sIdentity - Sichere und private Attributübermittlung an Internet-Dienste per Mobiltelefon

Lars Brückner und Marco Voss
IT Transfer Office
Technische Universität Darmstadt
{brueckner, voss}@ito.tu-darmstadt.de

Abstract: Internet-Dienste benötigen verschiedene persönliche Attribute der Benutzer. Dabei geht es nicht nur um die Erbringung des eigentlichen Dienstes, sondern auch um die Erfüllung von rechtlichen Auflagen (z.B. Jugendschutz). Bestehende Ansätze zur Übermittlung persönlicher Attribute sind entweder nicht hinreichend gegen Falschangaben der Benutzer und Identitätsdiebstahl geschützt oder mit hohen Kosten und einer totalen Identifizierung verbunden. In diesem Papier wird ein Protokoll beschrieben, das die GSM-Infrastruktur nutzt, um zertifizierte persönliche Attribute sicher und datenschutzfreundlich an Internet-Dienste zu übermitteln.

1 Einleitung

Viele Internet-Dienste benötigen persönliche Attribute. Darunter verstehen wir z.B. Name, Alter, Geschlecht, Nationalität, Gruppenzugehörigkeiten (z.B. Student) aber auch Pseudonyme, die sich rechtlich zurückverfolgen lassen. Besonders zur Verhinderung von Betrug oder zur Erfüllung gesetzlicher Auflagen (z.B. Jugendschutz) sind die Anbieter auf authentische Attribute angewiesen. Den Sicherheitsinteressen der Betreiber steht der Wunsch vieler Nutzer nach weitgehender Anonymität gegenüber. Die Benutzer sehen Gefahren durch Identitätsdiebstahl, unkontrollierte Weitergabe persönlicher Daten und das intensive Data Mining zu Marketingzwecken. Viele Dienste erheben weit mehr Daten als notwendig und stärken damit nur das Misstrauen.

Die zur Zeit verwendeten Techniken zur Authentifizierung von Attributen setzen einseitig auf die Sicherheitsbedürfnisse der Anbieter und sind zumeist mit einer persönlichen Identifikation des Benutzers verbunden.[1] Der Benutzer muss dabei oft mehr Daten preisgeben als unbedingt nötig, in der Regel durch Vorlage eines amtlichen Ausweises. Angemessene rechtliche Sicherheit wird zudem nur erreicht, wenn der Benutzer persönlich bei der Registrierungsstelle erscheint (z.B. das Post-Ident Verfahren der Deutschen Post). Die Registrierung bedeutet einen erheblichen Zeitaufwand, und die anfallenden Kosten schränken den Anwendungsbereich dieser Verfahren auf wenige Anwendungsgebiete wie Online-Banking ein. Die persönlichen Attribute werden bei der Registrierung überprüft, der Benutzer erhält anschließend Zugangsdaten (Passwort oder digitales Zertifikat), die den Benutzer gegenüber den Diensten ausweisen. Für die sichere Aufbewahrung der Zu-

[1] Einen Überblick zu dieser Thematik und zu verwandten Arbeiten ist in [BV05] zu finden.

gangsdaten ist in der Regel der Benutzer alleine verantwortlich. Die meisten Systeme erlauben es zudem nicht, die Menge der persönlichen Attribute für jede Transaktion anzupassen. So wird z.B. bei jeder Authentifizierung per X.509 Zertifikat das gesamte Zertifikat übermittelt. Zwar existieren Weiterentwicklungen wie *Anonymous Credentials* [CH02], die es erlauben zertifizierte Attribute anonym nachzuweisen. Es ist jedoch zur Zeit nicht absehbar, wie die entsprechenden Infrastrukturen aufgebaut und finanziert werden könnten. Zudem zeigen sich die meisten Benutzer und Anbieter noch durch Technologien wie die digitale Signatur und Public-Key-Verschlüsselung überfordert.

Die in diesem Papier vorgestellte Lösung nutzt den Mobilfunkprovider als dynamische Zertifizierungsinstanz für persönliche Attribute. Ein Mobilfunkprovider verfügt bereits über viele persönliche Daten wie Name, Adresse, Geburtsdatum und Bonität und ist selbst bei der Ausgabe von Pre-Paid-Karten gesetzlich verpflichtet, die Identität des Käufers zu verifizieren. Mit der SIM-Karte verfügt jedes Mobiltelefon über ein personalisiertes Sicherheitsmodul.

