Seminar: Smarte Objekte und smarte Umgebungen, SS 2005

Identitätsmanagement

Teil 1: Einführung und die ideale Sicht

Systeme aus der Forschung

Bettina Polasek

Betreuer: Harald Vogt
Prof. Friedemann Mattern

Zusammenfassung

Malcolm Crompton, Australian Privacy Commissioner, beginnt sein Paper über das Thema Identitätsmanagement [1] kritisch mit folgender Behauptung: Grösseres Vertrauen in die Identität von Individuen, speziell im elektronischen Kontext, bezweckt Schutz vor finanziellem, sozialem und wirtschaftlichen Betrug, sowie den Schutz der nationalen Grenzen, grössere nationale Sicherheit und die Möglichkeit, Kunden besser zu kategorisieren, um ihnen gezielter Dienstleistungen und Waren anzubieten. Und weiter auch: Viele von uns könnten sich vorstellen, wie viel angenehmer es wäre, wenn man zum Beispiel weniger PINs, Passwörter und Plastikkarten hätte. Identitätsmanagement scheint also die Lösung aller Probleme in der elektronischen Welt zu sein, Firmen sollen vor Betrug geschützt werden, Personen soll die Identifikation leichter fallen. Hinter dem Begriff Identitätsmanagement versteckt sich aber noch viel mehr. Es geht um eine umfassende Unterstützung der Internet-Benutzer in Belangen der Sicherheit, Privatsphäre und Authentifizierung.

1 Einleitung

1.1 Was ist Identitätsmanagement?

Aus der Sicht der Forschung sollte bei Identitätsmanagement das Individuum ganz klar im Mittelpunkt stehen. Der Identitätsmanager sollte die Person unterstützen, die im Internet mit verschiedenen Instanzen interagieren möchte. Zum Beispiel möchte die Person ihre Steuererklärung den Behörden einreichen. Bei dieser Interaktion zwischen Mensch und Staat steht klar das Ziel der Authentizität im Vordergrund: Beide Seiten müssen sich der gegenseitigen Identität versichern. Auf der anderen Seite kann eine Interaktion mit der Wirtschaft ein anderes Ziel verfolgen. Wenn eine Person online ein Kinoticket kaufen will, dann spielt die Authentizität keine grosse Rolle, dafür wird Anonymität ein wichtiger Aspekt. Die Käuferin will sichergehen, dass die Ticketfirma keine unnötigen Daten von ihr erfährt oder sogar speichert. Um solche Schutzziele zu erreichen, soll ein Identitätsmanagementsystem eingesetzt werden, welches den Benutzer bei solchen Interaktionen unterstützt. Um dies zu erreichen, müssen verschiedene Grundsätze eingehalten werden.

1.2 Grundsatz 1: Pseudonyme, Teilidentitäten

In unserem täglichen Leben sehen wir uns oft in verschiedenen Rollen, einmal sind wir Mutter, dann Managerin einer Firma, dann wieder Freundin. Mit diesen Rollen sind immer unterschiedliche Informationen unserer Identität verbunden, was zu der Bezeichnung einer Teilidentität führt. Zu einer Teilidentität gehören verschiedene Merkmale. In Abbildung 1 sehen wir eine Skizze solcher Teilidentitäten. Wir haben zum Beispiel die Teilidentität im Internet-Forum, in der keine Information zum wirklichen Namen enthalten ist, aber zum Beispiel zum Studiengang, weil dieser relevant für Beiträge im Forum ist. Weiter haben wir eine gewissen Bank-Identität. Die Bank kennt unsere persönlichen Daten und unser Einkommen. Bei Freunden hingegen gibt es keine Information zu Einkommen, dafür aber

