BUDAPESTI MŰSZAKI EGYETEM
INFORMÁCIÓ- ÉS TUDÁSMENEDZSMENT TANSZÉK

GULYÁS GÁBOR – PÓKA BALÁZS – SZILI DÁVID

EGY IDEÁLIS ANONIM CSEVEGŐ SZOLGÁLTATÁS KONSTRUKCIÓJA

TDK DOLGOZAT

KONZULENS: DR. SZÉKELY IVÁN

BME GTK
2006

TARTALOMJEGYZÉK

MELLÉKLETEK

ÁBRAJEGYZÉK

TÁBLÁZATJEGYZÉK

ABSTRACT

Az anonimitás, a kommunikáció bizalmassága, az információs önrendelkezés érvényesíthetősége az internet-használat kulcskérdései közé tartoznak. Különösen fontos e kritériumok biztosítása valós időben zajló, illetve több partnert érintő kapcsolatok esetén. A dolgozat e kérdéseket a csevegő szolgáltatások körébe tartozó azonnali üzenetküldő, illetve chat szolgáltatások sajátos területén elemzi és bemutatja az elemzés eredményeképpen kidolgozott, az ideális rendszert közelítő új szolgáltatás konstrukcióját, illetve annak a gyakorlatban kifejlesztett elemeit.

A szerzők, több mint féléves közös kutatási előzményükre támaszkodva, osztályozási szempontrendszert állítottak fel a létező csevegő szolgáltatások anonimitási és további kritériumainak kritikai vizsgálatára, majd kidolgozták egy ideális szolgáltatás szempontrendszerét és számbavették elvi megvalósítási lehetőségeit. Ezt követően kidolgozták egy gyakorlatban megvalósítható, új típusú rendszer technológiai és szolgáltatási tervét, amely role-based privacy alapon nyújt lehetőséget párbeszédes és csoportos, partnerlistás és csevegőszobás, illetve konferencia-kapcsolatok igénybevételére, és emellett a kényelmi szolgáltatások széles skáláját nyújtja a felhasználók egyéni és kollaboratív választása alapján.

A dolgozat előadásakor a szerzők a rendszer egyik már megvalósított alapvető elemének, a protokoll üzenetek szállítását végző hálózati rétegnek a működését valós idejű kísérletben demonstrálják. Ennek során két kliens üzeneteket küld egymásnak egy szerveren keresztül, egy szimulált támadó jelenlétében, amely lehallgatással, illetve forgalomelemzéssel próbálkozik, a közönség pedig diagramokon és a folyamat vizuális megjelenítésén követheti a történéseket. A dolgozat írott változatát CD melléklet egészíti ki.

1. PRIVACY, INTERNET, SZOLGÁLTATÓK

1.1. A privacy kérdése a csevegő szolgáltatásokban

A csevegő szolgáltatások több mint tíz éves pályafutása alatt a felhasználók és szolgáltatások száma egyre csak növekedett. A kezdetleges rendszerekben a felhasználók szobák között barangolhattak, s egyszerű szöveges beszélgetéseket kezdeményezhettek, ezek chat jellegű szolgáltatások voltak[1]. A nagy szemléletváltás 1996-ban következett be, amikor megjelent az első ingyenes azonnali üzenetküldő szolgáltatás, az ICQ [ICQ] [WPIM].

A két szolgáltatástípus útja különvált, az azonnali üzenetküldő szolgáltatások terjedtek el, 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[2] [COS1], s ezek a hálózatok hatalmas, több milliárd üzenetből álló forgalmat bonyolítanak le naponta[3] [CPW1].

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 [MIM1] [MIM2] [MIM3]. 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 konzorciumi projekt a Prime[4] [PRIME].

Az üzenetküldő szolgáltatások már manapság sem csak a magánélet részesei, számos munkahelyen használják őket a kollégákkal kapcsolattartásra, de ügyfélszolgálat is működhet (részben) azonnali üzenetküldő szolgáltatásra alapozva[5] [HPIM] [BOOM]. Mivel a vállalati használatban értékes információk utazhatnak át a rendszeren, több szolgáltatás speciális lehetőségeket kínál vállalatok részére [EIM].

Más alkalmazások is lehetségesek: könyvtárakban is működtetnek olyan ügyfélszolgálatokat, amelyek azonnali üzenetküldő szolgáltatásokon érhetőek el [LIB1] [LIB2], de a könyvtárakon és a munkahelyi alkalmazáson túl az azonnali üzenetküldő szolgáltatásoknak széles alkalmazási köre képzelhető el.

---

[1] A chat jellegű és azonnali üzenetküldő szolgáltatások típusdefiníciói megtalálhatóak a definíciós mellékletben [DEFS].

[2] 2006 februárjában Európában 82 millióan, Észak Amerikában 69 millióan használtak azonnali üzenetküldő szolgáltatásokat a ComScore áprilisi cikke szerint. [COS1]

[3] 2005-ben naponta átlagosan majdnem 14 milliárd üzenet volt az azonnali üzenetküldő hálózatok forgalma a ComputerWorld weboldal egy cikke szerint. [CPW1]

[4] A Prime projekt Role-Based Privacy alapötletéből és fogalomtárából merítettünk.

[5] [BOOM] szerint 2004-ben többféle célra használták a munkahelyeken is az IM-eket: 70% kollégákkal beszélgetett, 34% ügyfelekkel foglalkozott. 11%-uk használja a körülményes munkahelyi beszélgetések elkerülésére, 62%-uk időnként ily módon érintkezik a családdal.

Az elterjedtségnek köszönhetően mások is felfigyeltek a szolgáltatásokban rejlő lehetőségekre: egyre több vírus és féreg kering az azonnali üzenetküldő szolgáltatások hálózataiban, főleg a közkedveltebbekben [IMW1]. Bár a legtöbb szolgáltatásban már bevezettek védelmi megoldásokat, de a szűrési, védelmi kérdésekre nem létezik egyelőre átfogó, egyértelmű válasz.

1.2. Hol az anonimitás és a közösség?

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[6].

Mindemellett a jelenlétjelzés technológiának köszönhetően a partnereknek sűrűbben nyílik lehetősége arra, hogy felkeressék egymást, hiszen spontán lehetőségük nyílik beszélgetéskezdeményezésre, s lehetséges, hogy ennek egyetlen motivációja a partner jelenléte. Korábbi chat jellegű rendszerekben, mint például amilyen az IRC volt, a felhasználók úgy is használhatták a szolgáltatást, hogy egy új identitást választva léptek be. Egyes implementációk, mint például az UnrealIRCd [URID] a teljes identitásváltást is lehetővé tették, így a felhasználók anonim módon használhatták a rendszert[7]. A jelenlegi azonnali üzenetküldő rendszerekben nem lehetséges az anonimitás, ugyanis a felhasználókat egyértelműen azonosítja a partnerlistán a pszeudonim azonosítójuk[8]. A jelenlét és a látható állapot kezelése tipikusan a letiltás és rejtőzködés műveletekre korlátozódik.

A két szolgáltatástípus között teljes a szeparáció – a felhasználó választhat az anonim identitás lehetősége (chat jellegű rendszerek) és a pszeudonim megjelenés (azonnali üzenetküldő szolgáltatások) között. A két rendszertípusra további különbségek is jellemzőek. A chat jellegű szolgáltatásokban a rendszerben szobák találhatóak, amelyek – tipikusan – valamilyen érdeklődés alapján egységbe tömörült felhasználók csoportját jelöli, s a szobák között a felhasználók tetszésük szerint barangolhatnak, az ott fellelhető emberekkel ismerkedhetnek.

Azonnali üzenetküldő rendszerekben az ismerkedés, a közösség másképp, és kevésbé erőteljesen jelenik meg. Új felhasználókat keresni lehet például érdeklődési kör, különböző tulajdonság alapján, bizonyos rendszerekben lehet például kifejezetten csevegő kedvű felhasználókat, ilyen például a [BITW]. Szobákat létrehozni, közösséget összetartani nehezebb, ugyanis szobák helyett inkább konferenciákat lehet összehozni. Hátrányuk, hogy meghívásukkor jönnek létre, kevésbé statikus jellegűek, mint a szobák.

---

[6] Véleményünk szerint ez a helyzet a közeljövőben tovább fog súlyosbodni a modern mobil eszközök és a mobil azonnali üzenetküldők miatt.

[7] Az anonimitás elérése nem volt triviális ebben a rendszerben, hiszen néhány jellemzőt, mint például az IP címet, vagy a lokális felhasználó nevet nem lehetett csak úgy megváltoztatni bármelyik kliensprogramból, az előbbit is csak dinamikus IP kiosztás esetén lehetett cserélni, s akkor sem tetszőleges mértékben.

[8] Angol szakirodalomban az ún. „screen name”.

Véleményünk szerint egy ideális rendszer rendelkezik közösségi funkciókkal is, támogatja a különböző rendszerelemek jobb felismerhetőségét, így az ideális szolgáltatás konstrukciójában egy hibrid szolgáltatást mutatunk be.

2. A LÉTEZŐ CSEVEGŐ SZOLGÁLTATÁSOK VIZSGÁLATA

Ez a fejezet egy korábbi, fél éves alapozó kutatásunkra épül, amely során számos rendszert vizsgáltunk meg egy általunk felépített kritériumrendszer alapján, amelyet később be is mutatunk osztályozási szempontrendszer néven. A vizsgálatok eredményét összehasonlítva kiértékeltük a szolgáltatásokat magánszféra védelmi és adatvédelmi szempontból.

A fejezet legvégén a konklúziót megelőzően kiemelünk két olyan gyengeséget, amelyet a szolgáltatások tesztelése során fedeztünk fel. Itt kifejezetten magánszférát érintő gyengeségekről lesz szó.

2.1. Vizsgálati módszerek

A vizsgálatok előtt egyszerű próba jelleggel a leggyakrabban használt és néhány biztonságosnak ítélt szolgáltatást kipróbáltunk (az utóbbi szolgáltatásokat az EPIC ajánlásából válogattuk [EPIC]). Az így elkészült listát a [LLIS] mellékletben közöljük. A szolgáltatás listáról kiválasztottuk azokat a szolgáltatásokat, amelyek a legérdekesebb attribútumokkal rendelkeztek, illetve igyekeztünk a legszélesebb spektrumot lefedni a szolgáltatások skáláján.

Az alapozó kutatás óta további érdekes szolgáltatások jelentek meg, amelyeket szintén a rövidített lista mellékletében említünk meg, ugyanis szeretnénk ezeket a szolgáltatásokat is a későbbiekben elemezni [SLIS].

A szűk lista szolgáltatásait további vizsgálatok alá vetettük, s ennek alapján felépítettük azt a szempontrendszert, amely szerint a szolgáltatásokat besoroltuk – a taxonómiát a következő fejezetben részletesen tárgyaljuk. Részletes vizsgálatainkban *empirikus módszereket* alkalmaztunk, vizsgálataink során a szolgáltatásokat az osztályozási szempontrendszer alapján tételesen ellenőriztük, s a szempontrendszeren kívüli lehetőségeket, funkciókat is feljegyeztük.

Az empirikus vizsgálatok lezárulása után a felfedezett adatok alapján *elméleti vizsgálatokat* folytattunk. Amelyek eredményei alapján a vizsgálati taxonómián túlmutató módon próbáltuk osztályozni a rendszereket. Az elméleti vizsgálatok eredményeivel részletesen később foglalkozunk.

Különösen kiemelten foglalkoztunk a rendszerekben az *anonimitás és a privacy* kérdéskörével, ezeknek a kezelésével és a felhasználónak nyújtott lehetőségekkel.

A vizsgálatok során felfedeztünk néhány *implementációs gyengeséget* (több rendszerben is), amelyek közül kettőt a dolgozatban is megemlítünk, és tárgyalunk, mivel ezek privacy szempontból kiemelten kritikusak.

2.2. Néhány érdekesebb szolgáltatás

A szűkített listának az elkészítéséhez szükséges volt a szolgáltatásoknak megnézni az elérhető leírásait a weblapjukon, lehetőség szerint kipróbálni őket, és megtekinteni a beállítási lehetőségeket.

Az MSN [MSN] és Yahoo Messenger [YAHM] és ICQ [ICQ] szolgáltatások kiválasztásukat elterjedtségüknek és felhasználóbarát alkatuknak köszönhetik – bőségesen nyújtanak olyan kiegészítéseket a kliensprogramjaik, amelyekkel mások nyugalmát könnyen meg lehet zavarni. Az ICQ esetében döntésünk segítette, hogy hálózata igen régi és régóta elterjedt – spam-bot-ok[9], hirdetők legelőször ezekben a rendszerekben kezdtek tevékenykedni, s teszik azt ma is, éppen ezért kíváncsiak vagyunk védelmi és szűrőrendszerére.

A Skype [SKYPE], 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 (de hirdetőkről nem is hallani).

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

Nagyon szerettük volna kipróbálni az Ultramagnetic [ULTM] azonnali üzenetküldőt is, mivel igazán érdeklődéskeltő információkat lehetett fellelni róla [UTL1] [ULT2], de sajnos sem a kutatás kezdetekor, sem pedig lezárásakor nem volt elérhető működő verziója. Nem hivatalos csomagokat találtunk [ULT3], további kutatás keretében érdemes lenne kipróbálni azokat, mivel az Ultramagnetic a [ULT1] szerint nem csak bizalmasan szállítja az információkat, hanem anonimitást is nyújt. Működő változat csak a kutatás lezárása után jelent csak meg, s kiderült, hogy a külső világ felé nyújt anonimitást Tor [TORN] hálózat segítségével, egyébként különböző kliensprogramokat képes helyettesíteni különféle szolgáltatásokhoz, azaz ún. aggregátor kliens[10].

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

A Softros Lan Messenger [SLAN] specialitása, hogy biztonságos kommunikációt ígér egyenrangú kliensekkel (peer-to-peer) helyi hálózatra, amely elgondolás egész filozófiájában eltér az eddig megismert azonnali üzenetküldőkkel szemben. A PSST

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

[10] Az aggregátor kliensek egyszerre több szolgáltatást kezelnek, így a felhasználónak elegendő egyetlen programot futtatnia a számítógépén.

[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 (Az eredeti szabvány RFC-je: [IRCR]). Sok IRC szerver és kliens implementáció létezik. Első sorban szerveroldali megoldást kívántunk tesztelni, mivel már a mIRC [MIRC] klienshez rengeteg (ténylegesen több száz, ezer) kiegészítés található, amelyek között akadnak a kutatáshoz illők is, de ezek kiszűrése és végigpróbálása felemésztené a kutatás erejét. A szimpla mIRC klienst választottuk a kutatáshoz. Szervernek az UnrealIRCd-t [URID] választottuk, mivel sok magánszféra óvó szolgáltatása van, ingyenes és támogatja az SSL-t (TLS) a kliens-szerver szakaszon.

A több szolgáltatást átfogó üzenetküldők közül az összes közismertet kiválasztottuk, hogy lehetőség szerint minél többet leteszteljünk közülük. Esetükben a tesztek célja a magánszféra védelmi megoldások vizsgálata volt. Sajnos időhiány miatt csak a Gaim [GAIM] + OTR [GOTR] (Off the record messaging) tesztelésére szántunk volna időt, de a telepítési nehézségek miatt a tesztelést nem tudtuk elvégezni.

2.3. Osztályozási szempontrendszer

A taxonómia felállítását tehát a szűk 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 kritériumokkal foglalkozunk, a teljes taxonómia a [TAXO] mellékletben található. A bevezetett szempontok mögött néhány helyen példaként referálunk olyan rendszerre, amelyre ezek jellemzőek.

2.3.1. Általános szolgáltatási attribútumok

2.3.1.1. Csevegő szolgáltatások típusai és hálózati modelljei

Többféle taxonómia létezik a csevegő szolgáltatások osztályozására, mi igyekeztünk a főbb általános jellemvonásokat kiragadni és a vizsgált modelleket azok szerint értelmezni. A csevegő szolgáltatások típusdefiníciói megtalálható az a [DEFS] mellékletben: *azonnali üzenetküldő*, *chat jellegű* és *peer-to-peer*. Megemlítjük a *hibrid szolgáltatás típus*t, azonban mivel ilyen rendszert nem találtunk, nem vettük bele a taxonómiába[12].

A hálózati modellek szorosan kapcsolatban állnak az előbbi fogalmakkal. Megkülönböztetünk *központi szerverre* [BITW], az *elosztott szerverhálózatra* épülő szolgáltatásokat [URID], illetve a *peer-to-peer* jellegűeket [SLAN].

[11] A szűkítés oka a kutatás terjedelmének racionális korlátozása volt.
[12] Az ICQ szolgáltatás hibrid is lehetne, de valójában nem az, ennek a magyarázatát az eredmények kiértékeléséről szóló fejezetben adjuk meg.

2.3.1.2. Fedőnév választása, beszélgetési lehetőségek

Vizsgáltuk, hogy a felhasználók milyen fedőnévvel jelenhetnek meg a csevegő szolgáltatásban. Itt is két fő kategória különböztethető meg: a felhasználók vagy *tetszőleges fedőnevet* választhatnak [URID], vagy *regisztrálniuk* [BITW] kell. Egyes speciális esetek előfordulnak, amikor a program például a számítógépre bejelentkezett felhasználónevét alkalmazza [SLAN] (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[13]. Ennek megfelelően megjelöljük, hogy egy adott rendszerben mely médiumok használhatóak a *szöveges*, *VoIP* és *webkamerás* ([SKYPE] rendszerben mindhárom)lehetőségek közül.

Érdekes kérdés a szolgáltatások esetében, hogy milyen elképzelés szerint lehetséges a kommunikáció a *párbeszéd*, vagy *konferencia* lehetőségekből [SKYPE]. Egyes rendszerekben a konferencia alternatívája a *szoba,* vagy más nevén a *csatorna* [URID]. Fontos megjelölni, hogy a szöveges beszéd mellett *VoIP beszélgetésre* is van-e lehetőség, vagy *webkamera* használatára a többszemélyes beszélgetésekben.

2.3.1.3. Felhasználók keresése, a hálózaton való jelenlét ellenőrzése

Jellegzetesen három módja van a címben említett funkcióknak. Rá lehet *keresni*[14] az attribútumok valamilyen minta szerinti megadásával a felhasználókra [SKYPE], vagy ellenőrizni lehet valahogy a névnek az érvényességét. Lehet, hogy a név a *partnerlistán* [SKYPE] rajta van, így automatikusan kiderül az állapota (jelenlétjelzés), de lehet, hogy *külön lehet csak ellenőrizni*[15] [URID]. Ezen szempontok közül az első kettő több esetben egyszerre teljesül.

2.3.1.4. Egyéb kritériumok

A lefedett platformoknál csak az eredeti kliensprogramokat vesszük figyelembe (IRC esetében ez nem értelmezhető, ezért vettük fel zárójelesen, hogy mindegyik platformra létezik IRC kliens). Külön kiemelt a webes kliensek fontossága, hiszen ezek bárhol és bármikor (jellemzően) probléma nélkül használhatóak, mert nem igényelnek telepítést és nem hagynak az adott számítógépen maguk után a felhasználó tevékenykedésére nyomot (naplózás, esetleg a bejelentkezés is kikapcsolható).

[13] Például a Skype szolgáltatása elsősorban a VoIP hívások kiszolgálására készült.
[14] Keresés, ellenőrzés az – angol nevén – „user directory”-ban.
[15] Ilyen például az IRC „ison” funkciója, amely megadja, hogy a kérdéses felhasználó megtalálható-e a hálózatban vagy a szerveren. Ide sorolhatjuk egyes chat szolgáltatások névlista funkcióját, ahol minden felhasználó megtalálható. Ez a megoldási mód tipikusan a chat típusú szolgáltatások sajátja.

Egy csevegő szolgáltatás filozófiáját gyakran fellelhetjük a kezelési módjában – a *paranccsal vezérelt* ([URID] és [MIRC]) programok általában bonyolultabb és színesebb funkció palettával bírnak, mint a *grafikus felületű* [BITW], de felhasználóbarát programok. Vannak határesetek is, de ez az állítás ilyenkor is megállja a helyét, mint a tesztekből kiderült.

2.3.2. A négy fő magánéletvédő, adatvédelmi és kiegészítő kritérium

A négy fő magánéletvédő, adatvédelmi kritérium definícióját és értelmezését csevegő szolgáltatásokra vonatkozóan a [DEFS] mellékletben adtuk meg. Ez a négy kritérium a következő:

1. *Anonimitás*
2. *Pszeudonimitás*
3. *Megfigyelhetetlenség*
4. *Összeköthetetlenség*

5. *Összekapcsolhatatlanság* (kiegészítő kritérium)

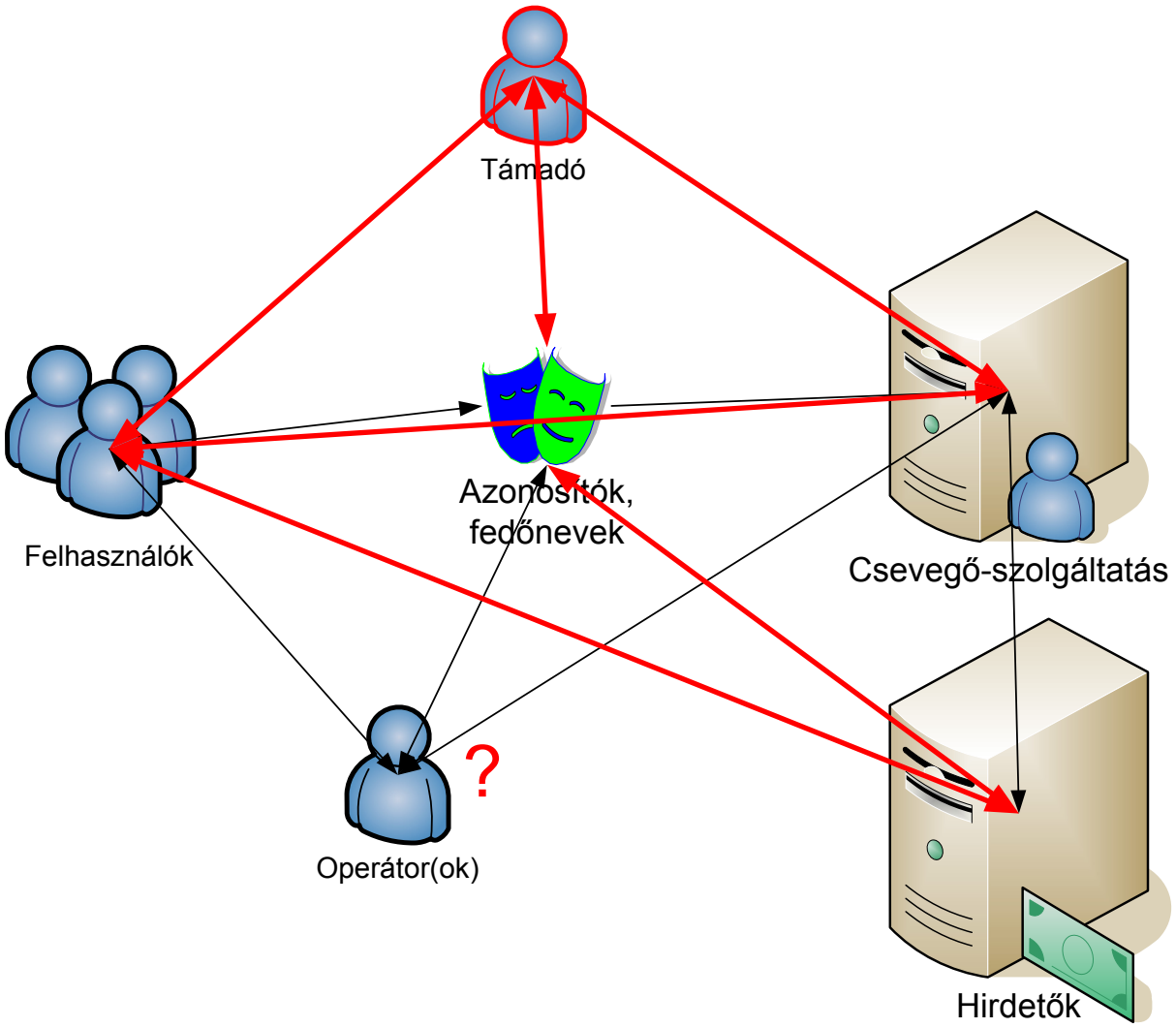
A rendszer következő szereplőit különböztetjük meg:

- 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.

2.3.2.1. A szereplők kapcsolatrendszere

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.



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 nem foglalkozunk, mert a technikai megvalósítás függvénye).

2.3.2.2. Anonimitás és pszeudonimitás

Megjegyezzük, hogy bár megfigyeljük az anonimitás lehetőségét a különféle rendszerekben, de a vizsgált rendszerek egyike sem tűzi ki célként az anonimitás lehetőségét (az, hogy az [URID] rendszerben megjelenik, de nehezen kihasználható az adott kontextuson belüli identitásváltás).

2.3.2.3. Anonimitás és pszeudonimitás a szereplők szemszögéből

- 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 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.

2.3.2.4. Megfigyelhetetlenség

A megfigyelhetetlenség tényének teljesülése fontos, mert ha nem teljesül, esetlegesen a tartalomból következtetni lehet a beszélgető felek kilétére. Még ennél is nagyobb problémát jelent, hogy a benne lévő információ lehallgatásával vissza lehet élni, marketing célokra fel lehet használni, vagy egyszerűen bizalmas, privát adatok, egyéb tartalom felfedéséről lehet szó.

A megfigyelhetetlenséget egy adott beszélgetési viszonyra értjük, amelyre teljesülnie kell, hogy a viszonyon kívüliek számára a tartalom fedve legyen. A megvalósításokban kétféle esettel találkozhatunk, az egyik a párbeszédek, a másik a csoportos beszélgetések. A megvalósíthatóság szempontjából ezek az esetek eltérnek.

2.3.2.5. Összeköthetetlenség

Az összeköthetetlenség alatt azt értjük, hogy a különböző tevékenységek – amelyek jelen értelmezésünk szerint nem csak egy személyre vonatkoznak –, mint az üzenetküldések, akciók, etc., ha megfigyelhetőek is, nem köthetőek össze egy (virtuális, vagy akár valós) személy, vagy csoport cselekvéssorozataivá.

Az összeköthetetlenségre már utáltunk az anonimitásnál is explicit formában – ha például a felhasznált fedőnevek (és a hozzájuk kapcsolódó tevékenységek) összeköthetőek, akkor az anonimitás csorbul. Az összeköthetetlenséget is értelmezzük csoportokra is, azaz vizsgálandó, hogy a különböző konferenciák, szobai beszélgetések összeköthetőek-e, így a csoportos beszélgetési viszonyok összefűzéséből kivehető-e annak az életfolyamata.

2.3.2.6. Összekapcsolhatatlanság (kiegészítő kritérium)

Ez a kritérium a felhasználók összekapcsolhatóságával foglalkozik, azaz hogy eldönthető-e egy rendszerben, hogy mely felhasználók beszélgetnek egymással. 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.

2.3.3. 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.

2.3.3.1. Megjelenési módok és rejtőzködési lehetőségek

Sokat számít, hogy a felhasználó eldöntheti-e, milyen néven akar megjelenni a rendszerben. Így igény lehet a az *anonim* megjelenés, és például az [URID] rendszerben ez lehetséges. Más rendszerekben a *regisztrációs azonosító* köti a felhasználókat, de speciális esetben ez csak a belépéshez kell, s tud egy független azonosítót választani.

A rejtőzködési általában lehetőségek 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 van rajta a partnerlistáján*. Így a felhasználó kizárhatja és felfedezheti 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*[16] műveletről beszélünk.

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

2.3.3.2. 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 a profilról*. 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.

2.3.3.3. Tevékenységek automatikus felfedése

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

2.3.3.4. Audiovizuális magánszféra védelme

Az audiovizuális magánszféra védelmére leginkább azoknak a rendszereknek kell felkészülni, amelyek sok erre tekintve sértő szolgáltatást nyújtanak. Idetartoznak a beszélgetésben szereplő különféle animációk, rajzok, képek, hangok, hangfelvételek,

[16] Angolul „ignore”.

stb. Idesoroltuk a kellemetlen kifejezések szűrését is. Hangok esetében különösen zavaró lehet az automatikus lejátszás.

2.3.3.5. Spam (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.

2.3.3.6. 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.

2.3.4. 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 (ilyen például a Gadu Gadu [GADU]). 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 [VS1] [VS2]. Innen már csak egy lépés eljutni a webkamerás beszélgetésekhez, amelyek valószínűleg ehhez hasonlóan egyre inkább elterjednek majd.

Egy korszerű kliensprogramtól elvárható, hogy *figyelmezteti 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.

2.4. Elméleti vizsgálatok eredményei

2.4.1. Rendszertípusok

Különféle rendszertípusokat már meghatároztunk az osztályozási szempontrendszer első fejezetében is. Az alábbiakban ezen kategorizáláson túlmenő következtetéseket fogunk levonni és ezekből származtatható osztályozásokat határozunk meg.

2.4.1.1. A rendszer típusa, és ami ebből jól láthatóan „következik”

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:

1. táblázat: a két fő rendszertípus összehasonlítása.

Chat jellegű szolgáltatás	Azonnali üzenetküldő szolgáltatás
Szabadon választható fedőnév	Kötött azonosító (a regisztrálthoz)
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, identitás váltás[17]	Tiltás, rejtett állapot
Központi szerver, elosztott szerverhálózat	Központi szerver, szerverfarm

A peer-to-peer rendszerekre tipikusan szabadon választható fedőnév, esetleg névlista használata [SLAN] jellemző. A felhasználók felderítése elosztott módon, automatikusan történik, vagy egy másik médiumon keresztül (például egymás IP címének cseréje [PSST]).

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 ide sorolhatnánk. 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 beszélgetéshez. 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.

2.4.1.2. A rendszerek filozófiája

A rendszer elgondolása, *tervezési filozófiája* alapján két részre osztjuk a szolgáltatásokat. Az egyik csoportba azok a rendszerek tartoznak, amelyek kevésbé, vagy egyáltalán nem tartalmaznak biztonsági megfontolásokat a kezdetektől fogva, és a szolgáltatás inkább a felhasználói élmény és a multimédiás elemek köré épül.

[17] Bizonyos esetekben egyszerű, de legtöbbször nem triviális feladat a felhasználó számára.

Ezen szolgáltatásoknál, ha találkozunk is biztonsági megoldásokkal, valószínűleg időközben építették bele őket a programba. Ezek a szolgáltatások a hálózati forgalmat egyáltalán nem védik, különféle veszélyes tartalmak ellen is csak részlegesen nyújtanak védelmet. Például [YAHM], [MSN][18], [ICQ].

A másik csoportba sorolt rendszerek tervezésekor figyeltek a megfelelő védelemre, óvják a hálózati forgalmat, a hangsúly nem a multimédiás elemeken van – a kevesebb audiovizuális magánszférát zavaró jelenség mellett erre védelmet se kell kiépíteni. Például [SKYPE], [BITW].

A chat jellegű szolgáltatásokat egy külön kategóriába sorolhatnánk, ugyanis a csevegő szolgáltatások legöregebb formáit jelentik, és sok változáson mentek keresztül az idők folyamán. Így bővült ki a szerveroldali alkalmazás az idők során SSL lehetőséggel a szerver-szerver, majd a kliens-szerver összeköttetésekhez, kerültek bele a különböző szolgáltatások (névszolgáltató szerver), spam és egyéb szűrők stb. Például az [URID] tehát a kor igényeinek megfelelően dinamikusan változó és a felhasználók kívánalmainak megfelelő, naprakész kiegészítésekkel rendelkező szolgáltatás, ezért egyik fenti kategóriába se sorolható.

2.4.2. Tipikus megoldások az adatok és 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 permanens listák, egyedül a [YAHM] szolgáltatás esetében találkoztunk ideiglenes listákkal – ilyenkor a felhasználó csak az adott 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] esetében (kikapcsolható a webes státusz megjelenés). Ez a két szolgáltatás és a [BITW] esetén a profil webes felületen nem jelenik meg, nincs ilyen kiszolgáló. A profilokat minden felhasználó megtekintheti, szabályozásuk egyszerű – a kitöltött mezők jelennek csupán meg, kitöltésük nem kötelező (például nem regisztrációhoz kötött). [MSN] és [YAHOO] 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, [YAHM], [ICQ] és [BITW] kliensek alatt a jelszót elfelejti a program, ha bejelentkezéskor nem kérjük a megjegyzését (direkt törlés nincs), a [SKYPE] felajánlja az automatikus indítást.

[18] MSN Messenger-nél a gyanús fájlok letiltásának védelme, a különféle kifejezések szűrése. Utóbbinál az ad-hoc jelleget precízen mutatja, hogy a Microsoft Ügyfélszolgálat nem tudott nekünk segíteni megkeresésükkor a szűrés leírásának kérdéseit tekintve.

Egyedül az [MSN] 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 felfedésére, sokszor állítható a várt eltelt idő, a kiírandó üzenettel együtt (és általában két fokozat jelenik meg). Néha további automatikus esemény-felfedés is értelmezett, mint például teljes képernyős programok futtatása, filmnézés, zenehallgatás, webkamera képe.

Az audiovizuális magánszféra védelem programonként viszont igen eltérő képet mutat. Ez nagyban változik aszerint, hogy a különböző programok milyen ide kapcsolódó elemeket nyújtanak. A későbbiekben tervezzük ennek kibővített vizsgálatát konkrét tesztelési tapasztalatokat bevonásával.

A spam védelem is sokféleképp jelenik meg a különböző programokban. Általában nincs konkrét védelemről szó, ilyen szűréssel egyedül az [ICQ] szolgáltatásban találkozhatunk. Az [MSN] szolgáltatásában ad-hoc módon fejlesztett, nem dokumentált szűrés van beépítve, a [YAHM] esetében pedig szavak szűrésére specializálódott védelem található. Ezek egyike se mondható túl hatékonynak, noha mivel a partnerkeresés nehézkes, ezért talán ezekben a hálózatokban nehezebben boldogulnak a hirdető robotok. Egy bizonyos, fenyegetettségük az [ICQ] hálózatában majdnem a legmagasabb, mindemellett érdekes kérdés, hogy a legfenyegetettebb rendszerben, az [MSN]-ben, miért nincs beépített védelem. [IMTH]

Ami külön pozitívumként jelenik meg a teszteltek esetében, hogy külső program használatát nem kényszerítik rá a felhasználóra.

2.4.3. Anonimitás és további kritériumok teljesülése

2.4.3.1. Anonimitás, pszeudonimitás

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 roppant 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 (tiltással). A [SKYPE] programja kiírja a főablakba, hogy hányan használják hozzávetőlegesen a szolgáltatását – ilyen többmilliós felhasználótábor esetén ilyen kiemelt felhasználókról nincs is értelme beszélni, inkább rendszeradminisztrátorokról. A

rendszeradminisztrátorok ebből a szempontból inkább egyenlővé tehetőek a szolgáltatással.

Hirdetőket jelen esetben csak azonnali üzenetküldő szolgáltatásban tudunk értelmezni, mivel a vizsgált [URID] és [MIRC] szerver-kliens párosban nincsenek hirdetésre alkalmas felületek, és ezek ingyenes programok.

Így egy felhasználó csak egy chat jellegű szolgáltatásban lehet anonim. IRC (a mérési összeállításban: [URID] és [MIRC] programokkal) esetén például akkor, ha az ident azonosító (ez [MIRC] esetében a lokális felhasználónév szokott lenni), teljes név adatok változtathatóak, és a host rejtett, akkor a felhasználó lehet anonim a többi felhasználó felé. A host rejtés opcionális, ha a szerver nem oszt ilyet, a felhasználónak még a láthatatlan fellépést követően fel kell vennie ezt a módot.

Az IRC szerveren (pontosabban a szerver láncon) lévő IRCop elnevezésű operátorok számára a felhasználó nem anonim. Ennek oka, hogy ők akkor is láthatják az igazi host-ját a felhasználónak, ha az titkosított módban van, és az IP címét is bármikor lekérdezhetik (egyébként az IP cím valamelyik értéke titkosított).

2.4.3.2. 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.

Eddig nem foglalkoztunk vele, és kimaradt az Osztályozási szempontrendszerből is, de fontos, hogy a kliens-kliens kapcsolatok is titkosak legyenek. Hiszen ha például két [URID] szerverből és kliensekből épül fel a hálózat, ahol minden egység SSL kapcsolatot használ, de a kliensek között a DCC[19] szöveges kapcsolatok nem rejtettek, akkor ez a hiba az anonimitáshoz, és a pszeudonimitáshoz szükséges kritériumokat meghiúsíthatja.

2.4.3.3. Összeköthetetlenség

Az összeköthetetlenség sok mindentől függ. 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 (pl. [TORN]), állandó szinten lévő forgalommal erősíthetjük.

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

[19] Angol szakirodalomban „Direct Client Connect”.

rendszerben akkor teljesülhet, ha a felhasználó képes minden adatának a megváltoztatására.

2.4.3.4. 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. IRC esetén például a szobák látogatóinak a nevét le lehet 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 kísérleti tapasztalatok szerint az azonnali üzenetküldő szolgáltatások szereplői nem tudják megmondani, hogy mely felek vannak konferencia módban. Ez valószínűleg a legtöbb esetben kompromittálható lehallgatással, így ez is indokolja a megfigyelhetetlenség kritérium fontosságát.

2.5. Privacyvel kapcsolatos gyengeségek

2.5.1. MSN Messenger 7.5

Az MSN Messenger ezen változatában felfedezett hiba segítségével a felhasználó állapota 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 (ez a 8.0-ás verziójú változat új neve), de megfelelő módon kísérletileg ezt még nem ellenőriztük.

2.5.2. 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 esetben 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 az ő egyéni dolga, és ha ezt közölni szeretné a letiltott partnerével, arról először nyilatkoznia kellene.

2.6. A létező szolgáltatások kritikája

A vizsgálatainkból kiderül, hogy a rendszerek között alapvetően két típus létezik – azaz a rendszerek vagy a kezdetektől fogva törekedni egy bizonyos biztonsági szint megvalósítására, vagy csak az idők során fellépő nyomásoknak engedve foltokkal próbálják az efféle hiányosságokat elfedni. Az előbbi kategóriába tartozás általában jelenthet már valamiféle garanciát, de ezek a szolgáltatások 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 kitűnően jó minőségű mérnöki munkára utal, de a belső modell hiányos – ahogy korábban leírtuk felfedezésünk, hiába lenne 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 anonimitás lehetősége nem cél. A kutatás lezárása után megismertünk olyan rendszereket [SCCH], amelyeknél az anonimitás megjelenik, de ezek a rendszerek is csak alacsony szintű, külső megfigyelők ellen nyújtanak anonimitást, de ez sem elegendő.

3. ELVI KRITÉRIUMOK EGY IDEÁLIS RENDSZERREL SZEMBEN

Mivel a kezdetektől fogva hibrid szolgáltatást terveztünk, így az ideális rendszerrel szemben támasztott követelményeknél járulékos szempontokat kell figyelembe vennünk. Fontos továbbá megjegyezni, hogy jelen dolgozat keretein belül egy szöveges szolgáltatás terveit mutatjuk be, így a rendszerrel szemben támasztott kritériumok tekintetében is erre a médiumra koncentrálunk.

A szolgáltatás készítésének alapelve, hogy kielégítse a négy anonimitási és néhány kiegészítő kritériumot (melyek kifejezetten anonim csevegő-szolgáltatásokhoz kapcsolódnak). Ezek az alábbiak:

- **Pszeudonimitás és Anonimitás**: Egyrészt elvárjuk e két kritérium teljesülését a hálózati forgalom szintjén, külső megfigyelőkkel szemben. Másrészt elvárjuk a rendszer résztvevőivel szemben is. Utóbbi eset alatt a következő lehetőségeket értjük:

  - *A többi felhasználóval szembeni anonimitás*, azaz, hogy egy adott pillanatban a rendszerben fellelhető információk alapján ne legyen lehetséges egy résztvevő kilétének hozzárendelése egy valós személyhez.

  - *A rendszert felügyelő személyekkel és a szolgáltatóval szembeni anonimitás*. A szolgáltató ismerheti, hogy a felhasználói honnan kapcsolódnak, milyen azonosítókat használnak. Ezek monitorozása, naplózása függvényében beszélhetünk anonimitásról. Ha a felhasználó tevékenységek, különböző használt azonosítói, nevei nem hozhatók összefüggésbe valós személlyel, akkor anonimnek tekinthetjük.

- **Megfigyelhetetlenség:** A megfigyelhetetlenséget anonim üzenetküldő szolgáltatás esetében egy adott beszélgetési viszonyra értjük, amelyre teljesülnie kell, hogy *a viszonyon kívüliek számára a tartalom fedve legyen* (pontos definíciót ld. a mellékletben). A rendszer részvevői esetében további két esettet kell figyelembe venni: az egyik a párbeszédek, a másik a csoportos beszélgetések. A megvalósíthatóság szempontjából ezek az esetek ugyanis eltérnek.

- **Összeköthetetlenség:** A mellékletben foglaltak alapján az összeköthetetlenséget megköveteljük mind *a párbeszédek, mind a csoportos beszélgetések esetében, belső és külső megfigyelőkkel szemben* egyaránt.