Wir stellen ein Protokoll vor, das einem Internet-Dienst Zugriff auf persönliche Attribute eines Benutzers erlaubt. Jeder Zugriff muss vom Benutzer autorisiert werden; außer den benötigten Attributen werden dem Dienst keine weiteren persönlichen Informationen übermittelt. Der Mobilfunkprovider garantiert für deren Richtigkeit. Zwischen Benutzer und Internet-Dienst wird nur eine Einmal-PIN übertragen. Damit ist das Protokoll sehr robust gegen typische Netzwerk-Angriffe. Identitätsdiebstahl ist nur durch Diebstahl des Mobiltelefons und der Zugangs-PIN möglich.

2 sIdentity Protokoll

Abbildung 1 zeigt den Aufbau des Systems. Ein Server des Mobilfunkbetreibers, der *Trust Provider*, bietet den Diensten eine Schnittstelle für Attributsabfragen an. Über die GSM-Infrastruktur hat der Trust Provider einen Kommunikationskanal zum Mobiltelefon des Benutzers. Auf dem Mobiltelefon ist eine spezielle sIdentity-Software installiert. Das Protokoll läuft wie folgt ab:

1. Der Internet-Dienst benötigt ein zertifiziertes Attribut. Er präsentiert dem Benutzer ein Web-Formular mit einer Beschreibung der Anfrage und einem Eingabefeld für eine sIdentity-PIN (sPIN).

2. Der Benutzer aktiviert die sIdentity-Software. Das Mobiltelefon kontaktiert den Trust Provider. Eine neue zufällige sPIN wird erzeugt und vom Trust Provider freigeschaltet. Der Nutzer gibt die sPIN in das Formular ein.

3. Nach dem Empfang der sPIN erzeugt der Dienst eine Attributsabfrage und sendet diese zusammen mit der sPIN an den Trust Provider. Dieser überprüft die Gültigkeit der sPIN. Jede sPIN ist nur für eine bestimmte Zeit gültig und kann nur einmal verwendet werden.

4. Bei einer gültigen sPIN leitet der Trust Provider die Anfrage an das Mobiltelefon

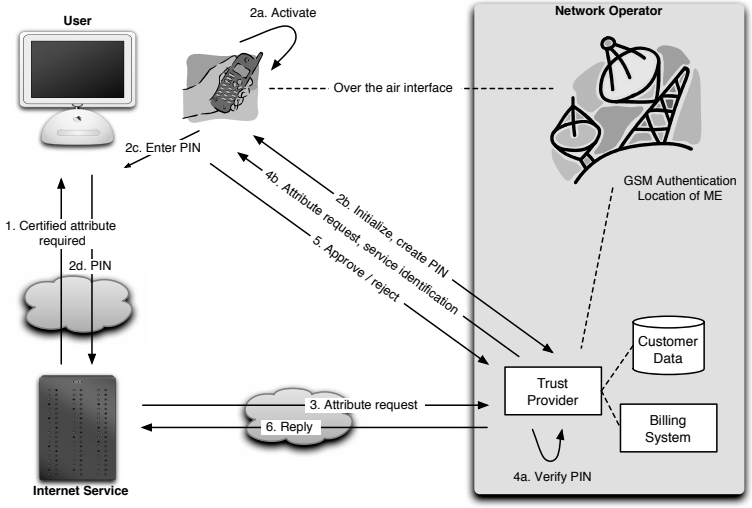

Abbildung 1: sIdentity Overview

weiter. Der Benutzer erhält eine genaue Beschreibung der angefragten Daten und den Namen des Dienstes.

5. Der Benutzer akzeptiert die Anfrage oder weist diese zurück.

6. Bei einer Bestätigung durch den Benutzer liefert der Trust Provider dem Internet-Dienst eine Antwort mit den Daten des Benutzers.

3 Sicherheit und Datenschutz

Als universeller Authentifizierungsdienst muss sIdentity den Konflikt zwischen den Sicherheitsbedürfnissen der Dienste und denjenigen der Benutzer ausgewogen lösen. Wir stellen im folgenden die wesentlichen Sicherheitseigenschaften dar.

