Általános célú biztonságos anonimitási architektúra

TÓTH GERGELY, HORNÁK ZOLTÁN

BME, Méréstechnika és Információs rendszerek Tanszék
tgm@mit.bme.hu, hornak@mit.bme.hu

Reviewed

Kulcsszavak: anonimitás, hálózati architektúra, biztonságos kommunikáció

A távközlésben legújabb követelményként napjainkban egyre inkább megjelenik az anonimitás (tipikusan elektronikus szavazás, közvélemény-kutatás vagy fizetés során). A jelenlegi hálózati réteghierarchia azonban önmagában nem tartalmazza ezt a funkciót. Ezen probléma megoldására tesz javaslatot a cikk egy általános célú biztonságos anonimitási architektúrával, amely a jelenlegiek mellett új, kifejezetten anonimitási funkciókat teljesítő rétegeket vezet be és meghatározza azok helyét a jelenlegi modellben.

Az elmúlt évtizedek során a számítástechnika, a hardver, a szoftver, valamint a távközlés terén tapasztalható rohamos fejlődés lehetővé tette a rendszerek egyre nagyobb fokú integrálását. Ez a tendencia az Internet térhódításával az informatika elé újabb és újabb kihívásokat állít. Az elsőként fellépő távközlési problémákra – a szükséges sávszélesség és megbízhatóság biztosítására – már léteznek átfogó architekturális megoldások.

Az előző évtizedben újabb igények merültek fel: a meglévő adottságok mellett már bizalmas információcserére is szükség volt. A titkosítás, integritás-védelem, hitelesítés stb. megoldására már szintén léteznek bevált megoldások [1].

Újabban a személyi és személyes adatok védelme került előtérbe. Ahogy egyre több adatbázist kapcsolnak össze és tesznek – részben nyilvánosan – kereshetővé, úgy lehet az egyes emberekről egyre több információt összegyűjteni. Egyfajta ellenintézkedésként ezért van szükség az adatvédelemre, a személyi és személyes adatok illetéktelen hozzáférés elleni védelmére.

Az anonimitást ezen belül tekinthetjük egyfajta extrém adatvédelmi módszernek, ahol az alany személyazonosságát rejtjük el, ezáltal szüntetjük meg (vagy csökkentjük elfogadható mérték alá) annak esélyét, hogy egy támadó az esetleg megtudható személyes adatokat hozzárendelje egy személyhez és így egy nem megengedett on-line profilt állítson össze [2].

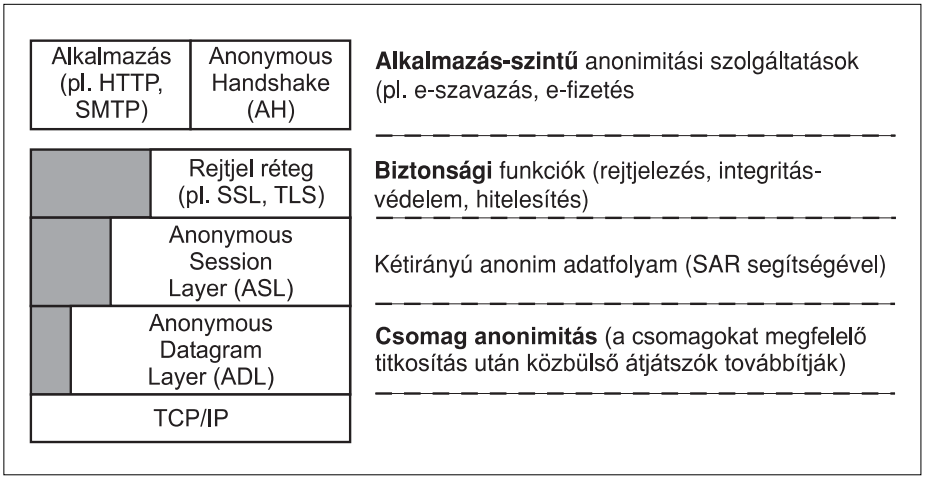
Anonimitás elérésére léteznek már különböző technikák, azonban hiányzik egy olyan egységes keretrendszer, ahol a biztonsági (rejtjelezési) módszerek mellett tetszőleges anonimitási szolgáltatás is megvalósítható. Az általános célú biztonságos anonimitási architektúra *(general-purpose secure anonymity architecture,* GPSAA) célja pont ennek az űrnek a betöltése, azaz a biztonsági funkciók ötvözése az anonimitási megoldások két nagy csoportjával:

• Anonim üzenetküldési technikák:

Két fél közötti kommunikáció során biztosítják, hogy még a hálózati forgalom megfigyelése és módosítása esetén sem deríthető ki adott küszöbértéknél nagyobb valószínűséggel, hogy ki kinek küld adatot [3]. Tipikus alkalmazás az anonim levelezés vagy anonim böngészés.

