SZABAD ADATOK, VÉDETT ADATOK 2. ITA 2008; 281–313.

Privátszféra-védelem szerep-alapú identitásmenedzsment alkalmazásával csevegő szolgáltatásokban

Gulyás Gábor György*

Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Híradástechnika Tanszék
1117 Budapest, Magyar tudósok körútja 2., I ép. IB 113.
Telefon: +36 1 463–3227, Fax: +36 1 463–3263
e-mail: gulyas@pet-portal.eu

Absztrakt

Az újszerű „webkettő" kategóriába sorolható közösségi szolgáltatások, köztük csevegő szolgáltatások hasonló kapcsolatrendszerre épülnek, s e rendszerek kapcsolatorientált funkcionalitása már más új szolgáltatásokban is megjelent. Kutatásainkban vizsgáltuk az identitásmenedzsment terén felmerülő nehézségeket és figyelembe vettük az információs önrendelkezéshez kapcsolódó igényeket is. A tanulmányban bemutatunk egy csevegő szolgáltatásokra specializált szerep- illetve profilalapú identitásmenedzsment modellt, továbbá tárgyaljuk a modell általános problémáit és korlátait, például az identitás–anonimitás paradoxonát, amelyre egy kompromisszumos megoldási javaslatot is teszünk. Ezután egy anonim szankciórendszert mutatunk be, amelynek segítségével finomhangolhatóvá és könnyen kezelhetővé válik az ismeretlen, feltehetően rosszindulatú felhasználók kizárása, majd a tanulmány végén a használhatóság tesztelésére készült rendszeren keresztül értékeljük az eredményeket.

Kulcsszavak: *anonimitás, privacy, közösség, RBP, csevegő szolgáltatás*

1. Bevezető: a szerep-alapú privátszféra-védelemről

A szerep-alapú privátszféra-védelem (az angol szakirodalomban Role Based Privacy, RBP) régóta létező fogalom, és alkalmazásuk nem ritka az ún. Privátszférát Erősítő Technológiák (PET) körében. [1] Működésének alapelve, hogy az adatalany szerepek definiálásán keresztül közli jelenlétét, tárja adatait a külvilág felé. A technika magját az identitásmenedzsment adja, aminek segítségével az adatalany a választott szerepeket úgy

* Gulyás Gábor György, a BME Villamosmérnöki és Informatikai Kar Híradástechnikai Tanszék doktorandusz hallgatója.

kezeli, hogy elérje a kívánt adatközlési állapotot, amelyben minden fél legfeljebb csak a számára, vagy csoportja számára engedélyezett információkhoz férhet hozzá.

A szerep-alapú megközelítés a nem-digitális világban is kézenfekvő: az adatalany egy beteg szerepében viszonyulhat orvosa felé, így orvosa hozzáférhet a páciens anamnéziséhez, míg a pénzügyi helyzetéhez nem. Ellenben bankja felé az ügyfél szerepbe bújik, és bár a bank számára nem hozzáférhető ügyfelük kórtörténete, viszont a tranzakciós előtörténete, adósságállománya igen.

Egy ideális világban ezek a szerepek kellően körülhatároltak, letisztultak, és valamennyi szereplő — legalább is elvben — betartja a rá vonatkozó írott és íratlan szabályokat (például a titoktartást), valamint az adatalany egyértelműen meg tudja határozni a szerepekbe foglalt adat-hozzáférhetőségi köreit. Emellett fontos, hogy visszamenőleg ellenőrizni tudja, hogy mely adataihoz ki férhetett hozzá. A tényleges hozzáférés ellenőrzése a másik szereplő érdekeivel ellentétes lehet, ezért csak *szándék alapú* szabályozással foglalkozunk a későbbiekben, ami figyelmen kívül hagyja, hogy mely felhasználó végül milyen adatokhoz fért hozzá. Olyan modellt szükséges építenünk, amely — a megfelelő feltételek mellett — garantálja, hogy a jogosulatlan hozzáférések nem történhetnek meg, sőt, kontextustól függően az anonimitás lehetőségét is felkínálja.

A PET technológiák multidiszciplináris tudományterületnek számítanak, a különféle személyes, csoportos, jogi motivációkat elsősorban menedzsment módszerekkel és kriptográfia alkalmazásával oldják meg, s így garantálják, hogy a jogi szabályozás mellett a szereplők nem csupán kötelesek betartani az adatokra vonatkozó kötelezettségeiket, hanem azokat vagy nem is tudják megszegni, vagy egyértelműen bizonyítható mulasztásuk.

Korábbi munkáink során az anonimitás és privátszféra-védelem lehetőségeit vizsgáltuk csevegő szolgáltatásokban [4], és alapozó kutatásunk eredményeire támaszkodva ebben a tanulmányban egy általános csevegő szolgáltatás modellt közlünk, amelyre egy RBP alapú korlátozott anonimitási lehetőséget nyújtó identitásmenedzsment rendszer alkalmazását mutatjuk be. A tanulmányban egy általános, hibrid csevegő szolgáltatás modellel[1] foglalkozunk, hogy eredményeink alkalmazhatóak legyenek valamennyi szolgáltatástípusra.

[1] A hibrid szolgáltatások egyidejűleg szobákat és konferenciákat is tartalmaznak, ellentétben a chat jellegű, valamint az azonnali üzenetküldő szolgáltatásokkal, amelyek rendre csak az egyik lehetőséget nyújtják a felhasználónak.

A szolgáltatás modelljének felépítése során feltételezzük, hogy annak az egésze megfelel a külső-belső világ paradigmának,[2] azaz a szolgáltatáson kívül eső megfigyelők nem képesek sem megismerni a rendszer belső állapotát, sem céljuknak megfelelően befolyásolni azt (legfeljebb a hálózaton továbbított üzenetek manipulálásával okozhatnak hibás működést, azonban tevékenységük eredményét nem képesek megismerni). Ez a feltétel garantálja számunkra azt, hogy a résztvevők anonimitását csak a belső szereplők képesek meghiúsítani. Célunk egy olyan módszer ajánlása a tanulmány fókuszában lévő szerep-alapú identitásmenedzsment rendszerrel, amely az anonimitás ellen irányuló támadásokat képes elhárítani.

2. Szolgáltatásmodell

Ahogy korábban is utaltunk rá, az alábbiakban egy hibrid szolgáltatásmodellről írunk, amely tartalmaz partnerlistát, szobákat és konferenciákat is. Ezt a szolgáltatásmodellt *AnonIM* névre kereszteltük el, amely az *Anonymous Instant Messenger* (anonim azonnali üzenetküldő szolgáltatás) kifejezés rövidítéséből származik.

A partnerkapcsolatok, párbeszédek, konferenciabeszélgetések mind kapcsolatokat realizálnak, amelyek összessége páros és közösségi kapcsolatok hálójaként is felfogható. Ebben a tanulmányban ezekre a speciális hálózatokra alkalmazott szerep-alapú privátszféra-védelmi módszert javaslunk, amelyet részletes elemzésnek vetünk alá, azonban megjegyezzük, hogy a javasolt modell egyszerűen kiterjeszthető kapcsolati hálókra is. Ezen a területen jelenleg is folytatunk kutatásokat.

2.1. Belső világ

A belső világ modell alatt a felhasználók által tapasztalt modell rendszert értjük, amelyben kapcsolatokat, beszélgetéseket létesíthetnek, más felhasználókat kereshetnek, és egyéb felhasználói közösségekbe (például szobák) csatlakozhatnak, vagy ilyen „csoportosulásokat” hozhatnak létre.

A belső világ modell implicit módon magába foglalhatja a működéshez szükséges protokollokat, de jelen esetben csak a virtuális világ absztrakt modelljének felépítését fogjuk bemutatni. A modell megalkotásakor fontos kiindulási alapnak számított az alapkutatásunk során vizsgált szolgáltatások némelyike.

[2] A külső-belső világ paradigmával részletesen foglalkoztunk [2]-ben az anonim böngészőkkel kapcsolatban, de a paradigma általános, így érvényes a csevegő szolgáltatásokra is.

2.2 Szereplők és kapcsolatok a virtuális térben

A modell legfontosabb szereplői a *felhasználók*. A felhasználókat jelen esetben egyenrangúnak tekintjük, és nem foglalkozunk a kiemelt szerepű felhasználókkal, akik operátori, moderátori szerepet tölthetnek be. A felhasználók elsődleges célja a kapcsolatteremtés, amit üzenetváltás, fájlcsere vagy tetszőleges interakció követhet. A kapcsolat felvétele több módon is történhet, például kereséssel, de az alábbiak erre alkalmas kontextusok.

A *partnerlista* célja a gyors és közvetlen kapcsolatteremtés a kiemelt partnerekkel. Itt megtalálhatóak csoportokra bontva a felhasználó kiemelt partnerei. A partnerlistára úgy tekintünk, mint a felhasználók fő navigációs eszközére. A partnercsoportokat a felhasználó maga határozza meg, és a csoportokba tartozást tetszése szerint változtathatja. A partnerlistára a keresőből, a szobákból, vagy más konferenciákból kerülhetnek fel partnerek, feltéve, ha a másik fél ehhez hozzájárul (mindkét partnerlistára felkerül mindkét fél). Valamennyi felhasználó azt is megtekintheti, hogy ő mely felhasználók partnerlistáján található meg.

A *szobákat* (a szakirodalom csatornaként is említheti) szolgáltatásoldali közösségek gyűjtőhelyeiként értelmezzük. A szobák alapértelmezés szerint nyilvánosak, bárki által kereshető, nyitott találkozóhelyként funkcionálnak. Modellünkben feltesszük, hogy szobákon belül további szobák nyithatóak, elméletileg lehetővé téve egy tetszőleges mélységű szobahierarchiát. Névütközés miatt csak azonos szinten lévő, ugyanazon szobából származtatott bennfoglalt szobák esetén tiltott az azonos nevek használata, egyéb esetben a „szülők” listája, valamint a név egyértelműen azonosítja a szobát. A szoba neve kötött, ha már létrehozták.

