Framework for the Integration of Anonymity Techniques

Gergely Tóth, Zoltán Hornák

Budapest University of Technology and Economics
Department of Measurement and Information Systems
H-1111 Budapest, Magyar tudósok krt. 2., Hungary

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

Anonymity seems to become the newest requirement for the electronic communication (typically for electronic voting, on-line polls or for e-payment). Unfortunately the current network layer hierarchy does not support this function. The introduced *general-purpose secure anonymity architecture* (GPSAA) aims to answer this need by defining new network layers.

For providing anonymity several techniques have already been proposed, however we lack a general framework, where together with security functions arbitrary anonymity services could be implemented. GPSAA aims to integrate security protocols with anonymity techniques, so that the building blocks are exchangeable without upper layers noticing it, this way seamless and reliable operation could be ensured. The two large groups of anonymity services considered are the *anonymous message transmission techniques*, where during communication between two parties the system ensures that an adversary is unable to link the communicating parties with a probability greater than a given threshold (typical examples are anonymous e-mail or web-surfing); whereas *anonymous authorization techniques* enable service providers to decide, whether an anonymous user (using anonymous message transmission techniques) should be allowed to access a certain service (typical scenarios are e-payment or e-voting).

Above the traditional TCP/IP network architecture GPSAA defines three new anonymity-providing layers in order to enable the implementation of the above functions. Right above TCP/IP ADL (*Anonymous Datagram Layer*) transmits fixed-sized packets anonymously in one direction. ASL (*Anonymous Session Layer*) provides bi-directional anonymous data streams based on the underlying ADL. Using these services security protocols can be used to provide encryption, integrity-protection and authentication. Finally on top of the hierarchy AH (*Anonymous Handshake*) is responsible for the anonymous authorization process.

This way the defined framework integrates different anonymity and security techniques so that they can be used efficiently in wide application areas.