• Anonim engedélyezési sémák:

Lehetővé teszik, hogy egy szolgáltató az anonimitási hatóság segítségével megbizonyosodjon, hogy egy számára anonim alany jogosult-e egy szolgáltatás igénybevételére. Tipikus alkalmazási területek: e-fizetés (az anonimitási hatóság a bank, az engedélyezés pedig az elektronikus pénz beszerzése és átadása a szolgáltatónak), e-szavazás.



1. ábra
Az általános célú biztonságos anonimitási architektúra rétegei

Architektúrális felépítés

A bevezetőben leírtak alapján egy olyan általános keretrendszerre van szükség, mely lehetővé teszi a fenti csoportokba sorolható tetszőleges anonimitási módszer megvalósítását és ezzel együtt biztonsági funkciók alkalmazását.

A távközlés során fellépő anonimitási problémák alapvetően az IP protokollcsalád tulajdonságából adódnak (egy tetszőleges lehallgatott IP csomag tartalmazza mind a küldőjét, mind a fogadóját). Azonban az Internet elterjedtsége miatt ezt megváltoztatni nem lehet, felsőbb rétegekben kell az anonimitást garantálni. Ezen megkötés mellett dolgozták ki a GPSAA rétegszerkezete *(1. ábra)*.

A TCP/IP feletti első réteg az ADL *(Anonymous Datagram Layer)*, melynek feladata fix méretű csomagok egyirányú anonim átvitele. Erre építve a következő réteg, az ASL *(Anonymous Session Layer)*, már képes kétirányú anonim adatfolyam kezelésére SAR *(Segmentation And Reassembly)* segítségével. Az anonim adatfolyamot felhasználva már alkalmazhatóak a bevált rejtjel rétegek. Végül legfelül helyezkedik el az AH *(Anonymous Handshake)*, mely az anonim engedélyezés alkalmazás-szintű feladatait látja el.

ADL – Csomagok anonimitása

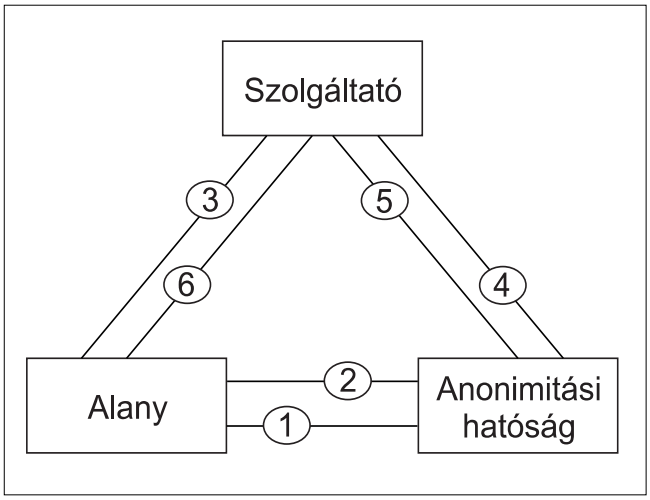
Az ADL réteg feladata két kommunikáló fél között egységes méretű csomagok anonim továbbítása. Ennek során *(2. ábra)* a feladónál a csomagot rejtjelezik, majd az ADL csatornán keresztül jut a fogadóhoz. Fontos megemlíteni, hogy egyrészt az ADL csatorna nem feltétlenül egy fizikai egység, lehet több átjátszó elosztott hálózata, másrészt minden egyes átjátszó átkódolja és összekeveri a csomagokat, annak érdekében, hogy ne lehessen a hálózat lehallgatásával azok útját követni.

Az, hogy az átkódolások milyen algoritmust követnek, hány átjátszó építi fel a hálózatot, nem része az ADL specifikációnak, a réteg meghatározásánál csak az interfészt rögzítik, mely a szolgáltatással kapcsolatos követelményeket tartalmazza.

ASL – Kétirányú anonim adatfolyam

Az ADL rétegre építve következő lépésként lehetővé kell tenni a kétirányú anonim adatfolyam kiépítését. Ezt a célt szolgálja az ASL réteg. Különösebb anonimitási funkciója nincs, egyedüli feladata, hogy a felsőbb rétegektől kapott adatfolyamot a küldő oldalon feldarabolja az ADL réteg által megkövetelt méretű fix csomagokra, majd a fogadó oldalon ezeket a csomagokat helyes sorrendben adatfolyammá állítsa össze, (hiszen az ADL a lehallgatók megtévesztése érdekében a csomagok kézbesítési sorrendjét tipikusan össze is keveri).