A *konferenciák* hasonlóak a szobákhoz, de ezek kötetlenebb beszélgetések, amelyeket a felhasználókhoz kötünk, azaz feltesszük, hogy jellemzően egymást ismerő felhasználók hoznak létre konferenciákat, vagy hívják meg egymást; az alapítójukhoz kötjük őket. Csak azok tekinthetik meg a nyilvános konferenciákat, akik az alapító taggal kölcsönösen felvették egymást a partnerlistájukra.

Állandó konferenciák akkor képzelhetőek el, ha a szolgáltatás engedélyezi a felhasználóknak, hogy az útlevelükben (2.3.1. pont) tárolják aktuális konferenciáikat, és bármikor újra létrehozzák azokat, vagy akár automatikusan is létrejöjjenek a bejelentkezés után. A konferencia neve bármikor megváltoztatható, nevének egyedisége csak az alapító tagnál fontos. A konferenciák egyszintű, nem hierarchikus rendszerbe szervezettek.

A *párbeszéd* a konferencia egy speciális — kétszereplős — alesete, amely kevesebb szolgáltatást nyújt, például nem listázható vagy hozható nyilvánosságra. Ebből adódóan kevesebb attribútuma is van, de a teljesség kedvéért feltételezzük, hogy bármikor átalakítható szobává, konferenciává, további tagok meghívásával.

2.3. Felhasználók

Ebben a fejezetben áttekintjük a felhasználókhoz kapcsolódó alapvető adatokat, információkat, valamint a számukra elérhető funkcionalitást.

2.3.1. Az útlevél

A felhasználó adatait a szolgáltatás az útlevélben[3] tárolja. A sikeres bejelentkezés után a felhasználó hozzáférhet a teljes útleveléhez (az azonosítás az útlevélbe bejegyzett adatok alapján történik, nem kizárólag jelszavas azonosítás alapján). Az azonosítás módszere tetszőleges, bármikor lecserélhető — a felhasználónak csak az azonosságát kell igazolnia, az útlevélben megadott módszernek megfelelően.

A regisztráció során a felhasználó maga megad, vagy a rendszertől kap egy egyedi azonosítót, amely alapján egyértelműen beazonosítható a rendszerben.[4] Erre a későbbiekben *regisztrációs azonosító* néven hivatkozunk. Az útlevél főbb részei:

- bejelentkezési adatok;
- „bűnügyi előélet”;
- profilok;
- kapcsolati listák: partnerlista, látogatott szobák, konferenciák.

A bejelentkezési adatok a rendszer választott azonosítási algoritmusához szükséges adatokat tárolják. A „bűnügyi előélethez” tartozó információkkal részletesen az anonim szankciórendszerben foglalkozunk majd; ez a rész a rendszer vagy a felhasználói általi nem megfelelő viselkedésre vonatkozó előtörténetet tartalmazza. A profilok és kapcsolati listák a szerep-alapú identitásmenedzsmenthez szükséges információkat tartalmazzák — erre később visszatérünk.

[3] Az angol szakirodalomban a magyar fordításnak megfelelően passport-ként emlegetik.

[4] Ezt az azonosítót nem mindig tesszük közzé, hiszen így nem beszélhetnénk anonimitásról vagy több pszeudonim identitásról; ezért csak a rendszer ismeri állandóan, és kontextustól függően a felhasználók is.

2.4. Partnerlista

A partnerlista célja, hogy a felhasználók a kiemelt partnereiket közvetlenül elérhessék, állapotukról tájékozódjanak, és emiatt fontos, hogy partnereiket egyértelműen be tudják azonosítani. Tehát a partnerlistán lévő felhasználók nem lehetnek anonimek, ezért pszeudonim azonosítóval rendelkeznek.

A partnerlista szereplői (és csoportjai) fastruktúrába vannak besorolva, és egyes rendszerektől eltérően[5] egy felhasználó legfeljebb egy csoportba tartozhat — csak így garantálható a fastruktúra. A csoportokba nem besorolt partnerek egy alapértelmezett csoportba kerülnek.

A partnerlistákon létrejövő kapcsolatok egy kapcsolati hálót realizálnak. Feltehetjük a kérdést a kapcsolatok titkosságáról: mely kapcsolatokat ismerhessék egyes partnerek, melyek lehetnek bizalmasak? Elég, ha a felhasználó számára rejtett a kapcsolat, de a privátszférát érintő kérdésekben segítő döntéstámogató rendszer ismeri azokat? A válasz természetesen nem, mivel különben ki lehetne „sakkozni" egyes titkos kapcsolatokat; tehát a felhasználónak pont azt a képet kell mutatnunk, amelyet az identitásmenedzsment rendszer lát az ő szemszögéből.

Újabb kérdés, hogy a titkosság menedzsmentjét hogyan valósítsuk meg. Később foglalkozunk a kapcsolati hálózattal, a kapcsolatok titkosságának kérdésével is, valamint hogy milyen problémát jelent ez a privátszféra védelmét tekintve.

2.5. Szobák, konferenciák

A szobák és konferenciák alapvető tulajdonságaikat, funkcionalitásukat tekintve igen hasonlóak, ezért a közös jellemvonásokat összevonva tárgyaljuk. Ahogy korábban említettük az alapvető eltéréseket, a szobákat keresőben lehet fellelni, illetve ki lehet listázni a fellelhető összes nyilvános szobát is, viszont az elérhető konferenciák közül csak azok listázhatóak egy felhasználó számára, amelyekben a partnerlistáján szereplő felhasználók részt vesznek, valamint ők a konferencia alapító tagjai is (ehhez nem szükséges valamennyi tagot ismerni).

A konferenciák ideiglenes jellegűek. A konferencia az alapító taghoz kötődik, és ha ő kilép, akkor a konferencia is megszűnik. Emellett az alapító tag elmentheti a konferencia beállításait, attribútumait, így később is megnyithatja azt (a meghívott partnerekkel együtt). A konferencia attribútumai is elmentésre kerülnek az ő útlevelében, de ettől függetlenül kilépésekor bezárulnak.

[5] Mint például a Windows Live Messenger.

A szobákat, hogy állandóak legyenek, külön regisztrálni kell a szolgáltatásban. Ekkor a szoba attribútumai adatbázisban tároltak, és az alapító tag személye kötött. A nem regisztrált szobák esetén az attribútumok (és például az alapító tag személye) addig érvényesek, amíg az utolsó látogató ki nem lép a szobából[6] (kivéve, ha van benne olyan szoba, amelyben van látogató, és így tovább rekurzív módon).

A szobahierarchiában bárki, bármely szobában létrehozhat további 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 szinten valamennyi szobát regisztrálták. 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 alábbi táblázatban modellünk szobái és konferenciái főbb tulajdonságait vetjük össze. Az attribútumokat négy csoportba soroljuk: *általános jellemzők, szűrési beállítások, privátszféra-védelmi funkciók és jellemzők,* valamint *speciális hozzáférési listák*, amelyek a felhasználói jogosultságokról és hozzáférésekről nyilatkoznak.

1. táblázat: szoba és konferencia főbb tulajdonságai

Közös	Szoba	Konferencia
• **Általános** o *Név* o *Mottó* (téma) o *URL* o *Leírás* o *Címkék* o *Alapító tag*	• **Általános** o *Név* (kötött) o *Belső szobák* (lista) • **Szűrés** o *Felhasználószám limit*: elérésekor átirányít másik szobába, vagy tiltja a belépést. • **Privátszféra-védelem** o *Átirányítás* (túl sok látogató esetén) o *Anonim olvasás, írás*	• **Általános** o *Név*, megváltoztatható • **Privátszféra-védelem** o *Bárki meghívhat* o *Láthatóság* (mely partnerlistás ismerősök láthatják a konferenciát) o *Anonim írás*

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

Látható a közös tulajdonságok alapján, hogy a szerver nem csak a szobák, hanem a konferenciák esetén is végez szűrést, bár ez nem lenne egyértelmű, mivel az utóbbiak inkább a kliensoldalhoz kötődnek. A közös üzenetszűrésen kívül a felhasználók saját szűrési mechanizmusokat is beiktathatnak.

A konferencia elmenthető a kezdeményező felhasználónál, és ő indíthatja el újra. Ekkor a korábbi beszélgető felek meghívása automatikusan újra megtörténik. A szoba beállításai elmenthetőek a szerveren, ha regisztrált; egyébként is elmenthetőek, de csak akkor aktiválódnak, ha ugyanaz felhasználó hozza létre (azaz a felhasználó útlevelében kerül elmentésre a szoba összes információja).

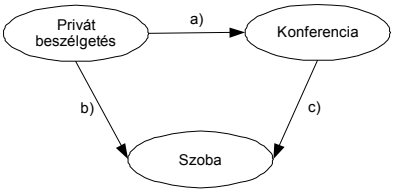
2.6. Párbeszédek

A párbeszédek speciális esetei a konferenciáknak. Ennek megfelelően csak bizonyos tulajdonságaival rendelkeznek, amíg át nem alakítják, ezért külön tárgyaljuk a tulajdonságaikat. Ide tartozik a többes beszélgetéseknél is megtalálható *mottó*, és a párbeszédek alapvetően zártak (*lakat*), amely zárat mindkét félnek fel kell oldania, hogy új partnereket vegyenek fel a beszélgetésbe.

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

2.7. Transzformációs lehetőségek (beszélgetéstípusok között)

A különböző beszélgetési típusok egymás között átalakíthatóak — e bővítési szabályoknak megfelelő átalakításokkal érhető el például, hogy egy párbeszédből konferencia vagy szoba legyen. Az átmeneteket az alábbi gráfon szemléltetjük.



