Anonymität bereitstellendes Netzwerkprotokoll
(Anonymity Enhancing Protokoll, *AEP*)

Zusammenfassung

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

Lehrstuhl für Messtechnik und Informationssysteme
Technische und Wirtschaftswissenschaftliche Universität Budapest

Mit der Verbreitung der Netzwerkkommunikation tauchte zuerst der Bedarf an Protokolle und Standards auf, die **sicherheitstechnische Funktionalität**, wie *Vertraulichkeit*, *Integritätsschutz* oder *Unleugbarkeit* liefern. Heutzutage stehen zahlreiche solche, gutbekannte, weitverbreitete, zuverlässige und ohne tieferes technisches Wissen anwendbare Protokolle zur Verfügung. Mit der Verbreitung ihrer Anwendung tauchten nach der Abschaffung der wichtigsten Probleme außer der einfachen, sicheren und authentischen Kommunikation neue Anforderungen auf. In jüngster Zeit bekommt der Schutz von persönlichen Daten (*privacy*) und damit das während der Kommunikation erreichbare höchstmögliche Niveau an **Anonymität** immer größere Bedeutung. Zur Befriedigung dieser neuen Anforderungen stehen nur Teillösungen zur Verfügung. Ziel unserer Arbeit ist die Planung und Spezifikation eines solchen Protokolls, das die bewährte und bekannte swicherheitstechnische Verfahren mit der bereits existierenden Anonymitätsmethoden verknüft und eine allgemein benutzbare, selbständige Anonimitätsschicht definiert.

Es existieren zahlreiche Schichten in der Netzwerkkommunikation, die sicherheitstechnische Funktionalität liefern. Eine solche ist das aus der Welt des Internet bekannte SSL, oder sein Nachfolger, das TLS, beziehungsweise das SSH, aber das im WAP benutzte WTLS is auch für solche Zwecke bestimmt. Diese werden meistens in client-server Kommunikation eingesetzt, während dessen sie PKI basierte Schlüsselaustauch, Verschlüsselung, Integritätsschutz und Server beziehungsweise Klientauthentikation bereitstellen. Zu der Schema dieser Schichten haben wir unser Protokoll zur Bereitstellung der Anonimitätsfunktionalität geplant.

Die zwei bekanntesten Methoden zur Sicherung von Anonimtät sind das "blinder Unterschrift" und das "Deckname" Verfahren. Das ursprünglich von David Chaum für anonyme Bezahlung im Internet entwickeltes dreiseitiges (Bank, Kunde, Lieferant**) blinder Unterschrift** Protokoll (*blind signature, DigiCash*) stellt volle, nich zurückverfolgbare Anonymität bereit. Seine verallgemeinerte Version kann auch in vielen anderen Bereichen (wie zum Beispiel anonyme Wahlen) eingesetzt werden. Das andere Grundverfahren trägt den Namen **Deckname** (*pseudo identity*), in dessen Fall die Identität des Subjekts ist geschützt, sie kann jedoch im Falle eines Mißbrauchs zurückverfoglt werden.

Das hier vorgestellte Protokoll baut auf eine Netzwerkschicht, die den sicheren Datentransport und die grund sicherheitstechnische Funktionalität (Verschlüsselung, Intergritätsschutz, Server- und Klientauthentikation) bereitstellt, da wir uns mit deren Imlementierung nicht beschäftigt haben.

Zur Beschreibung des Protokolls haben wir zuerst eine geeignete Presentationssprache gewählt. Danach haben wir mit Hilfe dieser Presentationssprache die in den verschiedenen Fällen möglicherweise auftauchenden abstrakten Kommunikationspartner und deren Tätigkeit beschrieben. Schließlich haben wir die in den konkreten Fällen benutzte Netzwerkkommunikation spezifiziert, zur welchen das Protokoll XML benutzt.

Das so entstandene Protokoll stellt auch Verfahren für die Verteidigung gegen den mit der Anonymität auftauchenden Mißbrauch und dessen nachfolgenden Aufdeckung bereit.

Neben der theoretischen Spezifikation haben wir das Protokoll in JAVA über TCP/IP und SSH2 auch verwirklicht. Zur Veranschaulichung, als demonstrative Anwendung haben wir einige Aspekte des Studentenlebens, die auch Anonimität benötigen, ausgewählt.