Abstract

Anonymity Enhancing Protocol (AEP)

Mit der Verbreitung der Netzwerkkommunikation tauchte zuerst der Bedarf an Protokollen und Standards auf, die **sicherheitstechnische** Funktionalitäten wie Vertraulichkeit, Integritätssicherung oder Nichtabstreitbarkeit anbieten. Heutzutage stehen schon zahlreiche solche, gut untersuchte, weitverbreitete, zuverlässige und ohne tieferes technisches Wissen anwendbare Protokolle zur Verfügung. Mit der Verbreitung ihrer Anwendung tauchten nach der Behebung der wichtigsten Probleme (der einfachen, sicheren und authentischen Kommunikation) allerdings neue auf.

In jüngster Zeit gewinnt der **Schutz der Privatsphäre** (*privacy*) und damit verbunden das während der Kommunikation erreichbare höchstmögliche Niveau an Anonymität immer mehr an Bedeutung. Zur Befriedigung dieser neuen Anforderungen stehen nur Teillösungen zur Verfügung. Ziel von AEP ist die Spezifikation eines Protokolls, das die bewährten und bekannten sicherheitstechnischen Verfahren mit den bereits bekannten Anonymitätsverfahren kombiniert und eine allgemein benutzbare, selbständige Anonymitätsschicht definiert.

Es existieren schon zahlreiche Schichten in der Netzwerkkommunikation, die sicherheitstechnische Funktionalitäten anbieten: z. B. SSL, TLS oder SSH aus der Welt der Internet oder WTLS aus der WAP-Welt. Diese setzen eine Client-Server-Architektur voraus, unterstützen einen PKI-basierten Schlüsselaustausch und ermöglichen Vertraulichkeit, Integritätssicherung und Server- bzw. Clientauthentizität zu erreichen.

Bei der Planung von AEP wurden die Eigenschaften dieser Schichten berücksichtigt. Neben der einheitlichen und einfachen Benutzung wurde die Ersetzbarkeit der verschiedenen Anonymitätsverfahren innerhalb des Protokolls als Voraussetzung definiert.

Die zwei bekanntesten Methoden zur Bereitstellung von Anonymität sind die Verfahren der blinden Unterschrift und der Pseudoidentität. Das ursprünglich von David Chaum für anonyme Bezahlungen im Internet (*DigiCash*) entwickelte Protokoll der **blinden Unterschrift** ermöglicht nicht zurückverfolgbare Anonymität. Das andere Grundverfahren wird **Pseudoidentität** genannt. Dabei wird die Identität des Subjekts geschützt, sie kann jedoch im Falle eines Missbrauchs zurückverfolgt werden.

Bei der Spezifikation des Protokolls wurde zuerst die geeignete Präsentationssprache ausgewählt. Danach wurden mit ihrer Hilfe die in den verschiedenen Szenarien auftauchende abstrakten Teilnehmern und ihre Tätigkeiten beschrieben. Schließlich wurde die in den konkreten Fällen ausgetauschten Nachrichten spezifiziert, für die AEP als Kommunikationssprache XML benutzt.

Das so entstandene Protokoll stellt auch verschiedene Möglichkeiten zur Verteidigung gegen die, mit der Anonymität gleichzeitig auftretenden, Missbrauchsmöglichkeiten zur Verfügung. Neben der theoretischen Spezifikation wurde auch eine JAVA-Implementierung des Protokolls bereitgestellt, das die Anonymitätsfunktionalitäten über TCP/IP und SSH2 anbietet.

Das Protokoll stellt eine **einheitliche**, **einfach benutzbare Umgebung** für die Realisierung verschiedener Anonymitätsverfahren zur Verfügung. Mit seiner Hilfe können Anonymitäts-dienste **ohne tiefgehendes technisches Wissen** in Anspruch genommen werden. Ähnlich zu den verschiedenen Sicherheitsprotokollen befindet sich AEP auch in einer **eigenen Protokollschicht** und ermöglich die **Ersetzbarkeit und Erweiterbarkeit der verschiedenen Anonymitätsverfahren**.