1. ábra: Beszélgetéstípusok közötti transzformációs lehetőségek

Az *a)* átmenet esetén mindkét fél feloldotta a korlátozást (a korábban említett „lakatot"), és kezdeményeztek egy konferenciabeszélgetést egy harmadik fél meghívásával. A kezdeményező félnek meg kell adnia a konferenciabeszélgetés nevét, és ő lesz az alapító tag.

A *b)* átmenet esetében — hasonlóan az előző esethez — mindkét fél feloldotta a korlátozást (lakat), majd a kezdeményező fél megad egy szobanevet (és egy alap címkét), ami után átkerülnek a beszélgető felek a szobába, a privát beszélgetés megszűnik.

A konferencia vezetője dönthet úgy, hogy szobává alakítja a konferenciát (ez a *c)* eset). 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 (ekkor már nem szükséges, hogy mindenki engedélyezze a műveletet, így ez esetben korlátozás-feloldásról nem beszélhetünk).

3. Anonimitás, privátszféra-védelem RBP alapokon

Ebben a fejezetben először a szerep-alapú privátszféra-védelmi rendszer csevegő szolgáltatásokra alkalmazott verzióját mutatjuk be, majd a fejezet végén általános szempontokat, magára a RBP rendszerekre vonatkozó kérdéseket is vizsgálunk, kiemelvén a rendszer általános vonásait.

Összetett rendszerre van szükség, az identitásmenedzsmenttel kapcsolatos problémák fő okai a csevegő szolgáltatásoknak és azonnali üzenetküldőknek a szereplőik között létrejövő sűrű kapcsolatrendszere, az erősen interaktív közegek, kapcsolatok. A kapcsolatrendszer gyakran változik, a különböző szereplők pedig könnyen együttműködhetnek egy másik felhasználó álcájának kompromittálása céljából, könnyen felfedezhetik a különböző kontextusokban megfigyelhető identitások között a kapcsolatot. A később bemutatott identitásmenedzsment műveletek alkalmazása során figyelni kell arra is, hogy egy szereplő minden szereplő nézőpontja szerint helyesen vegye fel az új (és esetleg anonim) identitását.

3.1. Célkitűzések, feltételek

Az előző fejezetben felállított csevegő szolgáltatás modellre ajánlunk egy RBP modellt, vizsgáljuk az anonimitás lehetőségét, ennek a kezeléséhez szükséges feltételeket, valamint hogy miképp lehet a különböző identitások közötti kapcsolatot felfedni. A csevegő szolgáltatásokra jellemző speciális tulajdonságokat is figyelembe vettük a rendszer tervezése során, mint például a gyorsan változó dinamikus kapcsolatrendszert, vagy a korlátok nélküli kommunikációs lehetőségeket.

Elsősorban a belső világ modell állapotára, állapotváltozásaira vonatkozóan vizsgáljuk az identitások kompromittálásának lehetőségét; az olyan eseteket, amikor a felhasználók saját identitásukat vagy a másik fél identitását kompromittálják, figyelmen kívül hagyjuk. Az identitások mögötti felhasználók azonosítása lehetséges az üzeneteik alapján felépített statisztikai profilok alapján is, a tanulmányban ezzel sem foglalkozunk.

3.2. RBP alapmodell

A RBP alapmodellben a különféle többes beszélgetésekben valamint a névlistán használatos szabályokat fektetjük le, azonban ezek mellett több más szempontot is figyelembe kell venni a privátszféra-védelmi rendszer kialakítása során.

3.2.1. Privátszféra-védelmi profilok

Hasznos lehet, ha a rendszer emellett összetettebb *privátszféra-védelmi profilokat* is támogat, amelyek között egy egyszerű váltással több beállítási paraméter együttesen változtatható. Ezen paraméterek általánosságban valamennyi privátszféra-védelmi funkciót magukba foglalják: valamennyi kimenő és bejövő esemény, üzenet, információ szűrése, menedzsmentje.

Ebben a fejezetben a privátszféra-védelem alapjait tárgyaljuk, a RBP rendszer működését, a következő, 4. fejezetben pedig azokat a kiegészítő technikákat, amelyekkel együttesen alkothatunk az identitásmenedzsmentet felhasználva privátszféra-védelmi profilokat. A kiegészítő technikák körében több olyan módszert tárgyalunk, amely privátszféra-védelmi profilokat is használ.

3.2.2. Profilok, identitások, műveletek

A felhasználók között kapcsolat többféleképpen is létrejöhet, ezeket nevezzük *virtuális kontextusnak.* Ilyen lehet például a korábban említett szoba, konferencia, vagy a felhasználó által gondozott partnerlista. A virtuális kontextusokban a felhasználók egymás jelenlétét *nézeteken* keresztül tapasztalják meg, amelyek célja, hogy többé-kevésbé megkülönböztessék a felhasználókat egymástól — tehát az egyedi azonosítás nem mindig cél.

A felhasználói szerepköröket ezekre a nézetekre beállított *profilok* valósítják meg. Ezeket a virtuális kontextuson keresztül tapasztalható profilokat nevezzük *identitásnak.* Az identitás, vagy más nevén profil, magába foglalja mindazon információkat, amelyeket a partnerek a csoportokban, partnerlistán láthatnak, mint például becenév, személyes üzenet,

kapcsolódási állapot, felhasználói státusz, stb. Tehát az identitások menedzselésével, az identitásokon keresztül szabályozhatjuk, hogy az egyes szereplők milyen információkat láthatnak rólunk.

A profilokat a felhasználók különféle partnercsoportokra definiálhatják, és a profilmenedzsment lényege a csoportok kiválasztásában, megjelölésében, valamint a profilok aktiválási módszereiben rejlik. A profil „célközönsége" magába foglalhat egy közös szobában tartózkodó partnereket, vagy a partnerlistáról kijelölt tetszőleges felhasználóhalmazt.

A profilok menedzselését *műveletek* segítségével tehetik meg a felhasználók. Egy művelet több részre bontható: ki kell jelölni a művelet *célcsoportjának tagjait*, meg kell adni a *kijelölés időtartamát*, vagy *feltételeit*, illetve a művelet *hatását* is definiálni kell.

A művelet összetevői, használatának feltételei kontextusonként változhatnak, most általánosságban vizsgáljuk meg ezeket. A célcsoport megadása történhet egyénenként, vagy felsorolás megadásával, lehet relációs (például összes közös ismerős letiltása), vagy a kontextus struktúrájától függő csoportos, illetve egyéni (például partnerek, szobák, azon belül felhasználók). Mindig a legmagasabb prioritású kijelölés van érvényben, ennek meghatározásához a következő prioritási sorrendet értelmezzük (balról jobbra nő a prioritás):

kontextusfüggő struktúra < relációs < felsorolás alapú

Továbbá a műveletek időtartama is kérdéses, ezt az alábbi listában rögzítjük; de bizonyos kontextusokban ez felülbírálható.

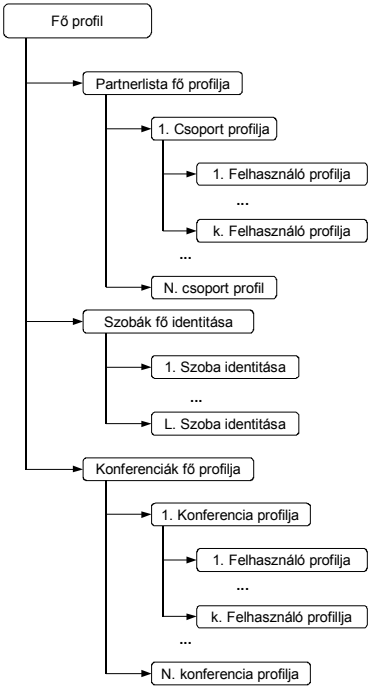
- *Ideiglenes*: a következő viszony elindításáig, vagy a művelet beállítása után valahány viszony indításáig, vagy visszavonásig él.
- *Végleges*: a kijelölés örökéletű, a felhasználói visszavonásig érvényes.
- *Egyszerű feltételes*: a feltételek teljesüléséig él, utána megszűnik.
- *Állandó feltételes*: amikor a feltételek teljesülnek, a művelet érvénybe lép.

A műveletek hatása (általában) két független részre bontható, az egyikben a felhasználó az üzenetek fogadásának és küldésének tiltásáról rendelkezik, a másikban pedig a megjelenített információkkal kapcsolatosan teszi meg ezt. Az alapműveletek kombinációjából létrehozhatóak a mai rendszerekben is használt műveletek:

- Üzenetek fogadásának tiltása.
- Üzenetek küldési lehetőségének tiltása.
- Profil beállítása.

Az előbbi hatások együttese lehet például partnerlistáról való törlés esetén: off-line profilt állítunk be, és az üzenetküldés, fogadás lehetőségét letiltja a rendszer. A műveletek ellenkezőjét is be kell vennünk a rendszerbe, vagyis az engedélyező műveleteket is.

A rendszer áttekinthetőségének érdekében kontextus struktúrában menedzselhető profilokat fa struktúrájú hierarchiában tároljuk, kontextusok szerint csoportosítva, a *2. ábrán* látható módon.



2. ábra: Profil-hierarchia

A rendszer alapállapotában feltételezzük, hogy valamennyi fél a „Fő profil”-ban beállított információkat láthatja, és ennek megfelelően a profil hierarchiában a profil beállítások értéke „üres”, relációk és felsorolások pedig nincsenek.

