ÁLTALÁNOS CÉLÚ BIZTONSÁGOS ANONIMITÁSI ARCHITEKTÚRA

Tóth Gergely, Hornák Zoltán
Budapesti Műszaki és Gazdaságtudományi Egyetem
{tgm, hornak}@mit.bme.hu

KULCSSZAVAK
anonimitás, hálózati architektúra, biztonságos kommunikáció

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

KEYWORDS
anonymity, network architecture, secure communication

ABSTRACT
In today's electronic communication anonymity is required more and more (typically for electronic payment, surveys or voting), however the current network architecture does not support this functionality. This paper provides a solution for this problem by proposing a general-purpose security anonymity architecture, which introduces new layers for providing anonymity besides the traditional ones and specifying their location in the current model.

BEVEZETÉS

Az elmúlt évtizedek során a számítástechnika, a hardver, a szoftver, valamint a kommunikáció 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. A kommunikációval szemben elsőként fellépő sávszélesség és megbízható adatátvitel problémákra már léteznek átfogó architekturális megoldások. Az előző évtizedben újabb igények merültek fel: a meglévő adottságok mellett már bizalmas kommunikációra 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 előli 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].

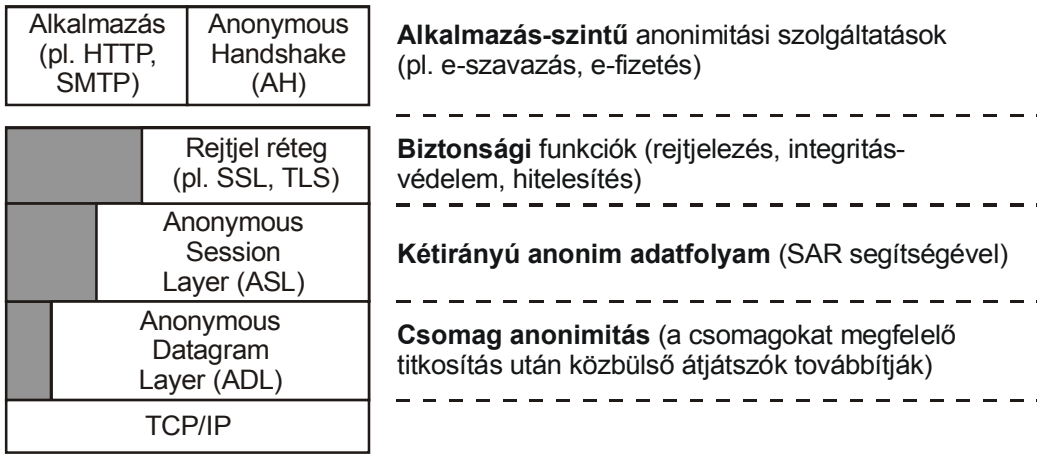
Anonimitás elérésére léteznek már különböző technikák, azonban hiányzik egy olyan egységes keretrendszer, ahol a biztonsági (rejtjelezési) módszerek mellett tetszőleges anonimitási szolgáltatás is megvalósítható. Az általános célú biztonságos anonimitási architektúra (*general-purpose secure anonymity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

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.

Az elektronikus kommunikáció 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 nincs mód, felsőbb rétegekben kell az anonimitást garantálni. Ezen megkötés mellett került kidolgozásra a GPSAA rétegszerkezete (lásd 1. ábra).



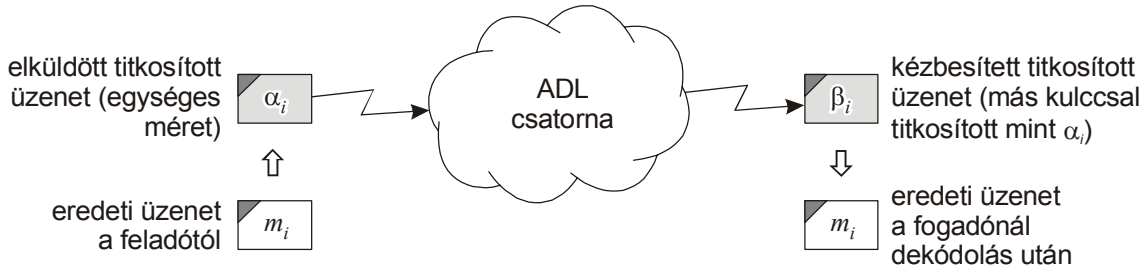
1. ábra
Az általános célú biztonságos anonimitási architektúra rétegei

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 (lásd 2. ábra) a feladónál a csomag rejtjelezésre kerül, 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 interfész került leírásra, mely a szolgáltatással kapcsolatos követelményeket tartalmazza.



