Anonymity Enhancing Protocol, *AEP*

Abstract

Gergely Tóth, Kristóf Kerényi, Attila Sili
Consultant: **Zoltán Hornák**

Department for Measurement and Information Systems
Budapest University of Technology and Economics

With the spreading of network communication first came the need for **security-related functionality** supplying protocols and standards that provide services such as confidentiality or integrity check. Today several such known, widely used, reliable and without deep technical knowledge useable protocols exist. After solving the most important problems with the broadening of their usage new security related needs came besides easy, confidential and authentic communication. In latest time protecting personal data (*privacy*) gets more and more emphasised and this way the highest possible level on **anonymity** as well. To meet these new needs only partial solutions exist. Aim of our work is to plan and specify such a protocol that combines the known successful security methods and basic solutions with the already existing anonymity providing technologies and to define a generally usable, independent anonymity network layer.

Several network communication layers exits that provide security-related functionality. Such is the SSH or SSL known from the Internet, and its successor TLS, or WTLS known from the WAP world. These usually assume client-server communication, during which they provide PKI based key-exchange, encryption, integrity-checking and client/server authentication. We have planned our anonymity-related functionality providing layer to their scheme.

For providing anonymity the two most widely used methods are the blind-signature and the pseudo-identity. The three-sided (bank, client, merchant) **blind-signature** protocol (*DigiCash*) has been originally developed by David Chaum for anonymous payments through the Internet and provides full, non-backtraceable anonymity. Its generalised version can be used in several other scenarios as well (e.g. anonymous voting). The other basic method is the **pseudo-identity**, where the real identity of the subject is protected, however in case of misuse the real identity can be traced back.

Our protocol is based on a network layer that provides reliable data transport and the basic security related functionality (encryption, integrity checking, client and server authentication), since we did not implement these.

For the specification of the protocol we first chose a suitable presentation language. In the next phase with the help of this presentation language we described the possible partners that can appear in the different situations and their actions. Last we have specified the network communication for the several possible cases, for which we have user XML.

The resulting protocol provides solutions to protect service providers against possible misuses and to support the subsequent clearing up.

Besides the theoretical specification we have also implemented the protocol in JAVA over TCP/IP and SSH2. For demonstrational purposes we have chosen some anonymity requiring aspects of the every-day student life.