Öröklési tulajdonság a profil-hierarchiában: ha egy csomópontban beállítunk egy profilt, vagy módosítjuk, ha már nem üres értékű, akkor az a változás valamennyi, a hierarchiában alatta szereplő profilra érvényesülni fog, kivéve, ha már ott is volt beállítás.[7]

Bizonyos szolgáltatásokban szükség lehet egyéb alapértelmezett értékekre, amelyeket nem szükséges ebbe a hierarchiába illeszteni, mint például a keresésnél megjelenő profilok, vagy külön profil-hierarchia arra az esetre, ha a felhasználó kijelentkezik a rendszerből, vagy más okok miatt off-line állapotban lesz (például letilt bizonyos felhasználókat). Ezekkel most nem foglalkozunk, az itt bemutatott modell alapján ezekre az esetekre is fel lehet készülni.

3.2.3. RBP műveletek

Ahogy korábban is hivatkoztunk rá, a magánszféra védelme az alapműveletek kombinációinak alkalmazásával állítható be a kívánt szintre, állapotra. A különféle kontextusokon belüli értelmezésre később térünk ki, itt a műveletek mögötti általános elgondolást ismertetjük.

Nem szükségszerű valamennyi kontextusra definiálni az összes műveletet és lehetőséget, ehelyett a célunk egy egyszerűen kezelhető, áttekinthető műveletcsoport értelmezése, amely nem korlátozza az adott kontextusban a felhasználó szabadságát a privátszféra-védelem kialakításában.

Erre egyszerű példát adhat az anonimitás lehetősége a partnerlistán. Ez utóbbinak a célja éppen a felhasználók rendezett gyűjtése, így itt az anonimitást nem szabad megengedni, különben funkcióját vesztené. Egy másik ellentmondást fedezhetünk fel, amikor egy partner tiltásának műveletet próbáljuk értelmezni a szobákra. Ugyanis ebben az esetben elegendő lenne a felhasználónak mindenkit letiltani, hogy ott rejtőzködve tartózkodhasson, attól függetlenül, hogy a többi felhasználó ebbe beleegyezik-e. A RBP műveletek:

- *Mellőzés*: a mellőzött partner üzeneteit nem képes eljuttatni a mellőző félhez, de láthatja a profilját (azaz állapotát is).
- *Tiltás*: a letiltott partner üzenetei mellőzésre kerülnek, valamint a tiltó fél off-line profilját látja.
- *Engedélyezés*: A tiltást és mellőzést feloldó művelet.

[7] E modell további nagy előnye, hogy a megvalósítás igen egyszerű: amikor egy profil értékére szükség van, addig kell a felsőbb szintek felé lépdelni, amíg nem üres értékkel találkozunk.

- *Álca, identitásváltás*: a profil módosításával, új profil bevezetésével a felhasználó hamis állapotot mutathat mások felé, identitást válthat (néhány „trükk” alkalmazásával), 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.

Az itt ismertetett RBP műveletek mind felépíthetők a *3.2.2. pontban* ismertetett alapműveletekből.

3.2.4. RBP műveletek különböző kontextusokban

A műveletek másképp értelmezhetőek valamennyi kontextusban: a névlistán, szobákban és konferenciákban. Ebben az alfejezetben az eltéréseket, a műveletek kontextusok szerinti értelmezését vizsgáljuk.

3.2.4.1. Névlista

Ebben az esetben a RBP műveletek a kijelölést ismertető fejezetekben leírtak alapján működnek. A felhasználók egyértelműen megjelölhetőek, hiszen csak álcázásra képesek, identitásváltásra nem — az őket megjelölő regisztrációs azonosító miatt (egyébként, ahogy korábban is jeleztük, a partnerlista értelmét vesztené).

A kapcsolati hálózatnak köszönhetően (a kapcsolatok titkosításának lehetőségével később foglalkozunk) felhasználók kiválasztására több lehetőség is adódik, néhány példa:

- *Felsorolással, egyénileg*: felhasználók listába fűzve szerepelnek egy művelet célpontjaként; az egyéni megjelölés csak egy speciális, egyelemű lista.
- *Közös ismerősök reláció*: Ismerősök azon 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 megjelölésekre értelmezzük a korábban bevezetett prioritási sorrendet. 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 nem befolyásolhatóak ugyan, de ezek kissé más szemléletet követnek, mint az eddigi csoportok. A felsorolt szempontok alapján az alábbi reláció megfelel a korábban említett prioritási sornak, a névlista kontextusára alkalmazva:

csoport < közös ismerősök reláció < lista

3.2.4.2. Szobák

Szobákban a műveleteket alapértelmezés szerint csak a szoba egészére lehet alkalmazni, egyénileg csak a mellőzés (és engedélyezés) és a felfedés műveleteket lehet. A RBP műveletek 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. A modell kiterjesztésével ez megoldható; vagyis úgy, hogy a profil fa a szobák struktúrájával egyezően hierarchikus legyen.

- *Mellőzés:* A mellőzés esetén a szoba közös beszélgetésében mellőzött a felhasználó. A mellőzés, ha a kijelölt felhasználó identitást vált, újra felbomlik; azonban globális megjelölést is kaphat a felhasználó — privát üzeneteket ezután nem tud küldeni.[8]
- *Tiltás:* A tiltás művelet esetében, ha a szobában engedélyezett, a felhasználó rejtett módba kerül, s a neve nem lesz látható. Ekkor csak anonim módon szólalhat csak meg (ha a szolgáltatás támogatja ezt a két funkciót). Egyéb esetben a tiltás művelet kiváltója a szoba elhagyása lehet.
- *Álca:* Az egyik lehetőség szerint felhasználó álcázza magát, azaz megváltoztatja a profilját a szoba felé. A másik lehetőség az identitásváltás, ekkor a megfigyelők számára úgy tűnik, mintha egy új beszélgető jelenne meg, függetlenül az addigi szereplőktől. Mivel egyszerre nem tartózkodhat senki sem több identitással egy szobában, néhány apró trükkre van szükség, hogy az identitásváltás hiteles legyen.[9]

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

[9] Például, a felhasználó megad egy elköszönő üzenetet, majd belép új identitásával. Időzítés szerint elköszön a régi identitás, és kilép – így az identitáscsere le is zajlott.

- *Felfedés:* Ha a felhasználó felfedi magát az egész szoba előtt, akkor a szoba tagjai a chat jellegű részre vonatkozó profilt fogják látni,[10] ugyanis ez áll a profil hierarchiában közvetlen a szoba felett.
- *Engedélyezés:* A mellőzések feloldhatók. A szobára vonatkozó és globális (privát beszélgetésre vonatkozó) mellőzések listája megtekinthető. Ugyanígy a rejtett állapotú felhasználó láthatóvá válhat.

Felfedésről beszélhetnénk más értelemben is: például hasznos, ha a szobás részen a felhasználók felfedhetik egymás előtt a regisztrációs azonosítójukat, így felvehetik egymást a partnerlistáikra, illetve bármikor megismerhetik egymást, álcáik ellenére is.

3.2.4.3. Konferenciák

A konferenciák egyesítik a szobák és a névlista tulajdonságait is. A konferencia-kezelés egyik fő 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. További nehézség, hogy a különféle helyekről meghívott felek a konferencia gazdájának más-más identitásait látják. Erre ad megoldást, hogy a felhasználók látják egymás regisztrációs azonosítóját a konferenciában, így ez a kérdés nem kritikus, de további vizsgálódást igényel.

A RBP műveletek lokális értelmezése:

- *Mellőzés*: egy felhasználó mellőzése vonatkozhat a szobáknál lévő értelmezéshez hasonló módon a közös beszélgetésre, illetve a privát üzeneteknek a küldésére is.
- *Tiltás*: mivel konferenciák esetén a rejtett mód nem lehetséges (a regisztrációs azonosító miatt), 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 konferenciák általános profilját fogják látni. A felhasználó bizonyos felhasználók előtt is felfedheti ezt az identitását.
- *Engedélyezés*: a mellőzések feloldhatók. A konferenciára vonatkozó és globális (privát beszélgetésre vonatkozó) mellőzések listáját célszerű megtekinthetővé tenni.

Ahogy korábban utaltunk rá, a konferencia a szobákhoz és a névlistához is hasonlóan működik.

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

3.3. Csevegő szolgáltatásokra jellemző és általános problémák

Ebben az alfejezetben a RBP rendszerre jellemző problémákat tárgyaljuk. A problémák egy része kifejezetten a csevegő szolgáltatásokra jellemző, mások pedig az alkalmazástól függetlenül megjelennek a RBP alapú identitásmenedzsment rendszerekben. Némelyikük még ennél is általánosabb, magára az anonim, vagy pszeudonim jelenlétet nyújtó rendszerekre is jellemző.

3.3.1. Ellentmondás a szembenálló felek között

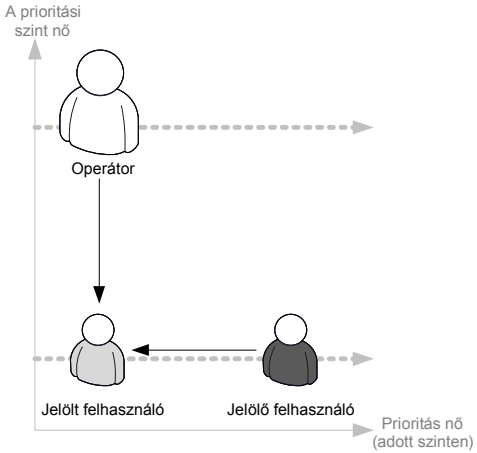
Amikor egy felhasználó a többi felhasználó vagy a moderátorok felé pszeudonim azonosítókon keresztül látható, és a megjelöléséről beszélünk, egy fontos kérdéshez érkezünk. Ez egy általános probléma, ami nemcsak a jelen rendszerben fordul elő. Meg kell határoznunk, hogy vagy az aktuális identitást, vagy a felhasználót magát jelöljük meg (jelen esetben ez alatt az útlevél megjelöléséről van szó).

