP címét is bármikor lekérdezhetik (amely szintén részben titkosított).

2.3.3.2. Megfigyelhetetlenség

A megfigyelhetetlenség csak azokban a rendszerekben teljesül, ahol a biztonsági funkcionalitás részben teljesülnek bizonyos feltételek: a hálózaton minden egység között (szerver–szerver és kliens–szerver kapcsolatok) titkosított az adatátvitel.

2.3.3.3. Összeköthetetlenség

Az összeköthetetlenség sok mindentől függhet. Mivel a felhasználói azonosítók szerepelnek például az azonnali üzenetküldők minden üzenetében, így csak a kapcsolat forgalmának titkosításával érhető el, hogy az üzenetek, és így a tevékenységek ne legyenek összeköthetőek egy külső szemlélő számára. Külső szemlélő számára az összeköthetetlenséget Onion Routing alapú MIX hálózattal, állandó szinten lévő forgalommal erősíthetjük, ha a kapcsolat titkosított.

Ha külső szemlélő számára már az összeköthetetlenség teljesül, utána a belső szereplők szempontjából kell vizsgálni a kritériumot. Mint korábban említettük, sajnos ez nem teljesülhet azonnali üzenetküldő rendszerekben, mivel az állandó azonosítók folyamatosan összekötik a szereplők minden mozzanatát. IRC alapú chat jellegű rendszerben akkor teljesülhet, ha a felhasználó képes minden adatának a megváltoztatására tetszőleges időpontokban.

2.3.3.4. Összekapcsolhatatlanság

Az összekapcsolhatóság erősen attól függ, hogy a protokoll párbeszédei lehallgathatóak-e (eszerint a titkosított folyamok ismét előnyt élveznek), illetve milyen lekérdezési módszerek léteznek a szolgáltatásban. A vizsgált chat jellegű szolgáltatás esetén például a szobák látogatóinak a nevét le lehet bizonyos esetekben kérdezni. Különböző módokkal a felhasználók kivonhatják magukat az ilyen listákból, illetve a szoba is lezárható. Más esetben itt ez nem áll fenn, mivel konferenciákra nincsen lehetőség.

A vizsgálati tapasztalataink szerint az azonnali üzenetküldő szolgáltatások szereplői nem tudják megmondani, hogy mely felek vannak konferencia módban (vagy mely felek folytatnak párbeszédet). Ez valószínűleg a legtöbb esetben kompromittálható lehallgatással, így ez is indokolja a megfigyelhetetlenség kritérium fontosságát.

2.3.4. Felfedezett privacy-védelmi gyengeségek

Ebben a fejezetben közöljük a vizsgált szolgáltatások közül kettőnek olyan privacy-védelemmel kapcsolatos gyengeségét, amelyre vizsgálataink során derítettünk fényt.

2.3.4.1. MSN Messenger 7.5

Az MSN Messenger ezen változatában felfedezett hiba segítségével a felhasználó állapota akkor is felfedhető, ha rejtett módban van jelen. Ehhez egy új partnertől (amelyet a támadó felügyel) felvételi kérelmet kell küldeni a felhasználó felé. Ha rejtett módban tartózkodik, és elfogadja a felvételi kérelmet, ez rögtön kiderül a felhasználó számára, és így az is nyilvánvalóvá válik, hogy rejtett módban, de jelen van a rendszerben. Speciális klienssel, amely a különböző eseményeket időpecséttel naplózza ez a tevékenység könnyen nyomon követhető, noha a módszer nem túl rugalmas és könnyen kivitelezhető.

A felfedezett gyengeség szerintünk működik az újabb változatban, a Windows Live Messenger-ben is, de megfelelő módon kísérletileg ezt még nem ellenőriztük.

Továbbá valószínűleg ez a kompromittálási megoldás más azonnali üzenetküldő rendszerekben is működhet, ugyanis a partnerlistára való felvételi folyamat ezekben a rendszerekben ugyanúgy működik.

2.3.4.2. Skype 2.5

A Skype-ban talált gyengeséget hasonlóan a láthatatlan mód felfedésére használjuk. A módszer sokkal egyszerűbb, többször kivitelezhető és független a másik féltől (az előző módszer esetében elutasítással a kísérlet meghiúsul).