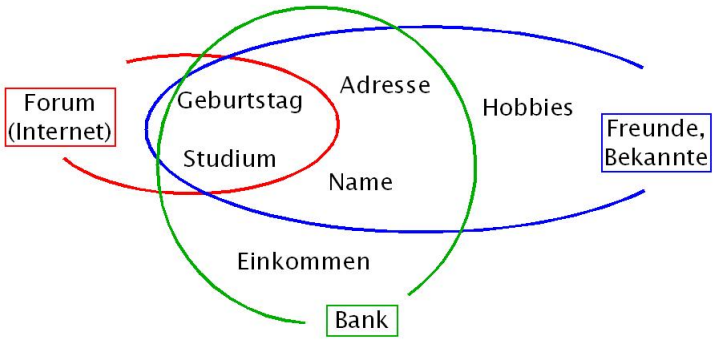

Abbildung 1: Teilidentitäten, Pseudonyme

zu Hobbies. Solche Teilidentitäten sind in der realen Welt vor allem intuitiv gegeben und wir möchten diese Idee nun in einen Internet-Kontext übersetzen. Mit jeder dieser Teilidentitäten verknüpfen wir ein Pseudonym, welches genau diese Informationen beinhaltet. Diese Pseudonyme können wir dann online verwenden, je nach Situation in der wir uns gerade befinden. Ein Identitätsmanagementsystem sollte und bei der Verwaltung solcher Pseudonyme unterstützen.

1.3 Grundsatz 2: Authentizität, Anonymität

Authentizität und Anonymität scheinen auf den ersten Blick nichts miteinander zu tun zu haben. Authentizität einerseits verlangt nach einer Bestätigung einer Identität, Anonymität hingegen möchte genau diese Information zur Identität schützen. In einem Identitätsmanagementsystem sollten aber auch beide Ziele gleichzeitig erreichbar sein. Die Idee dahinter ist, dass wir nicht eine Identität im Sinne von Personeninformation bestätigen wollen, sondern gewisse Eigenschaften, die auch Authentizität verlangen. Ein Beispiel dafür wäre, wenn eine Person von einer Autovermietungsfirma ein Auto mieten möchte. Die Firma muss im Prinzip nichts über ihre Identität wissen, sondern nur Bescheid wissen, dass sie einen gültigen Fahrausweis besitzt und somit berechtigt ist, Auto zu fahren. Eine Möglichkeit, so eine Interaktion zu realisieren, läuft über so genannte Trusted Third Parties (TTP). Der Kunde kann offline bei einer TTP seinen Führerschein vorzeigen, dieser wird überprüft, und online kann sich der Kunde ein Pseudonym ausstellen lassen, welches den Besitz des Führerscheins bestätigt. In diesem Fall kennt die TTP mehr Informationen über den Kunden, was im Falle eines Unfalls von Nutzen sein kann, weil dann der die Autovermietungsfirma weitere nötige Angaben zu der Person erhält. Ein Identitätsmanagementsystem

sollte den Benutzer dabei unterstützen, ihn gegebenenfalls zu authentifizieren, ohne dabei seine Anonymität aufzugeben

1.4 Grundsatz 3: Privatheit, Vertrauen

In einem elektronischen Kontext haben wir ein anderes Verständnis von Vertrauen als in der realen Welt. Wir wollen nicht nur dem Kommunikationspartner vertrauen, sondern auch dem Kommunikationskanal. Vertrauen in Kommunikationspartner schaffen zum Beispiel Privacy Policies. Diese versichern dem Kunden Datenschutz und Daten-Integrität. Weiter muss online auch etwas wie eine Vertragszeichnung stattfinden können, bei der beide Seiten signieren und so eine Vereinbarung treffen. Ein Identitätsmanager sollte mich unterstützen beim Verstehen solcher Privacy Policies, beim Unterzeichnen solcher digitalen Verträge und auch beim Schützen meines Kommunikationskanals.