Akár az egyik, akár a másik megoldást választjuk, az egyik a jelölő félnek, a másik pedig a jelölt félnek fog kedvezni, egyaránt jó megoldás nincs. Ha az identitást jelöli a művelet, akkor a jelölő fél privátszférája sérül: identitásváltással a jelölés feloldható, így a műveletet hatástalanná válik. Ha viszont a felhasználót lehetséges megjelölni, akkor a jelölt privátszférája sérül, hiszen a jelölésből identitásváltás után kiderülhet, hogy korábban már megjelölték, és ennek alapján következtetni lehet a korábbi identitására — tehát az identitások függetlensége sérül.

Csevegő szolgáltatásokban ez a probléma akkor jelentkezhet, amikor a felhasználók a korábban említett RBP műveleteket alkalmazzák egymáson valamelyik szobában, például a mellőzést (más kontextusban a regisztrációs azonosító ismert), illetve ha operátorok szeretnék megjelölni a felhasználókat.

A műveleteket két típusba sorolhatjuk: hátrányos és előnyös jelölésekre. Előnyös jelölések esetén a felhasználó maga fedheti fel a jelölést, illetve az előnyt nem szükségszerű használnia,[11] ezért véleményünk szerint ebben az esetben az útlevél jelölhető. Hátrányos jelölés esetén a következő prioritási rendet határoztuk meg: a jelölő fél privátszféra-védelme fontosabb, hiszen különben a RBP rendszer hasztalan lenne, valamint az operátorok a legmagasabb prioritásúak, ugyanis a jelölési művelettel csoportos érdeket szolgálnak. Ezt a prioritási elrendezést vizualizálja a következő ábra, amelyben a felhasználókat és operátorokat egy prioritási koordinátarendszerben helyeztük el.

[11] Például operátori jog szobán belül.



3. ábra: Prioritási koordinátarendszer hátrányos jelölések esetén

Tehát szobák esetén is az útlevelet jelölik az alkalmazott műveletek, és ez nem jelent problémát, mivel a jelölt fél le tudja magát buktatni, de a lebukása nem szükségszerű: ha például mellőzés esetén nem szólal meg a közös beszélgetésben, akkor ez sosem derül ki.

3.3.2. Titkos kapcsolatok a partnerlistán

Sok múlhat azon, hogy rejtőzéskor, álcázáskor ismert-e a kapcsolatrendszer. A felhasználó, vagy egy automatikus rendszer is figyelembe veheti, hogy bizonyos kapcsolatokat kik ismerhetnek, és figyelmeztethetik a felhasználót, ha álcáját mások kompromittálhatják. Úgy is fogalmazhatunk, hogy a felhasználó akkor tud biztos döntést hozni, ha minden őt érintő kapcsolatot ismer a felhasználók kapcsolati hálójából. Ez azonban mások érdekeivel ellentétes, ugyanis egyes kapcsolatok bizalmasak lehetnek, amelyeket így a felek titokban szeretnének tartani.

A partnerlistákon keresztül létrejött kapcsolatok elrejthetősége éppen ezért fontos, noha a döntések kimenetelének bizonytalanságát erősítik. A szobás részen nem lehetséges megmondani, hogy mely identitások tartoznak egy felhasználóhoz, ez hasonló problémát eredményez a partnerlistás kapcsolatrejtéshez. Ha már a szobás részen is elrejthetőek a kapcsolatok, a rendszer jellegéből fakadóan ez a partnerlistán sem jelent majd hátrányt.

3.3.3. A név egyedisége

Chat jellegű szolgáltatásokban a szolgáltatáson belül minden név egyedi, különben gondot jelentene a felhasználók megkülönböztetése. Azonnali üzenetküldő szolgáltatásokban ez általában nem probléma, ott más megkülönböztető azonosítók szerepelnek, mint például a regisztrációs azonosító. Hibrid szolgáltatásokban a különféle kontextusoknak megfelelően érdemes szétszedni a megoldásokat.

Névlistán egy egyedi azonosítót is kell a felhasználóhoz rendelni, hogy ha a nevét változtatja, azonosítható legyen. Mivel felhasználók csak kiválasztás, vagy engedélykérés útján kerülhetnek a névlistára, a relatíve kisméretű és ismert halmazból könnyen kikövetkeztethetőek lennének a felhasználók (főleg ha csoportosítva vannak). Továbbá az anonimitás lehetősége ellentmondana a partnerlista céljával is. A felhasználókat célszerűen a regisztrációs azonosítóval tesszük itt is egyedivé.

A többszereplős beszélgetések szétválnak. *Szobák* esetén nem szükséges az egyedi azonosító, bizonyos esetekben a felhasználó lehet névtelen, teljesen anonim is. Ha több felhasználó — különböző szobákban — használhatná ugyanazt a nevet, zavaró lenne. Tehát egy identitás több szobában is jelen lehet, de csak egyetlen felhasználóhoz tartozhat, és egy felhasználó több identitással is rendelkezhet.

A többszereplős beszélgetések másik formájában, a *konferenciák* esetén jelen lehetnek felhasználók különböző szobákból, bármely fél partnerlistájáról, vagy ezektől független résztvevők is lehetnek. A konferenciákban látható a regisztrációs azonosító, így ez egyértelműen azonosít mindenkit, s a névlistához hasonlóan itt tetszőleges név is megengedett.

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. A párbeszédek esetén a név egyediségéről nem érdemes beszélni, ez elsősorban attól függ, milyen kontextusban indult a beszélgetés.

3.3.4. Megszemélyesítés

Összefügg az előző ponttal a megszemélyesítés problémája: bár néhány kontextusban fontos, hogy az identitások ne legyenek egyedileg azonosíthatóak, emellett fontos, hogy bizonyos identitások mögött csak egy adott felhasználó állhasson, még ha nem is tudni, hogy kicsoda. Erre megoldást nyújthat, ha a felhasználók regisztrálhatnak a szobás részen olyan neveket, amelyeket csak ők vehetnek fel.

Ez nem rontja sem mások lehetőségeit, sem a felhasználóét, hiszen az identitáscseréhez szükséges új nevek számát a regisztráció lehetősége sem csorbítja, valamint attól még, hogy csak bizonyos felhasználók vehetnek fel egyes identitás-neveket, a mögöttes felhasználó kiléte még felfedetlen marad.

3.3.5. Névcsere megszólításkor

Miután emberek által használt üzenetküldő szolgáltatásról van szó, figyelembe kell azt is venni, hogy a felhasználók — akár véletlenül is — kompromittálhatják egymás álcáját. Ilyen például, amikor egy szobában a beállított identitás ellenére egy beszélgetés közben valakit egy másik nevén szólítanak, amely akár a regisztrációs azonosítójára is utalhat.

Ez elkerülhető különféle figyelemfelkeltő megoldásokkal, illetve például névcserével: ha a felhasználót az egyik rejtett nevén akarja egy felhasználó megszólítani, a rendszer figyelmeztetheti erre. A kifinomult megoldás meghatározása nem triviális probléma, egyszerű ajánlásként egy listás megoldást javaslunk, amely szerint a rendszer az aktuális és valaha használt neveket figyeli, és azokra figyelmeztet.

3.4. Kompromittálás-vizsgálat

Kompromittálásról akkor beszélünk, ha több felhasználó összejátszik, és az általuk látott nézeteket összevetve felfedik egymás előtt egy felhasználó álcáját, vagy két identitás között kapcsolatot vonnak, ami sérti az identitások függetlenségét.

A későbbiek során egy *szituáció* alatt a rendszer egy véges állapotát értjük, amelyben a felhasználók között különböző kontextusokon keresztül kapcsolat van. Kompromittálás-vizsgálat során e szituációkban azt vizsgáljuk, hogy a felhasználók látszólag független identitásai között kapcsolat vonható-e, vagy információterjedés léphet-e fel (a státusz kompromittálódik).

3.4.1. Példák két kooperáló felhasználóra

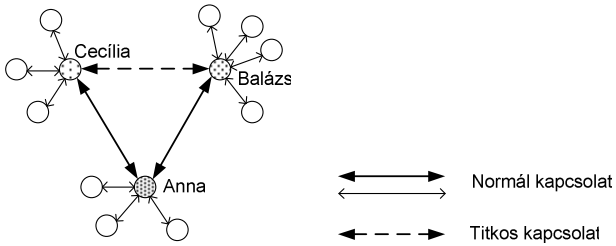
Vegyünk egy *szobában* játszódó esetet először. Ebben az esetben, ha egy felhasználó identitást vált, először el kell játszania, hogy az identitása elhagyja a szobát, vagy kilép, majd belépteti az új identitást.

Legyen két szoba, Hotel és Szálló néven. Legyenek a szobákban a vizsgálat szempontjából tetszőleges felhasználók, illetve Anna legyen ott mindkettőben, Balázs a Hotel szobában, és

Cecília a másikban. Balázs és Cecília beszélgetnek, Anna tudta nélkül; ők képesek lesznek kompromittálni Anna új identitását.

Anna identitást vált a Szálló szobában, s új identitásával belép Dezső néven. Majd távozik, s mikor kilép a rendszerből, egyszerre távozik a két szobából a két identitás — ebből Balázs és Cecília tudni fogják, hogy Dezső Anna identitása volt. Ha ezek az identitások regisztráltak, akkor a későbbiekben is ismerni fogják a kapcsolatot.

Egy másik példa, amikor a *partnerlistán* alkalmazott RBP műveletet kompromittálják. Az alábbi ábrán tüntettük fel a kapcsolati hálózatot. Cecília és Balázs ismerik egymást, de a kapcsolatuk rejtett, és mindketten ismerik Annát (a többi ismerőst most figyelmen kívül hagyjuk).