Az ASL réteg felett helyezkedik el a rejtjel réteg, mely az adatfolyamokon végzi a különböző biztonsági feladatokat. Ugyan már az ADL rétegben is van rejtjelezés, azonban ott csak az anonimitás kompromittálása ellen (mely során bizonyos átjátszók láthatják a kódolatlan üzenetet), itt pedig már az átjátszókban sem bízva a lehallgatás ellen kell végpont-végpont titkosítást végezni, ahol biztosítható, hogy csak a fogadó fél tudja dekódolni az üzenetet.



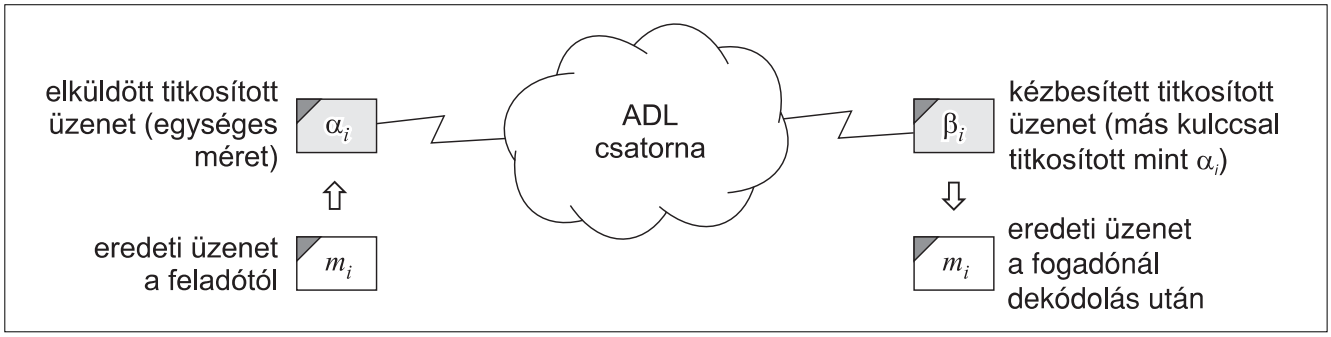
3. ábra Az anonim engedélyezés általános lefolyása az AH keretében

AH – Alkalmazás-szintű anonimitási szolgáltatások

A most már biztonságos, kétirányú anonim adatfolyam felett történhet meg ezek után az anonim engedélyezés az AH keretében *(3. ábra)*.

Az anonim engedélyezés folyamata két fázisból áll. Az első fázisban az alany az anonimitási hatóságtól beszerzi az anonimitási okmányokat (az ATM-es pénzfelvét analógiájára) (1) (2), melynek során nem anonim, sőt személyazonosságát kifejezetten igazolja.

2. ábra Csomagok küldése általános esetben az ADL rétegen keresztül



A második fázisban történik meg a szolgáltatás tényleges igénybevétele, itt már az alany anonim. Először átadja az okmányokat és kéri a szolgáltatást (3). Ezután a szolgáltató ellenőrzi az okmányokat (4), majd az anonimitási hatóság válaszától (5) függően teljesíti a kérést (6). GPSAA az AH keretében is csak követelményeket és egy interfészt fogalmaz meg, melyben ezek után különböző algoritmusok is megvalósíthatók.

Gyakorlati példaként említhetnénk a Chaum-féle vak aláírás módszerét [4], melyet elektronikus anonim fizetés lebonyolítására dolgoztak ki.

Alkalmazás

Amellett, hogy a GPSAA interfészeket és követelményeket definiál, folyamatban van egy referencia-megvalósítás elkészítése is, mely a *4. ábrán* ismertetett sémát követi.

A kezdeti tesztekhez ADL szinten a PROB-csatorna [5], míg AH keretében a Chaum-féle vak aláírás módszer [4] került felhasználásra.

Összefoglalás

A GPSAA egy olyan általános keretrendszer, mely lehetővé teszi különböző anonimitási módszerek és biztonsági szolgáltatások együttes alkalmazását. A keretrendszer megvalósítása után következő lépésként a rendszer által nyújtott anonimitás mérése és a rendszer finomhangolása következik.

Irodalom

[1] Dierks, T., Allen, C.:
RFC 2246 – The TLS Protocol Version 1.0.
Certicom, 1999

[1] Froomkin, A. M.:
Flood Control on the Information Ocean:
Living with Anonymity,
Digital Cash and Distributed Databases, 1996.,
http://www.law.tm/

[1] Reed M., Syverson, P., Goldschlag, D.:
Anonymous Connections and Onion Routing.
IEEE Journal on Selected Areas in
Communication Special Issue on Copyright and
Privacy Protection, 1998., pp.482–494.

[1] Chaum, D.:
Blind Unanticipated Signature Systems.
USA szabadalom: 4 759 064, 1998.

[1] Tóth, G., Hornák, Z.:
Megfigyelhető black-box csatorna
forrásrejtő tulajdonsága.
Híradástechnika, 2003/05, pp.41–44.

4. ábra Az általános célú biztonságos anonimitási architektúra implementációja