A felfedéshez elegendő egy üzenetet küldeni a gyanús felhasználónak. Ha a felhasználó nem elérhető, hamarosan megjelenik a beszélgetési ablakban a figyelmeztetés, hogy az üzeneteket nem lehetett továbbítani. Ha azonban a felhasználó mégis jelen van, akkor az üzenetet el tudja küldeni neki a kliens, és így ez a figyelmeztetés nem jelenik meg – ebben az esetben máris tudhatjuk a felhasználó valós állapotát.

Csupán a rendszer tervezőinek elgondolásától függően egy további gyengeség lehet, hogy a letiltott felhasználó tudatában van, ha letiltják, ekkor ugyanis megváltozik a partnere ikonja. Szerintünk az, hogy ki mely felhasználókat tiltja le a partnerlistáján az érzékeny információnak számít, és ha ezt közölni szeretné a letiltott partnerével, arról először nyilatkoznia kellene.

2.4. A vizsgálatainkból kimaradt érdekes szolgáltatások

Sajnos nem minden szolgáltatást állt módunkban megvizsgálni. Ilyen volt többek között az Ultramagnetic[15] azonnali üzenetküldő is, amely a fellelhető hírek szerint mindamellett, hogy bizalmasan szállítja az információkat, egy anonim csevegő szolgáltatás lesz. Sem a kutatás kezdetekor, sem pedig lezárásakor nem volt még elérhető változata. A kutatás lezárása után jelent meg a végleges verzió Scatter Chat néven[16], s kiderült, hogy a külső világ felé nyújtott anonimitást Tor [8] hálózat segítségével éri el. A program különböző kliensprogramokat képes helyettesíteni különféle szolgáltatásokhoz, azaz ún. aggregátor kliens.

A Skype szolgáltatáshoz a 3.0 béta verziójú kliens (a szolgáltatás támogatásával) 2006. november 8-án jelent meg. Ez az első valójában hibridnek tekinthető szolgáltatás. Eddig a felhasználók konferenciabeszélgetéseket hozhattak létre, viszont a szolgáltatás fő profiljának megfelelően a felhasználók már böngészhetnek VoIP alapú szobák között is.

A több szolgáltatást átfogó üzenetküldők közül a GAIM OTR (Off the record messaging) [9] kiegészítést szerettük volna tesztelni. Sajnos a tesztelést a telepítési nehézségek miatt a tesztelést nem tudtuk elvégezni. Ez a GAIM kiegészítés lehetőséget nyújt — a megfelelő kulcsmenedzsment segítségével — a beszélgetéseket a lehallgatástól védetté tenni, úgy, hogy ha valakinek még sikerül is lehallgatni egy beszélgetést az aktuális viszonykulcs feltörésével, a korábbi, vagy az aktuális beszélgetésekhez nem fog tudni hozzáférni. Ez teljesül arra az esetre is, ha a beszélgetéseket naplózzuk, és a támadó a naplófájlokhoz férne hozzá.

A GAIM SILC[17] kiegészítése a SILC (Secure Internet Live Conferencing) protokollra épül [13]. Hasonló az SSL technológiához, saját kulcscsere, hitelesítési, csomagvédelmi protokollja van, amelyek speciálisan az alkalmazási rétegbeli protokollhoz, a csevegő szolgáltatásokhoz fejlesztettek ki. A szolgáltatás és a protokoll vizsgálatát is szeretnénk a jövőben elvégezni.

A Secure IM[18] olyan kiegészítő az AIM felhasználói számára, amely a készítő szerint nagy biztonságot nyújt, ha a beszélgetőpartner is futtatja ezt a kiegészítést. Az említett szolgáltatásokkal, kiegészítésekkel együtt ezt a kiegészítést is szeretnénk megvizsgálni.

