Abstract

Anonymity Enhancing Protocol (AEP)

With the spreading of network communication first came the need for protocols and standards supplying **security-related** functionality that provide services such as confidentiality, integrity protection or non-repudiation. Today several such protocols exist that are widely known, reliable and usable without deep technical knowledge. After solving the most important problems, the broadening of their usage brought up new security-related needs besides the simple, confidential and authentic communication.

In latest time protecting personal data (**privacy**) and thus the highest possible achievable level of anonymity during network communication are becoming more and more emphasized. To meet these new needs only partial solutions exist. The aim of AEP is to specify a network 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 exist that provide security-related functionality. Such is SSL, TLS or SSH from the world of the Internet, or WTLS known from the WAP world. These usually assume client-server communication, during which they provide PKI based key exchange, encryption, integrity-protection, server side and optionally client side authentication

During the planning of AEP the properties of these layers have been considered. Besides the standardized and easy usage the changeability of the different anonymity methods within AEP have been defined as requirements.

For providing anonymity the two most widely used methods are blind signatures and pseudo-identities. The three-sided (bank, customer, merchant) **blind-signature** protocol has originally been developed by David Chaum for anonymous payments through the Internet (*DigiCash*) and provides non-traceable anonymity. The other basic method is the **pseudo-identity**, where the real identity of the subject is protected, however in case of abuse the real identity can be traced back.

For the specification first a suitable presentation language has been chosen. In the next phase with the help of this presentation language the possible partners and their actions in the different situations have been described. Finally the network communication for the several possible use cases has been specified, for which AEP uses XML.

The resulting protocol provides protection measures against possible abuses and means to recover from an abuse. During the specification a JAVA implementation of the protocol has also been developed, AEP provides anonymity functionality over TCP/IP and SSH2.

AEP provides a **standardized**, **easy-to-use framework** for the realization of different anonymity methods. With its help anonymity functionality can be accessed **without deep technical knowledge**. Like security protocols, it resides in a **separate protocol layer** and provides possibilities for **changing and extending the anonymity methods**.