Alapvető fontosságú megfelelő biztonsági protokollok alkalmazása a teljes kapcsolat biztonsága és sérthetetlensége érdekében. Hasonlóan fontos, hogy a hálózati forgalmat analizáló külső megfigyelő ne legyen képes a fenti anonimitási kritériumok megkerülésére.

A rendszer egyik sarokkövét az úgynevezett *Role-Based Privacy* (RBP) – vagyis szerep-alapú privacy megoldás – jelenti[20], amely szerint a felhasználók a különböző felhasználói csoportok (listán szereplés alapján, például tiltólistások, mellőzöttek, stb.) szerint megadhatnák saját virtuális vizualizációjukat, azaz identitásukat, amely tartalmazná a nevük, állapotuk és az egyéb információk láthatóságát (azaz egy komplett profilt). Hibrid szolgáltatás esetén mindezt a szobákra is alkalmazhatjuk, de bizonyos megszorításokkal, hogy ne okozzon nehézségeket, és ne (ne lehessen minden szobára más profilt építeni, hanem például egyetlen profilt minden szobához).

A szolgáltatások terjedésével egyre jobban szaporodnak az olyan hirdető botok [IMW1], [PHIM1], [PHIM2], amelyek felhasználókat keresnek fel véletlenszerűen, és hirdetéseket üzennek nekik, ezzel próbálva rávenni őket, hogy káros tartalmat töltsenek le magukhoz. A reklámüzenetek és hívatlan vendégek elleni védelmet teljes körűen *spim védelem* címszó alatt vizsgáljuk, meglétét szintén megköveteljük egy ideális rendszerben.

Egy korszerű kliensprogramtól elvárjuk, hogy *figyelmeztesse a felhasználót,* ha gyanús esemény következik be, például adathalászat (phising), [PHWP] gyanús URL, vagy ha valaki vírusgyanús fájlt szeretne neki küldeni.

Továbbá egy kliensprogramtól elvárható, hogy ha a felhasználóinak lehetőséget nyújt az üzenetekbe különféle színes, hangos, mozgó elemek elhelyezésére, akkor szükséges, hogy ennek megfelelően az *audiovizuális magánszférát sértő tartalmat szűrni lehessen*.

Mindenképpen szükséges a szolgáltatáson belül egy áttekintő rész, ahol a felhasználó minden fontos tudnivalót egyszerre meg tud nézni, és ennek alapján dönthet a beállítások kapcsán. Ide sorolhatóak lehetnek a különböző felhasználói listák, a különböző sémák állapotai, a felhasználó profiljai, és számos egyéb opció. A spim védelem és a figyelmeztetések használatánál előnyös lehet, ha a felhasználó a saját tapasztalatának megfelelően *beállíthatja a programban szkeptikusságának szintjét*, és hasonló módon menedzselheti a biztonsági beállításokat is.

[20] A szolgáltatást igénybe vevő felhasználó különböző szerepeket vehet fel, és a szerepek kezelésével meghatározhatja, hogy a többi felhasználó milyen képpel rendelkezzen róla, és így teljes önállósággal szabályozhatja a magánszféráját

4. ANONIM: EGY IDEÁLIS SZOLGÁLTATÁS KONSTRUKCIÓJA

Az AnonIM név rekurzív módon definiálható, *AnonIM: Anonim Instant Messenger*, azaz anonim azonnali üzenetküldő szolgáltatás. A rövidítést használják az angol szakirodalomban a leggyakrabban utalva a szolgáltatás típusára.

4.1. Az ideális rendszer főbb részei

Az ideális rendszer első változatát egy szerveres architektúrára kívánjuk építeni, ennek megfelelő szállító protokollal. Megvizsgáljuk azonban a többi hálózati architektúra lehetőségét is, azok előnyeit és hátrányait. Négy különböző *anonimizáló protokollt* veszünk sorra, összehasonlítva őket egy anonim azonnali üzenetküldő szolgáltatásban való alkalmazhatóságuk alapján, melyben szempontjaink többek között a rendszerek hatékonysága, biztonsága és megvalósíthatósága. Részletesen foglakozunk azzal a kérdéssel, hogy milyen *hálózati architektúrát* megvalósító rendszert érdemes használni egy ilyen nagy forgalmú és erősen valós idejű alkalmazásnál. A fentiek elemzése a következő fejezetben található.

A rendszer tervezésekor alkalmazzuk a *külső-belső világ paradigma*[21] elveit. Elemezzük modell használhatóságát, megjelenését más szolgáltatásokban. Ezt követően alkalmazzuk a modellt az ideális anonim üzenetküldő szolgáltatás esetében.

A külső világtól való szeparáció kivitelezéséért a *szállító protokoll* lesz felelős. Részletesen bemutatjuk ennek célját, a vele szemben támasztott elvárásokat, és ezek gyakorlati megvalósulását. Láthatjuk majd, hogyan működik együtt a többi réteggel, és hogyan biztosít védelmet a hálózati forgalom analízisével szemben.

A belső világ modelljében sorra vesszük a rendszerünk egyes egységeit (felhasználók, partnerlista, párbeszéden, konferenciák és szobák), és ezek különféle tulajdonságait.

Mindezek után a *Role-Based Acess Controll (RBAC)* alapú hozzáférés vezérlés részleteiről adunk ismertetést. Bemutatjuk annak feladatát, szabályrendszerének szerkezetét, és működését a gyakorlatban.

A belső világ által támasztott feltételek megvalósulásáért a *Role-Based Privacy* felelős. Ennek működéséről, használatának nehézségeiről, és a kutatásunk során felmerült kérdésekről és ellentmondásokról a későbbiekben adunk áttekintést, és külön kitérünk a profilozási rendszerre.

[21] A paradigma szerint létezik a belső világ, amely a szolgáltatásban résztvevőket foglalja magába, és a külső világ a rendszeren kívüli szereplőket foglalja magába. Részletesen ld. a „Külső-belső világ paradigma” c. fejezetben

Egy jelenlegi kliensprogramnak megfelelően, a rendszerünk szerves részét képezi a *spim védelem és a kifejezéscsere*. Gondot fordítottunk az üzenetek tartalmi szűrésének kérdésére is.

A fejezet zárásaként elemezzük a rendszerrel szemben támasztott követelmények megvalósulását a *privacy és a négy magánéletvédő kritérium* tekintetében.

4.2. Hálózati architektúra lehetőségek

4.2.1. Szempontrendszer

Az alábbiakban megvizsgáljuk egy anonim azonnali üzenetküldő szolgáltatásban való felhasználás céljából a jelenleg ismert anonimizáló protokollokat.

Ezen feltétel tette indokolttá, hogy a jelenlegi vizsgálatunkban nem térünk ki azokra protokollokra, melyek csak egy adott szolgáltatással működnek (mint pl. a Crowds [CROW], mely kizárólag HTTP protokoll felett működik). Helyettük kifejezetten olyan rendszerekre koncentráltunk, melyek felépítésükből következően megkönnyítik a későbbiekben implementált anonim üzenetküldő szolgáltatásba integrálásukat.

Az anonimizáló protokollok jobbjainak van néhány minőségbeli ismérve. Egyrészt nem igényelnek nagy mennyiségű erőforrást a kommunikáló felektől az anonimitás szintjének növekedésével. Másodszor, az anonimitás erősségének emelkedésével a támadó által az anonimitás megtöréséhez szükséges erőfeszítés is növekedjen. Végül, harmadik felek ne tudják felvenni a kommunikáció kezdeményezőinek szerepét.

A fentiek alapján a vizsgálatban szempontként szerepeltek az alábbiak:

- Valós idejű szolgáltatással történő alkalmazás
- Skálázhatóság
- Bizalmasság biztosítása
- Anonimitás biztosítása
- Összeköthetetlenség biztosítása

A vizsgálat az alábbi protokollokra terjedt ki:

- MIX-Net alapú
  - Onion Routing (Tor)
  - Hordes
- DC-Net alapú
  - Herbivore
- Broadcast[22] alapú
  - P^5

4.2.2. A rendszer által biztosított anonimitás

A rendszer *anonimitást biztosít a fogadónak*, akkor és csakis akkor, ha nem lehetséges megállapítani, hogy egy üzenet fogadója kicsoda.

[22] A hálózat minden tagjának küldött csoportos üzenet. Másképpen: üzenetszórás.

A rendszer *anonimitást biztosít a küldőnek*, akkor és csakis akkor, ha a fogadó (vagy egy külső megfigyelő) nem képes megállapítani, hogy az általa fogadott üzenet küldője kicsoda.

A rendszer *összeköthetetlenséget biztosít*, akkor és csakis akkor, ha külső megfigyelő nem képes megállapítani, hogy a rendszeren belüli eseményekért ugyanazon felhasználó felelős-e, vagy sem.

Az anonimitás szintjének megállapításához *a Levine-Shields féle* [HORD] *taxonómiát* használjuk. Ebben az anonimitás egy 0 és 1 közé eső érték, ahol a nulla az anonimitás teljes hiányát, az 1-es érték pedig a teljes anonimitást jelenti. Legyen $Pr_e(x)$ annak a valószínűsége, hogy x a kezdeményezője egy kommunikációnak az *e* megfigyelő szerint. Egy anonim csoport számára $\sum_{x \in S} \Pr_e(x) = 1$. Az *x* résztvevő számára biztosított anonimitás az *e* megfigyelővel szemben legyen $d_{x,e}(A)$, ahol A legyen a használt anonimizáló protokoll. Ekkor $d_{x,s}(A) = \sum_{y \in S \neq x} \Pr_e(x) = 1$ különböző értékeire:

- *Abszolút anonimitás* – Egy támadó nem képes megkülönböztetni a kommunikációkat: $d_{x,e}(A) = 1$.
- *Gyanú felett* – A kommunikáció néhány tényezője ismert a támadó számára, de a kommunikáció kezdeményezője nem megkülönböztethető a többi résztvevőtől: $d_{x,e}(A) \geq (1 - 1/|s|)$ és $d_{y,e}(A) \leq d_{x,e}(A)$, minden $y \neq x \in S$ -re.
- *Lehetséges ártatlanság* – annak a valószínűséggel, hogy egy x entitás kezdeményezője egy kommunikációnak nem nagyobb, mint annak a valószínűsége, hogy nem kezdeményezője, de a többi entitásnál nagyobb valószínűségű a támadó szemében: $1/2 \leq d_{x,e}(A) \leq d_{y,e}(A)$ minden $y \neq x \in S$ -re.
- *Leleplezve* – Fennáll még a valószínűsége annak, hogy a támadó nem tudja azonosítani a kezdeményezőt, bár ez meglehetősen kicsi. $0 \leq d_{x,e}(A) \leq ½$.
- *Bizonyítottan leleplezve* – A támadó képes bizonyítani a kezdeményező kilétét: $d_{x,e}(A) = 0$.

Az anonimizáló rendszerek végső célja a *Lehetséges ártatlanság,* vagy annál magasabb szint elérése. Az abszolút anonimitás nem megvalósítató, mert az Internet megosztott médium, így elképzelhető egy olyan megfigyelő, aki kellő erőforrással rendelkezik ahhoz, hogy közel minden hálózati forgalmat monitorozzon.

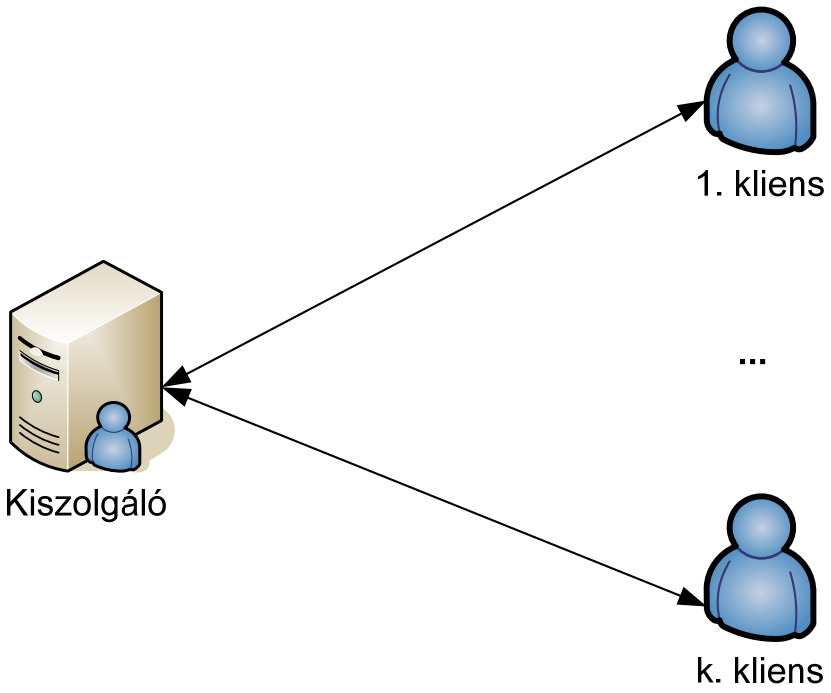
4.2.3. A lehetséges hálózati architektúrák

Az alábbiakban azt vesszük sorra, hogy milyen hálózati architektúrák jöhetnek szóba az anonimizáló hálózatok felhasználásával.

1.2.3.1. Egy szerver, anonimizáló hálózat nélkül

A legegyszerűbb hálózati architektúra, hátránya, hogy *nehezen skálázható.* Ugyan külön anonimizáló rendszerrel nem rendelkezik, de mivel az összes felhasználó rákapcsolódik a központi szerverre, és ha kizárólag azon keresztül kommunikálnak, a

felhasználók közötti kapcsolatok külső szemlélő számára *könnyen elrejthetőek* a kapcsolatok egyszerű TLS csatornába bújtatásával.

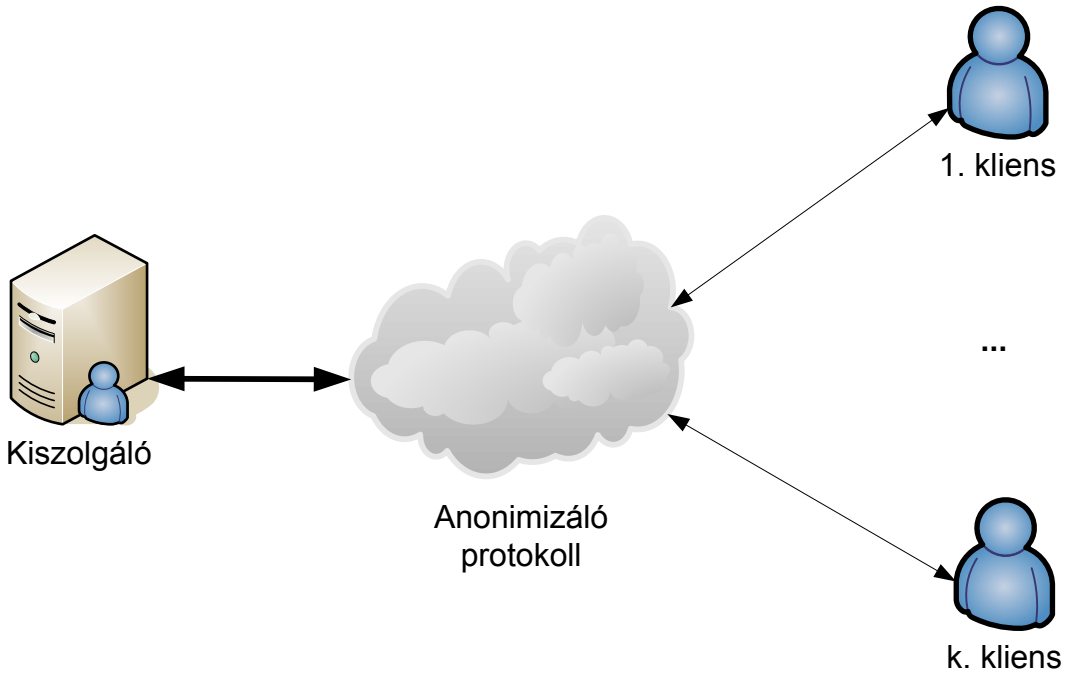


2. ábra: egy szerver, anonimizáló hálózat nélkül

1.2.3.2. Egy szerver, anonimizáló rendszerrel

Az előbbihez hasonló, szintén *nehezen skálázható* struktúra. Előnye lehet, hogy ha az anonimizáló hálózaton belül megoldható a név feloldás (a címzett pszeudonim, vagy anonim azonosítóval történik, közvetlen címzés egyik rendszerben sem értelmezhető), akkor a peer-to-peer kapcsolatok is lehetségessé válnak a kliens-anonimizáló rendszer-kliens útvonalon. A kliensek számára lehetséges a anonimizáló hálózaton keresztül a közvetlen címzés speciális esetekben, például fájlküldés esetén, ha mindkét fél beleegyezett a saját címének felfedésébe.

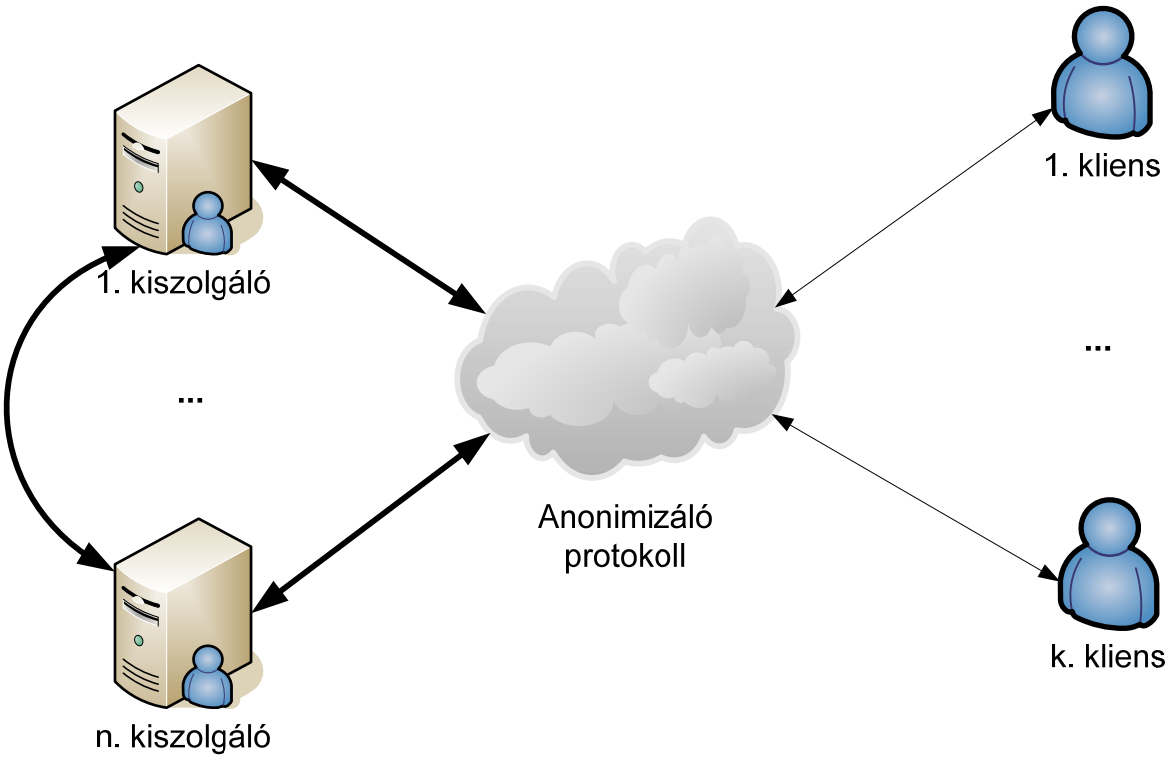
Az alábbi ábrán a hálózati architektúra elrendezését láthatjuk. A anonimizáló állomások lehetnek a kliens számítógépek is, de ezzel csak a következő fejezetben foglalkozunk.



3. ábra: egy szerver, anonimizáló hálózattal

1.2.3.3. Több szerver, anonimizáló rendszerrel

A többszerveres architektúra *rendelkezik az előző két rendszer előnyével*, viszont további előnyként megjelenik a *könnyű skálázhatóság*. Hátránya, hogy a belső világ modell (ld. a következő fejezetekben) elosztott rendszerben működik, ami *bonyolítja a rendszer megtervezését*, hiszen a szerverek közötti protokollok és az együttműködési mechanizmusok tovább bonyolítják a működést, ugyanis a különböző megjelenési formáknak (amelyek lehetnek anonimek is) pontosan egyszerre kell változniuk, az eseményeknél garantálni kell az atomi váltást az elosztott rendszer minden szegletében.



4. ábra: több szerver, anonimizáló hálózattal

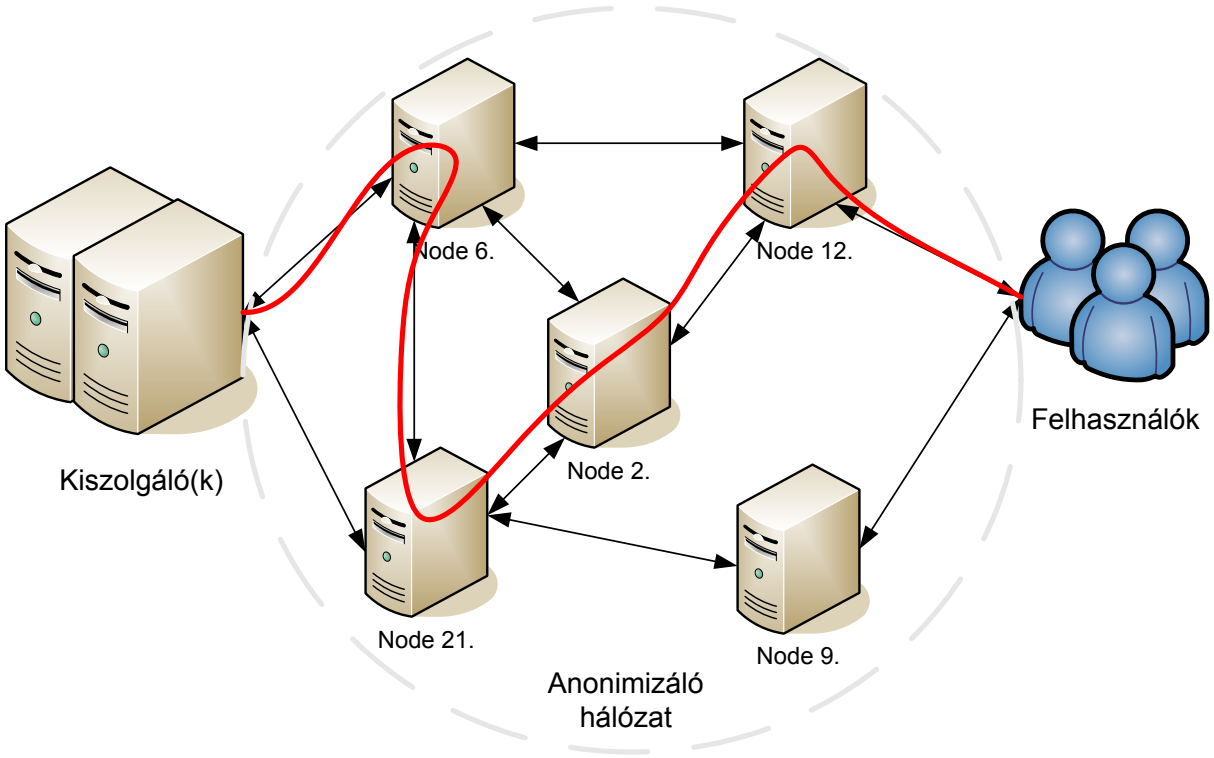
4.2.4. Anonimizáló rendszer architektúra lehetőségek

4.2.4.1. Önálló anonimizáló rendszer

A anonimizáló rendszer egységei különállóak, kizárólag az anonimizálás funkcióját látják el (és esetleg névfordítást, hogy a peer-to-peer kommunikáció a anonimizáló hálózaton keresztül lehetséges legyen), nem lehet kliens vagy szerver állomás.

Erre a feladatra a későbbiekben még tárgyalásra kerülő anonimizáló protokollok valamelyike lehet alkalmas. A MIX alapú anonimizáló hálózatok legtöbbször alkalmaznak változó késleltetéseket, amelyek miatt valósidejű rendszerekben nem használhatók kedvezően, de bizonyos módosításokkal erre is alkalmas lehet. Ezt mutatta meg például a Torpark [TORP] projekt.

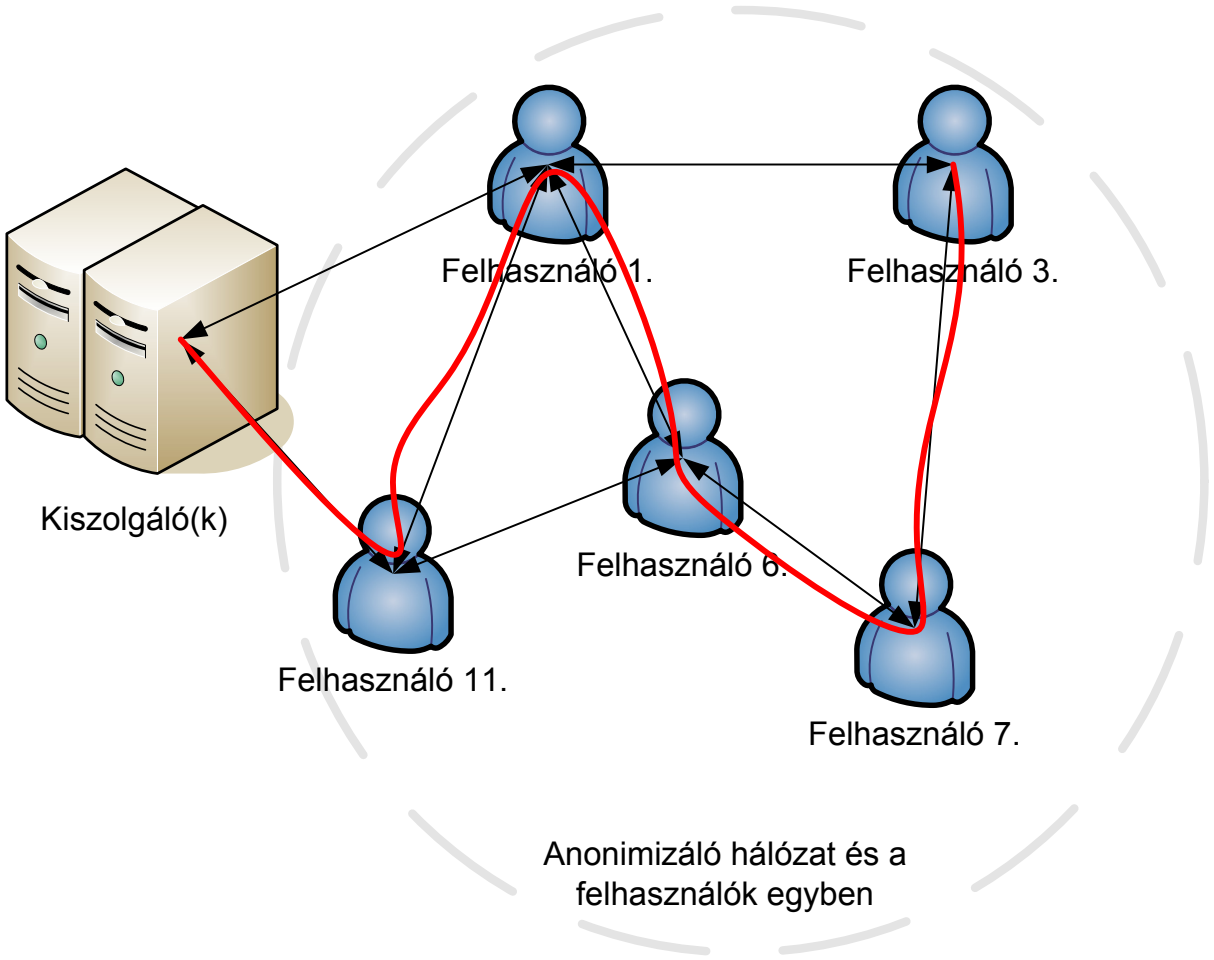
Több anonimizáló rendszer is létezik, amely erre a sémára épül. Egy másik fejezetben foglalkozunk azzal, hogy melyik lehet legalkalmasabb csevegő-szolgáltatásokhoz.



5. ábra: önálló anonimizáló rendszer

4.2.4.2. Felhasználói peer-to-peer anonimizáló rendszer

Elképzelhető egy olyan megoldás is, amelyben az *anonimizáló állomások a klienseken belül helyezkednek el*. Ebben az esetben a kliensek a forgalmat egymáson keresztül küldik tovább, ehhez hasonló megoldást alkalmaz például fájlküldésre a Skype [SKYPE].

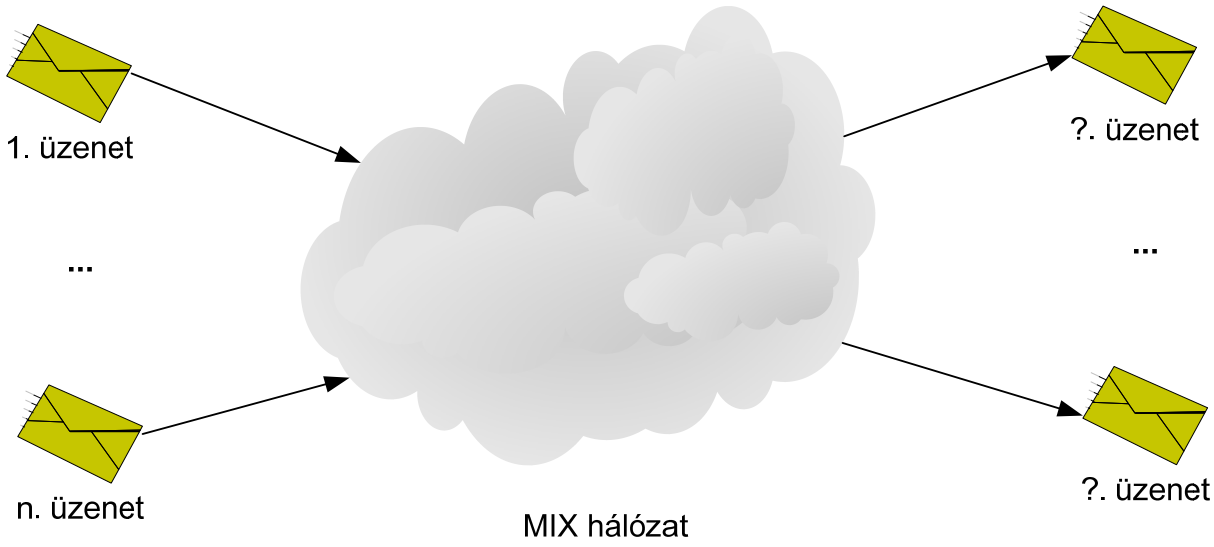


6. ábra: peer-to-peer anonimizáló rendszer

4.2.5. Az anonimizáló protokollok kategóriái

4.2.5.1. MIX-Net

A MIX hálózatok alapját a David Chaum-féle MIX-ek jelentik. A Chaum MIX azonos hosszúságú, különböző forrásból származó üzeneteket fogad, majd kriptográfiai műveletet végez rajtuk, végül továbbítja az üzeneteket a címzetthez, illetve hálózatban lévő következő MIX-hez valamilyen, a bemenetitől eltérő, véletlen sorrendben. (ld. az alábbi ábra.). A MIX tehát egy folyamat, mely *az anonimitást az üzenetek „keverésével" éri el*, megszüntetve az időbeli korrelációt a kimenő és bejövő üzenetek között.



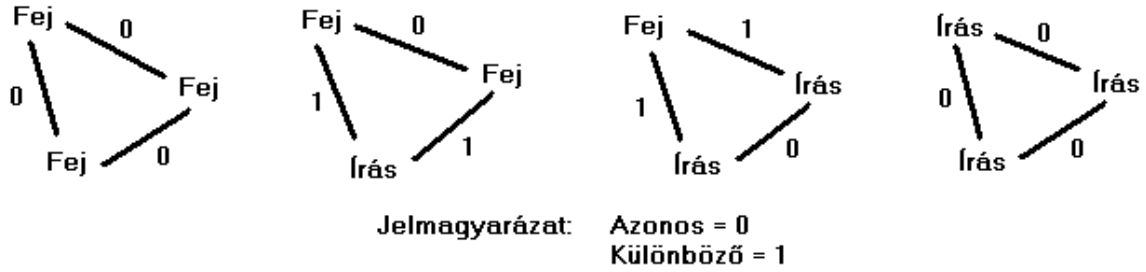
7. ábra: MIX hálózat

A MIX-ek leghatékonyabban hálózatban működnek, és a csomagok várakoztatásának elkerüléséhez állandó szintű forgalom szükséges. A MIX rendszerek egyike sem teljesen immunis a statisztikai analízisen alapuló támadások ellen, és az üzenetek várakoztatásának ideje arányos az általuk biztosított anonimitás szintjével. Mindezen felül az üzenet továbbításának ideje lineárisan függ az egymás után következő, az üzenet továbbításában részt vevő MIX-ek számával.

4.2.5.2. DC-Net

A Dining Cryptographer Network („Vacsorázó Kriptográfusok Hálózat”, röviden: DC-Net) szintén David Chaumtól származik, az általa felvetett Dining Cryptographer’s Problem („Vacsorázó Kriptográfusok Probléma”) általánosítása.

A probléma lényege röviden: három kriptográfus ebédel egy asztalnál. Az ebéd végeztével a pincér hozza a számlát, és elmondja, hogy az ebédet valaki kifizette már: vagy a kriptográfusok valamelyike, vagy egy kívülálló. A kriptográfusok szeretnék tudni, hogy közülük fizetett-e valaki, de anonim módon. Ekkor mindegyikőjük feldob egy érmét, és az eredmény megmutatják a tőlük jobbra ülő asztaltársuknak, majd a tőlük balra ülő érméjét látva kijelentik, hogy dobásuk azonos, vagy különböző volt. Amennyiben az egyik kriptográfus fizetett, úgy a valóságnak ellentétes kijelentést kell tennie. Ha valaki az igaztól eltérő választ adott, az eltérések paritása páratlan kell legyen, egyébkent páros (ekkor egy kívülálló állta a számlát - ld. az alábbi ábrát).



8. ábra: paritások a Vacsorázó kriptográfusok problémában

A DC-Net *nyilvános kulcsú infrastruktúrán alapul*. A felhasználók titkosított *broadcast üzeneteket* küldenek az egész csoportnak, ezzel biztosítva a fogadó anonimitást. DC-Net esetén egyszerre csak egy résztvevő küldhet üzenetet, így a sávszélesség egy része az ütközések valamint a versenyhelyzet feloldására fordítódik.

DC-Net alapú hálózat például a Herbovine protokoll.

4.2.5.3. Broadcast

A Broadcast alapú protokollok anonimitást biztosítanak a küldő és a fogad számára egyaránt. Minden részvevő fix méretű csomagokat küld, fix gyakorisággal. Mindezt úgy kell érteni, hogyha egy csomópontnak nincs küldendő csomagja, akkor *zajt küld*, a valós adatcsomagok küldésével megegyező módon. Ezek a csomagok a fogadó fél nyilvános kulcsával vannak titkosítva, így csak ő tudja dekódolni az üzeneteket. Tegyük fel, hogy adott egy rendszer, mellyel lehetőség van a küldő kilétének elfedésére egy olyan broadcast alapú hálózat implementálásával, mely egy alkalmazás szintű peer-to-peer gyűrű révén biztosítja, hogy *minden üzenet eljusson a hálózat minden tagjához*. Minden üzenet hopp-onként titkosított, így egy node számára nincs rá lehetőség, hogy a bejövő üzeneteket megkülönböztesse a kimenő üzenetektől.

Elképzelhető, hogy egy csomópont egy adott pillanatban nem folytat aktív kommunikációt, ám ahhoz, hogy a fix kommunikációs forgalom fenntartható legyen, mindenképpen üzenetet kell küldenie. Az ilyen csomagokat *noise csomagoknak* nevezzük, míg minden olyan csomag, mely egy meghatározott fél számra lett küldve *signal csomagnak* minősül.

Ilyen típusú hálózatot valósít meg a P^5 protokoll is.

4.2.6. Az aninonimizáló protokollok elemzése

A dolgozat jelen részében nem térünk ki az egyes protokollok ismertetésére (fontosabb jellemzőikről az [ANPR] mellékletben adunk tájékoztatást), hanem azt vizsgáljuk, milyen tulajdonságaik vannak, melyek alkalmassá tehetik őket egy anonim üzenetküldő szolgáltatásban való felhasználásra.

Említésre kerül a protokollok néhány ismertebb támadással szembeni ellenálló képessége is. A támadások rövid ismertetését szintén az [APAT] melléklet tartalmazza.

4.2.6.1. Onion Routing (Tor)

Az egyik legismertebb protokoll az Onion Routing [ONRO], mely szinte bármilyen Internetes protokollt képes kezelni.

Az Oninon routing *nem teljesen védett a lokális lehallgatással szemben* [ANOR]. Kellő mennyiségű adattal lehetséges olyan minták megfigyelése, melyekkel kikövetkeztethető az üzenete útja. Mindazonáltal az efféle támadások nagy mennyiségű adat megfigyelését igénylik a külső támadók részéről.

Predecessor támadással lehetőség van egy résztvevő anonimitásának szintjét *Leleplezés* ($0 \leq d_{x,e}(A) \leq ½$) szintjéig csökkenteni, de ez alá sohasem, mert egy felhasználó, véletlen események következtében is előfordulhat leggyakoribb félként a kommunikációban.

A szolgáltatás megtagadásra akkor lenne lehetőség az Onion Routing esetében, ha egy kompromittált csomópontnak lehetősége nyílina az üzenetek visszatartására. Mivel azonban az onion routing időbélyegeket használ a visszajátszás ellen, ez nem fordulhat elő, ám a *rosszul szinkronizált órák sérülékenységet jelentenek*. A TOR [TORD] ez ellen a rendszer robosztusságával ad védelmet.

Sybil támadásokkal szemben viszonylagos védettséget jelent a protokoll, mert minden résztvevő megválaszthatja, hogy ilyen útvonalon haladjon keresztül a küldött csomagja.

Ahhoz hogy az Onion Routing biztonságosabb legyen, a hálózati forgalomnak viszonylag állandónak kell lennie. Mindez hamis adatforgalom használatát jelenti, ha az adatforgalom alacsony. A második generációs TOR-ban nem alkalmaznak hamis adatforgalmat, hanem *különleges útvonaltervezéssel* biztosítja a kellő védelmet.

Az onion routing nagy előnyét jelenti, hogy könnyen adaptálható bármely alkalmazáshoz.

4.2.6.2. Hordes

A Hordes [HORD] egyik nagy előnye rejlik abban, hogy kihasználja a *multicast*[23] *üzeneteket,* hogy jobb teljesítményt érjen el ezzel az üzenetek továbbítása során. A multicast üzenetként érkező válaszok sokkal kisebb számítási igényűek, mint az üzenetek küldése a teljes hálózaton keresztül (minta a Crowds [CROW], vagy az Onion Routing esetében), hiszen a jondonak[24] csak a véletlen azonosítót kell ellenőriznie, hogy eldöntse, továbbítja, vagy eldobja a csomagot. Ebből fakadóan

[23] A hálózat bizonyos tagjainak küldött csoportos üzenet.
[24] A Crows és a Hordes rendszereben az egyes csomópontokat nevezik jondonak

egyetlen Hordes tagnak sem kell több számítási munkát végeznie, mint pl. egy Crowds béli jondonak, miközben az anonimitás végig biztosított.

A Hordes minimális anonimitási szintet valósít meg minden esetben, olyan esetekben is, ahol az Onion Routing, és a Cowds már nem. Az egyes jondo-kban nem kerül tárolásra routing információ, így passzív útvonal visszafejtés nem lehetséges.

Bizonyos támadások esetében viszont, bár a minimálisnál nagyobb anonimitást biztosít, a Cowds és az Onion Routing nagyobb szintű anonimitást jelent.

Lokális lehallgatással szemben például az Onion Routinghoz hasonlóan teljesítményt mutat. Ezzel szemben sybil támadás esetén a megfelelő számú csopópontot birtokolva a Hordes hálózat egy jelentős részét felügyelhetik a támadók.

A Hordes nem tesz külön erőfeszítést a szolgáltatás megtagadás alapú szemben. Az ilyen támadások megnövekedett forgalomhoz, és az üzetek elvesztéséhez vezethetnek.

Predecessor támadás esetén az Onion Routingnál elmondottak érvényesek: egy résztvevő anonimitásának szintje *Leleplezés* szintjéig csökkenthető, az alá nem.

Érdemes megjegyezni, hogy *lehetőség van pl. Onion Routing alkalmazására a Hordes továbbítási vonalában*. Ez persze több munkát igényel a titkosítás terén, de növeli a protokoll biztonságát és az anonimitást, és nem lenne szükséges Hordes proxy-t[25] futtatni a hálózat minden szerverén.

4.2.6.3. Herbivore

A Herbivore [HERB] protokoll három fő jellemzője:

1) Anonimitást biztosít a kommunikáció végpontjainak, még olyan támadókkal szemben is, akik korlátlan erőforrásokkal rendelkeznek a lehallgatásokhoz.
2) Nagy számú felhasználó esetén is jól skálázható
3) Hatékony a sávszélesség és a számítási idő tekintetében.

