Network architecture to provide secure anonymous communication

GERGELY TÓTH, ZOLTÁN HORNÁK

Budapest University of Technology and Economics, Dept. of Measurement and Information Systems
{tgm,hornak}@mit.bme.hu

Keywords: anonymity, network architecture, GPSAA, secure communication

Anonymity becomes more and more important in today's privacy-aware information society. Unfortunately the current network layer hierarchy does not support anonymous communication, thus new layers need to be introduced to provide anonymous, yet secure communication in a transparent and easy-to-use fashion. The introduced model of general-purpose secure anonymity architecture (GPSAA) aims to fulfill this purpose.

The rapid development in the area of computer science, software, hardware and communication made it possible to integrate information systems in a constantly increasing factor. This tendency with together with the spreading of Internet sets newer and newer challenges for the information science. For the first problems of bandwidth and reliable data transfer several general architectural solutions exist. In the last ten years new needs arose: besides the given features *secure* communication was also required. In the field of encryption, integrity-protection, remote authentication honored solutions are already known (such as SSL/TLS, SSH or IPSec).

The latest development brought the protection of personal data – *privacy* – into the spotlight. As more and more databases get connected and made – partially publicly – searchable, so will information gathering about persons become easier. As a kind of countermeasure that is why legal data-protection is needed. Anonymity can be understood as an extreme measure of such kind, where the identity of the subject needs to be hidden by technical means, this way eliminating (or at lease reducing to an acceptably small probability) the chance, so that an attacker may connect personal data to a person thus avoiding the creation of an unauthorized on-line profile [1].

For providing anonymity several different techniques exist, but we lack a uniform framework, where besides security techniques (e.g. encryption) arbitrary anonymity methods can be realized. The *general-purpose secure anonymity architecture* (GPSAA) aims to fill exactly this void – to combine security features with the following two kinds of anonymity techniques:

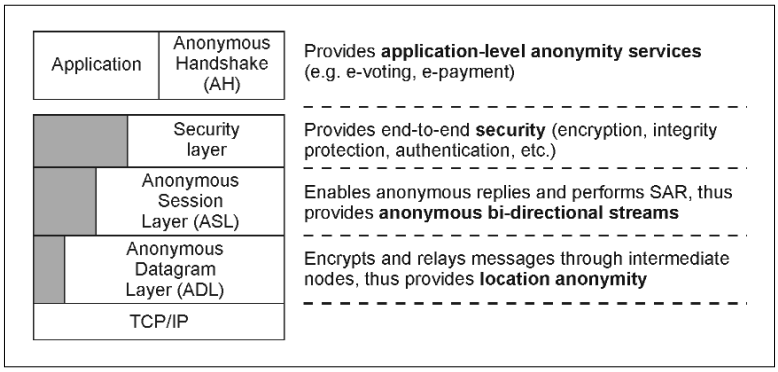
- *Anonymous message sending methods:* in the communication between two parties they make it hard to figure out (even with the help of eavesdropping on the communication channels) who sends messages to whom [2]. Typical scenarios include anonymous e-mail or anonymous web-surfing.
- *Anonymous authorization schemes:* with the help of an anonymity authority they make possible for a service provider to be certain that an anonymous subject is authorized to use a specified service. Typical application areas are: anonymous electronic payment (subject is the client, anonymity authority is the bank and the authorization is the payment) or anonymous electronic voting. In most cases in order to work correctly such schemes require anonymous message sending.

1. The Architecture

According to the introduction such a general framework is required, which enables to combine security features with techniques of the two above mentioned anonymity categories.

The anonymity problems during the electronic communication arise mainly because of the properties of the IP protocol family (i.e. each IP packet contains both the sender's and the recipient's IP address, which makes both of them back-traceable, not anonymous). However, since the popularity of the Internet changing these protocols is not an option, anonymity has to be provided in upper layers. The layer hierarchy of GPSAA was designed with these requirements *(Fig. 1)*.