4. ábra: Egy lehetséges partnerlista kapcsolati háló

Ez a szituáció kompromittálhatja Anna RBP műveleteit. Ha például rejtett módba megy Balázs előtt, de Cecília előtt továbbra is látható, akkor Balázs előtt felfedheti állapotát. Kapcsolati hálózatoknál az ilyen jellegű helyzeteket egylépéses kompromittálásnak hívjuk, mivel a valódi állapot egy felhasználón keresztül jutott el a művelet célszemélyéhez (egy lépés a kapcsolati háló gráfján).

Véleményünk szerint a többlépéses kompromittálással a legtöbb esetben nem érdemes foglalkozni, mivel a növekvő felhasználószám miatt a kooperáció valószínűsége gyorsan csökken, és egyébként is legfeljebb csak akkor, ha a lépések száma kicsi. A többlépéses kompromittálás az egylépéseshez hasonlóan küszöbölhető ki.

3.4.2. Kompromittálás-vizsgálati módszerek

A kompromittálás-vizsgálat többféleképpen is történhet. Vagy a tervezés során ellenőrizzük a rendszer állapotait, és ha a felhasználó kompromittálható állapotba készül lépni, erre figyelmeztethetjük előre, vagy az adott alkalmazást készítjük fel ezen állapotok felismerésére.

Célszerűnek tűnik egy formális ellenőrző módszer készítése, amelynek segítségével a különféle szituációk leírhatók és leírásuk alapján eldönthető, hogy az a szituáció kompromittálható-e, vagy sem. Ezt a leírást illetve ellenőrzési módszert a tervezés során is alkalmazhatjuk, valamint a készített alkalmazásba is beépíthető.

Egy, a tervezés során alkalmazható formális ellenőrző módszernek több olyan célja is lehet, amelyeket előnyként sorolhatunk fel az „on-line" ellenőrzésekkel szemben. Egy ilyen módszerrel ugyanis nem csak az dönthető el, hogy egy szituáció kompromittálható-e vagy sem. Ha megadunk egy szituáció-csoportot, amely megfelelően leírja a rendszert, vagy definiáljuk, hogy mikor ekvivalens két szituáció, és adunk egy algoritmust, amely valamennyi szituációját felsorolja a rendszernek, akkor belátható a rendszerről, hogy megfelelő: alkalmazása során a privátszféra nem sérül, vagy megmutathatóak a hibás szituációk, amelyek alapján a rendszert tovább tudjuk fejleszteni. Ilyen értelemben auditálásra is alkalmazhatunk egy ilyen módszert.

Jelenleg kutatunk ezen a területen, kutatásunk célja formális leíró valamint ellenőrző módszer készítése a fent felsorolt problémákra, általános esetben.

3.5. Anonim szankciórendszer

Egy anonimitást is nyújtó identitásmenedzsment rendszernél praktikus, ha a felhasználók egymás „bűnügyi előéletéhez" nem férhetnek hozzá (hiszen ez szolgálhat kvázi-egyedi lenyomatként), viszont a privátszféra-védelmet növeli, ha bizonyos helyzetekre előre feltételeket fogalmazhatnak meg erre. Például a keresőben csak olyan felhasználónál szerepelhet valaki a találatok között, ha még nem küldött spam üzenetet, vagy hasonló feltételt lehet megfogalmazni az idegenektől származó privát üzenet fogadását illetően is. Ez a módszer a mai szolgáltatásokban szereplő mechanizmusoknál kifinomultabb lehetőségeket kínál.

Ezzel nem csupán az illetéktelenektől védett módon kezeljük a rossznak minősített tevékenységeket (az elkövető magát buktathatja le), de a beállítási lehetőségeket

nagymértékben finomítjuk az alkalmazásával.[12] Ehhez azonban szükséges, hogy legyen például automatikus spam-szűrő vagy -felismerő a rendszerben, ami manapság nem jellemző, vagy csak nagyon egyszerű szűrőkről beszélhetünk, amelyek egyes esetekben ráadásul ad-hoc fejlesztések.[13]

Korábban az útlevél részeként említett „bűnügyi előélet" tartalmazza a felhasználó összes olyan cselekedetéért kapott figyelmeztetést, jelzést, címkét vagy leírást, amely befolyásolhatja másoknak az őfelé irányuló bizalmát. Javaslatunkban egy egyszerű változat szerepel, amelynek használata nem megy a szolgáltatás használati élvezetének rovására, és egy laikus felhasználó számára is egyszerűen értelmezhető.

A bizalmi szint könnyen megadható, ha számlálókkal, címkékkel engedjük jelölni a felhasználókat. Ezek feltöltése lehet automatikus, ahogy például a spam üzenet detektálását is a rendszer végzi (így az ezt tároló számláló automatikusan növelhető); vagy felhasználók által növelt, mint például a kirúgások száma; vagy rendszeroperátorok által szabályozott, mint például a címkék, amelyek leírják a felhasználó korábbi tevékenységeit. Egy lehetséges, de nem teljes összeállítást mutat az alábbi felsorolás.

- Spam üzenetek detektálásának száma.
- Globálisan kicserélt üzenetek: a kifejezés-cserék száma, például káromkodások cseréje.
- Címkék: operátorok által kezelt, számlálóval rendelkező címkék, 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.

Ezek közül az automatikusan generált spam- és kifejezéscsere mezők a legérdekesebbek, ezeket a mezőket a rendszer kezeli, így nem hamisíthatóak meg. A kirúgások, tiltások, operátori figyelmeztetések száma korlátozott mértékben, de manipulálható, az ezekre vonatkozó feltételeket óvatosabban kell megfogalmazni (vagy esetleg a számlálókat érdemes súlyozni).

[12] A jelenlegi rendszerekre bináris választási lehetőségek a jellemzők. Például ne tudjon nekem írni, akit nem ismerek, nincs a partnerlistámon.

[13] Ilyen például a Windows Live Messenger szűrője, amelyet nem dokumentáltak és csak bizonyos, férgek tevékenységéhez köthető üzenetek szűrésére fejlesztették ki.

Az „amnesztia” szükségessége miatt a bűnügyi előélet valamennyi értékét dátumhoz kötötten célszerű tárolni, hogy időnként csökkenhessen az értékük, vagy nullázódhassanak automatikusan. Szándékosan ezen értékekre csak a szolgáltatás operátorai lehessenek hatással, a rendszer felhasználói nem. A címkék eltávolítását csak szolgáltatás-szintű operátorok végezhessék, de az időnkénti amnesztia vonatkozzon a címkékre is.

4. Privátszféra-védelmet növelő kiegészítő funkciók

A bemutatott RBP rendszer teljesíti a célkitűzések nagy részét, de felmerülhet igény bizonyos kiegészítésekre, valamint más menedzsment jellegű kérdésekkel is foglalkozni kell. Szükség lehet az üzenetek feladóin kívül az üzenetek tartalmának, egyéb attribútumainak szűrésére, vagy éppenséggel a partnerek különféle akcióinak gyakoriságát szükséges korlátozni, és mindezt nem csupán a privát beszélgetésekben.

4.1. Speciális attribútumok

A többszereplős beszélgetéseknek számos olyan attribútumára van szükség, amelyek a csoportok közös privátszféra-védelmét erősítik; ezeket vizsgáljuk most konferenciák és szobák esetén. Az attribútumokat alapvetően az alábbi három csoportba sorolhatjuk.

A *szűrési beállítások* az üzenetek küldésére vonatkozó korlátozási lehetőségeket foglalják magukba (például gyakoriság, hossz), valamint a különféle tevékenységekre, akciókra is hasonló szabályozást szükséges lehetővé tenni, mint például a belépések, névváltások gyakorisága, fájlterjesztési korlátok. Ezekre már a korai rendszerekben is volt igény, amikor a rosszindulatú felhasználók az események gyakori, automatizált ismétlésével zavarták a beszélgetéseket.

Lehetnek a csoport moderátorai, alapító tagja által *szankcionált*, vagy *kiemelt jogú felhasználók* is, vagyis a rendhagyó esetekről is gondoskodni kell. Érdemes a felhasználókat listákban tárolni, azonban nem mindegy, hogy a listában hogyan azonosítjuk őket — ezzel korábban foglalkoztunk. Ilyen listák lehetnek például az operátorok, kitiltottak, mellőzöttek listái.

Az *anonim véleménynyilvánítás* lehetőségét szobák és konferenciák esetén is meg lehet adni (opcionálisan, tehát ha a moderátorok engedélyezik), illetve a *névtelen olvasás* lehetőségét is szobáknál — konferenciáknál nem, mivel ott az egyértelmű azonosíthatóságot megköveteljük. További *privátszféra-védelmi attribútumok* lehetnek például az alábbiak, a teljesség igénye nélkül:

- *Lakat*: beszélgetés lezárása, belépés nem lehetséges
- *Privát beszélgetés*: nem szerepel keresésekben, elérhető listákban
- *Kulcs*: azonosítás szükséges a belépéshez
- *Meghívásos*
- *Moderált*: üzenetküldés csak az erre engedélyezett felhasználóknak
- *Kopogás*: meghívás kérése a szobán kívülről
- *Spam-szűrés, kifejezéscsere engedélyezése*
- *Fájlterjesztés engedélyezése*
- *Belépési kritériumok* megadása az anonim szankciórendszer alapján

A privátszféra-védelmi attribútum-csoport célja, hogy a csoport moderátorai megfelelően tudják szabályozni a különböző akciók hatáskörét, ennek megfelelően az előbbi lista számos elemmel tovább bővíthető.

4.2. Szimbiózis az audiovizuális magánszféra-védelemmel

Az audiovizuális magánszféra-védelem a felhasználók által küldött üzenetek nem-szöveges tartalmának, a különféle vizuális vagy hanghatással járó eseményeknek a szűrését jelenti. Az efféle üzenet-csatolmányok zavarók lehetnek, de nem feltétlenül valamennyi felhasználótól, ezért a szűrés finomhangolhatósága itt is szükséges: melyik felhasználótól milyen csatolmányok, csatolmánytípusok engedhetőek meg (például az alapértelmezett emotikonok engedélyezettek, de a sajátok nem), s ha kell, e szűrések csoportos bontásban is elvégezhetőek legyenek.