A Herbivore a küldő és a fogadó számára egyaránt anonimitást biztosít.

A protokoll a skálázhatóság kérdését egyfajta „oszd meg és uralkodj” elv segítségével valósítja meg: decentralizált, peer-to-peer megközelítéssel a globális hálózatot biztonságosan osztja fel kisebb csoportokra, melyekben a anonim kommunikáció hatékonyan valósul meg.

Mivel a Herbivore DC-Net alapú, így *érzéketlen a predecessor támadásra*. Érzéketlen továbbá a lokális lehallgatással szemben is, mivel minden felhasználónak üzenetet kell küldenie és fogadnia minden hálózaton belüli adatküldés esetén.

[25] Egy adott komponens nem közvetlenül ér el a hálózaton egy másik komponenst, hanem egy un. proxy szerveren keresztül teszi ezt, és valójában a proxy kommunikál a céllal és a forrással, mint "köztes" elem. Ennek számos alkalmazási előnye van, mint amilyen a gyorsítótár lehetősége, vagy biztonsági megfontolások.

Ezzel szemben az üzenetküldések ütközésének feloldásából fakadó nehézségek miatt a DC-Net alapú hálózatok a *legsérülékenyebbek a szolgáltatás megtagadáson alapuló támadásokkal szemben*. A Herbivoire protokollban ilyen támadás esetén a felhasználók egyszerűen átléphetnek másik csoportba, ha egy csoporton belül lehetetlenné válik a kommunikáció. DC-Net alapú hálózatokban jelentős mennyiségű számítás és sávszélesség árán detektálható ugyan a szolgáltatás megtagadását kezdeményező felhasználó kilétének felfedése, de ezzel az eszközzel a Herbivore nem él.

A Herbivore a sybil támadásokkal szemben is nyújt némi védelmet a támadók detektálása nélkül azáltal, hogy limitálja, hogy egy csoportba hány új felhasználó csatlakozhat.

A Herbivore általános célú anonim kommunikációra ad lehetőséget, amely számos különböző alkalmazáshoz illeszthető. Virtuális hálózati rétegként működik, az anonim rétegbe ágyazva az IP alapú csomagokat. Ez a megközelítés előnyt jent, hiszen így a legtöbb létező alkalmazást csak kis mértékben, vagy egyáltalán nem szükséges módosítani.

4.2.6.4. P^5 – Peer-to-Peer Personal Privacy Protocol

A P^5 [P5AC] anonimitást biztosít a küldő és a fogadó fél számra, és teljesíti az összeköthetetlenség feltételét is. A P^5 a fentebb ismertetett broadcast csatorna alapelveire épül. A skálázhatóságot a *broadcast csatornák hierarchiába rendezésével* oldja meg. Nyilvánvalóan minden broadcast alapú rendszernél, alapesetben nem biztosít nagymértékű hatékonyságot mind abban a tekintetben, hogy hány bit információt igényel a küldő-fogadó párnak az információcsere, és mennyi extra bitet jelent a hálózati forgalomban egyetlen hasznos bit átvitele.

A protokoll a skálázhatóság kérdését egy broadcast hierarchia segítségével oldja meg. A hierarchia különböző szintjei különböző szintű anonimitást (és összeköthetetlenséget) biztosítanak, mindezt a sávszélesség és megbízhatóság terhére. A P^5 felhasználóinak minden esetben lehetőségük van az anonimitás szintjek csökkentésére/növelésére a hatékonyság szempontjából jobb/rosszabb csatorna választásával.

Predecessor támadásnál egy résztvevő anonimitásának szintje *Leleplezés* szintjéig csökkenthető, az alá viszont nem.

A szolgáltatás megtagadással szemben a P^5 az üzenetek eldobásának megfelelő implementálásával ad védelmet. Ehhez a linkenként várakozási sorok hosszát kell csupán megfelelően meghatározni.

A P^5-ben lehetőség van továbbá sybil támadásra, mivel egy támadónak lehetősége van megválasztani melyik broadcast csoportba kerüljön, mindezt a bináris fa felépítéséhez használt kulcsokra alkalmazott kimerítő támadással.

Lokális lehallgatással szemben a P^5 érzéketlen, hiszen a Herbivore-hoz hasonlóan ebben a protokollban is minden hálózaton belüli adatküldésnél minden felhasználónak üzenetet kell küldenie és fogadnia.

A csoportos üzenetküldés megoldása – melyben az üzenet csak a csoport egyetlen tagjának szól – kis mértékű üzenetkésleltetést jelent, bár a hasznos információ mennyisége *a sávszélességen csökken, ahogy az anonimitás mértéke nő*. A P^5-nek viszont megvan azon érdekes tulajdonsága, hogy a felhasználónak bármikor lehetősége van ennek az aránynak a változtatására. A protokoll ezen kívül jól skálázható, és könnyen hozzá illeszthető a jelenlegi Internetes protokollok mellé.

4.2.7. Hálózati teljesítmény az egyes protokolloknál

Az adott rendszertől függően, az anonimitás mértéke a sávszélesség, a számítási idő, esetleg mindkettő rovására növelhető. Az alábbi táblázatban foglaltuk össze, hogy a fenti protokollok esetében hány bit információ szükséges egyetlen hasznos bit átviteléhez.

2. táblázat: egy hasznos bit küldéséhez szükséges bitek száma

Onion Routing	(n + 1)
Hordes	(n + 1)
Herbivore	2*(m – 1)
P^5	$m*(2^{(D-d)} + d + 1)$

A táblázatban *m* jelöli a csoportok méretét a Herbivore és a P^5 esetében, *n* jelöli az útvonalban előforduló MIX-ek számát a Hordes és az Onion Routing esetében. Továbbá *d* jelöli a felhasználó broadcast címének „mélységét” a broadcast fában, míg *D* a fa maximális mélységét.

A fentiek alapján a *legnagyobb igénye a P^5-nek* van, de figyelembe kell venni, hogy az ott használatos üzenetdobási algoritmus miatt a fa magasabb csúcsaiban exponenciálisan növekvő valószínűséggel kerülnek eldobásra. Az Onion Routing és a Hordes igényének egyenlősége nem meglepő, hiszen *mindkettő MIX-eken alapul*. A Herbivore ehhez képest kétszer akkora igényű, és a csoportok mérete is nagyobb, mint a MIX alapú rendszereknél a továbbításban részvevő MIX-ek száma.

4.2.8. A protokollok alkalmazhatósága a csevegő szolgáltatásokban

A fejezetben foglaltak alapján, figyelembe véve az azonnali üzenetküldő szolgáltatások, és az ideális rendszer által megkövetelt anonimitási kritériumokat, a *több szerveres, anoinimizáló hálózatot használó rendszer* tűnik megfelelő architektúrának. Ennek oka, hogy így a rendszer megfelelően skálázhatóvá válik, bár maga a rendszer bonyolultabb. Mindazonáltal, mint azt fentebb említettük, a rendszer első változatát egy szerveres architektúrára kívánjuk építeni, hiszen a rendszer működőképessége ezen is jó követhető lesz.

Önálló anonimizáló rendszer használatával az ideális szolgáltatás fejlesztése is könnyebbé válik. Ennek a megoldásnak az alkalmazása nem jelent különösebb hátrányt a felhasználói peer-to-peer rendszerrel szemben.

A ma létező anonimizáló protokollokból eleve azokat vettük vizsgálat alá, melyek képesek (ha kis módosítással is) bármely Internetes protokoll kezelésére. A szempontrendszerünk alapján *az Onion Routing, illetve ennek második generációs változata, a TOR megfelelő lehet* egy azonnali üzenetküldő szolgáltatással való alkalmazásban. Mellette szól, hogy kellő védelmet biztosít az egyes támadások ellen, könnyen használható együtt szinte bármilyen alkalmazással, így a fejlesztésben sok könnyebbséget jelent.

Mindazonáltal a Hordes is ígéretesnek tűnik, előnyös tulajdonságai hasonlóak az Onion Routinghoz, lévén mindkét protokoll MIX alapú. Az Onion Routing-gal szemben azonban van egy komoly hátránya: nem áll rendelkezésre kiépített hálózat.

4.3. Külső-belső világ paradigma

4.3.1. Külső-belső világ paradigma általában

Korábbi vizsgálataink szerint [GGAB] úgy találtuk, hogy az anonim, anonimizáló szolgáltatások modelljei két fő részre bonthatóak a használt technológiák szempontjából.

A két modellrészlet jól értelmezhető, a fejlesztés során is előnyös. A szolgáltatásokban létezik a **belső világ**, amely a szolgáltatásban résztvevőket foglalja magába, és azt a rendszert, amely a szolgáltatáson belül körülveszi a szereplőket, és közvetlenül ezzel a világgal léphetnek kapcsolatba, és a világbéli reprezentációjukat vezérelhetik megfelelő módon.

A **külső világ** a rendszeren kívüli szereplőket foglalja magába, s a tervezés célja, hogy e szereplők legfeljebb más szereplőkön keresztül férhessenek hozzá a rendszerhez, más egyéb módon nem. A külső világ eme a hálózati alkalmazásokban a hálózatot, a hálózati kapcsolatokat, egyszóval a hálózati architektúrát (és a hálózati forgalmat) és a MIX rendszert – ha van – érinti.

Jellegzetesen más-más technológiát kell alkalmazni a megfelelő szintű pszeudonim vagy anonim jelenlét eléréséhez a két világrészben, mind a külső világbéli szeparációt tekintve, mind az anonimitást garantáló megoldásokat tekintve.

A külső-belső világ paradigma megjelenik például az anonim böngészőkben is. Például a Torpark projektben [TORP] kifejezetten a külső világtól való szeparációt oldották meg a fejlesztők TOR [TORN] hálózatra építve, de a belső működést módosító technológiát nem alkalmaztak. A Tor [TORN] MIX rendszer az Onion Routing [ONR1] technológiát használja.

Ehhez hasonlóan léteznek a csevegő szolgáltatásokban is olyan megoldások, amelyekben a fejlesztők a működési mechanizmust nem módosították, hanem a szolgáltatás alá beillesztettek egy TOR hálózatot. Ilyen jellegű megoldást nyújt a

ScatterChat [SCCH], amely több protokollt támogat, és azonnali üzenetküldő hálózatokhoz képes csatlakozni egy TOR hálózaton keresztül.

4.3.2. Külső-belső világ paradigma az AnonIM-ben

A külső-belső világ paradigmát az AnonIM rendszerében is szeparáltan kezeljük. A külső világtól való elszeparálódási mechanizmusokat, és anonimitást garantáló megoldás lehetőségeket az alábbi részben tekintjük át. A belső világ modellezésével és anonimitást garantáló technológiáival későbbi fejezetek foglalkoznak.

4.4. Szeparáció a külső világtól

A külső világtól való szeparáció megvalósítására szolgál *a szállító protokoll*. A továbbiakban leírt garanciák vállalásával meggyőződhetünk arról, hogy a rendszeren kívüli szereplőket e protokoll nagy biztonsággal távol tartja, *a rendszert megfigyelhetetlenné, hozzáférhetetlenné teszi*.

4.4.1. A szállító protokoll célja

A szállító protokoll általános célja, hogy szolgáltatásaival adott – bizonyítottan betartott – tulajdonságokat garantálva lehetővé tegye a rá épülő komponenseknek, hogy azoknak *ne kelljen foglalkozniuk azzal, hogy milyen átviteli közegen terjednek az adatok*, csak a szállító protokoll garanciáit figyelembe véve járhassanak el. Ez a feladatmegosztás és a komponensekre, rétegekre bontás alapvető mérnöki feladat, és az előzetes tervezés igen fontos része. Ha ugyanis bármelyik réteg téved, vagy összeomlik, a ráépülő rétegek meghatározhatatlan módon működésképtelenné válhatnak.

A szállító protokoll konkrétabb célja a későbbiekben specifikált *üzenetek* átvitele a rendszer két résztvevője között, a következő elvi kritériumok betartásával. Kiemelendő, hogy az üzenetek tartalmára és formájára semmiféle megkötést nem jelenthet az, hogy milyen átviteli közegre épül a szállító protokoll.

4.4.2. Elvi kritériumok

4.4.2.1. Harmadik fél támadási lehetőségei

- Passzív támadások
  - **Lehallgatás**: egy jogosulatlan szereplő megfigyeli az üzeneteket.
  - **Forgalomanalízis**: egy jogosulatlan szereplő következtetni próbál a tartalomra, esetleg másra a forgalom vizsgálatával.

- Aktív támadások

- **Üzenetek átszerkesztése**: egy jogosulatlan szereplő módosítja az üzeneteket.
- **Megszemélyesítés**: az adatfolyamba való beszúrást és az üzenetek átszerkesztését vagy eldobatását kombinálva lehetséges átvenni a teljes vezérlést egy tetszőleges szereplőtől. Továbbá lehetséges a másik nevében történő üzenetküldés.[26]
- **Visszajátszás**: egy jogosulatlan szereplő először megfigyeli az üzeneteket, pontosan tárolja azokat, majd valami cél érdekében később beinjektálja a megfelelően kiválasztottakat.

4.4.2.2. A védekezés lehetőségei

- **Bizalmasság**: az üzenet tartalma a feladón és címzetten kívül mindenkinek ismeretlen illetve érthetetlen, információt nem hordoz. Ez feltétlenül szükséges, ugyanis az átlagos felhasználó nem is gondolja, hogy amit ő közöl a partnerével, az akár 3. fél számára is értelmezhető lehet, visszaélhet vele. További követelmény lehet, hogy a köztes megfigyelő még azt se tudja megkülönböztetni, hogy egyáltalán *zajlik-e értelmes kommunikáció a felek között*, vagy sem.

- **Integritás**: a tartalom sértetlen marad, mind a szándékos és véletlen módosításokkal szemben. Szükséges, mert egyébként 3. fél az üzenetet módosítva bárkinek kiadhatná magát, módosíthatná az üzenetek információ-tartalmát, a lehetőségek korlátlanok. Technikai okú, véletlen sérülések esetén is szükség van erre.

- **Bizonyosság az üzenet megérkezéséről**: esetlegesen az integritás sérülése miatt az üzenet egyszerűen nem közvetítődik. Ilyenkor a felhasználó nem tudná, hogy valójában nem válaszol a másik fél, vagy technikai probléma, esetleg 3. fél által okozott probléma lépett fel. Ezt mindenképpen tisztázni kell.

- **Bizonyosság a feladóról**: szintén összefügg az integritással, hogy a feladónak ne legyen lehetősége másnak kiadnia magát. Ez minden szituációra vonatkozik, például egy üzenet tárolása, és későbbi továbbküldése esetén is biztos lehessen a címzett afelől, hogy a feladó valóban az, aki a feladó mezőben meg van nevezve.

- **Visszajátszás elleni védelem**: a korábban említett visszajátszás megakadályozása úgy, hogy egy külső támadó a megfigyelt üzeneteket visszajuttatva, a szállítási protokoll detektálja a hibát, és ne fogadja a hamisított csomagot, mint eredetit.

Látható, hogy a kritériumok egyes részei (pl. *Bizonyosság a feladóról*) a szállító protokollon túllépnek, abban meg nem oldható problémát okoznak, melyeket a rendszernek más szinten kell kezelnie (például digitális aláírással).

[26] Ezzel nem foglalkozunk a továbbiakban, ugyanis a szerver szintjén lehetséges egyszerűen védekezni, ugyanis miután egy felhasználó azonosította magát, lehetetlen hogy azon a kapcsolaton más felhasználótól jöjjön üzenet. Az adatfolyam átszerkeszthetőségével a többi kritérium foglalkozik.

4.4.2.3. Véletlen hibák, protokollvezérlési problémák és megoldások

Praktikus lehet megkötéseket tenni az átvitt üzenetek tartalma helyett az átvitel minimális sebességére, egy csomag átvitelének maximális időtartamára (késleltetés), a megérkezés sorrendjére, biztonságára is. Ezek a kritériumok teszik kényelmesen használhatóvá az átviteli protokollt. Összefoglaló néven ezeket *Quality of Service (QoS) jellemzőknek* szokás hívni. Fontos kiemelni, hogy ezek a garanciák a szállító protokoll szintjén, üzenetenként változhatnak. A QoS paramétereket ezen a felsőbb szinten kell garantálni, attól függetlenül, hogy milyen alacsonyabb szintű átviteli közeget használ a szállító protokoll.

4.4.3. Elvi kritériumok teljesülése a gyakorlatban

Az Internet megbízhatatlan közege alapvető problémát jelent a projekt megvalósításában. Az IP (Internet Protocol) az Internet forgalomirányítási, címzési protokollja. Mint ismeretes, alapvetően arra fejlesztették ki, hogy egy konkrét címzettel és feladóval kiegészítve a küldendő adatokat (és még egy kevés meta-információval), a hálózati csomópontok egyszerűen el tudják juttatni a csomagot az IP fejlécben nevezett címzett géphez. Igen szűkös szolgáltatásokkal rendelkezik e protokoll: az adatmező maximális mérete általában valamivel 1400 byte feletti, *semmiféle garanciát nem vállal arra, hogy egy küldött csomag meg is érkezik a címzetthez*, *illetve* arra sem, hogy sok egymás után feladott *csomag a küldés sorrendjében érkezik-e a címzetthez*. Ezen kívül természetesen *bárki módosíthatja és megnézheti* a csomag tartalmát az annak útjába eső csomópontokon. Ily módon egy nyers IP csomag összehasonlítható egy nyílt levelezőlappal, az elvi kritériumok egyikének sem felel meg.

Az IP-re épülő TCP (Transmission Control Protocol) egy szolgáltatási szinttel tovább lép: byte-szintű folyamként teszi kezelhetővé a sorrendezés és csomagvesztés problémáit, hogy azzal ne kelljen foglalkozni. Azonban még mindig bárki megtekintheti és módosíthatja a csomagokat, és ezzel az adatfolyam tartalmát. Ez a szint a QoS követelmények egy részét (sorrendezés, megbízható megérkezés) teljesíti, de semmi többet. Ráadásul a megbízható megérkezést általában technikailag nem is lehetséges megkérdezni a TCP csatornától, így ha úgy tekintjük, az sem biztosított. Külső beavatkozás esetén természetesen ezek a tulajdonságok is sérülhetnek.

Az előbbi kitekintés az Internet belső világába fontos a szállító protokollunk céljának megértéséhez, ugyanis a TCP által nyújtott szolgáltatásokat kell addig továbbfejleszteni, amíg azok megfelelnek az előbbiekben leírt *elvi kritériumoknak*.

A *bizalmasság és integritás* követelményeinek biztosítására legegyszerűbb a bevált, szabványos SSL/TLS (Secure Sockets Layer / Transport Layer Security) kriptográfiai protokollokat (a TLS az SSL továbbfejlesztése) használni, melyek a lehallgatást és üzenetmódosítást kísérelik megakadályozni. Ezeket TCP/IP felett használva rendelkezésre áll egy sorrendiséget és üzenetek veszteségmentes átvitelét (amely már TCP szinten is rendelkezésre állt), illetve bizalmasságot és integritást garantáló

pont-pont kapcsolat. Működésük alapja, hogy extrém nagy valószínűséggel csak gyakorlatilag megvalósíthatatlan mennyiségű számítások után lehetne dekódolni az adatfolyamot. Kiemelendő, hogy a tökéletes biztonság sem matematikailag, sem praktikusan nem lehetséges, mert igaz hogy az adatforgalom a két kommunikáló fél között zajszerűnek tűnik, de ha a kódolt adatfolyam részben ismert mintákat, vagy egyéb jósolható összetevőket tartalmaz, a kódolás egyszerűbben is megfejthető[27]. Ez a protokoll azonban nem foglalkozik a forgalom létének maszkolásával, azaz továbbra is megállapítható hogy mikor forgalmaz a két csomópont egymással adatot. Erre később visszatérünk a *forgalomanalízissel* kapcsolatos részben.

Az elvi kritériumok közül a *QoS* [QOS1] és a *feladó bizonyosságának* megvalósítása kérdéses még. Igaz, hogy a TCP+SSL/TLS megoldás garantálja az üzenet megérkezését, de csak abban az esetben, ha a kapcsolat hibamentes az üzenet visszaigazolásáig. Bármi hiba képződik (legyen ez akár egy ügyesen beszúrt, ártó szándékú csomag), a kapcsolat azonnal megszakadhat. Ez azt jelenti, hogy általában az üzeneteket minden hálózati protokoll szintjén külön vissza szokás igazolni, mert nem lehet eldönteni, hogy az üzenet ténylegesen elment-e, vagy csak vár a sorára a visszaigazolandó csomagok között. Az is lehet, hogy TCP szinten egy része ment csak át az üzenetnek. Ez indokolhatja az applikációs rétegbeli külön visszaigazolást, ha szükséges. A részletes QoS szintek definíciókkal a [QOSM] melléklet szolgál.

A különböző szintek felhasználásával változtatható az éppen küldendő üzenet besorolása, így spórolhatunk az erőforrásokkal, a sávszélességgel.

4.4.4. Védelem a forgalomanalízissel szemben

Forgalomanalízisnek nevezünk minden olyan módszert, mely a forgalom konkrét tartalmának ismerete nélkül, pusztán a minden közbenső csomópont által látható *forgalmi adatokból* (feladó, címzett, hossz, stb.), *statisztikai módszerekkel von le következtetéseket* a kommunikáló felekről. Gyakran elégséges tudni, hogy kik vagy mennyit kommunikálnak, milyen eloszlással. Azt szeretnénk, hogy ez nagyjából lehetetlenné váljon, tehát semmilyen hasznos információt se lehessen kinyerni a kommunikáció látszólagos tényéből.

A lehetséges megoldások közül először vizsgáljuk meg azt az esetet, amikor a forgalomanalízisnek való valamilyen ellenállást a szállító protokoll belső ügyeként tekintjük. Feltételezzük továbbá, hogy minden szállító protokoll[28] külső döntés nélkül, egymástól függetlenül hoz döntést arra vonatkozóan, hogy mikor milyen csomagot küld, milyen eloszlással. Az előbb leírt „üzemmódot” nevezzük *nem vezérelt*nek. A másik lehetőség, amely persze csak több szállító protokoll esetén különbözik az előbbitől, a *vezérelt üzemmód*, mely során a szállítási protokoll halmazt külső információk alapján közösen vezéreli egy döntéshozó modul. Ez a vezérlés az ismert

[27] Ez úgy lehetséges, hogy a megfigyelő számára ismert információt tartalmazó adatfolyam és a kódolatlan adatfolyam kölcsönös entrópiája csökken. Ennek egyik szélsőértéke az, hogy az eredeti és kódolt adatok külső megfigyelő számára teljesen függetlenek és véletlenszerűek. Másik szélsőértéke pedig az, hogy a kettő adatfolyam egymásból előállítható – ilyen a kommunikáció két résztvevője.

[28] Több szállító protokoll példány létezése alapvetően csak a központi kiszolgálón (kiszolgálókon) fordulhat elő, mert a kliensek mindig egyetlen kiszolgálóhoz kapcsolódnak.

szempontok alapján segítheti az anonimitás megőrzését a szerverhez közel lévő hálózati csomópontokon.

4.4.4.1. A nem vezérelt üzemmód, ideális esetben

Ideális esetben nem lehet megállapítani, hogy milyen végpontok között zajlik a kommunikáció, és nem is lehet annak mennyiségére vagy minőségére következtetni.

Az egyetlen megoldás, ami nem szolgáltat információt külső megfigyelő számára, az állandó sávszélességgel vagy üzenetsebességgel való adatforgalmazás. Ekkor a szállító protokoll alatti csatorna maximális sebességénél (S) kisebb sebességre ($S' < S$) korlátozzuk a szállító protokoll sebességét, majd állandó S' sebességgel véletlen zajt adunk ki a másik oldal számára[29]. Amikor valójában hasznos adatot kell átvinni, akkor *a véletlen zaj helyett a tényleges csomagot ugyanezzel az adatsebességgel adjuk át*, majd folytatjuk a zajgenerálást. Így külső megfigyelő számára azon kívül, hogy kapcsolatban van a kliens a kiszolgálóval, semmi sem derül ki. (Megjegyzendő, hogy megfigyelhető információ lesz azonban a beállított vagy detektált S' adatsebesség.) Természetesen a véletlenszerű sávszélesség korlátozások és a zaj használata miatt a csomagok küldési sorrendjének cseréjének nincs nagy biztonságtechnikai haszna, de ha például az adott véletlen sebességre minimalizálni szeretnénk a várakozó csomagok késleltetését, a küldendő csomagok akár meg is cserélhetők (kisebbek előrehozásával).

A valóság azonban több problémát tartogat:

- A véletlenszámok generálása zaj céljából a gyakorlatban kizárólag pszeudorandom számgenerátorokkal oldható meg. Biztonsági probléma, ha a megfigyelő a generátor belső állapotáról bármilyen információval rendelkezik, ugyanis akkor a teljesen véletlenszerű kereséstől eltérő módon, céltudatosabban kutathatja, hogy mi lehet a tényleges adatforgalom.

- A csatorna maximális S sebessége ingadozhat, illetve a csatornát más programok is közösen használják, ezáltal az S'-t is állandóan változtatni kellene.

- S közvetlenül nem megfigyelhető érték, csak becsülhető, vagy a felhasználótól megkérdezhető, tehát mindenképpen bizonytalan és változó.

- Ha állandó S', közel maximális forgalmat bocsátanánk ki, „kiéheztetnénk” a többi programot illetve a felhasználót, és használhatatlanná tennénk minden más tevékenységre az adott gépet.

- Ha ezekből kifolyólag erősen csökkentjük S' értékét, a maximális üzenetsebesség alkalmatlan lesz bármi nagyobb adatmennyiség tűrhető időn belüli küldésére.

[29] Fontos, hogy ne előre ismert adatokat vigyünk át ilyenkor, mert akkor kitehetjük a TLS kapcsolatot egy olyan támadásnak, melyhez szükséges tudni az átvitt kódolatlan és kódolt adatokat egyaránt.

4.4.4.2. A nem vezérelt üzemmód, nem ideális esetben

Ilyenkor is csak egyetlen szállító protokoll létezik, és a kapcsolaton belül szintén csak egy irányba tudja befolyásolni az adatküldést (hiszen a másik irányért a túloldali szállító protokoll a felelős).

A réteg célja ebben az esetben, hogy a *kimenet megfigyeléséből semmilyen következtetést ne lehessen levonni* a küldött adatokról, se arról, hogy mikor folyik tényleges kommunikáció, s ha kommunikáció van éppen, mennyi adatról van szó.

A kriptográfiának és az erős algoritmusok (és kulcsok) választásának köszönhetően biztosak lehetünk abban, hogy a rejtjelezett adatfolyam külső szemlélő számára zajnak tűnik, ezért attól függetlenül, hogy mikor küldünk véletlen adatot és mikor fontos adatokat, az mindig véletlen zajnak fog tűnni a külső megfigyelő számára.

Erre jó megoldás lehet, hogy ha a szállító vezérlője véletlen kisorsolja, hogy az adott időegység alatt mennyi adatot visz át, majd ha van átviendő adat, feldarabolja ennek megfelelően és átviszi az első darabot. A következő időegységnél hasonlóan cselekszik, és ez folytatódik tovább.

A megoldás jó, de nem minden szempontból előnyös – sajnos a csatorna kapacitásának csak a fele lesz kihasználva. Ugyanis ha a vezérlő egyenletes eloszlással választja ki a csatorna terheltségét 0 bájt és a maximális kapacitás közötti átvihető adatmennyiséget, akkor a kihasználtság a csatorna kihasználtságát leíró *egyenletes eloszlású valószínűségi változó várható értéke* lesz, ami pontosan $\frac{\max}{2}$ értéket vesz fel.

Egy hálózati alkalmazás esetén általában jó, hogy ha a sáv nem teljesen kihasznált, hiszen például, több csatorna lehet, illetve a működés rovására mehet. Ehelyett jobb, ha csak egy a *maximális kihasználtságot közelítő állapotot engedélyezünk*. Ha az előbbi egyenletes eloszlást alkalmazó vezérlést vesszük, az sem előnyös, hiszen ha túl alacsony értékeket sorsol, nagyobb forgalom esetén (például kisebb csatolt fájl) az átvitel belassulhat. A legmegfelelőbb, ha leginkább közepes méretű terhelési lehetőséget ad a vezérlő – ezt a legjobban egy normális eloszlású véletlen generátorral tehetjük meg, amelynél a minimum érték a csatorna átviteli kapacitásának 5-20%-os mezőjében, a maximális pedig a 90-95%-os mezőjében van, és a kettő közötti értékek közül normális eloszlás szerint választ. Így az átviteli sebesség kihasználatlan se lesz, és a maximumot se érheti el.

Célszerű ezen kritériumok figyelembevételével a csatorna kihasználtságát magasabbra helyezni, azaz a csatornát leíró valószínűségi változó várható értékét a *teljes kapacitás 70%-ra* helyezni. A megadott kritériumok alapján értelmezhetjük ennek a valószínűségi változónak a sűrűségfüggvényét.

Egy normális eloszlás sűrűségfüggvényét fogjuk alapjául venni az eloszlásnak. Ezt meg lehet oldani többféleképpen is, egy példa [MAT1] a következő sűrűségfüggvény:

$$f''(x) = \begin{cases} 0, x < 20 \\ \varphi_{70,25}(x) + a, 20 \le x \le 95 \\ 0, x > 95 \end{cases},$$

amelyre már teljesülnek a megfelelő feltételek.

Az implementációban praktikus lehet, ha a várható értéket, és a kétoldali szórásokat futásidőben dinamikusan be tudjuk állítani. Ez lényegében nem bonyolítja a módszert, ugyanis az $f''(x)$ függvény normális eloszlásból való származtatása nem túlzottan összetett.

További problémát jelent ebben a globálisan nem vezérelt esetben, ha minden átviteli csatorna a teljes sávszélesség felett rendelkezhet, ugyanis ebben az esetben megfelelően nagy érték választásával a terhelés nagyobb lehet a kiszolgálhatónál (könnyen belátható, hogy ez már néhány kapcsolat esetén is hamar előfordulhat). Ezért fontos, hogy a kliensek a központ felé egy kapcsolattal rendelkezzenek, a szerver pedig vagy egyenletesen (akár a teljes sávszélességet, vagy bizonyos előre megszabott sávszélesség darabokat), vagy valamilyen prioritás szerint ossza szét a kimenő sávszélességét a kliensek között. Emiatt sajnos *némi vezérlés mégis szükséges a rendszerbe*, legalább szerver oldalon.

4.4.4.3. A vezérelt üzemmód

Ebben az esetben nyilvánvalóan nem létezik ideális megoldás, mert akkor nem lenne mit vezérelni.

A vezérelt üzemmód legfőbb célja, az hogy össze lehessen hangolni több, párhuzamosan működő szállítási protokollt. Az összehangolás szükségessége kitűnik, ha felidézzük a *nem vezérelt, ideális* fejezetben említett nehézségeket, például a protokollok kimenő sávszélessége példányonként biztosan nem állandó *S* érték, hanem a protokollok éppen aktuális számától is változik, ugyanis a sávszélességek összegének maximuma a gyakorlatban konstans.

A felmerült vezérlési lehetőségek a következők (itt az adott műveleteket minden résztvevő protokollra elvégezzük):

- A pillanatnyi protokoll példányszámtól függően (legyen *n*) beállítjuk az *S'* értéket (itt legfeljebb *1/n*-re). Azon belül a protokoll eldönti, mit tesz ezzel a maximális sávszélességgel, ld. *nem vezérelt, ideális* vagy *nem vezérelt, nem ideális* fejezetek. Ez a legegyszerűbb információközlés, amit megtehetünk.

- A *nem vezérelt, nem ideális* alfejezetben leírtaknak megfelelően állítgatjuk a pillanatnyi sebességeket. Azonban itt *n* darab, egymással összefüggő *együttes eloszlású véletlen változót* generálva tesszük ezt, úgy, hogy a csatornakapacitások összege mindig megfelelően a maximum alatt maradjon. Ennek vizsgálata túlmutat e dokumentum keretein, azonban az előbbi eredményeket felhasználva egyszerű példa implementáció készíthető.

A vezérlést a szerveroldalon egy külön modul végezné, mely rálát az összes aktív szállító protokoll példányra és egyéb olyan információkra, amik a vezérléshez és az anonimitás követelményeinek való megfeleléshez szükségesek.

4.5. Belső világ modell

4.5.1. A belső világ modell szereplői

4.5.1.1. A belső világ, virtuális valóság modelljéről

A belső világ modell alatt a felhasználók által tapasztalt modell rendszert értjük, amelyben felhasználókat kereshetnek, kapcsolatokat, beszélgetéseket létesíthetnek, és egyéb felhasználói közösségekbe (például szobák) csatlakozhatnak.

A belső világ modell implicite magába foglalhatja ezen absztrakt modellen felül a modell működését megvalósító protokollokat, és mindent, ami a szolgáltatás belső működéséhez kapcsolódik, de jelen esetben csak a virtuális világ absztrakciós modelljének felépítésével fogunk foglalkozni.

A modell megalkotásánál figyelembe vettük előző féléves alapkutatásunk eredményeit, amely több manapság használt azonnali üzenetküldő szolgáltatást és egy chat jellegű rendszert vizsgált. A modellre nagy hatással volt ez utóbbi rendszer, az UnrealIRCd belső modellje [URID], főleg a szobákat érintő kérdésekben, továbbá megvizsgáltuk a hagyományos IRC rendszereket is [IRCR]. Az IRC több mint tíz éves múltra tekint vissza, s az évek alatt sok újítás jelent meg hozzá, ezek közé sorolható az UnrealIRCd is. Ez utóbbi bevált rendszer és sok magánszféraóvó megoldás található benne, ezért egyes megoldásokat mi is átvettünk a szobák attribútumai közé (a legtöbb esetben módosítva).

4.5.1.2. Főbb egységek

A **felhasználók** miután megérkeztek a rendszerbe, a navigációt saját partnerlistájuk alapján kezdhetik el, illetve megtekinthetik az elérhető (nyilvános) szobákat, a partnerlistán szereplő ismerőseik konferenciáit (amelyek szintén nyilvánosak). A szobák felhasználóival és a partnerlista szereplőivel beszélgetést kezdeményezhetnek, saját konferenciákat indítanak. A felhasználó új szobákat hozhat létre (a szobák esetleg regisztrálhatóak lehetnek).

A **partnerlista** biztosítja a fő mozgásteret, a felhasználó itt érheti el a közvetlen felvett partnereit. A partnerlistára a keresőből, a szobákból, vagy más konferenciákból kerülhetnek fel mások, ha a másik fél felvételi kérelmét elfogadják. A listán a partnerek csoportokba vannak rendezve. Ezeket a csoportokat a felhasználó maga határozza meg, és a csoportokba tartozást kénye kedve szerint változtathatja.

A **szobák** témával rendelkező közös beszélgetésre lehetőséget adó virtuális helyek, egyes közegekben csatornaként említik őket [URID]. A szobák a szerverhez kötöttek,

bizonyos feltételek mellett regisztrálhatóak (ez nem azonos a létrehozásukkal). Fő tulajdonságuk, hogy alapértelmezés szerint bárki számára nyitottak, a nevük a létrehozáskor határozhatja meg az alapító, utána a későbbiekben nem (habár nyithat egy új szobát azon a néven). A szobák hierarchikus rendszerbe szervezettek, azaz szobákon belül további szobák nyithatóak. A neveik egyedileg azonosítják magukat a hierarchiaszinteken belül, de globálisan szemlélve lehetnek azonos nevű szobák.

A **konferenciák** hasonlóak a szobákhoz, de inkább ideiglenes, egymást ismerő felhasználók közös beszélgetéseiként tekinthetünk rájuk. Nem listázhatóak globálisan, s mivel az alapítójukhoz kötöttek, azok tekinthetik meg a nyilvános konferenciákat, akik az alapítót felvették a partnerlistájukra. A konferenciát az alapító elmentheti később magának, hogy később újra aktiválhassa azt, és egyből meghívja az eredeti tagokat is. A konferencia neve változtatható, s egyedisége csak az alapítónál szükséges – azaz két ugyanolyan nevű konferencia egy felhasználónál nem lehet, de kettőnél már igen. A konferenciák egyszintű, nem hierarchikus rendszerben szerepelnek.

A **párbeszéd** a konferencia egy speciális – kétszereplős – alesete. Kevesebb attribútuma van, és a későbbiekben bármikor „átalakítható” szobává, konferenciává. Ezekkel a lehetőségekkel később foglalkozunk.

4.5.1.3. Részletes tulajdonságok

4.5.1.3.1. Felhasználó

A felhasználó adatait a szerver egy ún. útlevélben[30] tárolja. A sikeres bejelentkezés után a felhasználó hozzáférhet az útleveléhez (az azonosítás az útlevél alapján történik). Az útlevél részeit az alábbi vázlat szemlélteti:

- ***Útlevél***
  - **Bejelentkezési adatok**
    - A regisztrált pszeudonim fedőnév és jelszó.
  - **„Bűnügyi” előélet**
    - Nem nézheti meg senki, kivéve a felhasználó maga (és esetleg pár szolgáltatás szintű operátor), de szűrő feltételek felállíthatóak rá, például a szobák látogatóinak szűréséhez.
  - **Profilok**
    - A profilfelépítéssel és –kezeléssel részletesebben a RBP részben foglalkozunk.
  - **Partnerlista**
  - **Szobalista**
    - Belépés után automatikusan meglátogatott szobák.
  - **Konferencialista**
    - Az útlevélbe a felhasználó elmenthet konferenciákat, hogy azokat később bármikor meghívhassa.
  - **Egyéb tárolandó dolgok** (például állapot lista)

[30] Az angol szaknyelvben passport-ként emlegetik.

4.5.1.3.1.1. A felhasználók „bűnügyi” előélete

A „bűnügyi” előélet tartalmazza a felhasználó összes olyan cselekedetéért kapott figyelmeztetést, jelzést, címkét, amely befolyásolhatja a felhasználók iránta táplált bizalmát.

Eléggé el lehet bonyolítani ennek a rekordnak a kezelését – a tervezés során igyekeztünk itt is a lehető legegyszerűbb módszereket, megoldásokat használni, ezért az olyan lehetőségeket, mint például a SPAM (-mer) megjelölés elleni fellebbezés, elvetettünk. Az alábbiakban a szerintünk letisztult, egyszerű változat szerepel, amely használható, de használata nem megy a szolgáltatás használati élvezetének rovására.

- **„Bűnügyi” előélet**
  - *SPAM üzenetek detektálása*: a szerver, ha ilyet detektál, növeli eggyel ezt az értéket.
  - *Globálisan kicserélt üzenetek*: a kifejezés-cserék száma.
  - *Címkefelhő*: a szolgáltatást felügyelő operátorok megcímkézhetnek felhasználókat. A címkék számlálóval is tudnak rendelkezni, amelyeknél az utolsó növelés dátuma is szerepel.
  - *Kirúgások*: a felhasználót hányszor rúgták ki helyiségekből.
  - *Tiltások*: a helyiségekből való kitiltások száma.
  - *Operátori figyelmeztetések*: a felhasználót hányszor figyelmeztették operátorok szobákban.

Az SPAM és kifejezéscsere mezők a legérdekesebbek, hiszen ezek nem hamisíthatóak meg, ténylegesen a felhasználón múlik, hogy hány ilyen figyelmeztetése van (eltekintve néhány hibás negatív találattól a szűrőrendszerben). A kirúgások, tiltások, operátori figyelmeztetések száma korlátozott mértékben, de manipulálható, ezért óvatosabban kell bánni ezekkel az attribútumokkal.

4.5.1.3.1.2. Ki kap amnesztiát?

A bűnügyi előélet minden értékét dátumhoz kötötten célszerű archiválni. Ennek ellenére jó lehet, ha a számlálók nem csak hízni tudnak, hanem néha csökken az értékük, vagy nullázódnak. Mindenképp olyan megoldásra van szükség, amit legfeljebb csak a szolgáltatás szintű operátorok tudnak módosítani, de annak befolyásolására más felhasználók nincsenek hatással.

A kritériumnak megfelelően célravezető eszköznek tűnik az időnkénti csökkentés. Szerintünk nagyobb időközönként (például kéthavonta) érdemes csökkenteni, de akkor bizonyos érték felett csökkenteni, alatta pedig tiszta lapot adni. Például 10 figyelmeztetés felett kéthavonta 2-vel csökkentjük az értéket, de ha alá csökken, amnesztiát adunk. Ugyanez kombinálható az utolsó figyelmeztetés dátumával is. Bonyolultabb rendszerek is kidolgozhatóak lehetnének részletesebb statisztikával, például a „bűnözési” hajlam csökkenésének figyelembevételével („jó magaviselet”) – ez történhet például az archívum alapján. A legjobb megoldást valószínűleg empirikus tapasztalati értékek fogják majd meghatározni.

A címkék eltávolítását csak szolgáltatás szintű operátorok végezhetik, de az időnkénti amnesztia vonatkozhat a címkékre is (az utolsó címkézést és annak

dátumát így nem lehet elveszíteni, azaz a címke maga időnkénti amnesztiával nem veszhet el).

