Keretrendszer anonimitási módszerek integrálására

Tóth Gergely, Hornák Zoltán

Budapesti Műszaki és Gazdaságtudományi Egyetem
Méréstechnika és Információs Rendszerek Tanszék
1111 Budapest, Magyar tudósok krt. 2.

{gergely.toth, zoltan.hornak}@mit.bme.hu

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. A bemutatandó általános célú biztonságos anonimitási architektúra (*general-purpose secure anonymity architecture*, GPSAA) ezt a hiányosságot pótolja új hálózati rétegek bevezetésével.

Anonimitás biztosítására léteznek már különböző technikák, azonban hiányzik egy olyan egységes keretrendszer, ahol a biztonsági (rejtjelezési) módszerek mellett tetszőleges anonimitási szolgáltatás is megvalósítható, ezek akár ki is cserélhetők a felsőbb rétegek módosítása nélkül. GPSAA célja a biztonsági funkciók ötvözése az anonimitási megoldások két nagy csoportjával: (1) az a*nonim 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 (tipikus alkalmazás: anonim levelezés vagy anonim böngészés) míg az a*nonim engedélyezési sémák* lehetővé teszik, hogy egy szolgáltató egy anonimitási hatóság segítségével megbizonyosodjon, egy számára anonim alany jogosult-e egy szolgáltatás igénybevételére (tipikus alkalmazási területek: e-fizetés vagy e-szavazás).

A hagyományos TCP/IP hálózati architektúrát GPSAA három új, kifejezetten anonimitási szolgáltatásokat ellátó réteggel egészíti ki a fenti funkciók elérése érdekében. TCP/IP felett helyezkedik el az ADL (*Anonymous Datagram Layer*), melynek feladata fix méretű csomagok egyirányú továbbítása. Felette található az ASL (*Anonymous Session Layer*), amely már kétirányú anonim adatfolyamot nyújt a felsőbb rétegek számára. Efelett alkalmazhatóak a hagyományos rejtjel rétegek, amik végpont-végpont biztonsági funkciókat (rejtjelezés, integritás-védelem, hitelesítés) nyújtanak. Végül a hierarchia tetején található az AH (*Anonymous Handshake*), ami az anonim engedélyezés alkalmazás-szintű feladatait látja el.

Az így létrehozott keretrendszer alkalmazásával különböző anonimitási és rejtjel technikák integrálhatók, azok biztonságosan, csereszabatosan használhatók széles alkalmazói körben.