E beállítások összességét nevezzük *audiovizuális magánszféra-védelmi profilnak*, amelyekből a felhasználó célszerűen többet is definiálhat. A profilok különböző kontextusokban való alkalmazásával valósul meg az *audiovizuális magánszféra-védelem*. Ha megengedjük a felhasználónak, hogy az identitások profiljaiban beállítható állapotokhoz hozzárendelhessen audiovizuális magánszféra-védelmi profilokat is, az efféle tartalmak, események szűrése rendkívül egyszerűvé válik.

A működést egy egyszerű példán keresztül mutatjuk be. Definiálunk egy „lehalkított” nevű audiovizuális magánszféra-védelmi profilt, amelyben a hangot is tartalmazó csatolmányok nem kerülnek automatikusan lejátszásra, és az egyéb események, mint például a híváskezdeményezések némák lesznek. Ha ezt hozzárendeljük az „elfoglalt” állapothoz, akkor a felhasználó a profil „elfoglalt” állapotúra állításával elérheti, hogy az adott csoportba eső felhasználók, akikre a profilt beállította, ne zavarják.

4.3. Eseményvezérelt RBP rendszer

Az élet különböző helyzetei más-más RBP beállításokat követelhetnek meg, a felhasználó elfelejtheti ezeket átállítani, vagy miután rendszeresen szükség van ezekre a beállításokra, a folyamat automatizálása válik szükségessé. Például munkaidő letelte után, azon munkatársak számára, akikkel már nem folytat beszélgetést, a felhasználó off-line profilt szeretne megjeleníteni.

Az identitásmenedzsment ezen részét eseményvezérelt RBP rendszernek hívjuk. Az identitások változtatására felszólító események a kliensalkalmazáson egy moduljából érkeznek, például a rendszerórát figyelő (időpont), vagy a helyzetpozíció változását jelző modultól, amelyekre a következő két alfejezetben be is mutatunk egy-egy példát. Függhetnek más eseményektől is, például más felhasználók akciói alapján is generálhat a rendszer eseményeket.

4.3.1. Mobil eszközök és a helyfüggő szolgáltatások

Ha a felhasználó mobil eszközről jelentkezik be a szolgáltatásba, akkor helyzet-információk alapján is lehet vezérelni az identitásmenedzsment funkciókat (ez is alkalmazása az eseményvezérelt RBP rendszernek). Erre jó példa lehet felhasználónak az a több helyszínen is rendelő orvos, aki azt szeretné, hogy csak épp az aktuális rendelőhöz tartozó páciensek érhessék el, hívják, vagy írjanak neki.[14] [7]

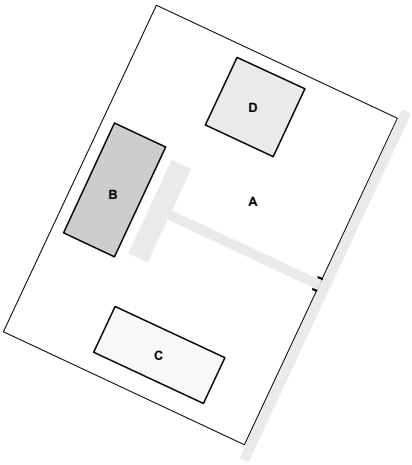
A megvalósítás egy zónajelző modulra építhető, amely zónaváltás esetén elküldi az aktuális (új) zónának az azonosítóját. A könnyű kezelhetőség és áttekinthetőség érdekében célszerű hierarchikus zónarendszert használni,[15] hiszen legtöbbször a privátszféra különböző fokozatai a térben is hasonlóan helyezkednek el, például másképp gondolunk a kertünkre, vagy azon belül a házra, vagy azon is belül a hálószobára is, de munkahelyünkön is könnyen találhatunk hasonló struktúrát.

A következő ábrán egy vállalat gondnokának a vállalati parkról készült hierarchikus területi felosztását mutatjuk be. Az ábrán a vállalat épületegyüttesének sematikus rajza látható, a parkon belül. A gondnok rendelkezik egy PDA egységgel, amely állandó internet-kapcsolattal, illetve egy GPS egységgel van felszerelve. Ezt arra használja fel, hogy jelezze

[14] Ilyen esetekben nem feltétlenül szükséges egy GPS egység, hanem lehet építeni más helyi jellegzetességekre, például egy bizonyos WLAN hálózat jelenlétére, amelyet a munkahelyi alkalmazottak vehetnek igénybe.

[15] Azzal a feltétellel, hogy minden azonos szinten lévő térrész legyen diszjunkt.

a vállalat dolgozói felé a helyzetét (hasonlóan jelezhetné barátai, családja, vagy más csoport, személyek felé is a helyzetét). Közvetlen koordinátákat nem akar elárulni, így a csevegő-szolgáltatás helyzetjelentő szolgáltatására épített RBP menedzsment rendszert használja, amelyen keresztül üzenni is tudnak neki, illetve hívni is tudják.



- A: vállalati partnerek számára elérhető helyzetjelzés a parkban tartózkodásról.
  - B, C, D: az épületekben tartózkodás jelzése.
- Egyébként: a vállalati partnerek számára nem elérhető.

5. ábra: a vállalat parkjának sematikus alaprajza

A térkép területi felosztása után meg kell adni a különböző területrészekhez tartozó privátszféra-védelmi profilt. A vállalat parkját A-val jelöltük, a különböző épületeket pedig a B, C, D betűkkel. Az ábra melletti listában összesítjük a területrészekre vonatkozó RBP műveleteket.

Egy másik értelmezés szerint akkor beszélhetünk a lokalitásról, ha azt vesszük figyelembe, hogy honnét jelentkezett be a felhasználó: ha mobil eszközről vagy számítógépről, más-más beállításokat alkalmazunk. Mobil eszköz használata esetén több korlátot is figyelembe kell vennünk, amelyek miatt a felhasználó esetleg le szeretné szűkíteni az őt elérő partnerek körét, vagy esetleg nem szeretne fájlokat fogadni.

4.3.2. Időrend-vezérelt működés

A határidőnapló analógiájának megfelelően értelmezhetünk ütemező jellegű RBP alapú rendszert, melyben időintervallumokra, időpontokra lehetséges különböző műveletek beállítása. Hasonlóan a határidőnaplóhoz, beállíthatja a felhasználó, hogy munkakezdéskor

vagy a munkaidő végén milyen csoportok számára legyen látható vagy épp nem elérhető állapotú, illetve az előre tervezett tárgyalásoknál beállíthatja a megfelelő állapotot, üzenetet.

Az alábbi táblázatban egy példát mutatunk az ütemezésre, amely például egy mobil telefonon használható csevegő szolgáltatást igénybe vevő felhasználó egy munkanapját mutatja. A példában a partnerlista csoportokra értelmezett műveleteket írtuk csak le, és csak egyszerű állapotmódosító műveletekkel foglalkoztunk. Látható, hogy időszakos és egyszeri időpontra értelmezhető műveletek is szerepelnek köztük.[16]

2. táblázat: Ütemezett műveletek

2008. június 30. hétfő	Esemény	Művelet
8:30	Munkakezdés	Elérhető a munkatársaknak, de senki másnak nem (a partnerlistán)
10:00 – 11:30	Tárgyalás	Elfoglalt a munkatársaknak
12:00 – 12:30	Ebéd	Ebéd jelzése a kollégáknak
17:00	Munkaidő vége	Elérhető mindenkinek, kivéve a munkatársaknak
18:00	Születésnapi ünnep	„Géptől távol” jelzése mindenkinek

A bemutatott példákhoz hasonlóan számos további alkalmazás felállítható a privátszféra-menedzsment kényelmességének növelésének érdekében, hiszen bármely, a rendszerből érkező eseményre lehet esemény-feltételt beállítani. Távolabbi cél lehet a különféle eseményekre szabott feltételek Boole kifejezését is kezelni képes rendszer kifejlesztése, így több eseményre egyidejűleg, vagy akár időbeliségre vonatkozóan is lehet feltételeket szabni.

5. Tesztrendszer: RBP bemutató alkalmazás

Az előző fejezetekben leírt RBP modell bemutatására készítettünk egy bemutató alkalmazást, amely a főbb modellbeli részeket magába foglalva demonstrálja a RBP működését. A tesztelésen túl ez az implementáció felfogható egy korai fejlesztésnek, amely egy később fejlesztendő csevegő szolgáltatás (AnonIM) része lehet — így a fejlesztési tapasztalatokról is írunk, és röviden az implementált modellel is foglalkozunk.

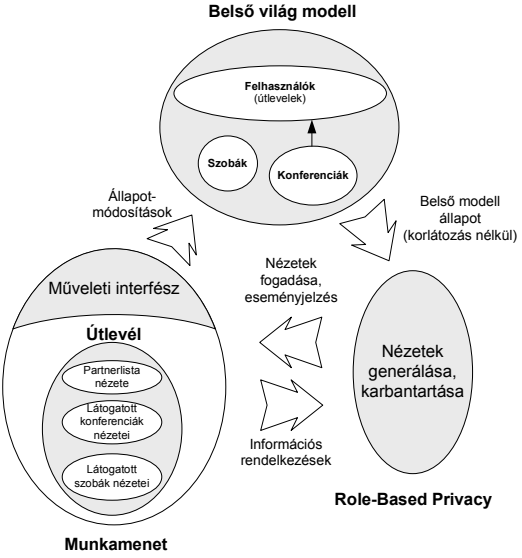
[16] Mivel eltérhet az események alakulása a tervezettől, érdemes rákérdezni az automatikus identitásváltások előtt. Ha például egy percig nincs válasz, a váltás megtörténik.