4.5.1.3.2. Szobák és konferenciák

A szobáknak és konferenciáknak az alapvető tulajdonságaik és lehetőségeik hasonlóak, ezért a közös jellemvonásokat összevonva tárgyaljuk. Láthatjuk a közös tulajdonságok alapján, hogy a szerver nem csak a szobák, hanem a konferenciák esetén is végez szűrést, bár ez nem lenne egyértelmű. A közös üzenetszűrésen kívül a felhasználók saját szűrési mechanizmusokat is beiktathatnak, de ezzel egy másik fejezet foglalkozik.

A szobákat keresőben lehet fellelni, illetve ki lehet listázni a fellelhető összes nyilvános szobát. Az elérhető konferenciák is listázhatóak, de csak azok nyilvánosak, amelyekben a partnerlistán szereplő barátaink részt vesznek, és ők is alapították.

A konferenciák csak nem perzisztens állapotúak lehetnek. Ha a konferencia alapítója kilép, akkor a konferencia is megszűnik. Emellett az alapító elmentheti a konferenciát, így később is meghívhatja, ekkor a konferencia attribútumai is elmentésre kerülnek. A szobák ellenben a konferenciával lehetnek perzisztensek és nem perzisztensek is. A perzisztens szobákat regisztrálni kell a szolgáltatásban. Ekkor a szoba attribútumai adatbázisban tároltak és az alapító tag személye kötött. A nem perzisztens szobák esetén a szoba attribútumai (és például az alapító tag személye, vagy a besorolási listák) addig élnek, amíg az utolsó látogató ki nem lép a szobából[31]. Ha az utolsó látogató kilép, akkor a szoba attribútumai elvesznek (kivéve, ha van benne olyan szoba, amelyben van látogató).

A konferenciák egyszintű rendszerben szerepelnek, ahol a legfelső központi elem maga a felhasználó, a konferenciák hozzá köthetőek. A szobák a szolgáltatáshoz tartoznak (a szolgáltatás részei, s nem egy felhasználóhoz köthetőek), faszerű hierarchiába szervezhetőek. A hierarchiában bárki, bármely szobában létrehozhat szobát, s annak a tulajdonosa ő lesz, továbbá tulajdonosi joggal bír a hierarchiában felette lévő összes szoba minden tulajdonosa is (egy szobának egy tulajdonosa lehet egyszerre, s ez a jog átruházható, de nem sokszorosítható). Egy szoba akkor regisztrálható, ha vagy a legfelső szinten van, vagy a felette lévő minden szint szobái regisztráltak. Annak a szobának a tulajdonosa intézi a regisztrációt, amelybe regisztrálni szeretnék, majd átadja a tulajdonosi jogot. A címkefelhő öröklődik a hierarchiában, csak további címkékkel egészíthető ki a címkefelhő.

Az alábbiakban a szobák és konferenciák közös tulajdonságait tekintjük át.

- **Általános**
  - *Név*
  - *Mottó = téma (topic)*
  - *URL*
  - *Leírás*

[31] Így amíg vannak a szobában, addig az alapító akár ki is léphet, mikor pedig visszatér, automatikusan megkapja a neki járó jogokat.

- *Címkefelhő (tagek)*
- *Alapító (tulajdonos személye)*

- **Szűrés**
  - *Üzenetküldési limit*
    - gyakoriság
    - méret
    - áteresztőképesség
  - *Akció limit*
    - *Belépés*
      - gyakoriság
    - *Fájlterjesztés*
      - gyakoriság
      - méret
      - kiterjesztés
    - *Kopogás*
      - gyakoriság
- **Privacy**
  - *Anonim hozzászólás engedélyezése*
  - *Lakat*: a belépési lehetőség lezárul, kivétel nincs.
  - *Privát*: nem szerepel listázásban.
  - *Kulcsos:* egy jelszó ismerete szükséges a látogatásához.
  - *Meghívásos:* belépés csak meghívással.
  - *Moderált:* csak az szólalhat meg, akinek engedélyezik külön.
  - *Kopogás*: meghívásért, vagy a kulcsért be lehet kopogni, a bent lévők ezt a közösben érzékelik (ha nyilvános a közös beszélgetés).
  - *Spam-szűrő engedélyezése* (szerveroldali)
  - *Kifejezéscsere lista használata* (szerveroldali, a témakörök az attribútumok között állíthatóak)
  - *Tartalomszűrés a beérkező üzenetekre* (szerveroldali)
  - *A névlista a helységen kívülről is elérhető*
  - *Bekiabálás engedélyezése*: nem tagok küldhetnek-e hozzászólást
  - *Fájlterjesztés engedélyezése*
  - *Az attribútumokat csak kiemelt személyek módosíthatják*: címkék és mottó
  - *Szűrés felhasználókra előéletük alapján*
  - *Figyelmeztetések összegyűlése esetén alapértelmezett műveletek:* ha a felhasználót adott számú alkalommal figyelmeztették egy ottléti viszony alatt egy helyiségben, a kijelölt műveletek hajtódnak végre (például kirúgás és tiltás, mellőzés)
- **„Halmazok”**
  - *Operátorok*: ők szerezhetnek kiemelt jogokat.
  - *Kivételek*: nem érvényes rájuk a kulcsos lezárás, meghívás kötelezettség, moderáltság, csak ha lakattal zárt a szoba.
  - *Kitiltottak*: nem léphetnek be
  - *Mellőzöttek:* csak olvashat, de nem szólalhat meg, akciókat sem küldhet be
  - *Beszédjogúak*: megszólalhatnak akkor is, ha moderált a szoba
  - *Meghívást nélkülözők*

- **Szoba különleges és eltérő tulajdonságai**
  - **Általános**
    - *Név*, de állandó
    - *Belső szobák*
  - **Szűrés**
    - *Akció limit*
      - *Felhasználószám limit*: elérésekor átirányít másik szobába, vagy tiltja a belépést.
  - **Privacy**
    - *Átirányítás*: mindenkit „átlök” egy másik, paraméterként megadott szobába.
    - *Anonim olvasás engedélyezése*: lehetnek rejtett, névtelen olvasók a szobában (azaz hozzászólni nem tudnak). Kikapcsolásakor a rejtett vendégek automatikusan kikerülnek a szobából. Ha az anonim hozzászólás engedélyezett, akkor az anonim olvasók is szólhatnak a szobába.

A beállításoknak elmenthetőnek kell lennie a szerveren, ha a szoba regisztrált. Egyébként is elmenthetőek, de csak akkor aktiválódnak, ha a felhasználó hozza létre a szobát.

- **Konferencia különleges és eltérő tulajdonságai**
  - **Általános**
    - *Név*, de megváltoztatható
  - **Privacy**
    - *Bárki meghívhat*: nem csak speciális rangú résztvevők képesek más felhasználók meghívására.
    - *Láthatóság*: a tulajdonos szabályozhatja, hogy a konferenciát mely ismerősei láthatják (a szobás részen természetesen senki), alapértelmezés szerint senki.

A konferencia elmenthető a kezdeményező felhasználónál, és ő indíthatja el újra.

4.5.1.3.3. Párbeszédek

A párbeszédek speciális esetei a konferenciáknak. Csak bizonyos tulajdonságai manipulálhatóak, amíg konferenciává nem alakítják át, ezért külön tárgyaljuk, hogy mely tulajdonságokkal rendelkezhetnek.

- **Általános**
  - *Mottó*
- **Privacy**
  - *Lakat*: a párbeszéd során a lakat speciális, nem egyetlen, globálisan feloldható szemafor, hanem feloldásához mindkét félnek hozzá kell járulnia. Ha ez megtörtént, a párbeszédből többszemélyes beszélgetés transzformálható.

A beszélgetés addig nem bővíthető harmadik fél által, amíg a lakat levételébe mindkét fél bele nem egyezett. Ha ez megtörtént, a kezdeményező felhasználó

dönthet a beszélgetés nevéről, majd eldöntheti, hogy konferenciát, vagy szobát szeretne létrehozni. Az így létrejött helyiségben a kezdeményező lesz az alapító tag, majd a helyiség felveszi az alapértelmezett beállításokat.

A párbeszédek beállításai csak akkor menthetőek el, ha a partnerlistáról beszélgetett a felhasználó valakivel.

4.5.1.3.4. Alapértelmezett beállítások

Az alapértelmezett beállítások szerint a kapcsoló jellegű beállítások mind kikapcsolt állapotúak, kivéve a szerveroldali Spam szűrést, a kifejezéscsere ajánlás (aztán kliensoldalon ez később tetszés szerint átállítható) és a tartalomszűrést, amelyek be vannak kapcsolva. A listák üresek.

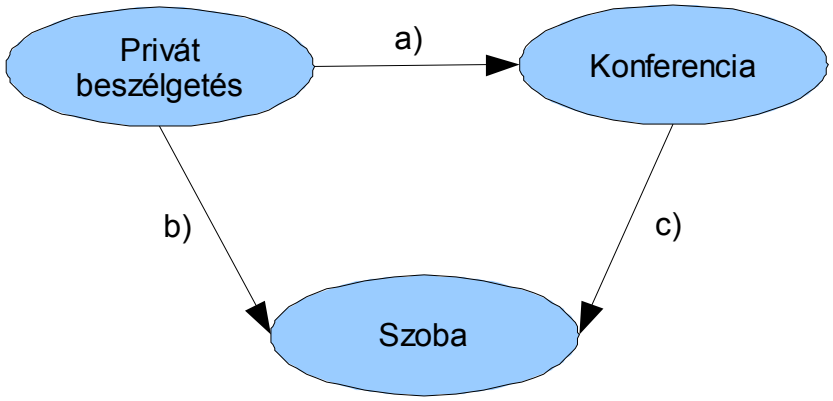
A regisztrált szobák, vagy elmentett konferenciák esetén

3. táblázat: alapértelmezett beállítások

Szoba	Konferencia	Privát
▪ *Alapító* a szoba alapítója, vagy a regisztrált tulajdonos. ▪ *Név* megadandó. ▪ Legalább egy *címke*. ▪ *Névlista kívülről is elérhető*.	▪ *Alapító* a konf. gazdája. ▪ *Név* megadandó. ▪ *Privát.* ▪ *Meghívásos, bárki meghívhat.*	▪ *Lakat*: lezárt mindkét fél részéről

4.5.1.3.5. Transzformáció a különböző kommunikációs lehetőségek közt

Az alábbi ábrán a lehetőségek közti átmeneteket szemléltetjük.



9. ábra: a kommunikációs lehetőségek közötti átmeneti lehetőségek.

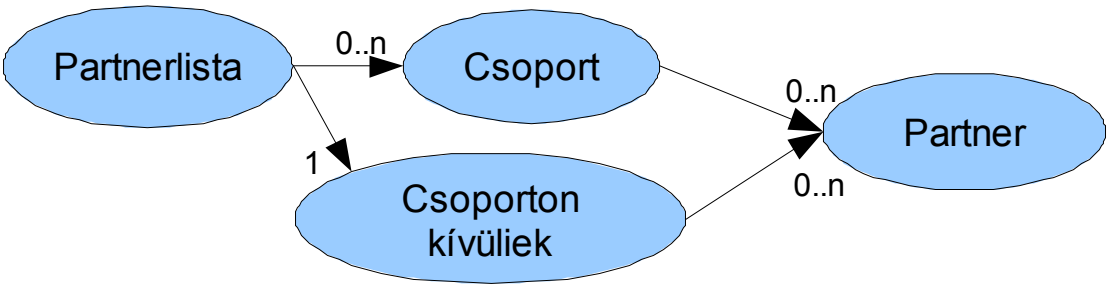
a) Ebben az esetben mindkét fél feloldotta a korlátozást (lakat), és az egyik fél kezdeményezett egy konferenciabeszélgetést egy harmadik fél meghívásával. Meg kell adnia a nevét a konferenciabeszélgetésnek (nem lehet ilyen már a kezdeményező félnél).

b) Ekkor mindkét fél feloldotta a korlátozást (lakat), és a kezdeményező fél megad egy szobanevet (ilyen nem létezhet még a szerveren), ide átkerülnek a beszélgető felek, a privát beszélgetés megszűnik.
c) A konferencia vezetője dönthet úgy, hogy szobává alakítja a konferenciát. Ekkor meg kell adnia egy olyan (szoba) nevet, ha a mostani már létezik a szerveren, amely egyedi, illetve egy címkét, ha ilyen a konferencián még nincs.

4.5.1.4. A partnerlista felépítése

A partnerlistán kivételesen a felhasználók nem lehetnek anonimek, ellenben a szobákkal, pszeudonim fedőnévvel azonosíthatóak itt (ennek a részleteivel a Role Based Privacy részben foglalkozunk bővebben).

A partnerlista szereplői és egyéb entitásai egy szigorú fastruktúrába épülnek az alábbiak szerint. Egy felhasználó a hagyományos rendszerektől (mint például [MSN]) eltérően az AnonIM rendszerében egy felhasználó logikailag csak egy csoportba tartozhat, így kerüljük a csoportok közötti keresztbe hivatkozást[32].



10. ábra: a partnerlista struktúrája.
(A partnerek legfeljebb csak egy csoportba tartozhatnak.)

A partnerlistán szereplő felhasználókra azt mondjuk, hogy kapcsolatban vannak a partnerlista tulajdonosával. Mivel a későbbiekben bizonyos esetekben feltételeket szabunk arra vonatkozóan, hogy mely felhasználók vannak kapcsolatban, így felmerül az a kérdés, hogy kinek van joga megtudni azt, hogy ki kivel áll kapcsolatban. Ha ez a lista nem is tekinthető meg direktben a feltételrendszer vizsgálatával kikövetkeztethető, ezért bár a privacy menedzsment csorbul, de lehetőséget adunk a felhasználóknak, hogy elrejtsék egyes kapcsolataikat. Egy kapcsolatot akkor már rejtettnek tekintünk, ha bármelyik fél rejteni szeretné.

[32] Ez a részlet a műveletek érvényesítésénél fontos, amellyel a Role Based Privacy fejezetben foglalkozunk.

4.5.2. Hozzáférés kezelés: Role-Based Access Control

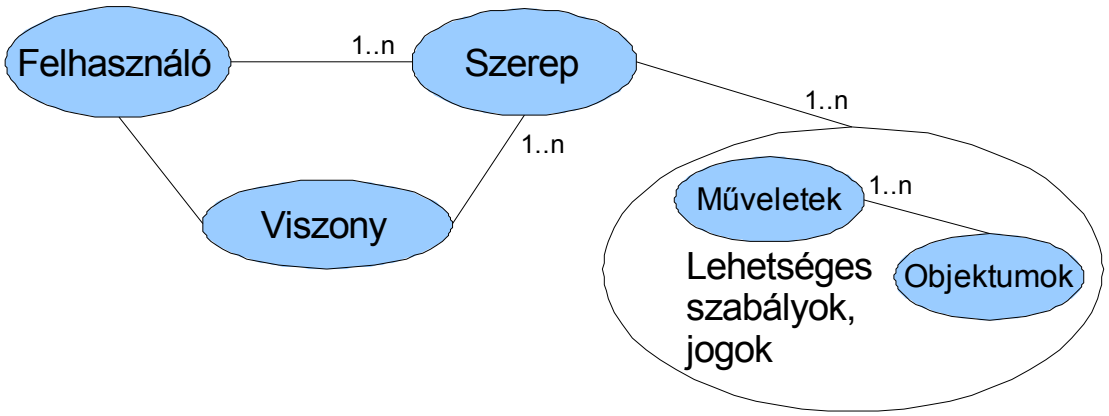
4.5.2.1. Miért kell hozzáférés szabályozás (Access Control)?

Egy elosztott, komplex számítógépes rendszerben sokfajta objektum létezik, melyek a belső modellt hivatottak reprezentálni. Az ezekkel való interakció jelenti a rendszer használatát. Az objektumokhoz számos különböző művelet rendelhető, ezek végzik a tényleges állapotváltozásokat és komplex lekérdezéseket a rendszerben, az objektumok tulajdonságai pedig a saját állapotukat tárolják.

Felmerül a kérdés, hogy egy több felhasználós (többek által konkurensen használt) programban minden felhasználó egyenrangú-e? A válasz nyilvánvalóan nemleges, ugyanis nem lenne túlságosan praktikus (és főleg nem anonim) az a rendszer, amelyben bárki bármilyen kérdésre a rendszer maximális belső tudásának megfelelő választ kap, tehát mindenki az „adminisztrátor” szerepében tényked het. Kell léteznie egy adminisztrátor szereplőnek, aki a rendszert üzemelteti és problémák esetén bármihez joga van a rendszeren belül. A normális felhasználóknak pedig, akik kívülről érkezhetnek és ismeretlenek, minimális jogokat szabad adni úgy, hogy a rendszer mindettől még használható maradjon számukra.

4.5.2.2. Az RBAC megoldása

A Role-Based Access Control [RBAC] ötlete nem új keletű, az összetett információs rendszerek fontos része az Internet hajnalától kezdve. Sőt, a UNIX operációs rendszerek már régóta hasonló megoldást használnak a fájlrendszer elemek jogosultságainak kezelésére.



11. ábra: RBAC struktúra.

Az RBAC modul feladata, hogy *nyilvántartsa a rendszer tetszőleges objektumán végezhető műveletekhez*, tulajdonságokhoz való *hozzáférést* vezérlő adatokat. A 11. ábrán látható alapstruktúrát képezzük le a saját rendszerünkre. Az ábra szerint minden objektumhoz tetszőleges mennyiségű, de legalább egy (1...n) művelet

tartozhat. A művelet/objektum párokra vonatkoznak a *lehetséges szabályok alkotta halmaz*. Ennek nem üres részhalmaza tartozhat egy adott szerephez, a szerepek közül pedig tetszőleges mennyiség lehet egy felhasználóhoz rendelve. A felhasználó itt általában egy természetes személyt jelent, aki közvetlenül használja a rendszer, de robotprogramok is ugyanilyen felhasználóként jelennének meg.

A szereplő az RBAC modellben egy szerepkört jelent, amely egy speciális funkciót végrehajtani képes jogokkal van felruházva a megfelelő szabályok által.

A felhasználóhoz lehet rendelni tetszőleges számú *szerepet*. Ennek előnye, hogy amennyiben sok hasonló hozzáférési tulajdonságokkal rendelkező felhasználó lesz, nem szükséges mindegyiknek külön-külön felvenni az összes jogát, ez túl sok ismétlődő adminisztrációval járna. Ehelyett fel lehet venni egy szerepet, annak a megfelelő jogokat, majd ezt a szerepet hozzáadni az összes hasonló felhasználó szerepköréhez.

További kapcsolódó adat a *hozzáférési szint*, mely az ábrán külön nem szerepel, ugyanis a szabályhoz tartozik. Ez egy olyan érték, mely megadja hogy az adott művelethez vagy tulajdonsághoz milyen fajta hozzáférés megengedett. Ez lehet például: semmi, olvasás, írás, végrehajtás, stb. Értelmezése tetszőleges, a jogosultság-ellenőrzés paramétereként jut szerephez.
A hozzáférési szint minden egyes szabály esetén egy halmaz, amely tetszőleges, de korlátos halmazból tartalmazhat bármennyi elemet. Ennek hiányában több szabályt kellene felvenni egy műveletre (vagy tulajdonságra), egyet például írási jognak, egyet olvasási jognak, így:

```
(Objektum, Művelet1_írás, Szerepkör),
(Objektum, Művelet1_olvasás, Szerepkör).
```

Ehelyett elégséges felvenni egy ilyen szabályt:

```
(Objektum, Művelet1, Szerepkör, {olvas, ír}).
```

Ez a szabályok számában jelentős megtakarítást jelent, ha sok hozzáférési szint van, ugyanakkor a halmaz megfelelő számítógépes ábrázolásával jóval gyorsabb és kezelhetőbb is egyszerre.

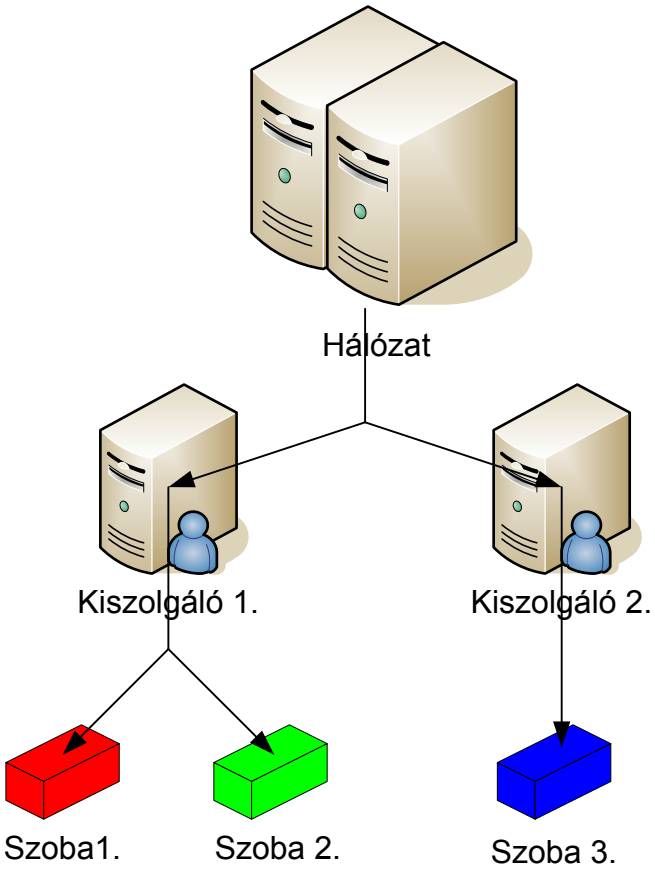
Egy művelet elvégzésének engedélye függhet még számtalan olyan dologtól, amiket nem lehet leírni egyszerű összefüggésekkel. Ezeket az összetett feltételeket az RBAC rendszeren kívül definiált programrészletek, *megkötések* (constraint) ellenőrzik majd. E megkötések tetszőleges paramétereket fogadnak, amiket felhasználva kiértékelhetik, hogy jogszerű-e a kért művelet elvégzése. Visszautasítás esetén a jogellenőrzés úgy tekinti, hogy az adott szabály nem engedélyezte a hozzáférést a kapcsolódó objektumhoz, illetve művelethez.

4.5.2.3. Hogyan épül fel a szabályok rendszere?

A rendszer objektumai gyakran *hierarchikusan egymásba ágyazottak*, ezt ki is fogjuk használni abból a célból, hogy ne minden létező objektum-szereplő párra külön

kelljen definiálni megengedő szabályt, amennyiben szükséges. Ez a jogosultságokat tároló struktúrát feleslegesen megnövelné. Ehelyett inkább számítási kapacitást feláldozva (több művelet elvégzése szükséges), egyfajta *öröklődést* definiálunk a szabályok között. Azaz, ha létezik egy konkrét szabály, akkor az sok más *szabályt implicit helyettesít*, egymagában.

Lássunk egy grafikus példát ilyenre (12. ábra: Hierarchikus objektumok)!



12. ábra: Hierarchikus objektumok.

Itt a hálózat objektum két kiszolgálót is tartalmaz, melyek rendre két, illetve egy szobát. Ha például egy rendszerszintű adminisztrátort szeretnénk felvenni, akkor nem lenne túlzottan praktikus, ha a világ összes objektumára külön kellene adni számára (illetve a szerepe számára) jogokat.

Ez a probléma azonnal megoldódik, ha a jogok öröklődnek, mert a „Hálózat” objektumnak adott jogok azonnal érvényesek lesznek a többi objektumra is, kivéve, ha azokat egy gyereknél explicit módon, tiltó szabállyal felülbíráljuk. Ennek a megoldásnak komoly komplexitás növelő hatása van, mert meg kell oldani az objektumok bejárását a gyerekek felől a szülők felé és fordítva. A jogosultságokat lekérdező algoritmus is lényegesen bonyolultabb lesz.

Másik lehetséges megoldás, ha a jogosultságok keresése közben eltekintünk a hierarchikus felépítés RBAC-ba való integrálásától, és az 2. ábrát tipikus példaként tekintve, az objektumok vízszintes osztályozásából indulunk ki. A hierarchikus rendben az egy szinten lévő (pl. közös szülőjű, nagyszülőjű) objektumok nagy

valószínűséggel egyfajták, azaz egy osztályba tartoznak. Az osztályozás természetesen tetszőleges is lehet, ezáltal igen rugalmas rendszer alakítható ki. Végül az egy osztályba tartozó objektumokhoz rendelhetünk az egész osztályra vonatkozó szabályt, amit bármikor felülbírálhat egy konkrét objektumra vonatkozó.

4.5.2.4. Az RBAC használata

Az RBAC nem más, mint az eddig leírtak szerint működő *összetett táblázatos struktúra*, melyen szerteágazó lekérdező és módosító műveletek képzelhetők el. Így jogosan felvetődik a kérdés, hogy az RBAC objektum módosítását nem kell-e szabályokhoz kötni? Elképzeléseink szerint nem, ugyanis ez az objektum nincs kitéve a felhasználók hozzáféréseinek közvetlenül, szigorúan a rendszerünk belső részének tekinthető.

Ily módon kizárólag *közvetett módon* nyúlnak hozzá a kliensek, például az RBAC lekérdezések használatával minden egyes kívülről elérhető objektummal végzett műveletnél. Különleges esetekben RBAC módosításokat is generálhat egy felhasználói beavatkozás. Erre példa egy szoba, konferencia létrehozása.

4.5.2.5. Konkrét műveletek jogköre

Rendszerünk belső világ modell című fejezetében hivatkoztunk a világ objektumainak műveleteire vonatkozó alapvető jogokra. Az alábbiakban áttekintjük a jogokat konferencia, szoba objektumra.

1. *Résztvevő besorolás megváltoztatása*: a beszélgetés résztvevőinek (egy identitás, ez nem okoz problémát, ugyanis egy szobában, konferenciában minden felhasználó egyetlen identitással rendelkezhet) az adott konferenciára, szobára nézve rendelkeznek egy tulajdonsággal, amely alapján előre definiáltan kapnak jogokat a szobával kapcsolatos műveletekhez. Ezek a szintek a

    - *Tiltott:* nem lehet a szobában, nem léphet be (ez ellentmondásnak tűnik azzal, hogy a beszélgetés résztvevője, ezért tekintsük potenciális résztvevőnek);
    - *Hallgató:* jelen lehet, de nem írhat semmilyen körülmények között;
    - *Normál:* írhat, amennyiben a szoba, konferencia nem *moderált* állapotú;
    - *Beszélő:* minden esetben írhat;
    - *Moderátor:* a nálánál kisebb besorolású felhasználók besorolását maximum „*beszélő”* szintig megváltoztathatja.
    - *Operátor:* a nálánál kisebb besorolású felhasználók besorolását maximum *moderátorig* megváltoztathatja, és rendelkezik magasabb szintű jogokkal, de a kritikus adminisztrátori jogokkal nem.
    - *Szoba adminisztrátor:* az összes felhasználó besorolását tetszőlegesen megváltoztathatja, és a szoba, konferencia minden műveletét végrehajthatja. A saját adminisztrátori voltát kizárólag valaki másnak átadhatja, így mindig összesen egy adminisztrátora lehet egy szobának. Hivatkozásul megjegyzem, hogy a *belső világ modell szereplői* fejezetben

leírtak szerint egy szoba a hierarchiában felsőbb szintű szobáinak adminisztrátorait is örökli.

Ezen kívül fontos, hogy minden résztvevő a saját besorolását bármikor a pillanatnyiról kisebbre állíthatja.

2. *Résztvevő figyelmeztetés*: egy darabbal növeli a résztvevő figyelmeztetéseinek számát. Moderátor vagy annál magasabb besorolás szükséges.
3. *Résztvevő figyelmeztetések törlése*: törli a résztvevő összes e szobában kiállított figyelmeztetését. Moderátor vagy annál magasabb besorolás szükséges.
4. *Automatikus meghívottak szerkesztése*: felvétel, törlés az automatikus meghívottak listáján. Operátor vagy magasabb besorolás szükséges.
5. *Kivételek szerkesztése*: felvétel, törlés a kivételek listáján. Szoba, konferencia adminisztrátor besorolás szükséges.
6. *Névlista lekérdezése*: minimum *hallgató* besorolás, kivéve ha kifejezetten titkos a szoba, olyankor további korlátozások lehetnek (kivételek listáján, automatikus meghívottak listáján való szereplés).
7. *Adatlap lekérdezése*: ugyanaz mint a névlista lekérdezésénél.
8. *Belépés*: minimum *hallgató* besorolás.
9. *Kopogás*: ugyanaz mint a belépésnél.
10. *Bekiabálás*: minimum *hallgató* besorolás, illetve engedélyezett a bekiabálás.

További példák szabályokra az [RBRM] mellékletben találhatóak, táblázatos formában.

4.5.3. Anonimitás Role-Based Privacy alapokon

A Role-Based Privacy alapelve, hogy a szolgáltatást igénybe vevő felhasználó különböző szerepeket vehet fel, és a szerepek megfelelő kezelésével tudja meghatározni, hogy a többi szereplő milyen képpel rendelkezik róla. Ennek a szerepkezelésnek a célja, hogy a felhasználó – a rendszer lehetőségeivel mérve – teljes önállósággal szabályozhassa a magánszféráját, azaz, hogy milyen információk jelennek meg róla és mely entitások tudják őt elérni.

4.5.3.1. Az RBP alkalmazása csevegő szolgáltatásokban

Az RBP módszert a csevegő szolgáltatás konstrukciójában profilok segítségével valósítjuk meg. A felhasználó szabályozhatja a többiek felé mutatott profilokat, segítségükkel tetszőlegesen megvalósíthatja az általa elképzelt nézetet. A profilok segítségével megvalósítható az anonimitás, akár egy időben több pszeudonim fedőnévvel is, amelyet a felhasználó több irányba mutat.

A profilok használatának nehézségét csevegő szolgáltatásokban és azonnali üzenetküldőkben a szereplők közötti sűrű kapcsolatrendszer és az erősen interaktív közegek, kapcsolatok okozzák, hiszen a szereplők könnyen kompromittálhatják egymás álcáit, identitások mögé bújását, tehát a műveletek alkalmazása mellett

figyelni kell arra is, hogy minden nézőpont szempontjából jól vegye fel az új (és esetleg anonim) identitását a szereplő.

4.5.3.2. A rendszer elemei

4.5.3.2.1. Profilok

A felhasználónak a nézetét a profil írja le. A profil tartalmazza például a felhasználó állapotát, képét, nevét és még további információkat, amelyek jellemzik a felhasználót. A szerepek befolyásolása a profil módosításával lehetséges és különféle profilok alkalmazása más felhasználók, felhasználó csoportok és bizonyos relációban szereplő felhasználók felé. A felhasználó profil által azonosított nézetét identitásnak nevezzük, noha az identitások a profil változtatásával nem mindig változtathatóak, ekkor egyszerűen álcázásról beszélünk.

A profilok dinamikus, valós idejű változtatását két műveletre lehet felhasználni, álcázásra és új identitás felvételére. Az utóbbira csak a szobás, chat jellegű részen van lehetőség, ugyanis ahogy korábban említettük, a felhasználó a partnerlistán csak pszeudonim lehet, anonim nem, ugyanis a neve mellett megjelenik a regisztrációs azonosító. Azért döntöttünk ez a megoldás mellett, mivel a névlisták a teljes anonimitás lehetősége mellett elvesztenék jelentősségüket, ugyanis a névlista nem lenne csoportokba rendezhető, és tipikusan káosz uralkodna az ott lévő felhasználók között. Így ugyan a felhasználó nagy szabadsággal rendelkezik a partnerlistáján az identitásváltoztatással kapcsolatban, hiszen „személyre szabható” álcákat is készíthet.

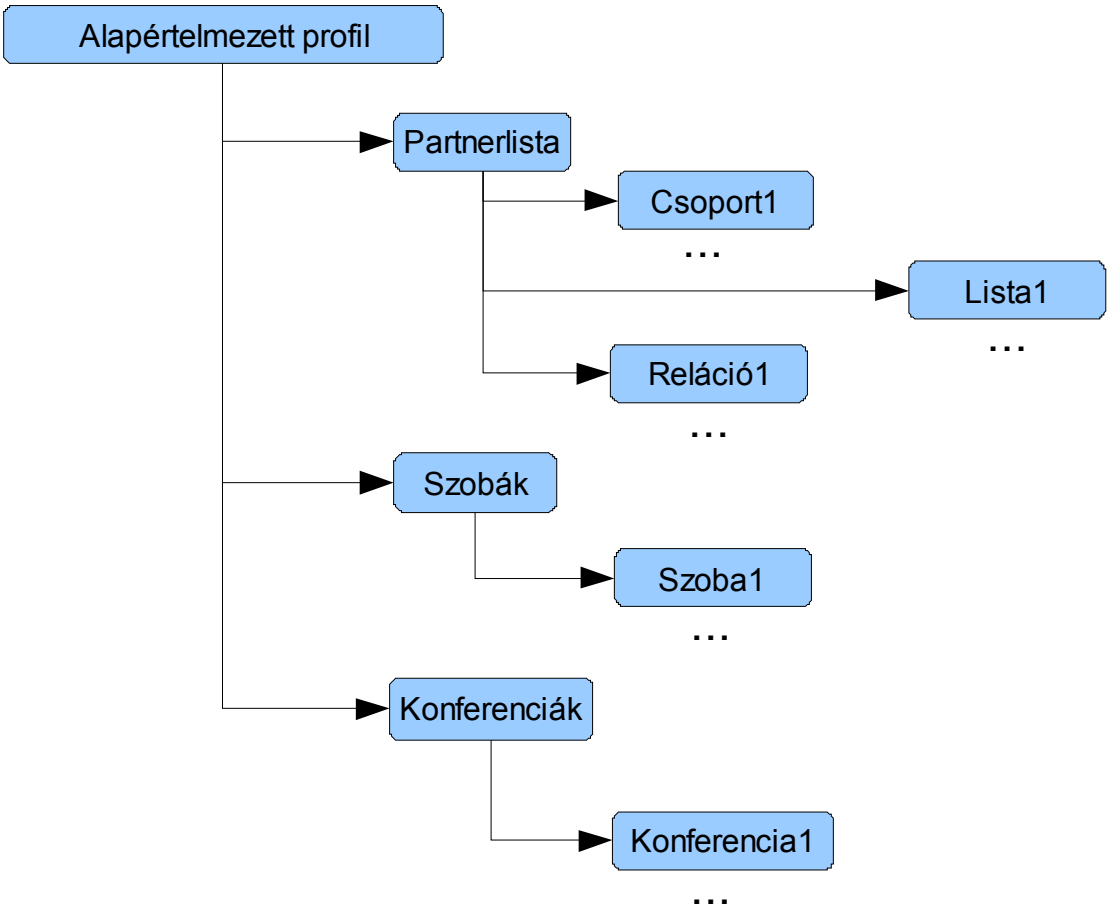
A szobákban és konferenciákban a felhasználó egy időben legfeljebb egy identitással tartózkodhat. Identitásváltáskor lehet kettő is, esetleg több, de ezek közül mindig legfeljebb csak egy felett rendelkezhet, a többi identitás ideiglenes, nem interaktív, az identitásváltás átvezetéséhez szükséges. Ha engedélyezzük több azonos helyiségben lévő identitás egyidejű vezérlését, az a felhasználó megzavarásához vezethet, továbbá egyéb problémákat vet fel, például a jogkezeléssel, kirúgással, kitiltással kapcsolatban. Ugyanis ezekben az esetekben az identitásra alkalmazott műveletet a többi kapcsolódó identitásra is alkalmazni kéne, ami kompromittálná az érintett identitásokkal rendelkező felhasználót. Ha ezzel nem törődnénk, akkor viszont a műveletet nem lehetne érdemben végrehajtani, mivel például kirúgás esetén a nem kívánatos felhasználó tetszőleges identitásai benn maradnának a helyiségben.

Kezdetekben a következő profilok léteznek, és ezek teljesen egyenlők:

- *Alapértelmezett profil*: névlistára, szobás részre, konferenciákra. Ez tovább osztható a felhasználók szerinti profil testre szabásával.
- *Off-line profil*: ha a felhasználó elhagyja a rendszert, vagy rejtett állapotban van jelen, ez a profil látható.
- *Egyéb profil*: globális névlistában és keresőkben mutatott profil.

Ezeket és a többi profilt az útlevélben tároljuk. A profil által megvalósított (virtuális) „felhasználóra” a továbbiakban identitásként is hivatkozunk.

Az alapértelmezett profil az alábbi hierarchia szerint öröklődik. Ha a fa struktúrában bárhol megváltoztatunk egy profilt, vagy egy identitást, akkor minden olyan elem örökli, ahol még nem adtunk meg mást. Ha már megadtunk egy másikat, akkor az az ág nem örökli tovább. A hierarchiába további elemek felvehetőek, illetve automatikusan fel is kerülnek (például egy szoba meglátogatásával).



13. ábra: a profilok öröklési hierarchiája.

4.5.3.2.2. Alapműveletek

Az alapműveletek segítségével valósítható meg a kívánt privacy szint. A különféle kontextusokon belüli értelmezésre később térünk ki, itt a műveletek mögötti alapvető elgondolást ismertetjük.

- *Mellőzés*: a mellőzött partner üzeneteit nem képes eljuttatni a mellőző félhez, de láthatja a profilját.
- *Tiltás*: a letiltott partner számára nem elérhető a felhasználó állapota, nem látja a valós profiljának az adatait, és nem tud üzeneteket küldeni neki – számára ő rejtett állapotban van.
- *Álca, identitásváltás*: a profil módosításával, új profil speciális bevezetésével a felhasználó hamis állapotot mutathat mások felé, illetve kiegészítő módszerek alkalmazásával identitást válthat, ezzel elérve az anonimitást.

- *Felfedés*: Egy másik, ismert profil felfedése, az előbbinek az ellentétes művelete, azaz egy felhasználónak így kivételező módon meg lehet mutatni a látott profil mögötti valódi identitást.
- *Engedélyezés*: A tiltást és mellőzést feloldó művelet.

4.5.3.2.3. Felhasználók kijelölésének időtartama

Ugyan a kijelöléseknek az időtartamát meghatározza, hogy meddig érvényes, de bizonyos kontextusokban ez felülbírálható. Ezt külön jelezzük.

- *Ideiglenes*: a következő viszony elindításáig él. Ekkor még meghosszabbítható a viszony idejére, illetve a következő valahány viszony idejére.
- *Végleges:* a kijelölés örökéletű, a felhasználói visszavonásig érvényes.

4.5.3.3. Az RBP rendszer alkalmazása

4.5.3.3.1. Egy egyszerűsített rendszer

Ha általánosságban alkalmaznánk egy ilyen a rendszert, azaz minden kontextusban minden alapművelet mindenkire, minden elképzelhető relációra értelmezhető lenne, akkor a felhasználó szemszögéből nézve túlságosan bonyolult rendszert kapnánk, amely a kezelhetőségnek erősen a rovására menne. Így egy kissé egyszerűsített rendszert alkalmazunk, amely egyszerűsíti a felhasználó elé tárt nyitott helyzeteket, ugyanakkor korlátozza a döntési szabadságban.

További problémát jelentene bizonyos műveletek értelmezése egyes kontextusokban, mint például a tiltás művelet értelmezése egyetlen partnerre egy szobában. Ugyanis ebben az esetben elegendő lenne a felhasználónak mindenkit letiltani, hogy ott rejtőzködve tartózkodhasson.

4.5.3.3.2. Ellentmondás a két fél privacy szempontjai között

Az egyéni és listás megjelölés esetén a következő kérdés merül fel: a felhasználókat miképp jelöljük meg, amikor a művelet alkalmazzuk rájuk? Itt ütközik a két fél érdeke: a megjelölő felhasználó szeretné úgy megjelölni a másikat, hogy az akkor is vonatkozzon rá, ha identitást vált. Ellenben a megjelölendő fél szempontja, hogy továbbiakban is képes legyen az identitását úgy változtatni, hogy az újra semmilyen korlátozás ne vonatkozzon.

Véleményünk szerint jobb, ha globális jelöléssel azonosítják ilyenkor a felhasználót, ekkor érvényesül a felhasználónak a magánszférája feletti önrendelkezése, a célponté kevésbé csorbul. Ellenkező esetben ugyan a célpont teljességgel rendelkezhet identitása felett, de a magánszféra védelmi eszközök teljesen értelmetlenné válnak. A pontos alkalmazást az alábbiakban, esetekre szétbontva vázoljuk fel.

4.5.3.3.3. Kapcsolatok titkossága

Sok múlik azon, hogy rejtőzéskor, álcázáskor ismert-e a kapcsolatrendszer. Úgy is lehet mondani, hogy a felhasználó akkor tud élni a privacy nyújtotta lehetőségeivel teljes körűen, ha minden kapcsolatot ismer. Ez azonban mások privacy-vel kapcsolatos érdekeivel mond ellent, ugyanis mások nem feltétlenül szeretnének minden kapcsolatot felfedni. Ezért vezettük be, hogy a partnerlistás kapcsolatok elrejthetőek. További indok, hogy a chat jellegű részben a kapcsolatok úgyis eltitkolhatóak az identitások változtatásával, és ezzel a problémával foglalkozni kell, nem okoz hátrányt, ha bevezetjük a lehetőséget a névlistás részen is.