1.5 Grundsatz 4: Benutzer-Kontrolle

Da ein Identitätsmanagementsystem klar auf die Benutzerunterstützung fokussiert, sollte der Benutzer auch so viel Kontrolle wie möglich erhalten. Der Identitätsmanager sollte dem Benutzer einen Überblick über seine Pseudonyme, seine persönliche Daten und über die Kommunikation, die er führt, schaffen. Weiter sollte das System sinnvolle Warnungen und Hinweise bei Verletzung gewisser Schutzziele geben, da das System nicht für den Benutzer entscheiden, aber ihn bei kritischen Situationen aufmerksam machen, soll. Solche Systeme können in einem breitem Umfeld erst dann eingesetzt werden, wenn auch Bedienung und Konfiguration sehr einfach und intuitiv gehalten wird. Gute Standardeinstellungen sind eine wichtige Grundlage, damit der Benutzer nicht mit unverständlichen Konfigurationsschritten überfordert wird. Ein schlechtes Beispiel hier sind zum Beispiel die Sicherheitseinstellungen, die bei gewissen Internet-Browsern vorgenommen werden können. Die Anzahl Fremdwörter und Einstellungsmöglichkeiten übertrifft das Verständnis eines durchschnittlichen Internet-Surfers. Der Benutzer soll sich von dem Identitätsmanagementsystem unterstützt fühlen und nicht überfordert.

1.6 Weitere Anforderungen

Neben diesen vier Grundsätzen sind auch weitere Anforderungen an ein solches System vorhanden. Ein Identitätsmanagementsystem sollte der Benutzerin immer beiseite stehen. Um das zu realisieren, ist ein hoher Grad an Mobilität und Verfügbarkeit notwendig. Wenn die Benutzerin in einem Internet-Café online einkaufen möchte, dann sollte auch dort ihr Identitätsmanager verfügbar sein.
Absolute Benutzer-Kontrolle steht in einem gewissen Gegensatz zu der Benutzerfreundlichkeit. Die Kundin möchte in erster Linie ein Produkt online erwerben, und möchte sich dabei eigentlich nicht um Sicherheits- oder Privatheitsaspekte kümmern. Darum besteht hier ein Trade-Off zwischen absoluter Kontrolle der Benutzer und Anwendbarkeit. Die Benutzerin sollte nur notwendige Konfigurationen vornehmen müssen, gewissen Grundeinstellungen

sollten unbedingt vorhanden sein.
Ein Identitätsmanagementsystem verlangt das Vertrauen der Benutzer, darum soll ein solches System auch verlässlich sein. Systeme, die anonymes Surfen anbieten, aber dies nicht wirklich technisch tun, sind sinnlos und auch unbrauchbar.
Um Dienste, wie das überprüfen von Privacy Policies, zu ermöglichen, müssen Standards definiert werden, die maschinenlesbarkeit ermöglichen. Ein solcher Standard ist P3P (Platform for Privacy Preferences Project), der ein XML-Format für die Spezifikation von Privacy Policies definiert. Solche Standards müssen einerseits definiert und eingehalten werden, andererseits müssen sie auch eine gewissen Rechtsverbindlichkeit besitzen.

2 Zwei Systeme aus der Forschung

Folgend sollen nun zwei Systeme der Forschung vorgestellt werden, die die Grundsätze des Identitätsmanagements implementieren sollen.

2.1 ATUS A Toolkit for Usable Security

ATUS ist ein System der Albert-Ludwigs-Universität Freiburg und wurde am Institut für Informatik und Gesellschaft entwickelt [8]. Die Entwickler beschreiben ihr System kurzgefasst so: *The iManager. It supports the user to obtain the desired security and to control his/her personal data.*