---

15 A szolgáltatás régi honlapja itt érhető el: http://ultramagnetic.sourceforge.net/

16 A Scatter Chat weboldala: http://www.scatterchat.com/

17 Elérhető az alábbi címen: http://www.silcnet.org/software/users/gaim/overview.php

18 Elérhető itt: http://www.vonnieda.org/SecureIM/

3. Összefoglalás

A vizsgálatainkból kiderül, hogy a rendszerek között alapvetően biztonsági, magánélet-védelmi szempontból két típus létezik — azaz a rendszerek vagy a kezdetektől fogva törekednek egy bizonyos biztonsági szint megvalósítására, vagy csak az idők során fellépő nyomásoknak engedve, foltokkal próbálják az efféle hiányosságokat elfedni. Az előbbi kategória programjai esetén tipikusan a külső megfigyelők és támadók ellen próbálnak védekezni, a belső támadók, mint például SPIM küldők ellen, kevés esetben van hatékony védelem.

Ilyen például a Skype esete, hiszen ennél a szolgáltatásnál a kivitelezés kiemelkedő mérnöki munkára utal, de a belső modell hiányos — ahogy korábban leírtuk felfedezésünket, hiába lehetséges egy felhasználónak láthatatlan módban elbújnia mások elől, egy egyszerű próbálkozással ez az állapot felfedhető.

Általánosságban elmondható, hogy a szolgáltatások a nyújtott lehetőségekkel szemben nem adnak kielégítő megoldást a felhasználó kezébe a magánszféra védelmének tekintetében, a védekezési lehetőségek korlátozottak és erősen hiányosak. Emellett az is általánosnak tekinthető, hogy a szolgáltatásokban az anonimitási lehetőség megvalósítása nem cél. A kutatás lezárása után megismertünk olyan rendszereket, amelyeknél az anonimitás megjelenik, de ezek a rendszerek is csak alacsony szinten, külső megfigyelők ellen nyújtanak anonimitást, de ez sem elegendő.

A szerző az itt ismertetett kutatás lezárása után kutatócsoportot alapított, és kutatótársaival 2006 nyarán-őszén felállított egy ideális anonim csevegő szolgáltatással szemben támasztott elvi kritériumrendszert. A kritériumokra, tervezési paradigmákra támaszkodva a kutatócsoport kidolgozta egy ideális szolgáltatás elvi megvalósítását és elkezdte annak implementációját is. A kutatócsoport tagjai a téma folytatásaképpen az Alma Mater sorozat következő kötetében további publikációkat terveznek megjelentetni.

Irodalomjegyzék

[1] Andrew Lipsman, ComScore press release, 2006
http://www.comscore.com/press/release.asp?press=800

[2] John Dickinson: Instant messaging and the security pro, 2006
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9003796&pageNumber=1

[3] Juan Carlos López Calvet: Mobile Instant Messaging, 2003
http://www.eurescom.de/message/messageDec2003/Mobile_Instant_Messaging.asp

[4] Robyn Greenspan: Mobile IM Usage Nearly Doubles, 2004
http://www.clickz.com/showPage.html?page=3400661

[5] A PRIME EU projekt weboldala: http://www.prime-project.eu

[6] Michael Stephens, Aaron Schmidt: Fast, Cheap and Easy: Instant Messaging in Libraries, 2004
http://www.tametheweb.com/presentations/IM_IL04_SchmidtStephens.ppt

[7] Az Eletronic Privacy Information Center több kategóriában ajánl programokat. Azonnali üzenetküldő szolgáltatások: http://www.epic.org/privacy/tools.html#chat

[8] Tor anonimizáló hálózat honlapja: http://tor.eff.org/

[9] Mayank Sharma: How to keep instant messaging off the record, 2005
http://internet.newsforge.com/article.pl?sid=05/10/07/1521221

[10] Cara Garretson: Phishing leverages VoIP in new scam model, 2006
http://www.networkworld.com/news/2006/042606-phishing-voip.html

[11] Joris Evers: Worms biting into IM, P2P, 2005
http://news.zdnet.com/2100-1009_22-5888062.html

[12] Gulyás Gábor György: Anonim-e az anonim böngésző? Technológiák és szolgáltatások elemzése. In: Alma Mater sorozat az információ- és tudásfolyamatokról 10. BME GTK ITM, Budapest, 2006. március

[13] A SILC protokoll leírása: http://en.wikipedia.org/wiki/SILC_%28protocol%29