4.5.3.4. Általános problémák az RBP alkalmazásakor

4.5.3.4.1. Név egyedisége

Chat jellegű szolgáltatásokban a szolgáltatáson belül minden név egyedi, nem lehetséges két azonos név, mert zavaró lehet. Azonnali üzenetküldő szolgáltatásokban ez általában nem probléma, ott más megkülönböztető azonosítók szerepelnek.

Egy ilyen hibrid rendszerben a rendszerek szétválásának megfelelően érdemes szétszedni a megoldásokat. *Névlistán* egy egyedi azonosítót is kell a felhasználóhoz rendelni, hogy ha a nevét változtatja, azonosítható legyen, mivel tetszőleges felhasználók nem kerülhetnek a névlistára, ezért egyértelmű kik lehetnek anonim szereplők ott – így itt a felhasználók egyedi azonosítása megengedett (de ez az RBP használatát nem csorbítja). Az egyedi azonosító a felhasználónév, amelyet a belépéskor kell használni.

A többes beszélgetések szétválnak, a megoldások nem hasonlóak. *Szobák* esetén nem szükséges az azonosító, a felhasználó lehet névtelen, teljesen anonim is. Ez esetben azonban garantálni kell, hogy a szobás, azaz chat jellegű szolgáltatásrész összes felhasználójának egyedi neve legyen. Meg lehetne engedni, hogy szobánként legyenek csak egyediek a nevek, azonban a korábbi rendszerekhez hasonlóan ez itt is zavaró tényező lenne.

A többszereplős beszélgetések másik formájában, a *konferenciák* esetén a helyzet jóval bonyolultabb, hiszen itt jelen lehetnek felhasználók különböző szobákból, a partnerlistáról, illetve olyan felhasználók is részt vehetnek ilyen beszélgetésben, akik egyik helyhez sem köthetőek. Természetesen ez a szobákra is igaz lehet, de a szobák kötöttsége miatt nem jelent akkora problémát – sokkal gyakoribb eset lehet, hogy egy konferenciabeszélgetésben az említetthez hasonlóan megosztott társaság verbuválódik össze. Ilyenkor kérdéses, hogy szükséges –e megjelölni egyedi azonosítóval a felhasználókat, illetve milyen méretekben lehet szükséges nézni az egyediséget a neveknél. Az egyedi megjelölést minden felhasználónál kötelezővé tesszük, így a név egyedisége a konferenciák esetén nem jelent problémát. Ezzel a megoldással a konferenciák kissé személyesebbé válnak, illetve így a nagyméretű

konferenciákból inkább szobák fognak alakulni. Fontos kitételként megemlítjük, hogy a párbeszédek esetén a regisztrációs azonosító csak akkor jelenik meg, ha azt a másik fél már korábban is ismerte – így szobákon belül privát beszélgetések indításával nem deríthető ki.

4.5.3.4.2. Megszemélyesítés

Ha a profilok tetszőlegesen változtathatóak, a felhasználók jól használt neveiket eldobva felszabadítják azokat, és így mások számára elérhetővé válik. Ha mások ezeket a neveket felveszik, akkor megszemélyesíthetik az illetőt. Ezért biztosítani kell, hogy a felhasználók néhány nevet regisztrálhassanak maguknak, és így azokat csak az ő útlevelükkel lehessen igénybe venni.

4.5.3.4.3. Névcsere a felhasználói ügyetlenségek ellen

Hogy ne hasson ösztönzőleg a felfedett profil a mások előtti felfedés irányába, ezért nem közvetlen a valós profilt jeleníti meg a program. A felhasználó a felfedetlen profilt (és a beállított nevet, stb.) látja alapértelmezés szerint, a felfedésre utaló ikon ott villog a neve mellett, megnézheti az eredeti profilt. Mivel nem az eredeti nevet látja, így például a több szereplős beszélgetésekben (konferenciában, szobában) nem ösztönző jellegű a név a véletlen, emberi hibából való felfedésre.

Ezen túl a felhasználók megadhatnak egy helyen (mondjuk a passportban) olyan álneveket, beceneveket (akár reguláris kifejezéssel is), amelyeket ha más netán beírna, akkor az kicserélődjék a valós névre. Ez természetesen csak felfedett felhasználóknál működik, és mivel kliensoldali, ezért kikapcsolható.

4.5.3.5. A rendszer működése alapjaiban tekintve

4.5.3.5.1. A névlistán

Ebben az esetben a működés egyszerű, az alapműveleteket és a kijelölést ismertető fejezetekben leírtak alapján működik. A felhasználók egyértelműen megjelölhetőek, hiszen a felhasználók csak álcázásra képesek, identitásváltásra nem az őket megjelölő regisztrációs azonosító miatt.

A felhasználók az alábbi módon választhatóak ki a névlistából:

- *Listával*: felhasználók listába fűzve szerepelnek egy művelet célpontjaként.
- *Egyénileg*: az egyéni megjelölés csak egy speciális, egyelemű lista.
- *Közös ismerősök reláció:* Azon ismerősök csoportja, amely a parancs használójával és a kijelölt személlyel közös kapcsolattal rendelkezik. A listára a felkerülés automatikus. Ha egy felhasználóra már nem teljesül a reláció, ezt jelezni kell, de automatikusan nem kerülhet le a listáról, máskülönben a kapcsolat elrejtésével kompromittálható a művelet.
- *Csoport:* A névlista bizonyos csoportjára vonatkozik, ezeket a csoportokat kizárólag a felhasználó kezeli.

A fenti megjelölések, azaz a lista, közös ismerősök reláció és a csoport között értelmezni kell egy prioritási sorrendet. A sorrend határozza meg, hogy ha egy felhasználóra több nézet is érvényes, akkor melyiket alkalmazzuk, ugyanis ezek közül csak egy lehet érvényes. A legfontosabbak a listák, hiszen ezek explicit módon a felhasználó akaratát jelölik (a kívánt szerep szempontjából), és nem befolyásolhatóak, mint például a közös ismerősök reláció. Ez utóbbi, például, akkor változhat, ha egy, a relációban lévő felhasználó és a reláció alanyaként szereplő felhasználó elrejti a kapcsolatát. A partnerlistás csoportok viszont ugyan nem befolyásolhatóak, de ezek kissé más szemléletet követnek, mint az eddigi csoportok.

A felsorolt szempontok alapján a

```
csoport < közös ismerősök reláció < lista
```

prioritást határozzuk meg (balról jobbra nő a prioritás).

4.5.3.5.2. Szobákban

Szobákban a műveleteket alapértelmezés szerint csak a szoba egészére lehet alkalmazni, egyénileg csak a mellőzés (és engedélyezés) és felfedés műveleteket lehet. Az alapműveletek részletes magyarázatánál a gyökérprofil a chat jellegű szobás résznek a legfelső szintű idevonatkozó profilja; alapértelmezés szerint a szolgáltatásban ezzel a profillal van jelen a résztvevő. Bár a szobák hierarchikusan rendezkednek el, a felhasználó által megnyitott szobák profiljai függetlenek, és legfeljebb a chat jellegű rész profiljától függenek.

- *Mellőzés*:
  - A mellőzést felhasználókra, pontosabban azok identitásaikra értelmezzük, ha a felhasználó identitást vált, a mellőzés újra felbomlik. Ez esetben a szoba közös beszélgetésében mellőzött a felhasználó.
  - Azonban globális megjelölést is kaphat a felhasználó – privát üzeneteket ez után nem tud küldeni[33].
- *Tiltás*:
  - A tiltás művelet esetében, ha lehetőség van rá, a felhasználó rejtett módba kerül, s a neve nem lesz látható. Ekkor, ha engedélyezett, anonim módon szólalhat csak meg.
  - Egyéb esetben a tiltás művelet kiváltója a szoba elhagyása lehet.
- *Álca*:
  - A felhasználó álcát vesz, azaz megváltoztatja a profilját a szoba felé, s így a bent lévők ezen túl azt érik el.
  - A felhasználó identitását másikra cseréli. Ez különböző módokon történhet, az alábbiakban felsorakoztatunk pár példát:
    - A felhasználó megad egy elköszönő üzenetet, majd belép új identitásával. Időzítés szerint elköszön a régi identitás, és kilép.

[33] A szerzők véleménye szerint ez egy jó kompromisszum a két fél magánszféráját érintő kérdések között. Célszerű a valós rendszert tovább bonyolítani azzal, hogy az ilyen jellegű tiltásokat csak bizonyos időre tesszük elérhetővé, például legfeljebb egy napra. Meghosszabbítani akkor lehet, ha a felhasználó ismeri a mellőzött személy egy aktuális identitását (és alkalmazza azon a műveletet).

        - A felhasználó régi identitása kiesik, mintha hálózati hibáról lenne szó, majd bizonyos idő múlva, vagy akár bőven a kiesés előtt megjelenik az új identitás.
- *Felfedés*:
    - Ha a felhasználó felfedi magát az egész szoba előtt, akkor a szoba tagjai a chat jellegű részre vonatkozó profilt fogják látni[34].
    - A felhasználó bizonyos felhasználók előtt felfedheti a valós identitását.
- *Engedélyezés*: a mellőzések feloldhatók. A szobára vonatkozó és globális (privátra vonatkozó) mellőzések listája megtekinthető. Ugyanígy a rejtett állapotú felhasználó láthatóvá válhat.

4.5.3.5.3. Konferenciákban

A konferencia-kezelés egyik legsarkalatosabb kérdése, hogy az újonnan nyitott konferenciák honnan származtatják a profilt, ugyanis a konferenciákba indításukkor nem csak a partnerlistáról lehet meghívni felhasználókat, hanem különféle szobákból is. A probléma alapját képzi, hogy a különféle helyekről meghívott felek különféle identitásait látják a konferencia gazdájának. Erre ad megoldást, hogy a felhasználók látják egymás regisztrációs azonosítóját a konferenciában.

A konferenciát hasonlóan kezeljük a szobákhoz és a névlistához is, az alapműveleteket az alábbiakban értelmezzük.

- *Mellőzés*: egy felhasználó mellőzése vonatkozhat a szobáknál látott módon a közös beszélgetésre, illetve a privát üzeneteknek a küldésére is.
- *Tiltás*: mivel konferenciák esetén a rejtett mód nem lehetséges, ezért a tiltás művelet nem értelmezhető (hiszen minden konferenciabeli partner letiltásával itt is rejtőzni lehetne). A felhasználó kiválthatja azzal, hogy elhagyja a konferenciát.
- *Álca*: a felhasználó álcát vesz, azaz megváltoztatja a profilját a konferencia tagjai felé.
- *Felfedés*:
    - Ha a felhasználó felfedi magát az egész konferencia előtt, akkor a tagok a számukra természetes profilt fogják látni.
    - A felhasználó bizonyos felhasználók előtt felfedheti a valós identitását.
- *Engedélyezés*: a mellőzések feloldhatók. A konferenciára vonatkozó és globális (privátra vonatkozó) mellőzések listája megtekinthető.

4.5.3.5.4. Felhasználók operátori megjelölése konferenciákban és szobákban

Fontos kérdés, hogy ha egy operátor meg szeretne jelölni egy felhasználót egy szobában, akkor a jelölés az aktuális profilra, vagy általánosan a felhasználóra vonatkozzon (hasonló a probléma ahhoz, ha a felhasználók másokat akarnak például a szobás részen mellőzni). A jelölés lehet egy tiltás (és mellőzés), vagy listázó

[34] Az ilyen jellegű identitás felfedés történhet egyszerűen, különféle trükkös módszerek alkalmazása nélkül.

művelet például. Ez utóbbinál a kompromittáció nem jelenthet problémát, ugyanis előnyökkel járó halmazokba is lehet a felhasználókat vinni, amellyel csak akkor kompromittálódik a felhasználó, ha él a lehetőséggel.

A használhatóság rovására menne, ha csak az adott identitást lehetne megjelölni, így engedélyezzük, hogy a felhasználóra vonatkozzon a jelölés. A jelölés azonosítására egy időbélyeg és az akkori profil szolgál, így kezelhetőek a jelölések egyértelműen át is tekinthetőek. A tiltás ilyen módú alkalmazása az új identitás lebukását nem fenyegeti közvetlenül, hiszen ha nem tud belépni a felhasználó, ritkán derülhet erre fény magától, leginkább magának kell erre felhívnia a figyelmet. A mellőzés esetén könnyebben kiderül a dolog, hiszen a felhasználó nem tud megszólalni identitásváltás után sem. Úgy gondoljuk, hogy még így is megfelelő a módszer, mert fontosabb, hogy a nem kívánatos személyek eltávolíthatóak legyenek, mint hogy identitásváltással kijátszható legyen a privacy védelem.

Konferenciák esetén a felhasználó megjelölhető hiánytalanul, hiszen itt ismert a valódi identitása, a regisztrációs azonosítója által.

4.5.3.6. A rendszer működése kompromittáció vizsgálattal

Problémás lehet, ha valaki előtt új identitást akarunk bevezetni, vagy ha új álcát, hogy ha többes nézettel rendelkezik egy adott identitásra. Ilyenkor a használható módszerek és lehetőségek korlátozottak.

Célszemélyként referálunk a későbbiekben arra a felhasználóra, akin a műveletet végre szeretnénk hajtani – egy művelet alkalmazásakor több célszemély is lehetséges, s ezen személyekre függetlenül kell végrehajtani a vizsgálatot. Továbbá általános esetben feltesszük, hogy ha valaki előtt megfelelően is álcáztuk magunkat, problémát jelentenek a közös ismerősök, a közös kapcsolatok, ugyanis ők kompromittálhatják az álcát.

Csak az egylépéses kapcsolatokkal foglalkozunk, a hosszabb kapcsolatokkal nem. A partnerlista, illetve a szobák és konferenciák névlistái alapján felépített kapcsolati hálón egylépéses kapcsolatnak azt nevezzük, amikor a célszemély és a felhasználó között van egy olyan harmadik személy, amelyik mindkettőjükkel kapcsolatban áll. Szobák esetén ez azt jelenti, hogy mindkét féllel legalább egy szobában közösen tartózkodik.

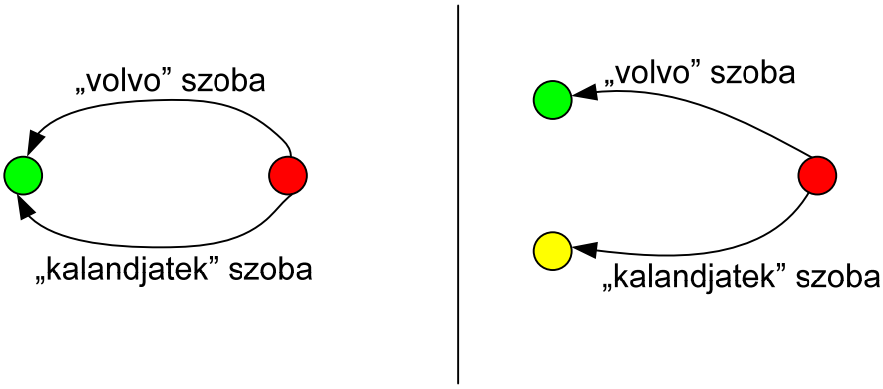
Foglalkozhatnánk a szobás részen azzal az esettel is, hogy a kompromittációra képes fél a felhasználóra rendelkezik csak nézettel, felderíthető kapcsolata a célszeméllyel nincs (azaz nincsenek közös szobában). Ebben az esetben mindenki gyanús lenne, akit csak láthat a felhasználó, s így a finomhangolás értelmét vesztené, ezért ezzel az esettel nem foglalkozunk.

Az ellenőrzés során megvizsgáljuk, hogy milyen identitásait látja a felhasználónak a célszemély, s azt is, hogy milyen nézeteken keresztül látja. A vizsgálat során nem foglalkozunk azzal, hogy a célszemély milyen identitásokkal rendelkezik, mert a rendszer célja, hogy ezeket ne ismerhessük fel, így feltesszük, hogy erre nem képes a vizsgálat során a felhasználó.

A vizsgálat során figyelembe kell venni az összes közös kapcsolatot is, hiszen ha két szobában van egyszerre jelen a felhasználó és a célszemély is, nem lehet a kiesés álcájával behozni egy új identitást az egyikbe. Emellett figyelembe kell venni az összes egylépéses kapcsolatot is, s mindezek figyelembevételével figyelmeztetni lehet a felhasználót a lebukás lehetőségére, s esetleg felajánlani egy jobb döntést.

4.5.3.6.1. Példa a vizsgálatra

A felhasználó szeretne egy szobában új identitást bevezetni. A probléma, hogy van egy másik felhasználó, aki egy másik szobában látja ugyanezt az identitását. Ekkor a hamis identitás bevezetéséhez nem használható hamis kiesés, szolgáltatás elhagyó üzenet, mert egyből kiderülhet a csalás, hanem csak például a szobát elhagyó álművelet lehetséges. Az ábrán a felhasználó egy identitásából kettőt hoz létre, azaz az egyik szobában identitást vált. A cél, hogy ezeket a célszemély ne tudja összekapcsolni, azaz tudni, hogy a két identitás mögött egy felhasználó van.



14. ábra: a példa illusztrációja, a kiindulási- és célszituáció. A bal oldalon a felhasználó, a jobb oldalon a „célszemély” identitása(i). A nyilak a nézeteket jelölik, a felirat a nézet származására utal.

4.5.4. Privacy-orientált állapotkezelés profilokkal

4.5.4.1. Megvalósítások más rendszerben

Már létező szolgáltatásokban találkozhatunk olyan állapotkezeléssel, amely magánszférát érintő szempontokat is figyelembe vesz. Ilyen rendszer (rendelkezik ennek megfelelő kliens programmal) például a Skype [SKYP], vagy az MSN Messenger [MSN]. Az előbbi például, ha elfoglalt állapotra vált a felhasználó az új beszélgetési ablakokat nem jeleníti meg, csak jelzi, hogy esemény történt. A hívások lenémulnak (ugyanígy minden esemény), s róluk is csak egy diszkrét jelzéssel vehet tudomást a felhasználó. Az MSN Messenger rendszerben hasonló működésről van szó, ott például, nem jelzi az eseményeket hang, de némely vizuális jelzések megmaradnak.

4.5.4.2. Profilok és állapotok

Mivel a profil[35], azaz a felhasználó magáról mutatott képének szerves része az is, hogy milyen állapotban van. A profil, mint az RBP-vel foglalkozó fejezetben is látható jól testre szabható, így felhasználónként változhat az is, hogy milyen állapotot látnak egy társukról.

Az állapotok teljesen testre szabhatóak, ugyanúgy a megnevezés és funkció szempontjából[36]. A felhasználó rendelkezik egy állapot palettával, és erről a palettáról rendelhet hozzá állapotokat a profilokhoz, és szabályozhatja a globális állapotát. A palettán egy kötelező állapot van, ez a rejtőző állapot. Rejtőző állapotban a partnerei az off-line profilját láthatják a felhasználónak.

További állapotok tetszés szerint felvehetőek és módosíthatóak, mivel ez csak a klienst érinti. Az állapotok tehát egy névből (és egy ikonból), illetve a letiltott felhasználói felület hatásaiból állnak, tehát teljes audiovizuális magánszféra védelmet biztosít az állapotkezelés.

A profilokhoz kötött állapotkezelés további előnye, hogy a magánszféra védelme tovább finomodik. Eddig a felhasználó a profillal és néhány RBP alapművelettel rendelkezett, de ezen túl azt is képes szabályozni, hogy mely felhasználók üzeneteiről, bejelentkezéséről szeretne figyelmeztetést kapni.

4.5.4.3. Globális állapot

A globális állapot elengedhetetlen a rendszer megfelelő magánszféra óvó működésének biztosításához. A globális állapot változtatásával egyszerre minden profilban megváltoztathatja a felhasználó a mutatott állapotát, amivel például egy telefonhívás esetén lenémíthatja a felhasználói felület összes audiovizuális jelzését egyszerre, illetve tetszés szerinti állapotban eltűnhet a rendszerből a rejtett mód globálissá állításával.

4.6. SPIM és kifejezés cserék

4.6.1. SPIM szűrés

4.6.1.1. Alapvető kérdések

Mint arra már korábban utaltunk, az azonnali üzenetküldő szolgáltatásokkal küldött kéretlen üzeneteket a szakirodalom nem *spam*-ként, hanem *spim*-ként említi [SPIM1] [SPIM2]. A hagyományos, elektronikus levelekkel terjesztett spam-hez képest több egyedi probléma adódik:

[35] A profilok részletes leírása a RBP részben olvasható.
[36] A jelenlegi rendszerek java része ilyet nem támogat, például [MSN]-ben is csak kiegészítéssel vehető igénybe ez a szolgáltatás. Ebben az esetben is csak új al-állapotokat definiálhat a felhasználó, amelyek egy korábbi állapottól függenek.

- *Kisebb üzenetek*: a szűrés az üzenetméret csökkenésével nehezedik, ezzel a spim-re jellemző mintákból kevesebb jut egy üzenetre, kisebb mintából pedig nehéz extrapolálni.
- *Valós idejű átvitel:* a döntést arról, hogy spim-e valami, gyorsan kell meghozni, ne késleltesse feleslegesen sokkal a jó üzenetek megérkezését.
- A spim-nek címkézett, de valójában legitim üzenetek száma minimális legyen.
- Semmi körülmény között ne szivárogjon ki identitással összefüggő információ még a spim üzenetekkel kapcsolatban sem.

4.6.1.2. Egyszerű megoldások

- *Ismeretlen felhasználótól kapott üzenetek teljes körű blokkolása:* nem lehetséges, ha például üzleti célból szeretnénk kapcsolatot tartani leendő vagy meglévő ügyfelekkel, és ezek az IM szolgáltatáson keresztül vennék fel velünk a kapcsolatot.

- *Spim-melőket egyenként blokkolni:* nem hatékony, ugyanis egy pillanatba kerül új felhasználót vagy identitást létrehozni. Természetesen ezek automatizált létrehozása megnehezíthető, illetve lehetetlenné tehető, megfelelő emberi beavatkozást igénylő ellenőrző adatok (challenge-response) bekérésével. Természetesen a tervezett rendszerbe az egyenkénti blokkolás funkció alapvetően anonimitási kritériumok miatt, nem spim szűrés miatt kerül bele.

4.6.1.3. Összetettebb megoldások

- *Kollaboratív módszerek:* a döntéshozó modul központosított módon épül be a rendszerbe, alapvetően az dönt egy-egy üzenet megbélyegzéséről. Azonban az így is „átcsúszott” kéretlen üzeneteket a felhasználók megjelölhetik. Lényegében a *felhasználók által felhalmozott információ* segíti a szűrő működését. Valószínűleg operátorok közbenjárása szükséges a beküldött jelentések ellenőrzésére és adminisztrálására. Komoly problémát jelenthet a legitim üzenetek eldobása, ezért végig kell gondolni, hova kerülnek az eldobott üzenetek.

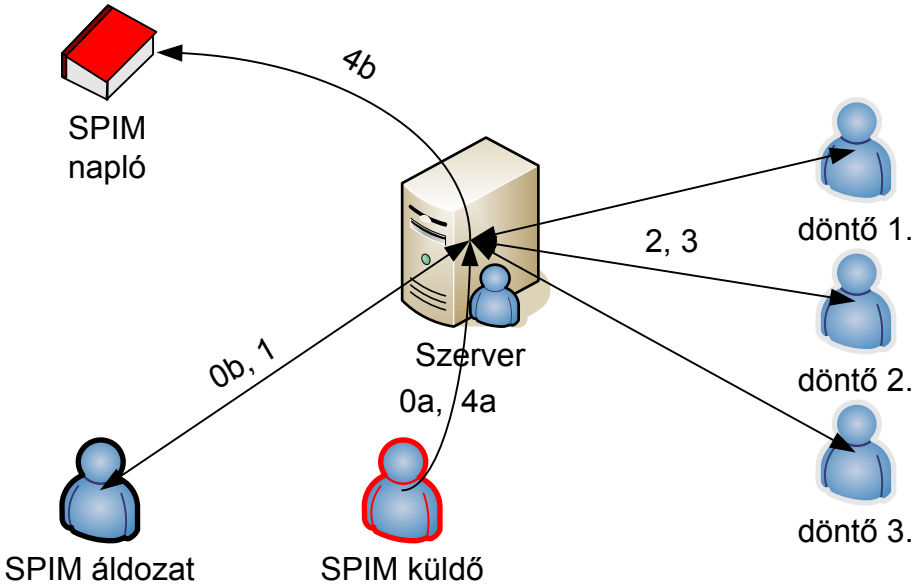
- *Automata szövegosztályozó algoritmusok:* mintákat keresnek szövegekben, melyek más ismert spim-mel hasonlóságot mutatnak. Nem feltétlenül egyenként vizsgálják az üzeneteket, lehetséges az is, hogy a beszélgetés *előzményeit* is figyelembe veszik. Ez feltétlenül központosítottan működik.

- *Elosztott döntéshozó rendszer:* egy ilyen rendszerben a kliensek egymástól is megkérdezik, az adott üzenet szemétnek minősülhet-e. Ez az elképzelés nyilvánvalóan *nem megfelelő* az általunk tervezett rendszerben, ugyanis kompromittálja az anonimitást, ha az üzeneteket sok résztvevőnek elküldi a szerver – éppen ennek minden lehetőségét szeretnénk elkerülni a titkosított kommunikációs csatornák használatával.

4.6.1.4. Ezek együttes alkalmazásával összeállított saját megoldás

Kéretlen üzenetek vétele esetén a következő folyamat zajlik le:

1. A címzett(ek) megjelölheti(k) az üzenetet, ezáltal potenciális spim státuszt kap. Ha nem jelölik, nem történik semmi. Ez jelenti a folyamat kollaboratív filteringet támogató részét.
2. A megjelölt üzenetet a szerver visszakapja és szétküldi egy speciális felhasználói halmazhoz, akik az elosztott döntéshozó rendszert alkotják. Ezek az alapvetően megbízható felhasználók jelenlévő, de minimumnál nagyobb hányada (vagy egyéb megkötések teljesülése esetén) szavaznak arról, hogy ténylegesen spim-e az üzenet.
3. Amennyiben a szavazás pozitív eredménnyel zárult, az üzenet és meta-adatai permanensen bekerül a szerver oldali adatbázisba. Ha negatívval, akkor nem történik változás.
4. A szerver(ek) az adatbázis alapján automatikusan szűrhetik a szűrendő üzenetfolyamokból a kéretlen üzeneteket.
5. Az adatbázis tartalmát az adminisztrátorok természetesen tetszőlegesen változtathatják, a döntők támogatásukkal csökkentik az adminisztrátorok terhelését.



15. ábra: Az együttes módszer alkalmazása.

Problémát jelent, hogy ha a szavazó felhasználói halmaz megbízhatatlan, például maguk is spammerek, akkor hatástalan a feljelentés mert direkt elutasítják az esetlegesen saját maguk által küldött üzenet spim státuszát. Megoldás lehet, hogy a szavazók halmazához való tartozásnak szigorú statisztikai feltételei legyenek, például hogy soha sem lehetett olyan üzenete (globálisan az egész rendszerben, mint felhasználó, és nem mint az egyik profilja), melyet a szavazók spim-nek elfogadtak.

Meggondolandó, hogy ebben az esetben milyen nehéz a szavazóknak egy felhasználó együttműködve „kiszavazni” maguk közül, tehát a szavazással megváltoztatni a felhasználó egyik olyan tulajdonságát, amely az új értékével már nem kvalifikálja az áldozat felhasználót a szavazók körébe való tartozásra. Ehhez először is szükséges egy üzenet, melyet a kiszavazni szándékozott felhasználótól érkezik. Utána a címzettek közül egynek legalább be kell jelölnie az üzenetet mint potenciális spim. Csak ezután jöhet a szavazás, ahol a többség a kiszavazandó felhasználó ellen kell legyen, ráadásul fel kell ismerniük a konkrét üzenetet anélkül, hogy látnák a tényleges feladót az üzenettel együtt. Ebből a példából talán látszik, hogy a szerver központosított szerepe miatt *nehéz kijátszani egy jól viselkedő szavazót*, mert nagyon speciális helyeken kell beépülnie a „többiekkel” kollaboráló felhasználónak, egy rosszul viselkedő viszont automatikusan lebukik. Lehetséges szűrni azokat a rossz szándékú felhasználókat is, akik statisztikailag kiemelkedő mértékben szavaznak ellentétesen a többséghez képest.

A szavazók körébe való bekerülés manuális jelentkezéssel történhet, akár például egy rövid motivációs levél kíséretében. Az adminisztrátorok így fel tudnak venni szavazókat. Az elutasítás illetve elbocsátás automatikus is lehet, amennyiben az érintett felhasználó egyik paramétere a megengedett tartományon kívülre kerül.

4.6.1.5. SPIM adatbázis menedzsment és ennek felhasználói vetülete

Amikor egy felhasználó spim üzenetet kap, azt az előző fejezetben folgaltaknak megfelelően megjelölheti. A döntők számára a folyamat egy külön adminisztrációs felületen jelenik meg a kliensen belül, ahol a hátralevő szavazások láthatók. Az adminisztrátorok számára az egész adatbázis kereshető módon hozzáférhető lenne. Amikor egy spim üzenet automatikus szűrésre kerül, a felhasználót figyelmeztetni lehetne, ugyanis egyébként soha nem értesülhet egy hibásan szűrt üzenetről. Így akár felül is bírálhatná annak az egy üzenetnek a SPIM státuszát, ezzel további visszacsatolást adva az adminisztrátoroknak illetve a döntőknek.

4.6.1.6. Használati módok

A szűrőt a felhasználó tetszőlegesen állíthatja a saját identitásai közül bármelyiknél. Ez természetesen csak a közvetlen üzeneteket befolyásolja. A konferenciák és szobák szintén állíthatók ilyen szempontból, de csak a teljes konferenciára illetve szobára vonatkozóan, az adott objektum tulajdonosa által.

4.6.2. Kifejezések cseréje

4.6.2.1. Célok

Az üzenetekben szereplő olyan kifejezések elfedése, melyek a felhasználó számára valamilyen okból nemkívánatosak. Ezek a kifejezések kategóriákba sorolhatók akár a kifejezés kontextusa szerint (pl. szalonképtelenség különböző fokozatai, vallási, kisebbségi kérdések), esetleg a szűrés oka szerint (pl. szülői felügyelet).

4.6.2.2. Megoldások

- **Egyszerű csere:**
  A kifejezések cseréjének technológiai megoldása legegyszerűbb esetben a konkrét szavak megkeresése a szövegben, majd találat esetén a csere végrehajtása (pl. csillag karakterekre). Ez a legtöbb esetben sajnos nem kielégítő, mert pl. a toldalékolás egyszerűen kikerüli a legelterjedtebb alakkal megadott szavakat. Amennyiben minden alakot megadja az adatbázis, akkor pedig sokszorosára duzzadhat, és az esetleges elírást így sem ismeri fel a program.
- **Részleges egyezéses csere:**
  A kifejezéseknél nem feltétlenül teljes egyezést, hanem pl. *reguláris kifejezésekkel,* vagy egyéb *logikai módon* leírható egyezést keresünk. Természetesen az egyszerű csere ennek egy speciális esete. A módszer teljesítményigénye sokkal nagyobb, mint az előzőé, de a felhasználó reakció sebességénél még sok szabály mellett is jóval gyorsabb. Valószínűleg ezt érdemes használni, ugyanis a kifejezés-listák egyszerűbben karbantarthatók lesznek, mert kiterjedésük a rugalmas definíciók miatt töredéke az egyszerű csere módszeréhez képest. A megfelelő formalizmussal adott kifejezés mellé felvehetők még tesztesetek is.

4.6.2.3. A rendszer használata

A célok fejezetben említett módszerrel kategorizálva a csereszabályokat, a felhasználóra lehet bízni, hogy mely szabályok alapján kíván szűrést végezni. A szabályokról egyenként eldönteni, hogy szükséges-e a felhasználónak, nyilván nem várható el. A kategorizálás arra szolgál, hogy nagyobb halmazokat jelölhessen ki egyszerre. Természetesen a csoportokon belül is beállíthat pozitív és negatív kivételeket.

A szabályok maguk egy központi adatbázisban tárolódnak, amelybe való bekerüléshez ajánlatokat lehet tenni bármelyik felhasználónak (akinek van hozzá joga, azaz akitől nem vonták meg), és azokat a javaslatokat a megfelelő joggal felruházott adminisztrációs személyzet ellenőrzés után ténylegesen beillesztheti.

A szabályok alkalmanként, vagy kérésre frissülhetnek a szerver oldali adatbázis alapján. A felhasználó saját szabályokat is hozzáfűzhet a saját adatbázisához, amelyek nem részei a központi nyilvántartásnak, de a frissítések során a saját gépén megmaradnak és szerves részét képezik az így összeálló saját adatbázisának.

A kifejezéscsere kategóriák előre nem meghatározottak, a legrugalmasabb megoldás valószínűleg tetszőlegesen létrehozható, törölhető, összevonható, stb. kategóriák támogatásával érhető el.

Fontos még megjegyezni, hogy a kifejezések cseréje nyelvfüggetlennek tekinthető, de ritkán mégis tévedhet a rendszer, például homonímia és homográfia esetén (azonos írásmóddal rendelkező szavak, akár nyelvek között is). Tovább bonyolítja a

helyzetet az összetett szavak vagy szerkezetek homonímiája. Praktikusan azonban a szűrendő kifejezések elenyésző arányban ilyen tulajdonságúak.

4.7. Audiovizuális magánszféra: üzenetek tartalomszűrése

4.7.1. Kommunikációs médiumok

A szolgáltatás vizsgálatát további igen bonyolult szintekre kellene továbbvinni, ha nem csak szöveges üzeneteket vizsgálnánk[37]. Szöveges üzenetek tartalmazhatnak csatolmányokat, sőt, olyan is előfordulhat, hogy egy üzenet csak csatolmányból áll. Az ilyen jellegű kommunikáció mégis alapvetően más problémákat vet fel. mint a VoIP és videó hívás alapú kommunikációk.

4.7.2. Szöveges üzenettípusok

A javasolt rendszerben az alábbi üzenettípusokat különböztetjük meg a címzett szerint:

- *Többes üzenet:* helyiségbe küldhető, névvel ellátott üzenet.
- *Privát üzenet:* a címzettje csak egy személy lehet.
- *Többes szórt üzenet*: tetszőlegesen kiválasztott, több címzettel rendelkező üzenet.

Az alábbi típusokat különböztetjük meg az üzenet jellege szerint:

- *Szöveges üzenet*: az üzenetben szerepel valamilyen szöveg, amelyet csatolmányok kísérnek.
- *Csatolmányt szállító üzenet:* az üzenet csak csatolmányt tartalmaz.
- *Akció:* az üzenet egy a feladó általi akciót ír le[38]. Az akcióban a feladó kiemelt az akció elején is, de tetszőleges helyen állhat.
- *Esemény:* egy eseményt tartalmaz, ilyen üzeneteket a szolgáltatás küld[39].
- *Anonim üzenet*: helyiségbe küldhető, ha engedélyezett, a feladó nem látszik.

4.7.3. Üzenetformázási és díszítési lehetőségek

Nincs elvi kritériuma annak, hogy a rendszer olyan jellegű üzeneteket tartalmazzon, mint a jelenlegi szolgáltatások, egyedüli kritérium, hogy megfelelően lehessen szűrni a különféle tartalmakra, csatolmányokra. A [GGIM] eredményei alapján a következő formázási lehetőségek képzelhetőek el:

- *Szövegformázás*: félkövér, dőlt, aláhúzott, méretezések, színezés, stb.

Az alábbi kiegészítések csatolmány formájában kerülnek továbbításra:

[37] Korábban utaltunk rá, hogy a tervezett rendszer csak szöveges beszélgetésekre lesz alkalmas, VoIP vagy videó hívásokra nem.
[38] Például: „(**János akciója) János** elment a számítógéptől, mert vendégei jöttek."
[39] Például egy beszélgetés beállításai megváltoztak, vagy valamelyik fél nevet váltott.

- *Grafikus emotikonok [EMOT]*
  - *Rendszer emotikonok:* alapból szerepelnek a rendszerben.
  - *Saját emotikonok:* a rendszer emotiokon felülírása, további képek, animációk is felvihetőek és szövegrészletekhez rendelhetőek.
- *Hangklip*: a felhasználó felveszi hangos üzenetét, majd ezt elküldi csatolmányként.
- *Hangbetét*: előre rögzített, kisméretű audio állomány, csatolmányként kerül küldésre.
- *Animáció*: lehet teljes képernyős, vagy diszkrét Flash [FLSH] animáció.
- *Háttérkép, megjelenési stíluscsomag*.

4.7.4. Üzenetek szűrése

Üzeneteket lehet szűrni a feladó, a típus és a tartalom szerint. A feladó szerinti szűréssel a Role Based Privacy fejezetben foglalkozunk bővebben. Az üzenetek jellegének típusa szerinti szűrése magától adódik – egyszerűen szabályozhatóvá kell tenni a típusok szerinti engedélyezést, illetve tiltást, a címzett szerinti szűrés felesleges, hiszen ezek az üzenetek szükségesek a rendszer működéséhez.

A tartalom és formázás szerinti szűrés szimmetrikusan kell, hogy felépüljön ahhoz, hogy milyen lehetőségek vannak a rendszerben, így garantálható a magánszféra teljes körű védelme. Az alábbi korlátozási (és engedélyezési) lehetőségek szükségesek:

- *Szövegformázások szűrési szintjei:*
  - *Színek szűrése*
  - *Szövegformázás alapműveletek szűrése:* ekkor nem formázott a szöveg.
- *Grafikus emotikonok korlátozásának szintjei*
  1. *Felhasználói animált emotikonok tiltása* (állókép helyettük)
  2. *Felhasználói emotikonok tiltása*
  3. *Animált rendszer emotikonok tiltása*
  4. *Rendszer emotikonok tiltása*: ekkor nincsenek képek a szövegbe ágyazva.
- *Hangklipek szűrése*
- *Hangbetétek szűrése*
- *Animációk szűrése*
- *Közös háttérkép, megjelenési stílusok szűrése*

Mindemellett meg szükséges azt a lehetőséget is adni a felhasználónak, hogy dönthessen a hangos csatolmányok hangerejéről, illetve arról is, hogy ha engedélyezi ezeket, automatikus lejátszásra kerülhetnek-e, vagy külön el kelljen-e indítani azokat.

4.8. A négy fő magánéletvédő kritérium teljesülése a rendszerben

4.8.1. Anonimitás

A rendszerünkben egy tetszőleges normál felhasználó a következő anonimitást potenciálisan sértő szereplőknek van kitéve: a rendszeren kívüliek, a többi normál felhasználó, a rendszer adminisztrátorai (a szolgáltatás szintű operátorok). A normál felhasználók közül a névlistán keresztül a felhasználóval kapcsolatban állók anonimitása persze korlátozott, ugyanis éppen azért vették fel egymást a névlistára, mert valamennyire ismerik egymást. Ugyanez igaz lehet a megfelelően beállított konferenciákra vagy szobákra. A speciális eseteken kívül azonban a többi szereplő mégsem képes (vagy egyáltalán nem, vagy nem tetszőleges mértékben, láthatatlanul) megsérteni bármelyik felhasználó anonimitását, az következő okok miatt:

Rendszeren kívüliek: ezek a *szállító protokoll* használata miatt el vannak különítve a rendszertől, ettől lesznek rendszeren kívüliek. A *külső-belső világ paradigma* is ezt hivatott modellezni. Mivel semmit nem tudnak a hálózati forgalomból beazonosítani, dekódolni, fel sem merülhet hogy bármilyen információt tudjanak kinyerni abból.

Adminisztrátorok: ők mindent tudnak a rendszerről, értelemszerűen bármit megtehetnek, így könnyűszerrel megsérthetik az átlagos felhasználó anonimitását. Ennek ellenére a *rendszer naplózás és adminisztrátor felügyelet* fejezetben kifejtett módszerek alkalmazásával ezeket az indokolatlan hozzáféréseket elfogadható szintre lehet csökkenteni a szolgáltatás szintű operátorok közötti kollaboratív ellenőrzéssel.

Többi felhasználó: mivel a rendszer azért jött létre, hogy velük kommunikáljon az adott felhasználó, a megoldások nagy része az anonimitás megőrzési valószínűségének maximalizálására irányul. Álnevek használatával mindenkinek lehetősége van, hogy akár személyes párbeszédnél, akár konferencia vagy nyílt szobában zajló beszélgetés résztvevői számára (és kívülállók számára is) ismeretlennek tűnjön. Általában a felhasználó viselkedéséből vonhatnak le következtetést a partnerek, ily módon csak a felhasználón múlik mennyire marad anonim, milyen információkat ad meg magáról, és azok igazak-e vagy nem.

A különböző lehetőségeket a következő bekezdés után tárgyaljuk.