Fig. 1. Layers of GPSAA



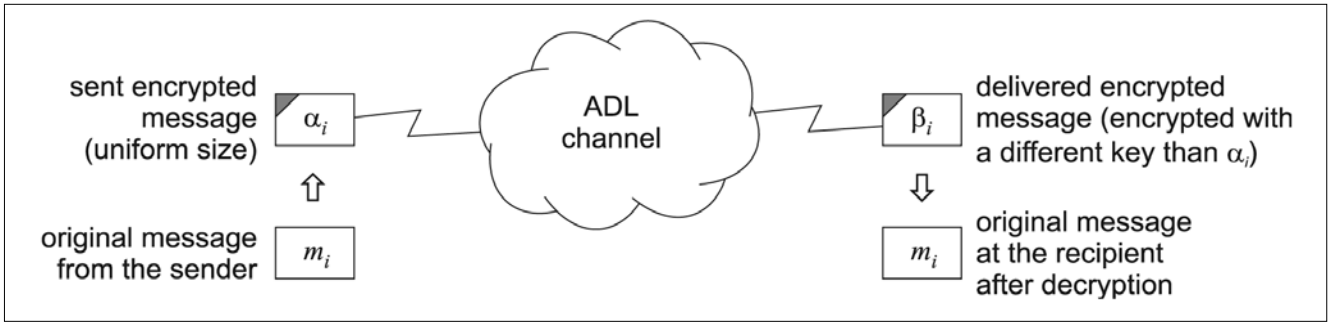


Fig. 2. Sending packets through ADL

The first layer above TCP/IP is the ADL *(Anonymous Datagram Layer)*, whose function is to deliver fixed size packets anonymously using relaying proxies that hide the source and destination of packages. The next layer, ASL *(Anonymous Session Layer)* builds on the services of ADL and is able to manage not just datagrams, but anonymous bi-directional streams. This layer has to solve also the problem of SAR (segmentation and reassembly). Based on anonymous streams, the conventional security layers can be applied. Finally, on the top resides AH *(Anonymous Handshake)*, which handles the application-level anonymous services, like authorization.

ADL – Anonymous Datagram Layer

Aim of ADL is to transport fixed size packets between two communicating parties anonymously *(Fig. 2)*. The packets will be encrypted at the sender, and will be delivered through an ADL channel. This channel is not necessary one physical unit, it can consist of several relaying proxies. Each relaying proxy encodes the packets further and reorders them as well so that by eavesdropping communication lines the routes of the packets cannot be followed.

How such encodings (encryption and decryption) work and how many relaying proxies are utilized is not part of the ADL specification. ADL aims to define an interface, which describes the requirements for possible implementations. By using such a general construction, one might use several different methods in an actual implementation.

ASL – Anonymous Session Layer

Building on ADL, the next step is to provide a bi-directional anonymous stream. Such bi-directional communication brings up some problems concerning anonymity, since with this scenario one party must not know the identity of the other. ASL handles anonymous addresses for this purpose. Besides that, no other anonymity functionality is defined for this layer, however its further task is to cut data received from upper layers into fixed size packets (as required by ADL) at the initiator side and to reorder (since in order to confuse attackers ADL reorders packages) and reassemble these at the responder side.

The security layer resides on top of ASL, which performs security functions on data streams. Although there is encryption in ADL as well, but it is used there only to provide protection against compromising anonymity so only provides link-by-link encryption. To provide end-to-end security, where even relaying proxies should not see the plaintext, the traditional security solutions should be applied (such as SSL, TLS or SSH).

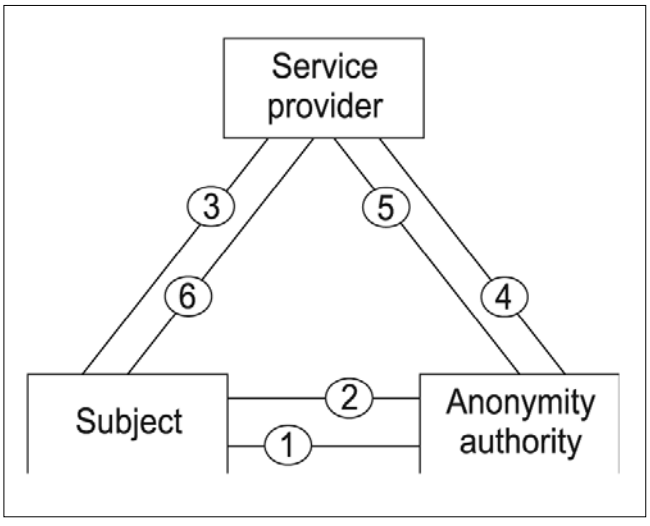
AH – Anonymous Handshake

Now we are ready to employ anonymous authorization above the secure bi-directional anonymous stream as part of AH *(Fig. 3)*.

Anonymous authorization consists of two phases. In the first phase the subject requests anonymity tokens from the anonymity authority (1) (2) during which the subject is not anonymous, on the contrary, he has to be authenticated. Actually accessing the service happens in the second phase, where the subject is already anonymous. He hands the tokens over to the service provider and requests the service (3). After this the service provider checks the tokens (4) and based on the answer from the anonymity authority (5) fulfills the request (6).