Authentizität der Attribute: Mobilfunkanbieter sind in den meisten Ländern gesetzlich dazu verpflichtet, ihre Kunden zuverlässig zu authentifizieren. Im Vergleich zur einfachen Falscheingabe in ein Internet-Formular oder dem Faxen eines fremden Ausweises müsste ein Angreifer hier eine erhebliche kriminelle Energie aufwenden. **Verhinderung von Identitätsdiebstahl**: Für den Diebstahl der Identität ist der Besitz des eingebuchten Mobiltelefons notwendig. Der Verlust des Mobiltelefons wird in der Regel schnell bemerkt. Im Gegensatz dazu bleibt der Diebstahl eines Passwortes unbemerkt. Ein gestohlenes Mobiltelefon kann umgehend geortet und gesperrt werden. Der Täter ist hier meistens im persönlichen Umfeld zu suchen. Eine extra PIN könnte den sIdentity-Dienst zusätzlich schützen. **Minimale Datenübertragung und Kontrolle durch den Nutzer**: Der Benutzer entscheidet, ob Daten übertragen werden oder nicht. Er bekommt auf dem

Mobiltelefon eine genaue Aufstellung der Daten und kann diese mit den Angaben des Dienstes auf der Webseite vergleichen. Das System erlaubt auch unscharfe Anfragen der Form *„ Alter zwischen 18 und 27 Jahre“* anstelle des exakten Geburtsdatums. **Verhinderung von Datendiebstahl durch Dritte**: Ein Angreifer könnte eigene Attributsabfragen an den Trust Provider schicken und hoffen, dass ein Benutzer die Attribute freigibt. Der Angreifer müsste zufällig eine gültige sPIN raten oder abfangen und vor dem legitimen Dienst an den Trust Provider schicken. Weiterhin müsste der Angreifer sicherstellen, dass er nicht vom Trust Provider aus zurückverfolgt werden kann. Auch wenn diese Art von Angriff z.B. durch ein Trojanisches Pferd nicht ausgeschlossen werden kann, bleibt für den Benutzer und den Trust Provider immer noch die Chance, die Fälschung zu bemerken und die Transaktion abzubrechen. **Vertraulichkeit des GSM Providers**: Mobilfunkanbieter verfügen systembedingt über großes Wissen über ihre Kunden. Dementsprechend gibt es für diesen Bereich bereits umfangreiche Datenschutzbestimmungen. Da es sich nur um relativ wenige Anbieter handelt, ist eine Kontrolle durch Behörden und Medien möglich. Um eine Profilbildung durch den Trust Provider zu verhindern, könnte eine anonyme Authentifizierung zwischen Dienst und Trust Provider vorgesehen werden. In diesem Fall wäre der Dienstname nicht mehr Teil der Abfrage. Der Benutzer verliert somit eine wichtige Information.

4 Zusammenfassung

Es wurde ein System vorgestellt, das die vorhandene Mobilfunk-Infrastruktur benutzt, um zertifizierte persönliche Attribute an Internet-Dienste zu übertragen. Gegenüber anderen Lösungen hat dieses System den Vorteil, dass die Infrastruktur durch den Telefonbetrieb bereits finanziert ist. Das Mobiltelefon dient zusätzlich als sicheres Endgerät, über das der Benutzer Attributsanfragen autorisieren kann. Die Menge der übermittelten Attribute lässt sich exakt auf den notwendigen Umfang begrenzen. Durch die Autorisierung jeder einzelnen Transaktion behält der Benutzer eine genaue Kontrolle über die übermittelten Daten. Das Protokoll ist für den Benutzer einfach zu bedienen. Durch die Verwendung von Einmal-PINs ist es sehr robust gegen Angriffe im Netzwerk, insbesondere gegen den PC des Benutzers.

In diesem Papier wurde sIdentity in erster Linie anhand demographischer Daten vorgestellt. Mögliche Erweiterungen sind die Übermittlung der (ungefähren) Position des Mobiltelefons, ein Login-Mechanismus oder die Integration eines Bezahl-Dienstes.

Literatur

[BV05] Lars Brückner und Marco Voss. Projekt Prima Homepage, 2005. http://www.ito.tu-darmstadt.de/projects/prima/sidentity/.

[CH02] Jan Camenisch und Els Van Herreweghen. Design and Implementation of the Idemix Anonymous Credential System, Research Report RZ 3419. Bericht, IBM Research Division, 2002.