4.8.2. Pszeudonimitás

Rendszerünkben egy felhasználó tetszőleges mennyiségű álnévre tehet szert anélkül, hogy sok külön felhasználót kelljen létrehozna. Ez segíti abban, hogy valóban képes legyen kihasználni a pszeudonim nevek és finomhangolható profilok nyújtotta előnyöket. Minden felhasználó egy adott kontextusban egy adott névvel van jelen, és ugyanígy a többi jelenlévőnek is csak a pszeudonim nevét látja. Plusz információval természetesen egy másik résztvevő képes lehet összekötni a különböző identitásokat, és feltárni a mögöttük húzódó kapcsolatokat, de ez leginkább hibás beállítás, vagy szándékos identitás felfedés esetén fordulhat elő. Az

adminisztrátorok természetesen itt is minden információt követni tudnak, azonban az anonimitás védelmére hozott intézkedések itt is hatásosak lesznek.

4.8.3. Kontextus szerinti anonimitás és pszeudonimitás

Üzenetküldés: privát üzenet küldése. A címzett a küldő felhasználó alapbeállítása szerinti, vagy speciálisan számára beállított identitást észleli mint az üzenet forrása. Az identitásból a kliens nem tudja megállapítani, hogy mely másik identitások jelentik ugyanazt a felhasználót, és csak olyan információkat lát a küldőről, amelyeket az megengedett a profiljában. Így akár egy teljesen külön személynek is kiadhatja magát a felhasználó.

Konferenciabeszélgetés és szobák: adott felhasználó tetszőlegesen választott identitásával megkísérelhet belépni bármelyikbe. A saját maga által létrehozott konferenciákkal és szobákkal (melyeknek tulajdonosa) kapcsolatban egyenként szabályozhatja, hogy ki láthatja azokat, ki kapcsolódhat be, milyen feltételekkel. A többi felhasználó az általában nem kérhet listát, hogy egy felhasználó adott identitással éppen mely konferenciákban és szobákban van jelen. Természetesen kivételek mindig beállíthatók. Ha valakit kitiltanak egy konferenciából vagy szobából, azt csak az adott identitásával tehetik meg, egyébként kiderülhetne, hogy mely identitásai összefüggőek, ugyanis másik identitásának letiltott állapota is megváltozna amennyiben bármelyiket letiltják. Ez természetesen gondot jelenthet a tiltónak, erre a *privacy* szempontból való vizsgálat során visszatérünk.

Az anonim hozzászólást engedélyező szobák még azt is lehetővé teszik, hogy identitás *nélkül* szólaljon fel a felhasználó, ezáltal még azt a kényelmetlenséget is megtakarítja, hogy új profilt kelljen manuálisan alkotnia.

Fájlküldés, egyéb két szereplős művelet: hasonló az üzenetküldéshez, csak az üzenet tartalma komplexebb. Az ilyen műveletek nem feltétlenül a központi szerveren keresztül továbbítódnak, ezáltal a kezdeményező felhasználót figyelmeztetni kell, hogy közvetlen kapcsolat esetén felfedheti például az IP címét. A címzettnél hasonló megerősítés szükséges. Lényegében bármilyen ebbe a kategóriába sorolható átvitel történik, a résztvevők felfedik egymásnak a hálózati topológiából, illetve a közvetlen csomagokra jellemző tulajdonságokból kikövetkeztethető adatokat.

4.8.4. Megfigyelhetetlenség

A megfigyelhetetlenségről a *szállító protokoll* gondoskodik, így az üzenetek megfigyelése kizárólag a szerver oldalán, feldolgozás közben képzelhető el, ami ismét visszavezethető az adminisztrátorok felügyeletére.

4.8.5. Összeköthetetlenség

Az összeköthetetlenség általunk definiált értelmében (ld. [DEFS]) az így kapott összetett feltétel egyrészt itt is a *szállító protokoll* felelőssége: cserélgeti az üzenetek sorrendjét, alkalmanként zajt küld, stb. Másrészt a központosított szerver miatt a rendszer elfedi minden egyéb felhasználótól a nem rá tartozó információt.

4.9. A rendszer elemzése privacy szempontból

A felhasználóknak fontos, hogy magánszférajukat ne sértse a többi felhasználótól vagy a rendszertől eredő hatás, illetve ne szivárogjon ki illetéktelen kezébe a felhasználóval kapcsolatos információ. Kellemetlen hatás lehet például a kéretlen kép, hang, szöveges üzenet, fájl. Ezek minél nagyobb hányadának küldésének megakadályozása, esetleg utólagos szűrése a cél.

Tételesen felsorolva a következő lehetséges támadások, problémák képzelhetők el:

- *Felhasználó állapotának kiszivárgása*: a felhasználó esetleg meg szeretné akadályozni, hogy más tudomást szerezzen például arról, hogy ő éppen beszélgetni készül, vár, a számítógép vagy más hozzáférési eszközön a rendszerbe bejelentkezett állapotban van, vagy azt éppen kikapcsolta. Ezt a rugalmas privacy orientált állapotkezelő rendszer jól megoldja, a *rejtőzködési lehetőségek* részben részletesen taglaltuk. Lehetséges identitásonként, vagy ahol az mások anonimitását nem sérti, felhasználónként különböző beállításokat alkalmazni.

- *Felhasználót zavaró üzenetek*: ezek lehetnek például SPIM, nem standard emotikonok, hangbetétek, videóbetétek. Amennyiben nem tetszőlegesen finomhangolható bármelyik, képes kellemetlenséget okozni. SPIM ellen a *SPIM és kifejezés cserék* fejezetben leírtak szerint lehet fellépni, a kifejezések, multimédiás tartalom szűrése ezzel rokon tevékenység. Az ezzel kapcsolatos beállítások igen szerteágazóak lehetnek, ideális módon akár üzenettartalomtól és típustól függően, felhasználónként, identitásonként megadható feltételekkel.

- *Nemkívánatos identitások, felhasználók*: Ezektől az identitásoktól a kontextustól függően letilthatóak a megfelelő események, előlük elrejthető a saját állapot, az aktuális profil és megtévesztő jelleggel álca, azaz hamis identitás is felvehető. Ennek módszereivel a Role-Based Privacy rész foglalkozik.

- *Bántó kifejezések*: az ilyeneket a *kifejezéscserék* fejezetben említettek szerint lehet semlegesíteni.

- *Beszélgetések rejtettsége*: bármilyen konferencia vagy szoba lehet privát, azaz semmilyen listán sem jelenik meg, és meghívásos alapon lehet csak csatlakozni. A privát beszélgetések mindig titkosak, lista, nyilvántartás szerveroldalon se készül a pillanatnyilag aktív beszélgetésekről.

- *Állapotfüggő profilok*: fontos igény, hogy egy adott felhasználóról különböző jelenléti állapotokban, különböző külső identitásoknak különböző profilt lehessen mutatni. Ezt rendkívül rugalmasan támogatja a *Role Based Privacy* modul.

- *Tevékenységek felfedése:* opcionálisan a gép előtt ülő felhasználó elárulhatja az épp aktuális tevékenységét és állapotát. Például, kiírhatja, hogy éppen mit csinál, automatikusan megjelenhet, hogy milyen zenét hallgat, stb. Ez is profilonként, identitásonként beállítható. Nagyon hasonló probléma, mint az állapot kiszivárgása, csak itt több opcionális adat publikálható.

Általánosságban elmondhatjuk, hogy a rendszer a magánszférát teljességben védi, nem hagy olyan lehetőséget a belső világ szereplőinek a kezében, amellyel a magánszférát zavaró hatásoknak lehetne kitenni.

5. A KUTATÁS JÖVŐBELI LEHETŐSÉGEI

5.1. Rendszernaplózás és adminisztrátorok felügyelete

Az előző fejezetek alapján láthatjuk, hogy a rendszer alapvető tulajdonsága annak feltételezése, hogy a például a szerver és a sok jogokkal rendelkező operátorok megbízhatóak. Semmiképp sem lehet céljuk kijátszani az anonimitási kritériumokat, sőt inkább védelmezniük kell azokat, egyébként az eredeti tervezési célok nagy része semmissé válik. Egy nagy forgalmú szervernél ezt garantálni (vagy akár elosztott szervereknél) képtelenség, valószínű, hogy előbb-utóbb lesz valaki, aki – akár belső, akár külső indíttatásból – rossz szándékkal akarja majd használni a szerveren tárolt információkat, vagy befolyásolni az átmenő forgalmat.

Ezt teljességgel kiküszöbölni nem lehet, de a láthatatlan behatolási lehetőségeket csökkenteni igen. Az összes adminisztrációs művelet naplózásával például visszakereshetővé válik az ártó szándékkal ténykedő operátorok viselkedése. Természetesen valaki mindig lesz, aki ezt is törölni tudja, például a futtatókörnyezet tulajdonosa. A napló legfeljebb egy elosztott rendszerben válik törölhetetlenné, ha a kiszolgálók egymást is naplózzák. Ekkor természetesen az összes legmagasabb szintű adminisztrátor szükséges az összehangolt törléshez. Mindezeket természetesen úgy kell véghezvinni, hogy a felhasználók semmit se érzékeljenek belőle, mert elveszítenék a bizalmukat a rendszerrel szemben, egy üres rendszerben nem sok megfigyelni való lenne.

A következő javaslatok, irányvonalak alapján lehet tovább kutatni:

- az operátorok, mint a rendszer közszereplői és felügyelői, korlátozottan megfigyelhetők lehetnének egymás vagy akár az összes felhasználó által;
- a megfigyelt információk természetesen nem konkrét műveletek teljes részletességgel, mert azok sérthetik az adatalanyok anonimitását, hanem szokásostól eltérő jellemzők, statisztikai eltérések, adatok szintén aggregált módon prezentálva;
- automatikus szűrése és nyilvánossá tétele a különleges eseményeknek;
- egységes, konzisztens, aláírt konfigurációt és program verziót futtató kiszolgálók garantálása;
- belenyúlás biztos (*tamper-proof*), elosztott naplózás;
- csak elosztott titokkal olvasható naplók;

Az említett technikai és adminisztratív megoldások mind a közös felelősségvállalás irányába mozdítják el a rendszert a teljhatalmú egyénhez képest, visszakereshetővé válnak a kritikus rendszerműveletek, mégis maximálisan tiszteletben tartják az anonimitást, amennyiben nem feltételezhető ártó szándék.

Ezekkel a módszerekkel felépíthető egy olyan adatgyűjtő rendszer, mely alapjául szolgálhat a behatolás detektáló modulnak (*IDS, Intrusion Detection System*), azzal a

kiegészítéssel, hogy nem csak operátorokat és adminisztrátorokat figyel meg, hanem az összes lehetséges gyanús felhasználói vagy rendszerbeli tevékenységet is.

5.2. Újabb programok tesztelése

Az alapozó kutatás befejezése óta számos új program jelent meg az EPIC honlapján is, de sok vizsgált változatból is új verzió jelent meg. Ezeket az új verziókat szeretnénk újra vizsgálni, továbbá újabb kutatásban megvizsgálni a ScatterChat és Gaim + OTR klienseket, amelyek különleges és egyedülálló megoldásokat tartalmaznak az azonnali üzenetküldő szolgáltatások között.

5.3. Ügyfélszolgálatok segítése

Ahogy a bevezető fejezetben is említettük, ügyfélszolgálatokat előszeretettel alkalmaznak azonnali üzenetküldőkre alapozva [BOOM] [HPIM] [LIB2]. Az ügyfélszolgálatok speciális működésének, igényeinek felmérése újabb kutatásokat igényel, s ennek megfelelően a szolgáltatás bővítése szükséges lehet.

A [LIB2] könyvtári ügyfélszolgálat honlapján közzétették az azonosítójukat, hogy azon keresztül elérhessék őket. Ezt a megoldást lehetne például tovább bővíteni úgy, hogy egy azonosítóhoz több ügyfélszolgálatos tartozik, amelyek közül a rendszer a terheltségük szerint választ (és ha nincs szabad ügyfélszolgálatos, akkor várakoztat). Ez a kiegészítés kombinálható a vállalati megoldásokkal.

5.4. Phishing kérdése csevegő szolgáltatásokban

A phising egyre gyakoribbak [PHWP], az azonnali üzenetküldő szolgáltatásokban is megjelent már, s elterjedt [PHIM]. További kutatásban szükséges lenne felmérni elterjedtségüket, megvizsgálni a többi rendszerbe beépített védelmeket. A kutatás egy jobb döntéstámogató rendszer is lehet.

5.5. Férgek, vírusok elleni védelem

A jelenleg is létező rendszereknek komoly problémát jelentenek a vírusok és férgek. Célravezető lehet a kész megoldások vizsgálata, analitikus elemzése, csoportosítása egy ad-hoc módon felállított szempontrendszer alapján. Ha ezek a rendszerek nem tudnak kielégítő hatékonysággal működni, akkor, ha lehetséges javaslatot kell tenni egy jobb vírusvédelmi rendszer működésére[40], de ez túlmutat a jelenlegi kutatás keretein. A dolgozatban szereplő ideális rendszer vizsgálata is érdekes eredményeket hozhat [IMPS].

[40] A cél nem az asztali, vagy szerveroldali vírusirtó és ellenőrző programok leváltása, hanem egy olyan döntéstámogató rész rendszer elkészítése, amely a fájlok fogadásával kapcsolatban tud a felhasználó segítségére válni.

5.6. Vállalati szintű lehetőségek: EIM vizsgálata

A vállalati szintű megoldások egészen más szemléletmódot követlenek meg annak megfelelően, hogy az adott cég mire használná a szolgáltatást. További kutatások szükségesek a vállalati megoldásoktól elvárt igényeinek, szükséges megoldások felméréséhez.

Lehetséges, hogy a szolgáltatás lokalizált kiterjesztésével megoldható a témakörhöz kapcsolódó néhány nehézség. Ilyen lehet például egy lokális szerverrel megoldani azt, hogy a helyi, azaz vállalati felhasználók oda kapcsolódjanak, s így a partnerlistán lokális kapcsolattal jelölt partnerekkel a kommunikáció helyben maradjon, s ne utazzon az Interneten.

Az előbbi példa csak egy kis szelete a témakörnek, amely további vizsgálatot igényel.

6. ÖSSZEFOGLALÁS

Ez a dolgozat a három szerző több mint féléves, összehangolt kutató-fejlesztő munkájának eredményét tartalmazza. E komplex tevékenység alapkutatási és empirikus kutatási, valamint fejlesztői elemeket tartalmaz, továbbá nemcsak informatikai, hanem társadalomtudományi aspektusokra is kiterjed. A közös kutatás indokolta azt, hogy nem három önálló, egymással összefüggő tudományos diákköri dolgozatot nyújtottunk be, hanem egyetlen, három szerző által jegyzett, terjedelmében és bemutatási körülményeiben a TDK szokásos kereteit meghaladó művet.

Kutatási eredményeinkből megállapítható, hogy a létező csevegő szolgáltatások, mind megvalósításuk elveit, mind gyakorlati kivitelezésüket tekintve, több szempontból nem kielégítők a magánélet és a személyes adatok védelme vonatkozásában. Legtöbb alkalmazás esetében esetben az adatok titkosítás nélkül utaznak a hálózaton, a beléptetés védelme sem mindig megfelelő. Az audiovizuális magánszféra és spim védelem szintje az egyes szolgáltatások esetén nagyon eltérő. Vizsgálataink során a közismert és tömegesen használt csevegő szolgáltatások néhány, ismereteink szerint eddig nem publikált magánélet-védelmi rését is feltárta.

A négy fő magánélet-védő kritérium és a kiegészítő kritériumok vizsgálatánál a Common Criteria, valamint a Prime elméleti megközelítését vettük kiindulásul, és ezeket a csevegő szolgáltatások sajátos területére vetítettük. E kritériumok érvényesülését empirikus kutatásaink és fejlesztő munkánk során is figyelemmel követtük.

Az empirikus vizsgálatainkhoz felállított osztályozási rendszer (amelynek teljes változatát mellékletben közöljük) szemléletében több új elemet tartalmaz és alkalmasnak bizonyult a létező megoldások összehasonlító vizsgálatára. Részben e vizsgálatok eredményei, részben a magánélet-védő elvi kritériumoknak a csevegő szolgáltatások területére vetítésének problémái ösztönöztek arra, hogy kidolgozzuk egy szempontjaink szerint ideális csevegő szolgáltatás elvi kritériumrendszerét. Ebben megköveteltük a négy magánélet-védő kritérium teljesülését, megfelelő spim-mel és gyanús üzenetekkel szembeni védelmet, az audiovizuális magánszféra védelmét, és hogy a fentiek felhasználók által könnyen kézben tartható legyen.

Az elvi kritériumrendszer alapján kidolgoztuk egy kivitelezhető rendszer konstrukcióját és annak egyes elemeit a gyakorlatban is megvalósítottuk. A tervezést a belső-külső világ paradigma elvei szerint végeztük. A külső világgal szembeni védelmet a megfelelő szállító protokoll és hálózati architektúra hivatott ellátni. Részletesen vizsgáltunk a lehetséges hálózati struktúrákat és protokollokat, valamint azt, hogy a szállítási rétegnek milyen feladatokat kell ellátnia. A belső világ támasztotta követelmények a Role-Based Access Control modulon keresztül valósulnak meg. A felhasználók anonimitását a Role-Based Privacy módszerével valósítjuk meg. Rendszerünk tervében helyett kapott a spim védelem, és a kifejezéscsere lehetsége megoldása is.

Külön figyelmet fordítottunk arra, hogy a számos rétegből álló új szolgáltatás egyik rétegét, a külső és belső világ szeparálását végző, a protokoll üzenetek szállítását végző réteget programozói munkával a gyakorlatban is megvalósítsuk, sőt, működését valós idejű kísérletben is demonstráljuk.

A kutatás számos olyan kapcsolódó kérdést is felvetett, amelynek vizsgálatára e tudományos diákköri dolgozat keretei nem adtak módot. Ilyen például a megfelelő rendszernaplózás, és az adminisztrátorok felügyelete, az empirikus alapkutatás óta megjelent új alkalmazások részletes vizsgálata, a phising és vírusokkal szembeni védelem, illetve a rendszer vállalati szintű alkalmazhatósága. Mindazonáltal szükségesnek tartottuk ezek rövid megemlítését, mert kijelölik a dolgozatban foglaltak továbbfejlesztésének egyik irányát a tudományos kutatás terén.

Ugyanakkor úgy véljük, hogy az általunk konstruált új rendszer a gyakorlatban is megvalósítható és kedvező feltételek mellett termékké is fejleszthető. A jelenlegi Internetes világban egyre nagyobb az igény a megbízható anonim kommunikációs lehetőségekre. Egy anonim üzenetküldő szolgáltatás segítheti a szabad véleménynyilvánítás gyakorlását, a felhasználók segítséget kérhetnek egymástól, megőrizve valódi kilétük titkát. A jelenlegi rendszerekkel szemben pedig megoldást kínálna az üzenetküldő szolgáltatásokban is egyre kritikusabbá váló spim kérdésében.

7. BEMUTATÓ: A SZÁLLÍTÓ PROTOKOLL IMPLEMENTÁCIÓJA

7.1. A kísérlet célja

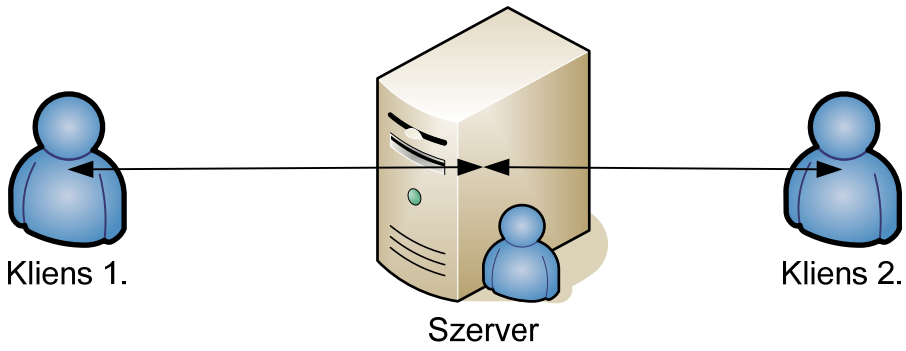
A kísérlet célja, hogy bemutassuk a hálózat azon rétegének működését, amely a protokoll üzenetek szállítását végzi. Ez a réteg felel a QoS paraméterek betartatásáért, a külső szemlélő előli anonimitásért, védjen a lehallgatások, forgalomanalízis ellen. A réget további feladata, hogy megakadályozza a megszemélyesítést, visszajátszást és a lehallgatott üzenetek szerkesztését.

A bemutatandó protokollra épül az összes kommunikáció, ez a réteg szigeteli el a belső működést a külvilág elől. A fejlesztés későbbi fázisaiban ugyancsak erre a rétegre épülnek majd rá a további hálózati rétegek, mint például a protokoll kommunikációt megvalósítandó modul. Éppen ezért ennek a rendszerelemnek a működése több mint kritikus.

A kísérlet során megvizsgáljuk a protokoll működését egy külső, harmadik fél szemszögéből, és megpróbáljuk belátni néhány kritérium teljesülését az implementációban.

7.2. Kísérleti hálózat architektúrája

A kísérletben három számítógép vesz részt: egy központi kiszolgáló és két kliens, amelyek a szerverhez kapcsolódnak, hogy a rendszer szolgáltatásait igénybe véve kommunikáljanak egymással. A két kliens nincs kapcsolatban egymással, így a kísérleti előfeltevés szerint a támadó a szervert lehallgatva próbál információhoz jutni.



16. ábra: a bemutató kísérleti elrendezése.

7.3. A kísérlet menete

A két kliens gép között egyszerű szöveges üzeneteket fogunk küldeni egymás felé egy privát jellegű beszélgetés szimulációjaként. Eközben egy a szerver programjába beépített speciális modul segítségével szimulálunk egy olyan támadót, amely a hálózati forgalom lehallgatásával próbálkozik, illetve a hálózati forgalom alapján próbál statisztikát készíteni.

A két gép között olyan egyszerű üzeneteket próbálunk, amelyek magyarul, vagy más természetes nyelven íródtak. Előre meghatározott mondatokkal is lehet folytatni a kísérletet, de helyben rögtönzött mondatokkal is működnie kell a kísérletnek.

7.4. Várt eredmények, megfigyelés

A kísérlet kimenetei és várt eredményei a következőképpen alakulnak:

- Kliens 1 – Szerver és Kliens 2 - Szerver kapcsolatának lehallgatása. A bárki által látható karakterek statisztikájával vázolni próbáljuk, hogy az itt zajló forgalom külső szemlélő számára véletlenszerű zajnak tűnik, noha titkosítva értelmes információ kerül átvitelre.
- A következő két diagram a statisztikai alapú analízis nehézségét igyekszik demonstrálni a Kliens 1 – Szerver kapcsolatnál. Idő – elküldött adatmennyiség diagrammok segítségével.
  - Az elsőn szemléltetjük, hogy mikor lépett fel adatküldési igény a két fél valamelyikének részéről.
  - A másikon a csatorna megfigyelését jelöljük, amelyben az időeltolás is megjelenik, illetve a véletlen csomagok is.
  - A cél, hogy a két grafikon között korreláció nem látható, és ezt próbáljuk az összevetésükkel megmutatni.

7.5. További magyarázat

A kísérlet eredményeivel próbáljuk igazolni, hogy a támadó nem tud a felsorolt lehetőségek közül támadást végrehajtani. A DOS jellegű támadásokkal nem foglalkozunk, amelyek az SSL / TLS csatorna használatából adódóan könnyen végrehajthatóak[41].

[41] Például az adatfolyamba egy véletlen csomag beszúrásával, ami elővigyázatossági okokból a kapcsolat megszakadását eredményezni.

REFERENCIÁK

[AIM] Az AIM (America OnLine Instant Messenger) azonnali üzenetküldő szolgáltatás honlapja:
http://www.aim.com/

[ANCO] Matthew Wright, Micah Adler, Brian Neil Levine, and Clay Shields. An Analysis of the Degradation of Anonymous Protocols. (2002)
http://freehaven.net/anonbib/cache/wright02.pdf

[ANOR] P. Syverson, G. Tsudik, M. Reed, and C. Landwehr. Towards an analysis of onion routing security. (2000).
http://www.onion-router.net/Publications/WDIAU-2000.pdf

[ANPR] *Anonimizáló protokollok részletes leírását* tartalmazó melléklet (6. számú melléklet).

[APAT] *Anonimizáló protokollok elleni támadások*at összefoglaló melléklet (7. számú melléklet)

[BITW] BitWise Instant Messenger azonnali üzenetküldő szolgáltatás honlapja:
http://www.bitwiseim.com/

[BOOM] Dinesh C. Sharma: Boom time for instant messaging
http://news.com.com/Business,+mobile+IM+on+the+rise/2100-1025_3-5322033.html

[COS1] ComScore cikk (2006)
http://www.comscore.com/press/release.asp?press=800

[CPW1] John Dickinson: Instant messaging and the security pro (2006)
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9003796&pageNumber=1

[CROW] M. K. Reiter and A. D. Rubin. Crowds: Anonymity for Web Transactions. (1998).
http://avirubin.com/crowds.pdf

[DEFS] A felhasznált fogalmak *definícióinak melléklete*, az 1. számú mellékletben található.

[EIM] Enterprise Instant Messaging (Enterprise IM), azaz vállalati azonnali üzenetküldő szolgáltatásokkal kapcsolatos hírportál:
http://www.instantmessagingplanet.com/enterprise/
A szerzők által jónak ítélt Enterprise IM szolgáltatás:
http://www.bitwiseim.com/features.php?f=ProOverview

[EMER] Az *empirikus mérési* eredmények jegyzőkönyve mellékletként szerepel (5. számú melléklet).

[EMOT] Emotikon szócikk a Wikipedia enciklopédiában:
http://hu.wikipedia.org/wiki/Emotikon

[EPIC] Az Eletronic Privacy Information Center több kategóriában ajánl programokat. Mi az azonnali üzenetküldő kategóriából válogattunk:
http://www.epic.org/privacy/tools.html#chat

[FLSH] A Flash-ről többet lehet megtudni a Wikipedia enciklopédiában:
http://hu.wikipedia.org/wiki/SWF

[GADU] A Gadu-Gadu lengyel nyelvű, azonnali üzenetküldő szolgáltatás honlapja:
http://www.gadu-gadu.pl/

[GAIM] A GAIM azonnali üzenetküldő szolgáltatásokat összefogó kliensének (IM Aggregator) honlapja:
http://gaim.sourceforge.net/

[GGAB] 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.

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

[HERB] Goel, S., Robson, M., Polte, M., Gun Sirer, E. Herbivore: A Scalable and Effecient Protocol for Anonymous Communication. (2003)
http://www.cs.cornell.edu/people/egs/papers/herbivore-tr.pdf

[HORD] Shields, C., Levine, B. A Protocol for Anonymous Communication Over the Internet. (2000).
http://prisms.cs.umass.edu/brian/pubs/brian.hordes.ccs00.pdf

[HPIM] Hewlett-Packard on-line ügyfélszolgálata.
http://welcome.hp.com/country/us/en/contact/chat_1.html

[ICQ] ICQ azonnali üzenetküldő szolgáltatás honlapja.
http://www.icq.com/

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

[IMW1] Will Sturgeon: IM threats – going one of two ways (2005)
http://software.silicon.com/security/0,39024655,39129676,00.htm

[IMPS] Az alábbi híroldal azonnali üzenetküldő szolgáltatásokkal kapcsolatos biztonsággal foglalkozik:
http://www.instantmessagingplanet.com/security/

[IRCR] Az IRC protokoll pontos leírása megtalálható itt:
http://www.irchelp.org/irchelp/rfc/

[LIB1] Michael Stephens, Aaron Schmidt: Fast, Cheap and Easy: Instant Messaging in Libraries (2004)
http://www.tametheweb.com/presentations/IM_IL04_SchmidtStephens.ppt

[LIB2] Egy létező könyvtári alkalmazása azonnali üzenetküldő szolgáltatásoknak:
http://www.umuc.edu/library/help/instantmessage.shtml

[LLIS] A vizsgált szolgáltatások részletes listája a *Bő lista* című mellékletben található (2. számú melléklet).

[MAT1] *A sűrűségfüggvény levezetése* című melléklet (9. számú).

[MIM1] Juan Carlos López Calvet: Mobile Instant Messaging (2003)
http://www.eurescom.de/message/messageDec2003/Mobile_Instant_Messaging.asp

[MIM2] Több „hagyományos" azonnali üzenetküldő szolgáltatás tölthető le telefonokra, kézi készülékekre (PDA – Personal Digital Assistant).
AIM: http://mobile1.aol.com/mobileaim
MSN: http://mobile.msn.com/ac.aspx?cid=uuhp_messenger
Skype: http://share.skype.com/sites/mobile/

[MIM3] Robyn Greenspan: Mobile IM Usage Nearly Doubles (2004)
http://www.clickz.com/showPage.html?page=3400661

[MIRC] A mIRC szoftver honlapja (IRC hálózati kliens):
http://www.mirc.com/

[MSN] Az MSN Messenger honlapja:
http://messenger.msn.com

[MSNP] Az MSN Messenger, vagy új nevén Windows Live Messenger kiegészítő szolgáltatása a Messenger Plus! Live.
http://www.msgpluslive.net/

[ONR1] A Wikipedia enciklopédia is ír az Onion Routing technológiáról:
http://en.wikipedia.org/wiki/Onion_routing

[ONRO] D. Goldschlag, M. Reed, and P. Syverson. Hiding Routing Information. (1996)
http://www.onion-router.net/Publications/IH-1996.pdf

[P5AC] Sherwood, R., Bhattacharjee, B., Srinivasan, A. P5: A Protocol for Scalable Anonymous Communication. (2000)
http://www.cs.umd.edu/projects/p5/p5.pdf

[PHIM1] Joris Evers: Worm, phising scam hit IM services (2005)
http://news.com.com/Worm,+phishing+scam+hit+IM+services/2100-7349-5719088.html

[PHIM2] Kelly Jackson Higgins: Instant Message, Instant Infection (2006)
http://www.darkreading.com/document.asp?doc_id=105252

[PHWP] A Wikipedia enciklopédia bejegyzése a phishingről, annak időszerű alakulásáról:
http://en.wikipedia.org/wiki/Phishing

[PRDF] Simone Fischer-Hübner, Christer Andersson: Prime Framework V0 (2004)
https://www.prime-project.eu/prime_products/reports/fmwk/pub_del_D14.0.a_ec_wp14.0_V6_final.pdf

[PRIME] A Prime Projekt weblapja:
http://www.prime-project.eu

[PSST] A PSST peer-to-peer alapú szolgáltatás honlapja:
http://psst.sourceforge.net/

[QOSM] *Szállítási protokoll QoS szintek* melléklet (8. számú).

[QOS1] MQTT protokoll
http://www.mqtt.org

[RBAC] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, R. Chandramouli: Proposed NIST Standard for Role-Based Access Control (ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001, Pages 224–274.)
http://csrc.nist.gov/rbac/rbacSTD-ACM.pdf

[RBRM] *RBAC szabályok* melléklet (11. számú)

[SCCH] A ScatterChat több protokollt támogató azonnali üzenetküldő program (Gaim kiegészítés), amely alacsony szintű anonimitás biztos Tor hálózattal. Honlapja:
http://www.scatterchat.com/

[SKYPE] Skype azonnali üzenetküldő szolgáltatás honlapja:
http://www.skype.com

[SLAN] A Softros Lan Messenger peer-to-peer jellegű szolgáltatás honlapja:
http://messenger.softros.com/

[SLIS] A kiválasztott szolgáltatások mellékletként megtalálható: *Szűk lista* című, 3. számú melléklet.

[SPIM1] Zhijun Liu, Weili Lin, Na Li, Lee, D.: Detecting and filtering instant messaging spam – a global and personalized approach (2005)
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1532048

[SPIM2] Z. Liu, V. Reddy, R. Shenai: P2P based SPIM detection and filtering (2004) http://www.cse.ohio-state.edu/~liuzh/presentation/P2P%20based%20SPIM%20detection%20and%20filtering1.ppt

[TAXO] Az *osztályozási szempontrendszer* a dolgozat mellékleteként megtalálható (4. számú melléklet).

[TORD] Roger Dingledine, Nick Mathewson, Paul Syverson. Tor: The Second-Generation Onion Router. Usenix Security (2004) http://tor.eff.org/tor-design.pdf

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

[TORP] A Torpark projekt egy pendrive-on hordozható anonim böngésző (Mozilla Firefox alapon), amely a TOR hálózatot használja. Honlapja: http://torpark.nfshost.com/

[TNET] Egy hazai chat jellegű szolgáltatás, amely UnrealIRCd alapokon fut: http://chat.trefort.net/

[TRST] *A szállító protokoll formális struktúráját* leíró melléklet (10. számú).

[ULTM] Az UltraMagnetic azonnali üzenetküldő szolgáltatás honlapja (a szolgáltatás új neve és honlapja [SCCH]): http://ultramagnetic.sourceforge.net/

[ULT1] Egy érdekkeltő hír az UltraMagnetic-ről: http://www.learninglinux.com/modules.php?name=News&file=article&sid=435

[UTL2] UltraMagnetic honlapján gyakori kérdések és válaszok (érdeklődés keltő): http://ultramagnetic.sourceforge.net/faq.html

[ULT3] A kezdeti UltraMagnetic verziók csomagjai innen letölthetőek voltak: http://rpmfind.net/linux/rpm2html/search.php?query=ultramagnetic

[URID] Az UnrealIRCd chat jellegű szolgáltatás szerver kiszolgálójának a weblapja (elérhető SSL-es szerver és jó minőségű dokumentáció): http://unrealircd.org
A dokumentáció címe: http://www.vulnscan.org/UnrealIRCd/unreal32docs.hu.html

[VPS1] Cara Garretson: Phishing leverages VoIP in new scam model (2006) http://www.networkworld.com/news/2006/042606-phishing-voip.html

[VPS2] Tóth Balázs: Alacsony vagyok szuperhősnek (Philip R. Zimmermann interjú) (2006) http://index.hu/tech/biztonsag/philz060208/

[WPIM] A Wikipedia enciklopédia azonnali üzenetküldőkről szóló történelmi áttekintése:
http://en.wikipedia.org/wiki/Instant_messaging#History

[YAHM] Yahoo Messenger azonnali üzenetküldő szolgáltatás honlapja:
http://messenger.yahoo.com/

MELLÉKLETEK

1. számú melléklet

Definíciók

[DEFS]

Négy fő magánéletvédő, adatvédelmi kritérium

Az alábbi négy definíciót első sorban a Prime [PRDF] alapján értelmeztük. A csevegő szolgáltatásokban azonosítónak tekintjük azokat a profilokat, amelyek a felhasználót azonosítják az adott szolgáltatáson belül (és azon belül a megfelelő kontextusokban), jelölik az üzeneteit, tevékenységeit.

Anonimitás

Először feltételezzük, hogy a felhasználó személye nem határozható meg akkor sem, ha ismerjük a szolgáltatást igénybe vevő összes felhasználót, vagy valamilyen egyedi azonosítójukat[1].

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

A 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

Az összeköthetetlenségnél a Prime[2] és a Common Criteria V3.1.[3] értelmezését egyesítettük: külső megfigyelő ne legyen képes megállapítani, hogy a rendszeren

[1] Például IP címét.

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 csoportos beszélgetési viszonyok összefűzéséből nem legyen kivehető annak az életfolyamata.

Csevegő szolgáltatások típusai

Azonnali üzenetküldő szolgáltatás, Instant Messenger, IM

Az *azonnali üzenetküldők* használatához előre kell regisztrálni egy felhasználói azonosítót, amely jellegzetesen állandó[4], és a partnerek számára mindig látható. A felhasználói fiókhoz tartozik egy partnerlista, ahol láthatjuk a partnerek aktuális neveit, állapotuk, esetleg ikonjukat[5]. A szolgáltatás első sorban úgy van kialakítva, hogy a partnerlistánkon lévőkkel beszélgessünk (de ez nem jelenti az új felhasználók felvételének, megismerésének nehézségét).

Chat jellegű szolgáltatás

A *chat jellegű szolgáltatások* a választott fedőnév[6] szempontjából kötetlenebbek (regisztráció itt is lehet), sokszor nem szükséges a regisztráció a szolgáltatás igénybevételéhez[7]. Partnerlista sincs, hanem a szolgáltatást igénybevevő felhasználókról bizonyos listák lekérdezésével, felhasználók keresésével, illetve szobák felkutatásával bizonyosodhatunk meg.

Hibrid szolgáltatás

Az előbbi két szolgáltatás tulajdonságait ötvözi (akár a következő szolgáltatástípus jellemzői is megjelenhetnek).

Peer-to-peer szolgáltatás

---

[2] „*Unlinkability* of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) means that within the system (comprising these and possibly other items), from the attacker's perspective, these items of interest are no more and no less related after his observation than they are related concerning his a-priori knowledge.15,16"

[3] „*Unlinkability*, requires that users and/or subjects are unable to determine whether the same user caused certain specific operations."

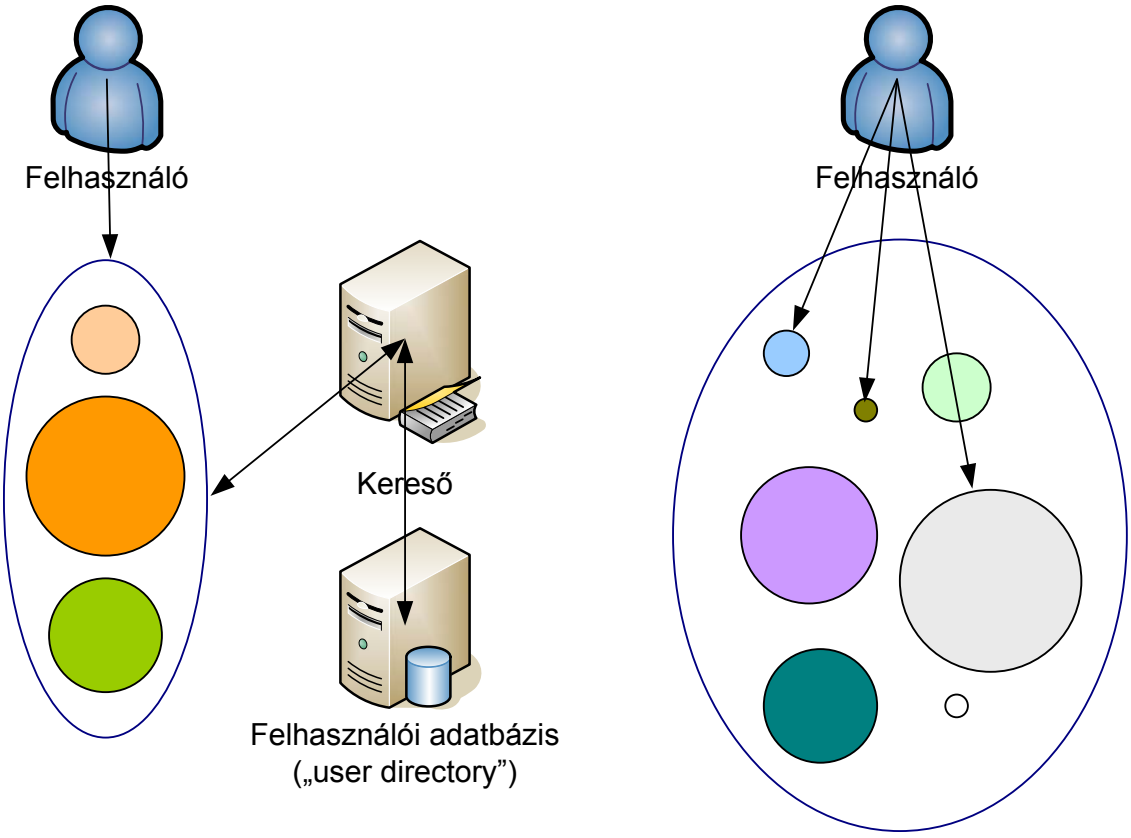
[4] Az MSN szolgáltatásban ez elvileg megváltoztatható már, a gyakorlatban ez a lehetőség halott (igénybevétele nem is ajánlott, mivel az a felhasználói fiók tönkretételét jelenti).

[5] Angol nevén „avatar".

[6] A fedőnév, azonosító az angol szakirodalomban „pseudonym, nym" formában jelenik meg.

[7] Ilyen az IRCnet például, amelyre mIRC programmal például a [8] szerverek valamelyikén át csatlakozhatunk. Az aktuális lista [10]-en tekinthető meg, kiinduláshoz [9]

Léteznek egyéb, *peer-to-peer* típusú szolgáltatások, amelyekben csak kliensek vesznek részt, és önmagukban építenek ki hálózatokat (vagy a kapcsolódás előtt egymás elérését más médiumon keresztül egyeztetik a felek). Ilyen jellegű szolgáltatásokkal is foglalkoztunk a kutatás során, de jelentőségük nem számottevő az előbbi két típus mellett.