Abbildung 2: ATUS Identitätsmanager

Abbildung 3: Übersicht der Pseudonyme und im speziellen die Bank-ID

2.1.1 Design von ATUS

Im Beispiel sehen wir das System auf einem PDA angewendet. Der iManager verfolgt einen sehr Benutzer-orientierten Ansatz. Der Identitätsmanager soll den Benutzer bei der Verwaltung seiner verschiedenen Pseudonyme unterstützen. Das aktuell verwendete Pseudonym ist unten in der Leiste immer angezeigt, wie in Abbildung 2 ersichtlich ist. In Abbildung 3 sehen wir die Übersicht, die der Benutzer über seine Teilidentitäten hat. Als Beispiel sehen wir in Abbildung 3 die Bank-ID und wie man die verbunden Daten mit dieser Identität bestimmen kann. Die Darstellung und der Umgang mittels an- oder abkreuzen scheint sehr intuitiv und erfüllt den Grundsatz der Benutzer-Kontrolle. In Abbildung 4 sehen wir die Interaktion des iManagers mit dem Benutzer. Im Beispiel hat die Applikation E-Ticket, die es ermöglicht, online Zugbillettes zu kaufen, gewisse persönliche Daten angefordert, die in der momentan genutzten Identität Anonym-ID nicht freigegeben sind. Der Benutzer erhält nun also die Warnung des Systems, dass die verwendete Applikation mehr persönliche Daten anfordert. Der Benutzer kann jetzt mögliche Massnahmen zur Lösung des Konflikts ergreifen. Er kann zu einer passenden Teilidentität wechseln, eine neue erstellen oder einfach die Anfrage zurückweisen. Der iManager versucht also, den Benutzer aufmerksam zu machen und unterstützt so unter anderem den Grundsatz der Anonymität.

2.1.2 Funktionalität von ATUS

Der Identitätsmanager von ATUS agiert als eine Art Firewall zwischen Netzwerk und Applikation. Er bietet den verschiedenen Applikationen ein Netzwerk-Inferface an und stellt so Sockets für die Internet-Verbindung zur Verfügung. So soll der iManager auch

Abbildung 4: Warnungen des Identitätsmanagers

für alle verschiedenen Applikationen, wie email, www,etc., verwendbar sein. Generische Sicherheitsmechanismen, wie kryptographische Protkolle und digitale Unterschriften, sind als Plug-Ins eingebunden. Die Hauptfunktionalität des iManagers liegt aber im Filtern der ein- und vor allem ausgehenden Daten. Der Filter soll erkennen, welche Daten zum Beispiel von einem HTML-Formular verlangt werden, dieses dann gegenenfalls schon ausfüllen, oder den Benutzer warnen, wenn mehr Daten als freigegeben verlangt werden. Weiter gibt es verschiedene Datenbanken, wobei eine für so genannte Rules verwendet wird. Hier werden vom Benutzer spezifizierte Privatheits- und Sicherheitswünsche gespeichert und können dann so beim Filtern überprüft werden.

2.2 DRiM Dresden Identity Management

DRiM ist ein System der Technischen Universität Dresden und wurde an der Fakultät fr Informatik entwickelt [7]. Die Entwickler beschreiben ihr System wiederum kurzgefasst so: *Im Projekt DRiM werden Grundlagen, Techniken und Einsatzszenarien für ein datenschutzgerechtes Identitätsmanagement erforscht.*

2.2.1 Funktionalität von DRiM

DRiM ist nicht ein alleinstehender Identitätsmanager, sondern ein ganzes Applikations-Paket mit Sicherheitsfunktionalität. Wichtige Grundlage dabei bildet das SSONET (Sicherheit und Schutz in offenen Datennetzen), welches eine Java-Bibliothek zum Aufbauen mehrseitig sicherer TCP-IP-Verbindungen ist. Alle Applikationen, die das Identitätsmanagement nutzen möchten, müssen auf diesem API aufbauen, was wiederum heisst, dass alle

Beteiligten einer Interaktion DRiM unterstützen müssen. SSONET übernimmt auch die Verhandlung von der Sicherheitskonfiguration einer Verbindung. Weiter ist an das SSONET eine Applikation angebunden, die anonymes Surfen erlaubt, d.h. die IP-Adresse anonymisiert. Der IDMAN übernimmt dann die für den Identitätsmangager typische Aufgabe der Pseudonym-Verwaltung, dabei können hier Dauer der Gültigkeit des Pseudonyms sowie der Anonymitätsgrad festgelegt werden. Pseudonyme sind immer verbunden mit einer digitalen Signatur. Weiter bietet dieses Paket noch einen Identitätstreuhänder, eine so genannte public key infrastucture (PKI), an. Dieser soll das Vorgehen mit einer TTP simulieren. Die Benutzerin kann sich offline registrieren lassen, und dann online Zertifikate für bestimmen Pseudonyme ausstellen lassen.