2. ábra
Csomagok küldése általános esetben az ADL rétegen keresztül

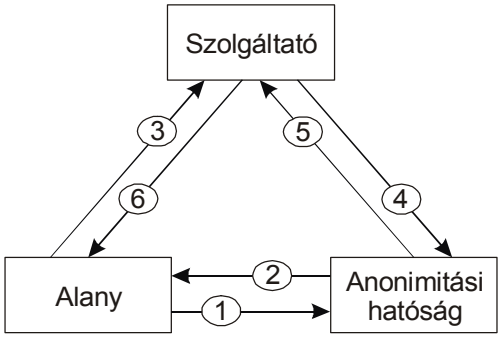
ASL – Kétirányú anonim adatfolyam

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.

AH – alkalmazás-szintű anonimitási szolgáltatások

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

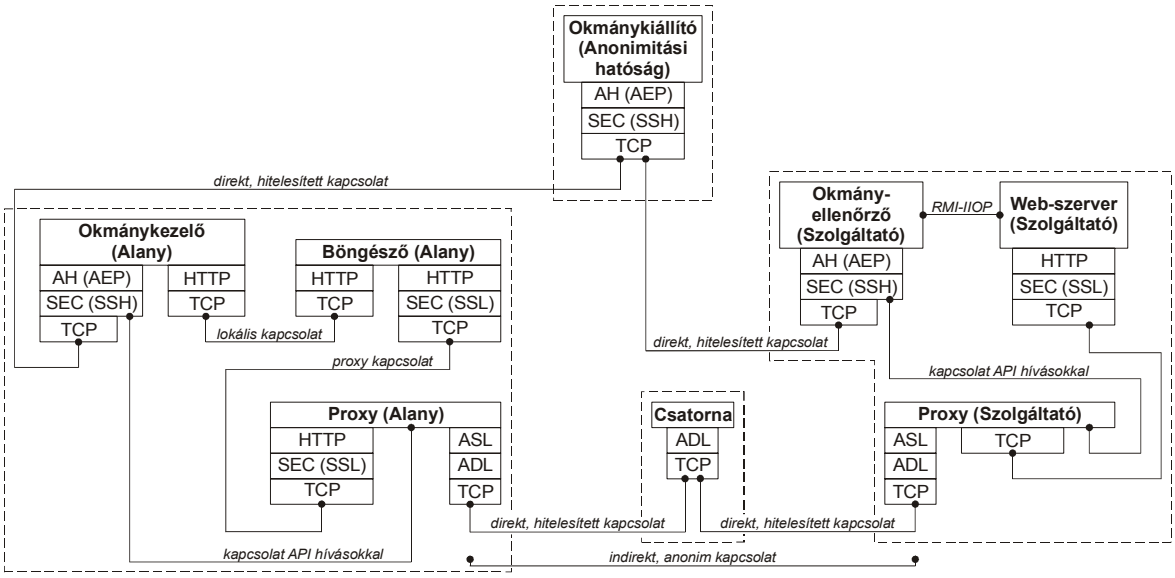


3. ábra
Az anonim engedélyezés általános lefolyása az AH keretében

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. 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.

IMPLEMENTÁCIÓ

Amellett, hogy a GPSAA interfészeket és követelményeket definiál, folyamatban van egy referencia implementáció 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 implementálásra.



4. ábra
Az általános célú biztonságos anonimitási architektúra implementációja

ÖSSZEFOGLALÓ

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

IRODALOMJEGYZÉK

[1] DIERKS, T., ALLEN, C.: **RFC 2246 – The TLS Protocol Version 1.0**. Certicom, 1999

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

[3] 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. 482-494. old.

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

[5] TÓTH, G., HORNÁK, Z.: **Megfigyelhető black-box csatorna forrásrejtő tulajdonsága**. Híradástechnika, 2003/05, 41-44. old.