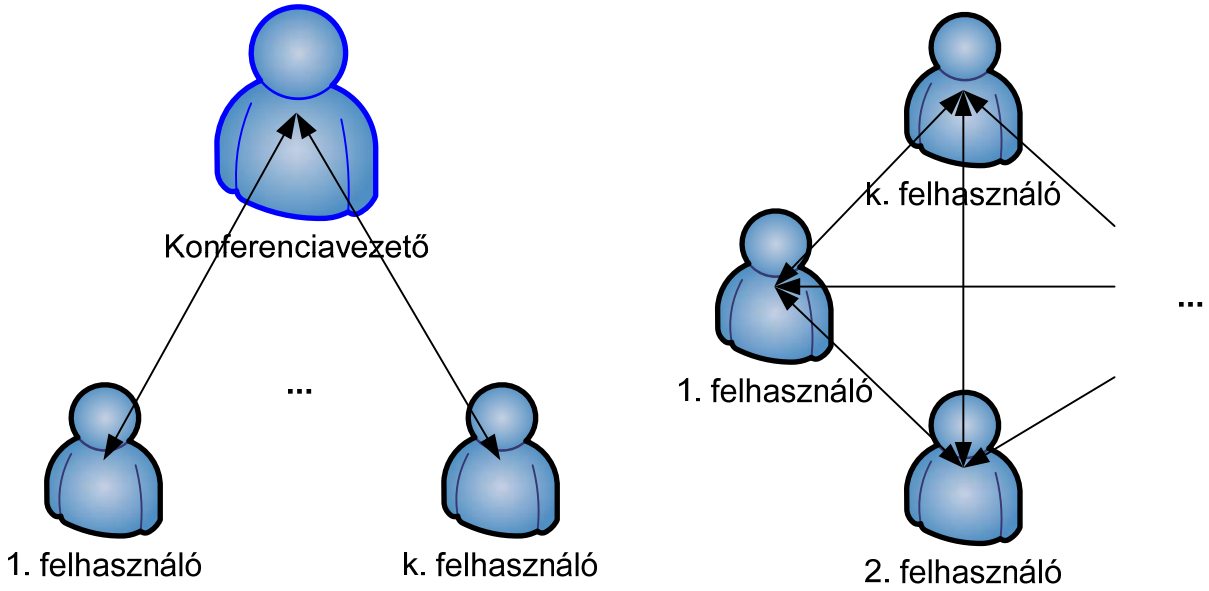
Azonnali üzenetküldő:
partnerlista, csoportok

Chat jellegű szolgáltatás:
szerver szobákkal

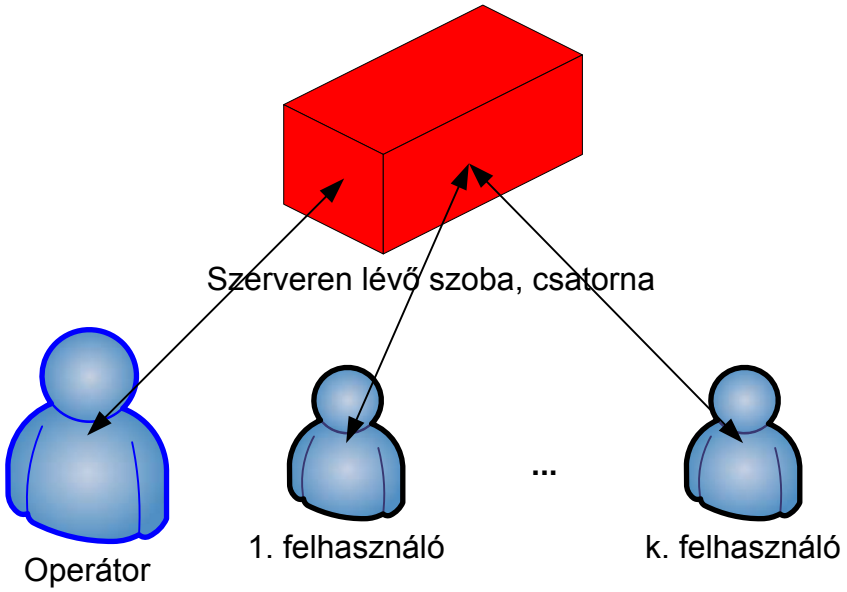
17. ábra: csevegő-szolgáltatások a partnerekhez hozzáférés módjai szerint. a) Az azonnali üzenetküldők esetében a felhasználó a partnereit egy lista alapján éri el, és egy keresőn keresztül bővítheti, illetve érhet el más felhasználókat.

b) A chat jellegű szolgáltatásokban a felhasználók különböző csoportok között vándorolhatnak, így vehetik fel további felhasználókkal a kapcsolatot.

Szobák és konferenciák összehasonlítása



18. ábra: konferenciatípusok.
a) A konferenciák első típusa esetén a kiemelt, a konferenciát létrehozó felhasználótól függ tipikusan a beszélgetés léte, és ő moderálja a beszélgetést. b) A második típus esetén a felek egyenrangúak, bárki kiléphet és meghívhat további feleket (az üzenettovábbítás magas szintű, logikai multicast jellegű).



19. ábra: szobamodell.
A szoba beállításai a szervertől függenek, ott tárolódnak (így lehet statikus is). A beszélgetést egy, vagy több operátor moderálja.

2. számú melléklet

Bő lista

[LLIS]

A melléklet a kutatás elején összeállított azon listát tartalmazza, amelybe minden érdekes szolgáltatást felvettünk.

4. táblázat: Azonnali üzenetküldők

Név	*URL*
MSN	http://messenger.msn.com
ICQ	http://www.icq.com/
Skype	http://www.skype.com
Google Talk	http://www.google.com/talk/
Yahoo Messenger	http://messenger.yahoo.com/
AOL Instant Messenger	http://www.aim.com/
Gagu-Gadu	http://www.gadu-gadu.pl/
LAN Messenger	http://messenger.softros.com/
Praize Messenger	http://www.praize.com/IM/
Eyeball (video)	http://www.eyeballchat.com/
Odigo	http://www.odigo.org/
Instant-T	http://www.bigblueball.com/im/others/instan-t.php, http://www.interactiveni.com/IMSite/indexim.htm
Ultramagnetic	http://ultramagnetic.sourceforge.net/
imGiant	http://www.imgiant.com/
BitWise IM	http://www.bitwiseim.com/
Hush Messenger	https://www.hushmail.com/services.php?subloc=messenger
iGo Incognito	http://www.igo-incognito.com/main.html
PSST	http://psst.sourceforge.net/
Encrypted Messenger	http://www.secureshuttle.com/

5. táblázat: Chat jellegű szolgáltatások

URL	*Név*
magyar IRC hálózat, mIRC klienssel	(http://www.mirc.com/)
Trefort-Net chat	http://chat.trefort.net
Unreal IRCd	http://www.unrealircd.com/

6. táblázat: Több protokollt használó programok

URL	*Név*
Miranda	http://www.miranda-im.org/
Gaim	http://gaim.sourceforge.net/
IM2	http://www.im2.com/
Trillian	http://www.ceruleanstudios.com/

3. számú melléklet

Szűkített lista

[SLIS]

A kísérletezés alapján a következő eredmények születtek:

- Az Instant Messenger kategóriából egészében le kell tesztelni az alábbi programokat:
  - **MSN**: A legszélesebb körben használt szolgáltatás, éppen ezért orvosi lóként funkcionál, a legtöbb probléma bemutatására alkalmas.
  - **ICQ**: Rendelkezik spam-bot és spam védelemmel (talán ebben a rendszerben a legaktívabbak a spim-merek), a legrégebbi rendszer.
  - **Skype**: Egyszerű, de az egyik legbiztonságosabbnak ígérkező rendszer.
  - **Yahoo Messenger**: Lényegében nagyon hasonló az MSN-hez, de érdekes újításokat is tartalmaz.
  - **BitWise Instant Messenger**: Saját útvonal választó (routing) szerver is felállítható. Szimpatikus, biztonságosnak tűnő rendszer. (Privacy védelem nem jelenik meg.)
- Ugyanebből a kategóriából érdemes megvizsgálni még speciális architektúrája, vagy más okok miatt:
  - **AIM**: Univerzális címjegyzék, reklámok a felületén, adatvédelmi beállítások.
  - **LAN Messenger**: Többszemélyes peer-to-peer LAN hálózati architektúra, adatvédelem.
  - **PSST**: Két végpont összekötése, azaz kizárólagosan peer-to-peer szolgáltatás.
- A chat jellegű szolgáltatásokból **UnrealRCd** szervert kell alkalmazni és kliensként **mIRC**-et kell használni (ez a páros is teljes körű elemzést igényelne, első sorban a szerveroldali funkciókra koncentrálva).

Az alábbi szolgáltatásokat szerettük volna még tesztelni, de sajnos különféle okok miatt erre nem volt lehetőség:

- **Gaim + OTR**: telepítési nehézségek adódtak
- **ScatterChat**: korábbi nevén UltraMagnetic, és a kutatás lezárása után jelent meg

4. számú melléklet

Osztályozási szempontrendszer

[TAXO]

A másodlagos elveket szürkével jelöltük (az alapkutatás idején időhiány miatt jelöltük meg ezeket).

Általános szolgáltatási attribútumok

1. **Szolgáltatás típusa**
    a. Chat jellegű
    b. Instant Messenger
    c. Peer-to-peer programok
2. **Hálózati modell**
    a. Központi szerver (-farm)
    b. Elosztott szerverek csoportja
    c. Peer-to-peer
3. **Fedőnévválasztás**
    a. Regisztráció köteles
    b. Tetszőlegesen választható
    c. Egyéb módon meghatározott
4. **Használható médiumok (az elsődleges kiemelt)**
    a. szöveges
    b. hang
    c. videó (és hang együtt)
5. **Beszélgetési lehetőségek**
    a. Privát beszélgetés két fél között
    b. Szoba, csatorna több fél között
    c. Web-kamera (két személyes)
    d. Mikrofon (két személyes)
    e. Konferenciák
        1. szöveges
        2. hang
        3. videó (hanggal)
6. **Felhasználó adatbázis (user directory)**
    a. Keresés
    b. Partnerlista
    c. Pszeudonim állapotának ellenőrzése
7. **Lefedett operációs rendszerek**
    a. Windows
    b. Linux
    c. Webes elérésű felület
    d. Macintosh
    e. Pocket PC, mobiltelefon
8. **Kezelőfelület**
    a. Grafikus
    b. Parancsvezérelt

A négy fő magánéletvédő, adatvédelmi és kiegészítő kritériumok

1. **Anonimitás**
2. **Pszeudonimitás**
3. **Megfigyelhetetlenség**
4. **Összeköthetetlenség**

Kiegészítő kritérium

1. **Összekapcsolhatatlanság**

Egyéb magánszféra és adatvédelmi szempontok

1. **Megjelenési módok**
    a. Anonim
    b. Regisztrációs pszeudonim, azonosító
    c. Tetszőleges pszeudonim, független a regisztrációs azonosítótól
2. **Rejtőzködési lehetőségek**
    a. Láthatóság felhasználónként
        i. ideiglenesen látható marad a felhasználó
        ii. ideiglenesen láthatatlan lesz a felhasználó
        iii. örökre láthatatlan lesz a felhasználó (letiltás)
        iv. örökre látható lesz a felhasználó (rejtőzködő mód ellenére is)
    b. Láthatósági listák
    c. Lista a felhasználót partnerként felvettekről
    d. Láthatatlan üzemmód (és bejelentkezés)
    e. Mellőzési lista
    f. Keresési és listára felvételi kritériumok
3. **Rendelkezés a profilról, a felhasználóhoz kapcsolódó adatokról**
    a. Rendelkezési lehetőségek
    b. Webes felületen megjelenhet-e
    c. Látható-e ismeretlenek számára
    d. Web-kamera, mikrofon jelenlétének felfedése
    e. Naplózási kérdések
    f. Belépési adatok kezelése
4. **Adatvédelmi nyilatkozat**
5. **(Adatvédelmi elvek)**
6. **Tevékenységek automatikus felfedése**
    a. Lejátszott zenék, filmek címének kiírása
    b. Játékok
    c. Web-kamera képernyőjének mutatása
    d. Eltávozás a számítógéptől, állapotváltoztatások
7. **Audiovizuális magánszféra védelme**
    a. Hangklipek tiltása
    b. Emotikonok tiltása
    c. Felhasználói képek és emotikonok tiltása
    d. Hangbetétek tiltása (dal, zenerészletek)
    e. Animációk tiltása

   f. Közös háttér, megjelenítési stílus tiltása
   g. Bizonyos üzemmódban a hangok tiltása
   h. Beérkező (VoIP) hívások tiltása, vagy csendes üzemmód
   i. A kellemetlen kifejezések szűrése
8. **Spam védelem**
   a. Spam-botok elleni védelem
   b. Hirdetési üzenetek szűrése
9. **Kapcsolódó szolgáltatások rákényszerítése a felhasználóra**
   a. Telepítéskor felmásolt programok, kiegészítések
   b. Tartalmi szolgáltatások (időjárás jelentés, hírek, stb.)

Biztonsági funkcionalitás

1. **Beléptetés védelme**
2. **Védett szakaszok (és alkalmazott technikák)**
   a. kliens-szerver
   b. szerver-szerver
3. **Védelem típusai a különböző médiumokra (szöveg, hang, videó)**
4. **Figyelmeztetés gyanús eseményekre, fájlokra (pl. phising)**
5. **A biztonsági „szint” beállíthatósága**

Audiovizuális magánszféra elemeinek magyarázata:

- Hangklip: mikrofonnal rögzített felvétel, amelyet
- 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.
- 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.

5. számú melléklet

Empirikus mérési eredmények jegyzőkönyve

[EMER]

A táblázatok, jelzések, számozások az Osztályozási szempontrendszerből kiolvashatóak, azaz a [TAXO] mellékletben találhatóak.

7. táblázat: általános szolgáltatási attribútumok szolgáltatásonként

	1.	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**8.**
MSN	b	a	a	a(bc)	acde:i	b[1]	ace	a
ICQ	b	a	a	a(bc)	abcd	ab	ac	a
Skype	b	a	a	b(ac)	acde:i ,ii	ab	abde	a
Yahoo	b	a	a	a(bc)	acde:i ,ii,iii	b	a	a
BitWise	b	a	a	a(b)	ace:i[2]	ab	abd	a
AIM	b	a	a	a(bc)	acde:i ,ii	b	abd	a
LAN	c	c	bc[3]	a	ae:i[4]	b	a	a
PSST	c	c	b	a	a	-[5]	ab	a
mIRC + unreal IRCd	a	b	ab	a	ab	c	a(bcde)	b

[1] A Windowsba való bejelentkezéskor használt felhasználónév jelenik meg felhasználói névként, de ez megváltoztatható.
[2] „Broadcast” (üzenetszórásos) üzenet küldési lehetőség
[3] A VOIP (Voice over IP) konferencia lehetőségét technikai okokból nem tudtuk kipróbálni.
[4] A PSST esetében ki kell jelölnünk az IP címet, ahová csatlakozni szeretnénk, nincs lehetőség más felhasználók keresésére, ellenőrzésére (legfeljebb egy figyelő PSST programéra).
[5] Van keresés a programban, de felhasználók keresésére eredményesen nem használható.

MSN [MSN]

Magánszféra és adatvédelmi szempontok

1. **Megjelenési mód:** b
2. **Rejtőzködési lehetőségek**
    a. Láthatóság felhasználónként: iii
    b. Láthatósági listák: csak tiltás lista
    c. Lista a felhasználót partnerként felvettekről: van
    d. Láthatatlan üzemmód: van, bejelentkezés: van
    e. Mellőzési lista: nincs
    f. Listára felvét: engedéllyel, keresési feltételek: MSN Space-n belüli felhasználókat
3. **Rendelkezés a profilról, a felhasználóhoz kapcsolódó adatokról**
    a. Rendelkezések: láthatja, aki (beállítható)
        - Bárki
        - A blogot (MySpace) láthatja
        - Engedélyezett MSN-en
        - Barát listán van, vagy a barátaim baráti listáján
        - Külön kijelölt kapcsolatok, kapcsolat csoportok
    b. Webes felületen megjelenhet-e: csak ott
    c. Látható-e ismeretlenek számára: ha engedélyezett
    d. Web-kamera, mikrofon felfedése: csak webkamera, állítható
    e. Naplózási kérdések: utolsó beszélgetés végének megjelenítése az ablakban, állítható globálisan
    f. Belépési adatok kezelése: törölhető minden adat
6. **Tevékenységek automatikus felfedése**
    - Winamp (engedélyezni kell)
    - Windows Media Player (engedélyezni kell)
    - Teljes képernyős alkalmazás -> elfoglalt (engedélyezni kell)
    - Nincs a gépnél bizonyos idő után (engedélyezni kell)
7. **Audiovizuális magánszféra védelme**

a.	b.	c.	d.	e.	f.	g.	h.	i.
- [6]	+	+	+ [7]	+	[8]	+	[9]	-

8. **Spam védelem**
    Van, de nem hivatalos.[10]
    - Nem tudni, pontosan mit szűr
    - Nem szól, ha kiszűrt valamit
    - Nem állítható

[6] Amikor teszteltünk, ez a szolgáltatás nem volt elérhető
[7] Csak MSN+ kiegészítéssel működik, a hangok csak elfoglalt állapotban nem kerülnek automatikusan lejátszásra.
[8] Rákérdez mindenképp, csak az automatikus elfogadás állítható.
[9] Csendes üzemmód: elfoglalt állapotban, de a beszélgetésekre való felhívás, mint üzenet, ilyenkor is megjelenik.
[10] Forrás: http://en.wikipedia.org/wiki/MSN_Messenger

9. **Kapcsolódó szolgáltatások rákényszerítése a felhasználóra**
   Nem tudunk ilyenről.

Biztonsági funkcionalitás

1. **Beléptetés védelme:** nincs
2. **Védett szakaszok (+ alkalmazott technikák)**
   - kliens-szerver: nincs
   - szerver-szerver: nem áll rendelkezésre információ
3. **Védelem típusai a különböző médiumokra (szöveg, hang, videó)**: nincs

Megjegyzések:

- Rossz a rendelkezésre állás
- A protokollban inkonzisztencia lép fel néha: valaki offline, de mégse
- Az üzeneteket néha nem küldi el
- Néha úgy viselkedik, mintha nem küldené el, de mégis
- Profil
  - Születési dátum
  - Lakóhely országa
  - Szűrhető reklámkérés email, telefon, cím szerint (MSN vagy más kategóriában), 10 nap leállási határidővel
- Anonim adatgyűjtés, belegyezési alapon (opt-in), az opciók között kiválasztás

ICQ [ICQ]

Magánszféra és adatvédelmi szempontok

1. **Megjelenési mód:** b
2. **Rejtőzködési lehetőségek**
   a. Láthatóság felhasználónként: iii, iv
   b. Láthatósági listák: rejtőzködési és felfedési
   c. Lista a felhasználót partnerként felvettekről: nincs
   d. Láthatatlan üzemmód: van, bejelentkezés: nincs
   e. Mellőzési lista: nem lehet mellőzni, csak tiltás (VOIP mellőzés van!)
   f. Listára felvét: engedélyhez köthető, keresés: van, bárkire rá lehet keresni
3. **Rendelkezés a profilról, a felhasználóhoz kapcsolódó adatokról**
   a. Rendelkezések: önkéntes, nem kötelező egy adat sem
   b. Webes felület: státusz csak
   c. Látható-e ismeretlenek számára: igen
   d. Web-kamera, mikrofon felfedése: mindkettő
   e. Naplózási kérdések: igen/nem jellegű
   f. Belépési adatok kezelése: jelszót mentse-e
6. **Tevékenységek automatikus felfedése**
   - „Away”, „N/A” bizonyos idők után, távollét idejének opcionális mutatása
7. **Audiovizuális magánszféra védelme**

a.	b.	c.	d.	e.	f.	g.	h.	i.
x	-	x	x	x	x	+[11]	+	-[12]

8. **Spam védelem**[13]
   Csak a listán lévők üzenhetnek, listán kívüliek üzenetét nem automatikusan, csak jóváhagyás után fogadja el. Ezekre az üzenetekre a spam filtert is lefuttatja.
   Szűrés megadható még a weboldalakról küldhető üzenetekre (ICQ World-Wide-Pager) és a levelekben küldhető üzenetekre (ICQ Email Express).
   Az 5-ösben szavakra szűrni nem lehet, de a 2003b-ben volt ilyen.
9. **Kapcsolódó szolgáltatások rákényszerítése a felhasználóra**
   Nem tudunk ilyenről.

Biztonsági funkcionalitás

1. **Beléptetés védelme:** nincs
2. **Védett szakaszok (+ alkalmazott technikák)**
   - kliens-szerver: nincs
   - szerver-szerver: nem áll rendelkezésre információ
3. **Védelem típusai a különböző médiumokra (szöveg, hang, videó):** nincs

Megjegyzések:

[11] Kikapcsolhatóak a hangok külön. Állapottól egyébként nem függ.
[12] Lásd spam védelem.
[13] Forrás: http://www.icq.com/support/security/spam.html#filter

- ICQ 5 volt a kísérlet alanya az eltérő biztonsági és privacy lehetőségek miatt
- Ismeretlen bejegyzések az invisible és a visible listákon
- Multi User Chat: nagyon elrontott IRC kliens (UnrealIRCd a szerver), érdemes lesz megvizsgálni
- Az AIM hálózatát használja! (A lehallgatott üzenetek és az AIM kliens alapján is.) A két kliens között az átjárhatóság nagyon kezdetleges, de pl. a Gaim nevű kliens is közösen kezeli ezt a két csevegőhálózatot.

Skype [SKYPE]

Magánszféra és adatvédelmi szempontok

1. **Megjelenési mód:** b
2. **Rejtőzködési lehetőségek**
   a. Láthatóság felhasználónként: iii
   b. Láthatósági listák: tiltási lista
   c. Lista a felhasználót partnerként felvettekről: nincs
   d. Láthatatlan üzemmód: van, bejelentkezés: nincs
   e. Mellőzési lista: nincs
   f. Listára felvét: név, Skype név, email alapján, visszaigazolással; keresés: van, sok adat megadható a keresési feltételek között
3. **Rendelkezés a profilról, a felhasználóhoz kapcsolódó adatokról**
   a. Rendelkezések: Egy külön menü szolgál a Profil (Adatlap) módosítására. A partnerek száma, és a felhasználó helyi ideje alapból publikus. Az E-mail-t hash-elve tárolják, így csak az e-mail címet ismerők kereshetnek ez alapján[14]
   b. Webes felületen megjelenhet-e: nem
   c. Látható-e ismeretlenek számára: igen
   d. Web-kamera, mikrofon felfedése: automatikusan
   e. Naplózási kérdések: alapbeállításként aktív, majdnem nyílt szöveg formában a felhasználó gépén
   f. Belépési adatok kezelése: A Windows-os kliens minden bejelentkezésnél felkínálja az automatikus indítást, és bejelentkezést, a Linux-os nem.
6. **Tevékenységek automatikus felfedése**
   - „Nincs a gépnél”, „Nem érhető el” állapotok bizonyos idő után
7. **Audiovizuális magánszféra védelme**

a.	b.	c.	d.	e.	f.	g.	h.	i.
x	+[15]	x	x	x	x	+	+	-

8. **Spam védelem**
   Nincs.
9. **Kapcsolódó szolgáltatások rákényszerítése a felhasználóra**
   Tudomásunk szerint ilyen nincs.

Biztonsági funkcionalitás

1. **Beléptetés védelme:** külön nincs (ld. védett szakaszok)
2. **Védett szakaszok (+ alkalmazott technikák)**
   - kliens-szerver: van
   - szerver-szerver: nem áll rendelkezésre információ

[14] http://support.skype.com/index.php?_a=knowledgebase&_j=questiondetails&_i=390
[15] Az emotikonok nem csak letilthatóak, hanem animáltról állóképre is kapcsolhatók.

3. **Védelem típusai a különböző médiumokra (szöveg, hang, videó)**
    - szöveg: AES-256
    - hang: AES-256
    - videó – nem tudni, de valószínű van és AES-256

Megjegyzések:

- Jól használható tudásbázis, jól megszerkesztett, összeszedett honlap
- Privacy mód „feltörése”
- Létezik harmadik félen keresztül történő adatátvitel (relayed transfer) NAT mögötti kliensek esetén.[16]

[16] http://support.skype.com/index.php?_a=knowledgebase&_j=questiondetails&_i=125

Yahoo [YAHM]

Magánszféra és adatvédelmi szempontok

1. **Megjelenési mód:** b
2. **Rejtőzködési lehetőségek**
    a. Láthatóság felhasználónként: i, ii, iii
    b. Láthatósági listák: ignore lista (listán kívülieknek), kiegészítés: online, offline, permanens offline felhasználónként
    c. Lista a felhasználót partnerként felvettekről: nincs
    d. Láthatatlan üzemmód: van, bejelentkezés: van
    e. Mellőzési lista: nincs
    f. Listára felvét: kérelem és visszaigazolás; keresés: nincs
3. **Rendelkezés a profilról, a felhasználóhoz kapcsolódó adatokról**
    a. Rendelkezések: állapot megjelenítése Yahoo! weblapokon (alapból aktív); alapvetően nem létezik profil (üres), megjelenítési opciók (alapból kikapcsolva):
        - 18 éven felüliek nézhetik csak meg
        - Megjelenjen-e a Yahoo! Member Directory-ban?
        - Nyilvános-e, hogy az előbbiben az illető mennyi ideje tag
        - +1: a regisztrációs email cím része alapból, de nem látható.
    b. Webes felületen megjelenhet-e: alapvetően webes.
    c. Látható-e ismeretlenek számára: igen, erre nincs szabályozás.
    d. Web-kamera, mikrofon felfedése: kiválasztásra lehet valakiért megtekinteni, el is lehet ezt utasítani – automatikus felfedés nincs.
    e. Naplózási kérdések: külön állítható a hívásokról (csak VOIP) és a szöveges beszélgetésekről. Fokozatok: be, ki, illetve ideiglenes – kijelentkezésig.
    f. Belépési adatok kezelése: csak úgy törölni nem lehet, hanem kérni lehet a bejelentkezés utáni elfelejtését az adatoknak.
6. **Tevékenységek automatikus felfedése (mind opcionálisan választható)**
    - A Yahoo! rádiószolgáltatásának használata
    - Webes játékok használata a szolgáltatáson belül
    - Webkamera mutatásakor
    - „Idle” állapot bizonyos idő után, opcionálisan mutathatja a távollét idejét is.
7. **Audiovizuális magánszféra védelme**

a.	b.	c.	d.	e.	f.	g.	h.	i.
x	+	x	+[17]	+[18]	+	-	-	+

8. **Spam védelem**
   Word filter, három fokozattal: ki, alacsony és magas hatékonyság.
9. **Kapcsolódó szolgáltatások rákényszerítése a felhasználóra**
   Opcionálisan kikapcsolható a telepítés folyamán az összes.

[17] Audibles néven fut, ugyanez tekinthető az *e*. pontban szereplő animációknak
[18] Az Audibles tekinthető ennek

Biztonsági funkcionalitás

1. **Beléptetés védelme**: nincs kiemelt (de nem biztos)
2. **Védett szakaszok (+ alkalmazott technikák)**
    - kliens-szerver: nincs
    - szerver-szerver: nem áll rendelkezésre információ
3. **Védelem típusai a különböző médiumokra (szöveg, hang, videó)**: nincs valószínűleg

Megjegyzések:

- A tesztelés során többször lefagyott.
- Az Audibles néven futó animáció / hangfelvétel dolgok színvonalasak és roppant szórakoztatóak.
- A szöveges átvitel, nagyon lassú.

Bitwise [BITW]

Magánszféra és adatvédelmi szempontok

1. **Megjelenési mód:** b
2. **Rejtőzködési lehetőségek**
   a. Láthatóság felhasználónként: iii, iv
   b. Láthatósági listák: mindig látható, mindig láthatatlan, blokkolt (+ személyes távollétet jelző üzenet)
   c. Lista a felhasználót partnerként felvettekről: nincs, de ha felvesznek kérhető jelzés
   d. Láthatatlan üzemmód: van, bejelentkezés: van
   e. Mellőzési lista: nincs
   f. Listára felvét: bárki felvehet, keresési feltételek: white list esetén csak a már meglévő felhasználók léphetnek kapcsolatba a felhasználóval (a felvételre is igaz)
3. **Rendelkezés a profilról, a felhasználóhoz kapcsolódó adatokról**
   a. Rendelkezések: állítható a tartalma (alapból üres), a keresési információknál csak a felhasználónév szerepel („user dir”)
   b. Webes felületen megjelenhet-e: nincs ilyen
   c. Látható-e ismeretlenek számára: igen
   d. Web-kamera, mikrofon felfedése: csak mikrofon lehetőség, de nem jelzi
   e. Naplózási kérdések: kliens oldalon, plain text alapból, de több formátum támogatott[19]
   f. Belépési adatok kezelése: jelszó elfelejtése a következő belépésre
6. **Tevékenységek automatikus felfedése**
   - távolléti állapot (bekapcsolható)
7. **Audiovizuális magánszféra védelme**

a.	b.	c.	d.	e.	f.	g.	h.	i.
x	x	x	x	x	x	-	-	-

8. **Spam védelem**
   Nincs.
9. **Kapcsolódó szolgáltatások rákényszerítése a felhasználóra**
   Nincsenek.

Biztonsági funkcionalitás

1. **Beléptetés védelme**: védett szakasz
2. **Védett szakaszok (+ alkalmazott technikák)**
   - kliens-szerver: van
   - szerver-szerver: nem áll rendelkezésre információ
3. **Védelem típusai a különböző médiumokra (szöveg, hang, videó)**
   - szöveg, hang (utóbbi nem biztos): 128 bit kulcshosszú BlowFish (BIM Plus: 256 bites kulcsú BlowFish, Prof. 448 bit), 512 bites kulcsú RSA (Plus: 1024 bit)

[19] http://www.bitwiseim.com/wiki/index.php?title=URL_History

Megjegyzések:

- Problémák, ha NAT-os router az átjáró az Internet felé
- Hozzáértőknek előnyös, jól konfigurálható
- Érdekes megoldás a beállításoknál: ’Send to server’ gomb
    - Jelszó elfelejtése esetén új kérése, és akkor is van lehetőség, ha a regisztrációs email cím már nem él

UnrealIRCd + mIRC (SSL kapcsolaton keresztül) [URID]

Magánszféra és adatvédelmi szempontok

1. **Megjelenési mód:** ac
   Megjegyzések: Anonim, mivel a pszeudonim tetszőlegesen cserélhető. Ennek ellenére más információkkal az összeköthetetlenség meghiúsul. A „c" lehetőség értelmezése: speciális felhasználók esetén (pl. IRC szerver operátor), vagy más felhasználók esetében az azonosítás szükséges lehet. Ez esetben is lecserélhető a pszeudonim.
2. **Rejtőzködési lehetőségek**
   a. Láthatóság felhasználónként: nincs
   b. Láthatósági listák: nincsenek
   c. Lista a felhasználót partnerként felvettekről: nincs partnerlista
   d. Láthatatlan üzemmód: igen („+i usermode"), bejelentkezés: előzővel
   e. Mellőzési lista: van, „ignore list", „/ignore felhasználónév"
   f. Listára felvétel: nincs partnerlista, keresési feltételek: nincsenek, bárkire lehet keresni, kivéve +i felhasználókra

   Itt a „userdirectory" másképp néz ki, mint az IM-ek esetében. Nincs felhasználói partnerlista, hanem a felhasználóknak csupán a jelenlétét lehet ellenőrizni: „/ison", „/whois".
3. **Rendelkezés a profilról, a felhasználóhoz kapcsolódó adatokról**
   a. Rendelkezések: nincs profil.
   b. Webes felületen megjelenhet-e: nincs profil.
   c. Látható-e ismeretlenek számára: nincs profil.

      Megjegyzés az a, b, c pontokhoz: ha NickServ is fut a szerveren, akkor az tárol néhány információt, de ez a szolgáltatás webes felülettel nem rendelkezik. Továbbá a „whois" parancs is szolgáltat némi információt, noha ezek javarészét a felhasználó állítja be a kliens programban.

   d. Web-kamera, mikrofon felfedése: nem támogatott. Szinte biztosan léteznek olyan plugin modulok a mIRC alá, amelyek lehetővé teszik.
   e. Naplózási kérdések: A kliens csatornákat vagy privátokat naplóz (alap: mindkettő). A szerver beszélgetéseket nem, hanem üzeneteket és eseményeket naplóz.
   f. Belépési adatok kezelése: örökre megjegyzi. Jelszót alapesetben nem kezel a program, mivel általában nem szükséges; alapesetben a jelszavak a belépéshez a szerverhez és nem a felhasználóhoz köthető. Vannak a szervernek olyan moduljai, amivel ez megoldható, ennek a neve NickServ.

      Megjegyzés: kliens oldalon a profil jellegű adatok nagy része mind szerkeszthető. (Sok mindenre lehetőséget nyújt ugyanis a szerver is.)
6. **Tevékenységek automatikus felfedése**
   Nincs ilyen (legfeljebb kliensoldali kiegészítésekkel, erre számtalan példa létezik, de csak az alapklienssel foglalkozunk).
7. **Audiovizuális magánszféra védelme**

a.	b.	c.	d.	e.	f.	g.	h.	i.
x	x	x	x	X	x	x	x	+[20]

8. **Spam védelem**
   Van és nagyon korszerű, ám a használata nem egyszerű.
   - Védelem: spam, hirdetések, férgek és hasonló kártevők ellen
   - /spamfilter [add|del|remove|+|-] [type] [action] [tkltime] [reason] [regex]
   - type: üzenet típusa, mint például privát, csatorna, stb.
   - action: kill, …
   - tkltime: a büntetés időtartama
   - reason: a büntetés oka, magyarázat a filter mellé
   - reguláris kifejezés: a szűrendő kifejezés reguláris kifejezés alapú mintája
   - A szűrés alól egyedüli kivételek a szerver operátorok és a szolgáltatások.
   - A parancs hatása **globális**, az egész hálózatra kihat.
   - Ha konfigurációban szerepel, a hatás lokális csupán.
9. **Kapcsolódó szolgáltatások rákényszerítése a felhasználóra**
   Nincsenek, se a szerver, se a kliensprogramban.

Biztonsági funkcionalitás

1. **Beléptetés védelme**: SSL (ha mindkét oldal támogatja), STunnel-SSL (kliens-szerver)
2. **Védett szakaszok (+ alkalmazott technikák)**
   - kliens-szerver: SSL (ha mindkét oldal támogatja), STunnel-SSL (kliens-szerver)
   - szerver-szerver: SSL, ha be van állítva
3. **Védelem típusai a különböző médiumokra (szöveg, hang, videó)**
   - Szöveg: SSL (ha mindkét oldal támogatja), STunnel-SSL (kliens-szerver)

Egyéb védelmek, privacy nyújtó kényelmi megoldások:

- **Elárasztásos támadás elleni védelmek:**
  - Üzenetküldési sebesség limit
  - Belépési limit
  - Névváltás limit
  - +f mód szobákra: pl.: *+f [10j, 50m, 7n]:15*: 10 belépés, 50 üzenet, 7 névváltás legfeljebb minden 15 másodpercben, további opciók:
    i. j (+i), m (m), n (+N)
    ii. c (+C): CTCP (Client-To-Client-Protocol)[21]
    iii. k (+K): kopogások limitálása, +K védelem a szobára. kopogás: behívásos alapon működő szobára csak.
    iv. t (kick): ?
    v. *#Rn*: 5 percig érvényes a tiltás, korlátozás, pl. #K5: öt perc után leveszi a 'knock' korlátozást
- **Tiltás a szobákból**
  - nick!user@host alakban, * használható

[20] Szerver oldalon.
[21] http://en.wikipedia.org/wiki/CTCP

  - kiterjesztett tiltások (tiltások (+b) és kivételek (+e) is):
    i. ~<type>:<ext> alakban.
    ii. q: csöndes tiltás (ban). Az illető beléphet, de nem tud megszólalni. pl.: ~q:nick!user@host
    iii. n: tiltott névváltás. pl. ~n:nick!user@host
    iv. c: csatornán való jelenlét alapján tiltás. pl.: *~c:%#lamers*
    v. r: a megadott név ha tartalmazza, nem léphet be.
- **Tömeges tiltás:** IP csoportok tiltása
- **Tiltás a konfigurációban:** felhasználók tiltása különböző adatok (név, IP, host, valós név, verzió) alapján. + kivétel lista
- Szinte mindenre létezik kivétel lista, ez a konfigurációban is megadható.
- **További tiltások**:
  - Fájlküldés (engedélyezés szabály is van)
  - Szerver verzió: a szerver nem kapcsolódhat a hálózatba nála (erre a tiltásra általános szabály is van)
  - Szobanév: átirányítással (engedélyezés szabály is van)
  - Tiltott szavak: a tiltott szót lecseréli a megadottra
- **Szobamódok (kb. 25, csak a lényegesebbek):**
  - Színezések szűrése
  - Tiltott szavak szűrése a csatornán
  - Különböző operátori jogok: beszéd jog, fél-operátor, operátor, alapító
  - Meghívásos szoba
  - Tiltások, f mód
  - Kulcsos szoba
  - Átirányítás másik szobába, maximális felhasználó szám limit
  - Szoba regisztráltaknak
  - Moderált beszélgetés (beszéd joggal rendelkezőknek)
  - Névváltás tiltása
  - Privát, titkos szoba (nem listázható? mi a különbség?)
  - Tiltott témaváltoztatás
- **Felhasználó mód (nagyon sok, a lényegesebbek):**
  - Láthatatlan mód
  - Tiltott szavak szűrése
  - „whois” lekérdezések jelentése
  - Védelem a CTCP parancsoktól (pl. ping, finger, version, time)
  - Fertőzött DCC fájlküldésnél jelentést kap a kimoderálásról a felhasználó
  - Titkosított hosztnév
  - Jelzés arról, hogy a felhasználó SSL klienst használt-e.
  - Rengeteg operátor „flag”
- **Lényeges (a tanulmány számára érdekes) parancsok:**
  - whois: teljes név, hoszt, felh.név, kurrens csatornák, operátori státuszok, és extrák
  - who: keresés becenév, hosztmaszk, csatornanév szerint
  - whowas: whois, csak már kilépett felhasználókra. Ezen információk csak egy rövidebb ideig tárolódnak.
  - ison: felhasználói jelenlét ellenőrzése
  - version: egy adott felhasználó kliensprogramjának a verziójának és típusának a lekérdezésére szolgál
  - kick: ezzel lehet kirúgni egy felhasználót egy szobából

  - away: saját állapot beállítás, amolyan személyes üzenet jellegű kiegészítéssel
  - watch: felhasználókat figyel a rendszer és szól, ha csatlakoznak
  - list: szobák keresése
  - vhost: virtuális hoszt felvétele
  - userip: felhasználó IP-je
  - dns: felhasználó DNS információja
  - sethost, setident, stb.: a whois információk megváltoztatása, de csak operátoroknak
- **Kliens beállítások**
  - Minden lényegi üzenet kiírása állítható, a legtöbb eseményre való reakcióval együtt.
  - URL, email címek gyűjtése, megnyitása.
  - Különböző kifejezések kiemelése
  - Fájlfogadási beállítások: automatikus fogadás, elutasítás
  - Rengeteg kiegészítés, szkript létezik mIRC-hez, ezek rengeteg nagyon sok kiegészítő szolgáltatást tartalmaznak.

Megjegyzések:

- Telepítéskor tetszésnek megfelelő SSL tanúsítványt lehet létrehozni, méghozzá OpenSSL segítségével. Úgy tűnik, hogy feltelepít egy ilyet is.
- **Nagyon jó** dokumentáció.
- Úgy tűnik, hogy hálózatba csak azonos szerverekkel fűzhető.
- Cloaking: a valódi host és IP cím lekódolása.
- IPV6 is támogatott.
- ZIP links

További szolgáltatások vizsgálata

Gaim [GAIM] [GOTR]

- **MSN**
  - Elsőre látszik gyorstipp jelleggel, hogy ki az, akinek rajta vagyok a listáján, kinek nem – ez nagy előrelépés az eredeti kliens programhoz képest.
  - Külön figyelmeztetést lehet beállítani minden felhasználóra. Pontosan meg lehet adni, hogy milyen esemény esetén és mivel figyelmeztessen.
  - A profil rögtön megjeleníthető – ha létezik.
- **ICQ**
  - IP címet kiírja
  - Mióta van bejelentkezve a felhasználó
  - A két kliens közti képességek
- **Yahoo**
  - Szobalista
  - Ki léphet kapcsolatba velem:
    - Mindenki
    - Partnerlista
    - Felhasználólista
    - Mindenki tiltása
    - Lista tiltása
- **Gaim általában (érdekesebb beállítások)**
  - Távollét automatikus jelzése, bizonyos idő után. Beállítható automatikus üzenet.
- **Gaim OTR**[22]
  - Amit nyújt (más szolgáltatások nem írják le, hogy implicit módon ilyet nyújtatnának): bizalmasság (kódolással), a másik fél azonosságának biztossága, letagadhatatlanság, Perfect forward privacy.
  - Sajnos a telepítése nem sikerült Fedora Core 4 alá (függőség feloldás sikertelen).
  - Létezik PROXY változat is.
  - Diffie-Hellman protokollt használ kulcscserére (SS=g^xy), AES-t használ (EK kulccsal), Hash(SS) = EK, Hash(SS) = MK
  - MAC kódot is alkalmaz, MAC(Enc_EK(M), MK).
  - Minden üzenet után új kulcsot választanak, a régieket biztonságos módon törlik.