5.1. Koncepció és megvalósítás

A tesztrendszer megvalósításakor egy olyan bemutató alkalmazás elkészítését tűztük ki célul, amely a későbbiekben is felhasználható RBP és belső világ modell modulokra épül. Ezeket a bemutató alkalmazás egyszerűen csak felhasználja, és grafikus felületet nyújt a modulok teszteléséhez.

A teszt célja a szolgáltatás statikus állapotainak a modellezése a privátszféra szempontjából, amelyben megfigyelhetjük a felhasználók által alkalmazott RBP műveletek hatásait a többiek szemszögéből is. Ebből a rendszerből az üzenetek továbbítását kihagytuk, és csak a belső világ modellt építettük fel, az ahhoz szükséges műveletekkel együtt (például partnerlistás kapcsolatok kiépítése, szobalátogatás). Az alaprendszert teszteltük, így néhány funkció nem került megvalósításra, mint például az eseményvezérelt működés vagy a relációs identitásmenedzsment.

A koncepció modelljét mutatja a következő ábra. Valamennyi felhasználó azonosítás után egy munkamenetet kap, amellyel parancsokat hajthat végre, nézeteket kérdezhet le (a valós rendszerben ezen keresztül kommunikálhatna). A munkamenet jelenti a kapcsolatot a belső világ modell felé, a műveleti interfészén keresztül kommunikálva.



6. ábra: A tesztrendszer működési sémája

A műveleti interfészre készítettünk egy grafikus felületet a nézetek megjelenítéséhez, illetve értelmezőt a parancsok végrehajtásához, de a tesztalkalmazás használatából jól látható, hogy hálózaton keresztül is jól vezérelhetőek a munkamenetek. Ennek a felépítésnek további előnye a tesztalkalmazás oldaláról, hogy a szimulált felhasználók között egyszerűen válthatunk (vagy váltás nélkül parancsokat adhatunk bármely felhasználó munkamenetének),[17] és az aktuális munkamenet segítségével korábbi eseményeket vizsgálhatunk, illetve így több felhasználónak is adhatunk ki parancsot.

A rendszer a *6. ábrán* látható három fő egységből épül fel. A *munkamenet* modul teszi lehetővé a beavatkozást a belső világba, valamint ezen keresztül tekinthetőek meg a felhasználó számára látható nézetek és események. A *belső világ modell* a különféle kontextusok realizációit[18] és az útleveleket foglalja magába. A *Role Based Privacy* modul a belső világ modell állapota, a felhasználók beállításai alapján generál nézeteket a különböző felhasználók lekérdezései alapján.

Látható, hogy rejtetten, de kettéválasztottuk a RBP privátszféra-védelmi funkciókat. A RBP műveleteket kezelő résznek a nézetek megvalósításáért felelős modulhoz kellene tartoznia, de végül a munkamenetbe építettük.

A tesztelő a belépett felhasználókkal navigálhat a három fő kontextusban, állíthat a különféle profilokon, és a kontextusokon belül értelmezett RBP műveleteket alkalmazhatja partnerekre. A tesztrendszernek nem volt célja a kommunikáció demonstrációja; elsősorban a szerepek láthatóságára, az identitásmenedzsment problémakör megoldásaira koncentrál.

A megvalósítás során több szempont figyelembevételével a Java technológia [5] mellett döntöttünk, és a tesztelés hordozhatósága, az egyszerűen felépíthető tesztkörnyezet létrehozása érdekében beépített adatbázist választottunk, amely a HSQLDB [6] rendszer volt. Így a különféle teszt-eseteket más-más kiindulási állapottal lehet felállítani, amelyeket SQL parancsokat tartalmazó állományokból lehet betölteni.

5.2. Az eredmények értékelése

A különféle RBP műveleteket néhány előre összeállított teszt-eset szerint teszteltük, melyek során figyelembe vettük a műveletek hatékonyságát, hogy a tesztelésben megvalósított modellre épülő gyakorlati rendszer kivitelezhető lesz-e.

[17] E funkció egyszerű megvalósítása miatt döntöttünk első sorban a parancssor alapú vezérlés mellett.

[18] A tesztrendszerben a párbeszéd kontextusát nem implementáltuk, mivel a RBP tesztelése szempontjából nem lényeges.

Véleményünk szerint a rendszer kezelése nagyban hasonlít a manapság használatos csevegő szolgáltatásokéra, és várakozásaink szerint a felhasználók többségének nem okozna különösebb problémát egy ilyen rendszer használatának megtanulása.

Bár a korábban tárgyalt profil-hierarchián alapuló identitásmenedzsment kezelése valóban egyszerű volt, de úgy véljük, hogy újabb műveletekre is szükség lehet. Például előfordulhat, hogy a profil-hierarchiában magasabb szinten elhelyezkedő profil egy részét, mondjuk, az állapot attribútumát megváltoztatjuk, és szeretnénk, ha ez az alacsonyabb szinten is változna a többi profilban (csak ez a jellemző). A tanulmányban felvázolt RBP rendszer erre lehetőséget nem ad, de ez a megfelelő hatékonyság elérése miatt úgy véljük, szükség van rá.

Összességében viszont a rendszert megfelelőnek találtuk, és szeretnénk egy laikus, de rendszeres csevegőszolgáltatás-használókból álló tesztcsoport véleményét is kikérni, azonban erre még a jelenlegi tesztrendszer kevésbé alkalmas.

6. Kitekintés: PRIME

A PRIME (PRivacy and Identity Management for Europe, [8]) európai uniós projekt, célja egy interdiszciplináris, az informatikán túlmutatva jogi, szabályozási, gazdasági területeket is érintő, összetett identitásmenedzsment rendszer tervezése és megvalósítása, megfelelő tudományos kutatásokra alapozva. A 2008-ban lezáruló projektben és utódában, a PrimeLife-ban [10] nagy multinacionális fejlesztő cégek, nagy alkalmazók, valamint több európai egyetem és kutatócsoport vesznek részt. A távlatilag megvalósuló rendszer a mai informatikai rendszerek nagy részét érinteni fogja, nem csupán az internetet; alapvető célja a digitális világba kerülő személyes és egyéb adatok menedzsmentjének megvalósítása az adatok születésétől kezdve teljes életciklusukon keresztül, oly módon, hogy a felhasználók megfelelően kontrollálhassák az adataik elérhetőségét a különböző szolgáltatók, szervezetek számára, valamint hogy ellenőrizhessék, ki fért hozzá az adataikhoz és melyik szolgáltató milyen adatokkal rendelkezik róluk.[19] A PRIME Role Based Privacy alapú szerepmenedzsmentet nyújt majd, így tulajdonképpen a jelen tanulmányban ismertetett elveknek egy általánosabb szinten történő megvalósítását célozza.[20]

[19] Erre élethű példát mutat be a PRIME White Paper dokumentuma.

[20] Magyar nyelven lásd [9]-ben.

7. ábra: A PRIME felhasználó-vezérelt identitásmenedzsment koncepciójának illusztrációja

7. Összefoglalás

A mobil internet elterjedése, a mobil eszközök fejlődése a mindennapi használatban előtérbe helyezi a csevegő szolgáltatásokat is, és már ma számos más példát is említhetnénk a tanulmány minden egyes példája mellett. A mobilitásból adódóan nem csupán a korlátok miatt vagyunk kénytelenek újragondolni a szolgáltatások privátszféra-védelmének koncepcióját, hanem új kihívásokkal, igényekkel kell szembenéznünk.

A tanulmányban bemutatott Role Based Privacy alapú identitásmenedzsment módszer választ ad az új kihívásokra, és a konstrukció vizsgálatán keresztül más, hasonló szolgáltatások problémakörébe is betekintést nyerhetünk. A bemutatott identitásmenedzsment megoldás használható például általánosságban is a helyfüggő magánélet-védelem, a Location Privacy problémakörében, és úgy véljük, hogy közösségi vagy kapcsolati hálón alapuló rendszerekben is nagy segítséget nyújthat a felhasználóknak.

A szerző a továbbiakban tervezi egy egyszerűen kezelhető tesztrendszer elkészítését, amelynek segítségével laikus, csevegő szolgáltatást igénybe vevő felhasználók bevonásával a gyakorlatban is felmérheti a rendszer használhatóságát.

Hivatkozások

[1] Ian Goldberg, David Wagner, Eric Brewer: Privacy-enhancing technologies for the Internet. *Proceedings of the 42th IEEE Spring COMPCON, 1997,* pp. 103–109.

[2] Gulyás Gábor György — Schulcz Róbert: Újgenerációs anonim böngészők. *Híradástechnika,* 2007. augusztus, 24–27. old.

[3] Jonna Häkkilä — Ilkka Känsälä: Role Based Privacy Applied to Context-Aware Mobile Applications. *IEEE Internation Conference on Systems, Man and Cybernetics, 2004.* pp. 5467–5472

[4] Gulyás Gábor György: Az anonimitás és a privacy kérdései csevegő szolgáltatásokban. In: *Tanulmányok az információ- és tudásfolyamatokról 11.* Alma Mater sorozat, BME GTK ITM, Budapest, 2006 október.

[5] Java technológia
http://java.sun.com

[6] HSQLDB, SQL kompatibilis Java technológiával készült adatbázis rendszer
http://hsqldb.org

[7] Jay Parkinson, akit több csevegő szolgáltatáson keresztül is elérhetnek a betegei
http://www.jayparkinsonmd.com

[8] PRIME Projekt
https://www.prime-project.eu

[9] Hasznics Milán: Globális perszonalizáció — kapcsolati hálózatkezelés PRIME környezetben. In: *Tanulmányok az információ- és tudásfolyamatokról 10.* Alma Mater sorozat, BME GTK ITM, Budapest, 2006. március.

[10] PrimeLife Projekt
http://www.primelife.eu