GPSAA only formulates requirements for the AH, no special algorithm is envisioned, the main emphasis is to be as general as possible, in order to allow interchangeable suites, like in other widely accepted solutions (e.g. SSL).

Fig. 3. General data flow of the anonymous authorization as part of AH



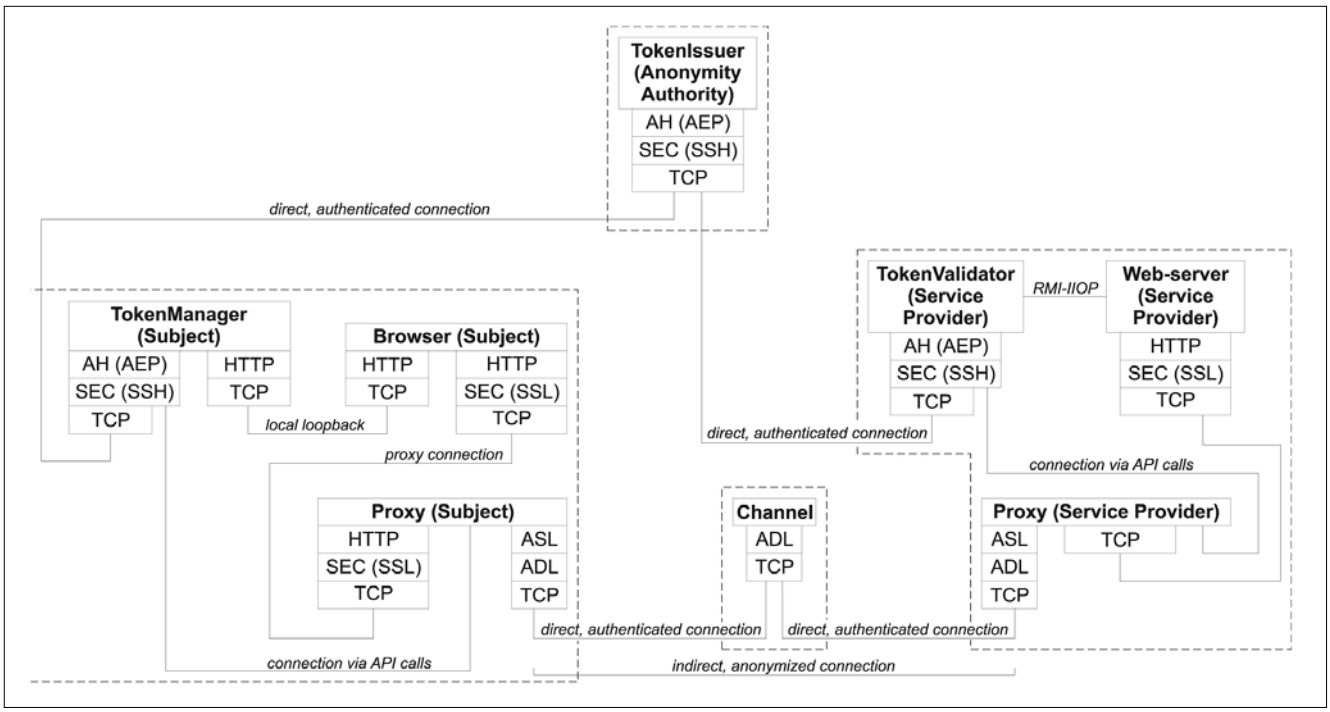


Fig. 4. Implementation scheme of GPSAA

2. GPSAA Implementation

Besides formulating interfaces and requirements as part of GPSAA, implementing the architecture is under way. This reference implementation follows the details of *Fig. 4.* For the first tests at ADL the PROB-channel [4], and at AH level the blind-signature scheme of Chaum [3] was implemented.

3. Conclusion

The general-purpose secure anonymity architecture is a general framework, which enables the combined usage of security functions and anonymity services. With the help of three newly introduced layers (ADL, ASL and AH) the current network hierarchy can efficiently extended to support secure anonymous data transfer – a key building block of today's communication.

References

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

[2] 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.

[3] Chaum, D.:
Blind Unanticipated Signature Systems. US Patent #4 759 064, 1998.

[4] Tóth, G., Hornák, Z.:
Measuring Anonymity in a Non-adaptive, Real-time System, Proceedings of the Privacy Enhancing Technologies Workshop, Toronto, 2004.