AIM [AIM]

- Universal Address Book: összevonja az Outlook, Outlook Express, Yahoo! és Hotmail címjegyzékeket egy kalap alá. Innen automatikusan kerülnek a felhasználók a felhasználói listára.
- Gyötrelmesen lassú.

[22] http://www.cypherpunks.ca/otr/otr-codecon.pdf

- Privacy beállítások (ilyen felállás még nem volt):
  - Blokk mindenkire, vagy listára.
  - *Kapcsolatfelvétel engedélyezés mindenkire, a kapcsolat listára, vagy egy külön megadott listára.*
  - Távolléti állapot látható-e mások számára.
  - *Gépelés jelzése.*
  - *Mobil eszköz használata esetén annak felfedése.*
- Reklámok: vagy a felhasználó lista felett, vagy a csevegő ablakokban.
- *A beszélgetések automatikus elutasítása (ezt tekinthetjük az eddigieknél nem szereplő mellőzésnek)*.

LAN Messenger [SLAN]

- LAN hálózatra, elosztott jelleggel: broadcast címen hirdetik a helyi hálózaton magukat a megjelenő kliensek UDP csomagokkal.
- Használ titkosítást: Blowfish 128
- Nincsenek szobák, konferenciák, csak olyan többes küldés van, amit a kijelölt felhasználók mind megkapnak.

PSST [PSST]

- **PSST 0.2**
  - Végpont-végpont összeköttetés
  - Erős titkosítás: 128 bites, algoritmus (vélhetően AES)
- **PSST II**
  - RSA: 1024-4096 bit + BlowFish 256 (kézzel generálva hozzá egy jó nagyméretű, nagy entrópiájú bitfolyam)
  - Kulcsok exportálása után, manuális kulcscserével történik a felhasználók felvétele
  - Nem tudtam kipróbálni, a két kliens nem tudott csatlakozni.

6. SZÁMÚ MELLÉKLET

AZ EGYES ANONIMIZÁLÓ PROTOKOLLOK RÉSZLETES ISMERTETÉSE

[ANPR]

ONION ROUTING (TOR)

Anonim kommunikációt biztosít speciális proxy szerverek és routerek révén. Elrejti a routing információt azáltal, hogy az adatfolyamot több routeren keresztül juttatja el a célhoz. Az útvonat az első node határozza meg, aki egyben egy proxy is az éppen igénybevett szolgáltatáshoz. Mindennek következtében az első node a legsérülékenyebb.

A kezdeményező és a fogadó közti kapcsolat kiépítéséhez a kezdeményező proxyja a lehetséges routerek sorából egy útvonalat választ a hálózaton belül és előállítja az onionnak nevezett csomagot, mely magába ágyazva tartalmazza a routing útvonalat.

Az adatszerkezet egymásba ágyazott titkosított rétegekből áll, egy palyload-dal körülvéve. Az onion felépítésének alapja az útvonal, melyet a küldő fél meghatározott az üzenet küldése előtt. Mindezek alapján a küldő az üzenetet először a fogadó fél kulcsával titkosítja, majd az útvonalban a fogadó előtt következő routerével, és így tovább, egészen az első routerig, akinek végül elküldi az oniont. Mikor az onion-t valaki megkapja, tudni fogja, hogy kitől kapta, és hogy kinek kell továbbítania, azonban semmit sem tud a többi node-ról, sem azt, hogy hányan vannak a láncban, és azt sem, hogy ő hányadikként szerepel benne.

Az X node a következő csomagot kapja: *{időbélyeg, következő hopp,* F_f*,* K_f*,* F_b*,* K_b*, payload}*$_{Kx}$ ahol: K_x az X node nyilvános kulcsa. A dekódolt üzenet egy időbélyeget tartalmaz a visszajátszás ellen, valamint a következő node címét, a payloadot, és két funkció/kulcspárt, meghatározva a kriptográfiai eljárást és a kulcsot, melyet az üzenetküldés során kell használni. Az (F_f, K_f) pár az onion eredeti útvonalirányához, az (F_b, K_b) pár a vissza irányhoz használatos.

Minden hoppnál az onionból lefejtődik egy réteg. Megakadályozandó, hogy a monoton csökkenő méret alapján egy külső megfigyelő meghatározza a routing útvonalat, minden egyes hopp után megfelelő hosszúságú véletlen adat fűződik a payload végére a továbbítást megelőzően. Az utolsó proxy az egyetlen, aki tisztában van vele, hogy az üzenet mekkora része payload. Még a konstans méretű onionok is lekövethetők lennének, ezért minden onion azonos méretű kell legyen.

Nem szükségszerű, hogy a teljes útvonal meg legyen határozva a kezdeményező által. Meghatározhat bizonyos nodokat, melyek az útvonal során meghatározatnak egy saját routig vonalat. Ez egyrészt a biztonság tekintetében hasznos lehet, lévén több hoppot ad hozzá a lánchoz. Lehetőséget ad továbbá arra, hogyha egy node

nem ismer a másikhoz vezető összefüggő útvonalat, akkor is küldhessen számára üzenetet.

A válaszüzeneteket válasz onionok segítségével lehetséges megoldani. Hasonlóan az egyszerű onionhoz, csak a következő hopp ismeret az üzenetet továbbító node számára. A válasz onion felépítse is teljesen megegyezik az egyszerű onion-éval, így az útvonalon lévő nodeok nem tudják megkülönböztetni őket, és a válasz onionok is csak egyetlen egyszer használhatóak fel.

A **TOR** hálózat voltaképpen az onion routing második generációját jelenti, és az eredeti protokolltól néhány tekintetben eltér:

- A többszörösen titkosított adatszerkezet mellett a TOR speciális útvonaltervezést használ. A kezdeményező minden egymást követő hoppal egy viszony kulcsot egyeztet. Ezek a kulcsot a használat után törlődnek, így a kompromittált csomópontok nem képesek a régebbi forgalom megfejtésére.
- A TOR SOCKS proxy interfészt használ, ezáltal biztosítva a legtöbb TCP alapú program használatát különösebb módosítás nélkül. Továbbá a TOR a Privoxy nevű alkalmazás szintű PET proxy-n alapul, felhasználva annak filterező képességeit.
- A TOR *egyelőre* nem alkalmaz forgalommanipulálást, üzenetkésleltetést.
- Multiplexálja a TCP folyamokat az egyes csomópontok között, ezzel növelve az anonimitást és a hatékonyságot.
- Néhány csomópont központi szerverként működik, és ismert routerek nevét, valamint állapotát tárolják. A felhasználók HTTP-n keresztül töltik le ezeket az információkat bizonyos időközönként.
- A TOR az adatokat integritás védelemmel látja el, mielőtt küldésre kerülnének (az eredeti onion routing protokoll semmilyen integritásvédelmet nem tartalmazott).
- A TOR-hoz nincs szükség kernel kiegészítésekre az operációs rendszerben, sem külön hálózati verem támogatásra.

HORDES

A Hordes a Crowds protokollján alapul, és hozzá hasonlóan több proxy-t használ, hogy a csomagokat eljuttassa a fogadó félnek. Különbség azonban, hogy a HTTP proxy-k helyett a jondo-k (Corwds-ban a mixek neve) UDP kapcsolatokhoz szolgálnak proxyként. Az üzenet útvonalának felépülése a Crowds analógiájára történik, de további eltérés, hogy a válaszok multicast üzenetekként valósulnak meg. Mikor valaki üzenetküldést kezdeményez, egy multicast cím rendelődik hozzá.

Hordes csak a küldő számára biztosít anonimitást, a fogadó fél számára nem, mert az utolsó jondo-nak kapcsolódnia kell hozzá. Hacsak a fogadó fél nem vesz részt egy anonim kapcsolatban, a támadó észlelheti az üzenet fogadását. A küldő-fogadó összeköthetetlenség ezzel szemben mindig garantált.

A multicast használata több tekintetben is támogatja az anonim kommunikációt: Egyrészt a célállomás IP címe helyett a multicast csoport IP címe szerepel, és nem valamely host címe. Másodszor: nehéz megállapítani a valamely multicast csoportba

való tartozást. Harmadszor pedig, ha a multicast csoportba való tartozás ki is derül, a csoport tagjai jelentette fogadó készlet még mindig biztosítja az anonimitást.

A multicast révén a Hordes-nak majdnem fele annyi időre van szüksége, egy üzenetváltáshoz, mint a Crowds-nak.

Az ***inicializáció*** (új tag felvétele a hálózatba) öt lépésből épül fel:

1) A kezdeményező küld egy felvétel kérelmet a szervernek, hogy csatlakozhasson a Horde hálózathoz. Ez tartalmazza az IP-jét és egy nonce-ot, és a publikus kulcsát.
2) A szerver egy aláírt nyugtázást küld, mely tartalmaz egy új nonce-ot és a kezdeményező nonce-át.
3) A kezdeményező válaszként aláírva visszaküldi a nonce-okat.
4) Ha a visszaküldött nonce-ok jók voltak, akkor a szerver egy multicast báziscímet, melyet minden Hordes résztvevő használ, valamint az összes résztvevő listáját és a publikus kulcsaikat.
5) Végül a szerver egyetlen multicast üzenettel informál minden felhasználót, hogy a kezdeményező csatlakozott a Hordes-hoz.

Adatátvitel során, mivel a Hordes kezdeményező unicast üzenetet küld a fogadó félnek, és multicast üzenetben kap választ, így szabványos TCP kapcsolat nem használható. Ehelyett a kezdeményező és fogadó közötti TCP üzenetek UDP csomagokba beágyazva jelennek meg, melyek a továbbítási útvonalon szereplő jondo-k között közlekednek, illetve válaszadás során a fogadótól a kezdeményező felé mennek multicast UDP csomagok.

Az adatátvitel lépései:

1) A kezdeményező (és minden más jondo) véletlenszerűen választ néhány jondot a összes közül, hogy rajtuk keresztül küldjön üzenetet. Mindegyiküknek elküldi egy szimmetrikus kulcsot, a jondo nyilvános kulcsával titkosítva, és a kezdeményező által aláírva.
2) A kezdeményező választ egy multicast csoportot a teljes tartományból, melyen a Hordes jondo-i osztoznak. Ennek lényege, hogy felossza a lehetséges fogadókat, így a fogadókon nem megy át minden adat. Ekkor a kezdeményező csatlakozik a választott multicast csoporthoz, hogy megkaphassa a válasz üzeneteket.
   Adat küldéséhez a kezdeményező az 1-es pontban kiválasztott jondo-k közül választ egyet véletlenszerűen, és küld neki egy üzenetet, mely a fogadó címét, a megválasztott multicast csoportot, ahova a fogadó küldhet választ, egy véletlen számot az ütközések elkerüléséhez, és a küldendő adatot. Mindezt az 1-es pontban megosztott szimmetrikus kulccsal tikosítva küldi a kezdeményező.
3) Minden jondo, aki megkapja az üzenetet, $1 – p_f$ valószínűséggel a fogadónak küldi az üzenetet, és p_f valószínűséggel pedig egy másik jondo-nak a 2-es pontban kiválasztottak közül.
4) Néhány hopp megtétele után az utolsó jondo továbbítja az üzenetet a címzettnek.
5) A fogadó fél válaszát a kezdeményező által választott multicast csoporthoz küldi (az üzenet a véletlen számot, a fogadó azonosítóját és a választ tartalmazza).

A Crowds-hoz hasonlóan a Hordes esetében is ahelyett, hogy minden hoppnál véletlenszerűen választanánk meg a következő jondo-t, az összes jondo egy kisebb csoportjából választjuk ki az üzenet továbbítóját.

HERBIVORE

A Herbivore a DC-Net elvén alapul, mely elegáns megoldást jelent az anonim kommunikáció megvalósítására. A DC-Net elvi alapjai fentebb már ismertettük, azonban van néhány egyéb megvalósításhoz szükséges megkötés:

1) Az üzenetek küldéséhez és fogadásához minden résztvevőnek egy kulcsát tartalmazó gráfba kell szerveződniük. A Herbivore protokoll az optimális kommunikáció megvalósítása érdekében csillag topológiába szervezi az egyes node-okat.
2) Biztosítani kell, hogy egy időben csak egy node küldjön üzenetet. Ha többen akarnak üzenetet küldeni egy DC-Net-ben, az ütközést jelent, melynek eredményeként hibás üzenetek keletkeznek.
3) A hálózat megszervezése igényel némi üzenetváltást a résztvevők között, és egy anonim hálózatban nyilván ennek is anonim kell zajlania.

A DC-Net egyik gyengeségét jelenti, hogy a 2-es pont megkötéséből következően egy támadó könnyedén Szolgáltatás megtagadás (Denial of Service - DoS) alapú támadást indíthat. Tovább nehezíti a helyzetet, hogy mindezt anonim módon teheti. Bár léteznek módszerek az ilyen támadások azonosítására, melyek „csali” üzenetek küldésén alapulnak, amik segítségével nem csak a támadás, hanem a támadó kilétének felderítésére is alkalmasak. Mindennek persze megvan a maga ára: a protokoll bonyolultabbá válik, biztosítani kell, hogy a támadókon kívül a résztvevők anonimitását ne veszélyeztessék a „csali” üzenetek, és a sávszélesség a részét ezen csomagok számára kell fenntartani.

Összegezve azt mondhatjuk, hogy a DC-Net alapú protokollok erős anonimitást biztosítanak, de hatékonyságban és skálázhatóságban nehézségeik vannak.

A Herbivore protokoll két fő komponensből épül fel: a legalacsonyabb szinten a *round protokoll*, mely szabályozza, hogy a résztvevők között hogy történik az adatok küldése. Ez a protokoll biztosítja az erős anonimitást a DC-Net révén. A magasabb szinten lévő *global topology control* algoritmus a skálázhatóság, és támadók elleni védelem megvalósításáért felelős. Lényegében kisebb anonim csoportokra osztja fel a hálózatot. A Herbivore garantáltan k node-ot tartalmazó csoportokat hoz létre, ahol k egy előre meghatározott konstans a rendszerben, mely egyben a biztosított anonimitás erejét is meghatározza. Új csoportok automatikusan jönnek létre, ha egy adott csoport túl nagy méretűvé válik ahhoz, hogy hatékonyan működhessen.

A **Global Topology Control** legfontosabb része az **Entry Control Protocol**, mely három célt szolgál:

1) Megakadályozza, az olyan jellegű támadásokat, melyek az egyek node-ok anonimitásának kompromittálódásához vezetne. Ha egy node meghatározhatná, hogy melyik csoporthoz csatlakozzon, lehetővé válna, hogy támadók egy csoportban minden helyet elfoglaljanak, egyetlen egy kivételével.

2) Biztosítja, hogy az egyes csoportok létszáma hozzávetőleg egyenlő legyen azáltal, hogy az újonnan csatlakozókat véletlenszerűen sorolja be.
3) Kihívás alapú protokoll segítségével limitálja a hálózathoz csatlakozó node-ok szintjét.

Round Protokoll:
Mint már említésre került, ennek a protokollnak feladata, hogy egy adott csoporton belül szabályozza a node-okat, biztosítja az anonim adattovábbítást, és megfelelő adattovábbítási sebességet biztosít. Az adattovábbítás minden esetben három lépésből épül fel:

1) *Foglalási Fázis:* minden node, aki ebben a ciklusban szeretne üzenetet küldeni egyaránt véletlenszerűen választ egy i számot {1…m} halmazból, majd anonim módon elküld egy m-bit hosszú vektort, az i-edik helyen egy 1-es értékkel, és minden más helyen 0-val. Akik nem akarnak küldeni, azok mind a 0 vektort küldik. Ha egynél több node szeretne egy adott szeletet lefoglalni, akkor ez nyilván ütközést jelentene, és ekkor a node-ok egyszerűen várnak a következő ciklusra, és ott újra megpróbálnak küldeni.
2) *Átviteli Fázis:* minden node, aki sikeresen lefoglalt egy szeletet, elküldi a csomagját a megfelelő szeletben, mindenki más 0-t küld. Minden node egyszerre küld és fogad ebben a fázisban. Ezzel a node-oknak lehetősége van detektálni a támadót, hiszen a csatorna figyelésével észlelheti, hogy a csatornán észlelt csomag nem egyezik meg az általa küldöttel. Azok, akik ütközést észlelnek, várnak a következő ciklusra, és ekkor próbálnak meg újra küldeni.
3) *Kilépési Fázis:* ennek a fázisnak a feladata, hogy biztosítsa, hogy a hosszú ideje fennálló kapcsolatok védettek legyenek a hálózati forgalomanalízis ellen. A fázisban eldől, hogy egy adott ciklus alkalmas-e rá, hogy változzon a csoport felépítése.

Hálózati Topológia:
Az anonimizáló csoportok a Herbivore-ban csillag topológiába szerveződnek. Minden node elküldi a kulcsának és – ha van – akkor az üzenetének XOR-ját a csillag közepének, aki aztán továbbítja a dekódolt üzenetet a csillag maradék k-1 tagjának. Az ilyen topológiájú hálózatban 2*(k-1) bit küldésére van szükség, hogy egy node 1 bitet anonim küldhessen.

P^5 – PEER-TO-PEER PERSONAL PRIVACY PROTOCOL

A P^5-ben nincs szükség globális nyilvános kulcs infrastruktúrára, azonban feltételezhető, hogy ha két fél kommunikálni szeretne, akkor megtudhatják egymás nyilvános kulcsát, valamilyen szolgáltatástól független módon. Vegyünk N egyént, akik egy anonim kommunikációs rendszert szeretnének kiépíteni a P^5 segítségével. Mindegyikőjük rendelkezik $K_0,\ldots,K_{n-1}$ nyilvános kulcsokkal. A protokoll ezen N résztvevő kulcsait – melyeket *kommunikációs kulcsoknak* nevezünk – fogja felhasználni, hogy kiépítsen egy *logikai broadcast hierarchiát*.

A logikai broadcast hierarchia egy bináris fa (*L*), mely a $K_0,\ldots,K_{n-1}$ kulcsok felhasználásával épül ki. Az *L* fa minden tagja egy meghatározott hosszú bitsorozatot

birtokol. Egy adott csoportba tartozást jelöljön (*b/m*), ahol *b* a bitsorozat, és *m* az érvényes bitek száma.

L fa gyökere a null bitsorozatot tartalmazza a nulla hosszúságú maszkkal. Jelöljük a gyökeret (*/0) –val. A gyökér bal fia tartalmazza a (0/1) csoportot a jobb fia pedig az (1/0) csoportot. Hasonlóan (0/1) bal fia (00/2) lesz, míg jobb fia (01/2), és így tovább.

Egy üzenetet elküldenek egy adott csoportnak, akkor az továbbítódik a rendszer összes résztvevőinek egy részhalmazához. Például, ha az A felhasználó a (*b/m*) csoportnak küld üzenetet, akkor az üzenet továbbítódik a B felhasználónak is a (*b'/m'*) csoportba akkor és csak akkor, ha a k legnagyobb helyértékű bitek *b*-ben és *b'*-ben megegyeznek., ahol k = min {*m, m'*}.
Tehát egy (*b/m*) csoportnak küldött üzenetet az *L* fa három különböző részére lesz elküldve:

- **Lokális:** a (*b/m*) csoportnak küldött üzenet a (*b/m*) minden tagja megkapja.
- **Gyökérig vezető útvonal:** Minden *m'*<*m* esetén az üzenet el lesz küldve a ($b_{m'}$/*m'*) csoport minden tagjának, ahol $b_{m'}$ a *m'* hosszú prefixét jelöli *b*-nek.
- **Részfa:** Minen *m''*>*m* esetén az üzenet el lesz küldve minden (*b*|**/m''*) csoportnak, ahol *b*|**/k* nem más, mint bármilyen *k* hosszú bitsorozat, mely a *b* bitsorozattal kezdődik.

A felhasználók leképezése az *L* fába hash függvény (H(.)) segítségével történik. Vegyük az *A* felhasználót, és az ő K_A nyilvános kulcsát. Legyen $b_A=H(K_A)\ modulo\ 2^L$. Az *A* felhasználó ekkor a (b_A/*m*) csoporthoz fog csatlakozni. Az *m* maszk hosszát az *A* felhasználó választja meg, minden tényezőtől függetlenül és véletlenszerűen. A választott *m* paramétert titokban kell tartania, hogy ne derülhessen ki, pontosan melyik csoportnak tagja. Habár a nyilvános kulcsok ismeretében mindenki által ismeretes, hogy a felhasználó mely csoportoknak lehet tagja, de azt azonban nehéz meghatározni, hogy ebből a készletből konkrétan melyik csoportba tartozik.

Az üzenetek azonos hosszúságúak, és hopponként titkosítottak, ebből következően nem lehetséges egy kimenő üzenetet azonosítani egy a node által korábban fogadottal. Azonban egy passzív megfigyelőnek lehetősége van statisztikai támadásra, és lekövetheti a kommunikációt azáltal, hogy egy forrástól induló csomag folyamot összefüggésbe hoz egy nyelővel. Éppen ezért a protokoll *nosie* (azaz zaj) csomagokat használ, melyek révén az efféle statisztikai támadás költsége megnő, és alkalmatlanná válik a megfigyelésre.

A P^5 felhasználók minden időpillanatban fix nagyságú forgalmat generálnak egy véletlenszerűen meghatározott csatornára. Egy node által küldött csomag az alábbiak egyike lehet:

- A csomag (noise vagy signal) valamely bejövő interfészen érkezett, és a node egy másik csatornára továbbítja.
- Signal csomag, melyet helyileg generáltak
- Noise csomag, melyet helyileg generáltak

A P^5-ben a tagok egyszerűen eldobnak minden üzenetet, melyhez nincs meg a megfelelő számítási, illetve sávszélesség béli kapacitásuk. A rendszer globális jellemzői attól függnek, hogy az üzenetek eldobása hogy zajlik. Két különböző algoritmus jöhet szóba:

- Egységes csomagdobás: ez a legegyszerűbb séma, melyben az üzenetek a bemeneti sorból egyenlő valószínűséggel lesznek eldobva, egészen addig, amíg a bemeneti sor mérete nem csökken a maximális küszöb alá.
- Nem egységes csomagdobás: ebben a sémában az *L* fa magasabb csúcsaiban a csomagok nagyobb eséllyel kerülnek eldobásra.

7. SZÁMÚ MELLÉKLET

NÉHÁNY ISMERTEBB TÁMADÁS ANONIMIZÁLÓ HÁLÓZATOK ELLEN

[APAT]

Predecessor támadás: a támadás alapját megfelelő módon és megfelelő időben együttműködő támadók jelentik. A támadás során a fogadó felet használjuk referenciának, és minden üzenetváltásra rögzítjük a lehetséges kezdeményezők halmazát. A kommunikáció feltételezett kezdeményezője az lesz, aki a fenti lehetséges kezdeményezők halmazaiban a legtöbbször szerepel.

Szolgáltatás megtagadás (Denial of Service - DoS): az ilyen típusú támadások lényege, hogy lehetetlenné tegye a kommunikációt. Anonimizáló hálózatok esetében külön nehézséget jelent, hogy mivel a kommunikáció anonim, így a szolgáltatás megtagadási indító támadó kiléte sem ismert.

Sybil támadás: a támadás során több támadó csatlakozik a hálózathoz, és valamilyen módszerrel (legtöbb esetben szolgáltatás megtagadás révén) rákényszerítik a felhasználókat, hogy velük egy időben csatlakozzon egy csoporthoz, ezzel kompromittálva az anonimitását.

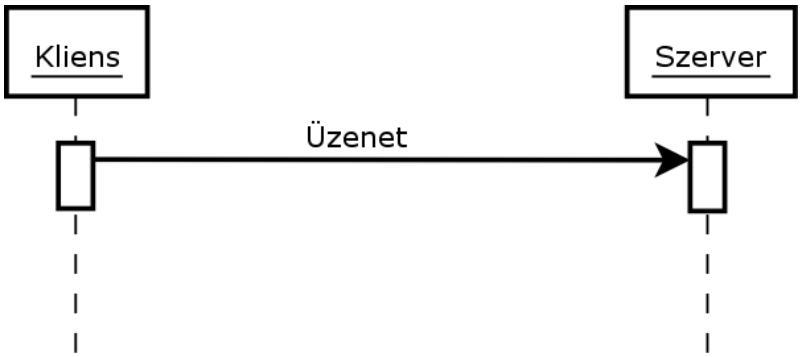
Lokális lehallgatás: a támadás akkor jelent veszélyt, ha a protokollban lehetőség van arra, hogy nem minden résztvevő küld és fogad egyenletes mértékben. Ebben az esetben ugyanis, ha a támadó kellően nagy erőforrásokkal rendelkezik, akkor a küldők üzeneteinek időzítés alapú analízisével mód nyílik a fogadók lehetséges listájának meghatározására.

8. SZÁMÚ MELLÉKLET

SZÁLLÍTÁSI PROTOKOLL QOS SZINTEK

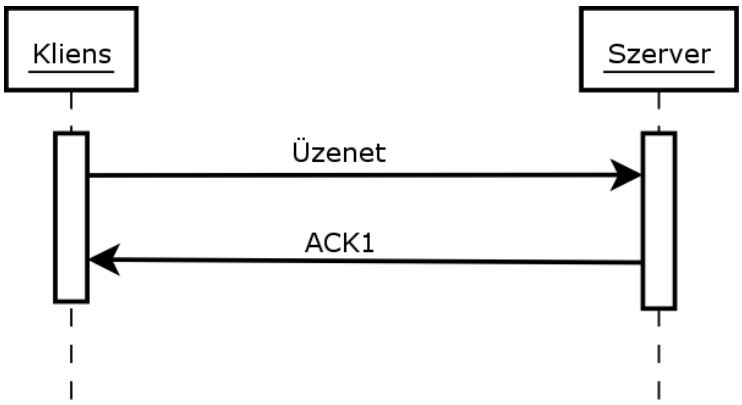
[QOSM]

Több üzenetközvetítési megbízhatósági szintet különböztethetünk meg [*QOS1*]:



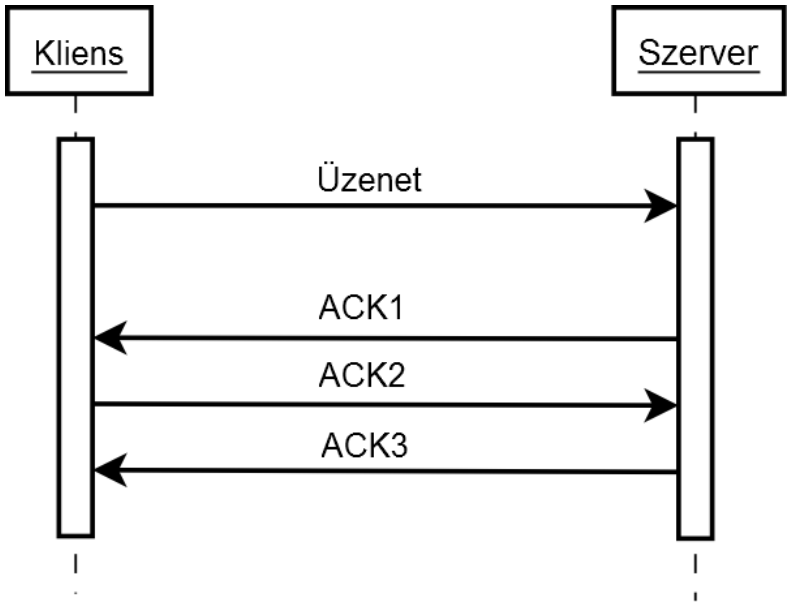
20. ábra: Legfeljebb egyszer megérkező (at most once) üzenet

- Legfeljebb egyszer megérkező üzenet: nem szükséges visszaigazolni, ugyanis vagy megérkezik egyszer, vagy soha nem érkezik meg.



21. ábra: Legalább egyszer megérkező (at least once) üzenet

- Legalább egyszer megérkező üzenet: akkor ismételjük meg az üzenetet (sorszámmal címkézve), ha nem érkezik visszaigazolás a megérkezéséről. Így egyszer legalább megérkezik, amennyiben elegendő ideig vagy alkalommal próbálkozunk.



22. ábra: Pontosan egyszer megérkező (exactly once) üzenet

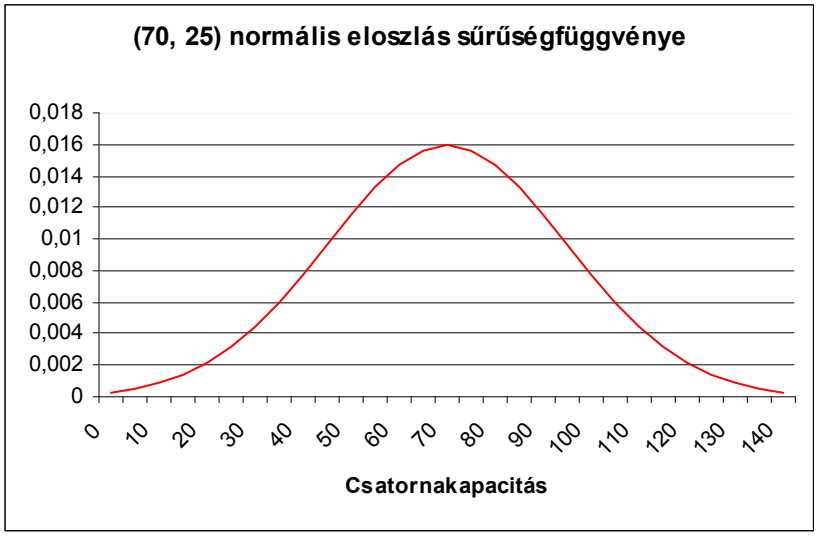
- Pontosan egyszer megérkező üzenet: nem elegendő csak visszaigazolásra várni (*ACK1*), mert akkor az előbbit kapnánk. A visszaigazolást (*ACK1*) is vissza kell igazolni (*ACK2*), hogy a távoli csomópont tudja, hogy megkaptuk az *ACK1*-et. Mivel mindkét résztvevő követi az üzenetek sorszámához kapcsolódó állapotot, így a feladó az *ACK1* érkezésekor azt tudja, hogy megérkezett az üzenete, a címzett az *ACK2* érkezésekor pedig azt, hogy soha többé nem fogja újraküldeni azt a feladó. Ezt a címzett *ACK3*-mal nyugtázza, és az eredeti üzenetet továbbítja a felsőbb réteg felé. Amennyiben az üzenet vagy *ACK1* elvész, nincs gond, hagyományos újraküldés történik, és mivel az üzenet nem lett még továbbadva, nem lesz kétszerezés a felsőbb protokoll szinten. Az *ACK2/ACK3* szekvencia ugyanilyen újraküldéses megoldás, ha bármely elvész, a megfelelő oldalon újraküldik.

9. SZÁMÚ MELLÉKLET

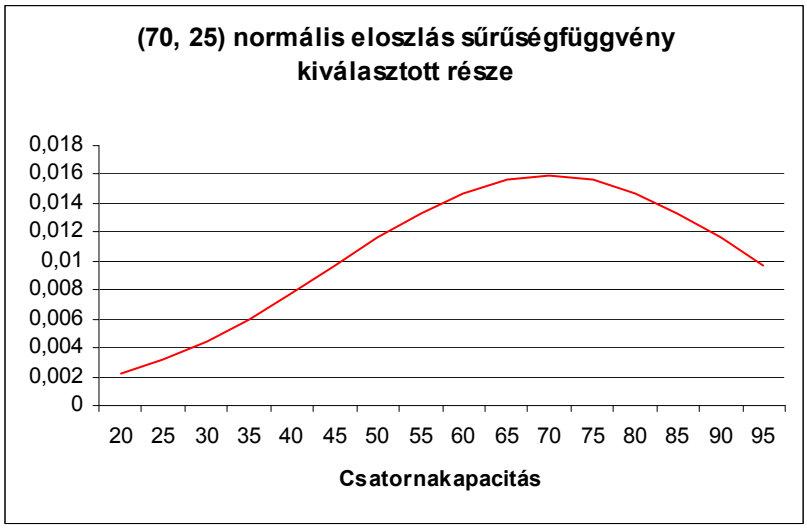
A SŰRŰSÉGFÜGGVÉNY LEVEZETÉSE

[MAT1]

Egy normális eloszlás sűrűségfüggvényét fogjuk alapjául venni az eloszlásnak. A várható értéke, szórása legyen olyan, hogy a csatorna kihasználtsága 20-95% között ingadozik. Az így előállított sűrűségfüggvény, normális eloszlásból származtatva, nem megfelelő, ugyanis a függvény teljes tartományra vett integrálja nem 1. A csatorna maximális kapacitását C_{MAX} –al jelöljük. Az eloszlás várható értéke $\mu = 0.7\, C_{MAX}$, szórása $\sigma = 0.25 C_{MAX}$. A sűrűségfüggvényből így a várható értéktől pozitív irányba egyszeres, negatív irányba kétszeres szórást engedélyezve az így elért felső határ legyen $0.95\, C_{MAX} (B_{MAX} = 95)$, az alsó pedig $0.2\, C_{MAX} (B_{MIN} = 20)$, tehát a csatorna kihasználtsága 20-95% között ingadozik. Az alábbi ábrán látható a sűrűségfüggvény és a figyelembe vett tartomány:



23. ábra: a (70, 25) normális eloszlás sűrűségfüggvénye a csatornakapacitás százalékos értékeit tekintve. A csatornakapacitás 100% fölé nem mehet, az ábra csak az átláthatóság kedvéért teljes.



24. ábra: A 20-95%-os értékeket felvevő tartománya az előbbi eloszlásnak.

Ez a sűrűségfüggvény még nem megfelelő, ugyanis nem teljesül rá a sűrűségfüggvények azon, tulajdonsága, hogy $\int_{-\infty}^{+\infty} f'(x)dx = 1$ (ahol az *f'(x)* a 20-95 tartományban értelmezett sűrűségfüggvény, amelyet $\varphi_{70,25}(x)$-ből származtatunk), hiszen ezt a sűrűségfüggvényt nem a teljes értelmezési tartományán vesszük. Tegyük fel, hogy $1 - \int_{-\infty}^{+\infty} f'(x)dx = c$, ekkor hogy teljesüljön a hiányzó kritérium, növeljük meg a kiintegrált területet épp *c*-vel, ehhez „egy *c* területű téglalapot illeszthetünk a függvény alá". A téglalap egyik oldalhossza 75 (= 95-20), a keresett magasság legyen *a*. A $c = a * 75$-ből kiszámolható, hogy a függvénynek a magassága $a = \frac{c}{75}$. Így a kívánt sűrűségfüggvény:

$$f''(x) = \begin{cases} 0, x < 20 \\ \varphi_{70,25}(x) + a, 20 \le x \le 95 \\ 0, x > 95 \end{cases},$$

amelyre már teljesül, hogy

- $\int_{-\infty}^{+\infty} f''(x)dx = 1$
- $f''(x) > 0$.

A 23. és 24. ábrák példájánál maradva, $a = \frac{1 - (\varphi_{70,25}(95) - \varphi_{70,25}(20))}{75} \cong 0{,}00242$. Mivel követelmény az eloszlás dinamikus változtathatósága, ezért általánosan megfogalmazva: $a = \frac{1 - (\varphi_{70,25}(B_{MAX}) - \varphi_{70,25}(B_{MIN}))}{B_{MAX} - B_{MIN}}$. Természetesen a szórás és a várható érték is paraméterezhető lehet.
Kiemelnénk, hogy az így kapott új sűrűségfüggvény számítási módszere csak egy származtatási lehetőség a sok közül.

10. SZÁMÚ MELLÉKLET

SZÁLLÍTÓ PROTOKOLL FORMÁLIS STRUKTÚRÁJA

[TRST]

A SZÁLLÍTÓ PROTOKOLL KOMMUNIKÁCIÓS FELADATAI

A szállító protokoll feletti réteg vezérli a protokoll párbeszédeket, s felelős azok megfelelő formátumú és üzenetváltású lefutásukért mind a szerver, mint a kliens architektúrában. Ez a réteg az elküldendő üzeneteit megfelelően címezve és paraméterezve átadja a szállító protokollnak, amely egy struktúrába rendezi azt. Ez a struktúra az alsóbb rétegekhez kerül, majd azok végzik a szállítását a célhoz. A cél a struktúra kicsomagolásával át tudja adni a felsőbb rétegbeli protokollértelmezőnek azt.

A struktúra valósítja meg a megfelelő címzést, hiszen az alsóbb rétegekben az nem lehetséges, mert a peer-to-peer kapcsolatok nem megengedettek, így valamely központi elem végzi a célállomás feloldását. A címzett és feladó adatain kívül tartalmaznia kell egyértelmű utalásokat a szállító protokoll verziójára, az üzenet típusára és pontos tartalmára.

FORMÁLIS STRUKTÚRA

A struktúra a könnyű bővíthetőség és rugalmasság miatt XML alapú. Megkülönböztetünk kötelező mezőket, amelyeket minden üzenetnek tartalmaznia kell. Továbbá üzenettípusonként[1] további mezők és bináris csatolmányok is szerepelhetnek az üzenetek részeként.

Kötelező mezők

8. táblázat: a szállító protokoll struktúrájának kötelező mezői és magyarázatuk.

Mező	Szerep
Protokoll verzió	Annak a protokollnak a verziója, amelytől érvényez az üzenet. Például „1.0.5”. Ezen mező alapján egyből eldöntheti a kliens, hogy értelmezi, vagy eldobja-e az üzenetet.
Feladó	A feladót egyértelműen azonosító érték.

[1] Az üzenettípusok meghatározása a protokoll párbeszédek meghatározásánál szerepel, ugyanis a lehetséges üzenetformák onnantól ismeretesek.

	Például az UID értéke.
Címzett	A címzettet egyértelműen azonosító érték. Mivel a címzett egyértelmű jelölésére nincs lehetőség, ezért a mezőben profilazonosító szerepel. A profilazonosító és a feladó alapján a címzett feloldása a központi adatbázis alapján már lehetséges.
Üzenet típusa	Az üzenet pontos típusát megadó mező. Ilyen lehet például a bejelentkezés során generálódott belépést kérvényező üzenet, amelyet jelölhetnénk „login-request” azonosítóval is, így az üzenet típusa ez lehetne.

További mezők

További mezők deklarálásának csupán az üzenettípusok meghatározása mellett van értelme, hiszen ezek típusonként eltérőek lehetnek. A protokoll üzenet típusok meghatározása után kell a további mezőket típusonként tételesen meghatározni.

Bináris csatolmányok

A protokoll alapvetően kisebb méretű bináris csatolmányok számára készül. A nagyméretű bináris fájlok (például, amelyeket a felhasználók egymásnak küldenek) közvetlenül egy bináris módú csatornán keresztül továbbítják egymás felé[2]. A protokoll által továbbított, és szöveges módúvá kódolt csatolmányok tipikusan legfeljebb 100-150 KB méretűek. Az alábbi táblázat a bináris csatolmányok kötelező mezőit szedi össze. Ezek a mezők üzenettípusonként tovább bővíthetőek.

9. táblázat: a szállító protokoll bináris fájlcsatolmányainak kötelező mezői és magyarázatuk.

Mező	**Szerep**
Szöveges azonosító	Azonosítja a bináris csatolmányt, hiszen több is előfordulhat egy üzenet csatolmányaként. Lehet egyszerű referenciaszöveg, de fájlnév is. Például „meduza.jpg”. De lehet például „nicsak”, amely egy emotikont tartalmaz, és a szövegben hivatkoznak rá. Például „:nicsak:” szintaktikával.
MIME típus	A csatolmány MIME típusa. Pl. „image/jpeg”.
Méret	A csatolmány pontos mérete bájtban

[2] Itt közvetlen peer-to-peer csatornáról van szó. Ennek a veszélyességére fel kell hívni a felhasználók figyelmét, hiszen az ilyen kapcsolat felfedi a felek között a másik fél IP címét.

	megadva.
Tartalom	A tartalom szöveges formátumúra fordítva. A fordítást lehetne végezni base64 kódolással.

A bináris csatolmányok kerülhetnek későbbi felhasználás céljából eltárolásra is (cache mechanizmus). Ennek célja, hogy a gyakran küldött csatolmányokat ne kelljen a hálózaton mindig átküldeni, így a terhelés kisebb legyen.

11. SZÁMÚ MELLÉKLET

ROLE-BASED ACCESS CONTROL SZABÁLYOK

[RBRM]

10. táblázat: Role-Based Access Control szabályokra néhány példa.

Művelet	Szerepkörök	Megjegyzés, megkötések
RBP műveletek [Tiltás, mellőzés, engedélyezés]	Felhasználó sajátja	A felhasználó szerepkörébe fel kell venni a műveletek engedélyezését.
Álca, felfedés [Látható adatlap (későbbiekben profil) megtekintése]	Felhasználó sajátja	A felhasználó szerepkörébe fel kell venni a műveletek engedélyezését.
Meghívás szobába	Szoba operátor	
Meghívás konferenciába	Konferencia operátor	
Privát beszélgetés kezdeményezése (és tetszőleges üzenetek küldése)	Felhasználó sajátja	A felhasználó szerepkörébe fel kell venni a műveletek engedélyezését.
Fájlküldés	Felhasználó sajátja	A felhasználó szerepkörébe fel kell venni a műveletek engedélyezését.
Felvételi kérelem a partnerlistára	Felhasználó sajátja	A megadott szereplő felvehető kell legyen, létezzen, stb.