2.3 Vergleich der zwei Systeme

Beide Systeme sind auf den vier Grundsätzen aufgebaut. Es handelt sich bei beiden noch klar um Prototypen, wo zwar viele Idee vorhanden, aber noch nicht implementiert sind. Es gibt einen wesentlichen Unterschied in den Grundideen der Implementation bei den zwei Systemen: Während ATUS eine Art extended firewall anbieten, fokussiert sich DRiM auf ein ganzes application framework. Die Idee von ATUS einfach Daten zu filtern scheint auch etwas mutig, da es hier zu grossen Fehlern führen könnte. Bei DRiM kann durch den Ansatz, ein ganzes Paket anzubieten, wirklich der Identitätsmanager die Grundlage der ganzen Applikationen bilden und so auch gezielt eingesetzt werden.

3 Probleme von Identitätsmanagementsystemen

Ein Identitätsmanager sollte klar nicht als ein "eine Nummer pro Person"-System verstanden werden, da dies ein allzu leichtes Zusammenführen der Daten ermöglicht. Identitätsmanagement sollte vielmehr dazu führen, Anonymität sicherzustellen. Problem eines solchen Systems kann zum Beispiel die Sicherheit der Daten sein. Da das System über viele sehr wertvolle Daten verfügt, wird es automatisch zum attraktiven Ziel von Attacken. Weiter muss geklärt sein, wer solche Systeme anbietet. Es müssen vertrauensvolle Institutionen sein, wie zum Beispiel der Staat, die hinter solchen Systemen stehen. Sonst können Benutzer eventuell das Vertrauen in ihr eigenes System verlieren. Wenn wir weiter irgendwann in ein Stadium kommen, wo wir ohne Identitätsmanager nicht mehr sein können, besteht hier eine grosses Abhängigkeitpotenzial, das sich auch ins Negative auswirken könnte.

4 Schlussfolgerungen

Zusammenfassend kann gesagt werden, dass Identitätsmanagement ein grosses Thema in naher Zukunft sein wird. Vielleicht haben wir uns gestern noch nicht so viele Gedanken um unsere verschiedenen Identitäten gemacht, aber heute im Umgang mit der online-Welt kommt dieses Bedürfnis immer mehr und wir brauchen gute Systeme, die uns dabei unterstützen. Morgen wird Identitätsmanagement eine noch grössere Herausforderung sein,

da wir womöglich keinen klaren Wechsel mehr haben zwischen digitaler und realer Welt. Dann müssen solche Systeme noch weitere Grundfunktionen, wie zum Beispiel Kontexterkennung, unterstützen. Weiter kann man sich fragen, was dann überhaupt noch Begriffe wie Vertrauen bedeuten, wenn wir mit Alltagsgegenständen kommunizieren. Die Forschung auf diesem Gebiet wird noch grosse Schritte machen müssen, um die auf uns zukommenden Problemen effizient zu lösen.

Literatur

[1] Malcolm Crompton **Proof of ID Required? Getting Identity Management Right.** Australian IT Security Forum, 2004

[2] Sven Wohlgemuth, Uwe Jendricke, Daniela Gerd tom Markotten, Felix Dorner, Günter Müller **Sicherheit und Benutzbarkeit durch Identitätsmanagement.** Aktuelle Trends in der Softwareforschung - Tagungsband zum doIT Software-Forschungstag 2003, 2004

[3] Ernesto Damiani, Sabrine De Capitani di Vimercati, Pierangela Samarati **Managing Multiple and Dependable Identities.** IEEE Internet Computing, 2003

[4] Sebastian Clauss, Marit Köhntopp **Identity management and its support of multilateral security.** Computer Networks, 2001

[5] Uwe Jendricke, Daniela Gerd tom Markotten **Usability meets Security - The Identity-Manger as your Personal Security Assistant for the Internet.** Proceedings of the 16th Annual Computer Security Applications Conference, 2000

[6] Uwe Jendricke, Michael Kreutzer, Als Zugenmaier **Pervasive Privacy with Identity Management** Workshop Security, Göteborg, Sweden, Ubicomp, 2002

[7] URL: http://drim.inf.tu-dresden.de/index.de.html

[8] URL: http://www.iig.uni-freiburg.de/telematik/atus/