M. Herczeg, W. Prinz, H. Oberquelle (Hrsg.): Mensch & Computer 2002: Vom interaktiven Werkzeug zu kooperativen Arbeits- und Lernwelten. Stuttgart: B. G. Teubner, 2002, S. 395-396.

Privatheit bei Verwaltung von Benutzerprofilen

Wolfgang Wörndl, Michael Koch
Technische Universität München, Fakultät für Informatik

1 Motivation und Problemstellung

Die weltweite Vernetzung von Informations-Quellen führt u.a. dazu, dass Benutzer Probleme haben, in der Fülle von Information die für sie wichtige und relevante herauszufinden. Ein erfolgversprechendes Konzept ist hier die Personalisierung von Informationsangeboten. Entsprechend gibt es mittlerweile viele Systeme, die Benutzerdaten wie Interessensgebiete oder getätigte Transaktionen sammeln und versuchen, aus diesen *Benutzerprofilen* persönliche Web-Seiten oder Empfehlungen abzuleiten.

Das Problem bei der bisherigen Anwendung von Personalisierung ist, dass die Benutzerprofile an unterschiedlichen Stellen erfasst und gespeichert werden, und Benutzer somit wenig Kontrolle und Übersicht haben, welche Daten wo, wie und von wem verwaltet werden. Weiterhin ist, auch wenn der Benutzer dies wollte, nicht immer alle im Netz verfügbare Information zu einem Benutzer zugänglich. Der Umstand, dass jeder Dienst neu mit der Informationssammlung beginnt, führt zum sogenannten Kaltstartproblem bei Personalisierungsdiensten. Eine mögliche Lösung für die Probleme wäre, die Benutzerprofile gesammelt in Benutzerprofilagenten unter der Kontrolle des Benutzers zu speichern, so dass die gleiche Benutzerinformation für verschiedene Personalisierungsdienste verwendet werden kann.

Benutzer wollen allerdings nicht alle Informationen im Profil für jeden Dienst zur Verfügung stellen. Die *Privatheit* (engl. *privacy*) der Benutzer bzw. Benutzerprofile muss gewährleistet werden. Für das *Identitätsmanagement* im Internet (Koch & Wörndl 2001; Köhntopp & Bertold 2000) nach obigem Beispiel braucht mal also einen Mechanismus zur Kontrolle von Zugriffen auf die Benutzerprofilinformationen. Wichtig dabei ist eine Modellierung von Aspekten, die bei der Verwaltung von Benutzerprofilen wichtig sind, wie z.B. der Zweck eines Zugriffs oder die Erlaubnis zur Weitergabe von Informationen.

2 Lösungsansätze

Im Projekt IMC/Cobricks (http://www11.in.tum.de/proj/cobricks/) werden Ansätze zur anwendungsübergreifenden Nutzung und Verwaltung von Benutzerprofilen (Identitätsmanagement) und zur Personalisierung im Community-Unterstützungsbereich verfolgt (Koch 2000). Es geht also um Anwendungen, welche eine Gruppe von Benutzern bei der Kommunikation untereinander und beim Informationsaustausch unterstützen (sogenannte Community-Unterstützungssysteme). Community-Unterstützungssysteme verwalten dabei Mitgliederlisten und Beiträge von Mitgliedern und stellen Dienste wie Empfehlungsgenerierung

bereit. Dieses Poster beschreibt ein Teilprojekt von Cobricks, in dem es um die Untersuchung und Bereitstellung von Privatheit in diesem Szenario geht.

Der Benutzerprofilzugriff besteht dabei aus zwei Phasen, zunächst einer Aushandlung von Zugriffsrechten, wobei Benutzerinteraktion erforderlich sein kann, und dann dem (effizienten) Zugriff auf die Benutzerdaten. Die Aushandlung der Zugriffsrechte basiert auf dem Platform for Privacy Preferences Projekt (P3P) des World Wide Web Consortium (W3C). Ziel dieses Projektes ist es, Datenschutzerklärungen (Privacy Policies) von Web-Servern zu standardisieren und diese maschinen-lesbar abzulegen. Zum Beispiel soll eine Community-Plattform festlegen können, ob die Interessen eines Benutzers explizit anderen Mitgliedern der Community zugänglich gemacht werden oder nicht. Ein Benutzerprofilagent kann dann aus den Präferenzen des Benutzers ableiten, ob in diesem Kontext der Zugriff auf Benutzerinteressen im Profil erlaubt wird oder nicht. Das Ergebnis dieser Aushandlung zwischen Benutzer- und Community-Agent in Phase 1 ist ein *Access Ticket* mit dem dann in Phase 2 der eigentliche Datenzugriff erfolgt. Das Access Ticket ist ein digital signiertes XML Dokument, das die Zugriffsrechte einer Community-Plattform auf die angeforderten Benutzerprofildaten spezifiziert. Die traditionelle Menge von Zugriffsrechten wird dabei erweitert, z.B. um „Read Once“ (einmaliges Leserecht) oder „Read & Distribute“ (Weitergabe der Information erlaubt). Das Access Ticket dient auch der Transparenz für den Benutzer und enthält u.a. ein verpflichtendes Element für den Zwecks jeden Zugriffs.

Ein wichtiger Punkt beim Identitätsmanagement und Teil der Aushandlung der Zugriffsrechte ist auch die Verwaltung mehrerer Identitäten (z.B. beruflich und privat). Benutzer können Identitäten mit zum Teil gleichen und zum Teil unterschiedlichen Profilinformationen und Zugriffsrechten handhaben und ggf. auch anonymisiert kommunizieren. Weiterhin ist eine Untersuchung der Abbildung des Zugriffskontrollsystem in geeignete Benutzerschnittstellen Teil des Projektes. Auch ist eine Erklärungskomponente nötig, die es Benutzern jederzeit erlaubt, den Zugriff auf Profildaten nachvollziehen zu können, und überprüfen zu können, welche Informationen an welche Community herausgegeben wurde.

Literaturreferenzen

Koch, M.; Wörndl, W. (2001): Community Support and Identity Management. In: *Proc. Europ. Conference on Computer-Supported Cooperative Work (ECSCW2001).* Bonn, S. 319 – 338.

Koch, M. (2000): Cobricks – Eine agentenbasierte Infrastruktur für Community-Anwendungen. In: Reichwald, R.; Schlichter, J. (Hrsg.): *Proc. D-CSCW 2000*. Stuttgart u.a.: Teubner. S. 265 - 266.

Köhntopp, M.; Bertold, O. (2000): Identity Management Based on P3P. In: *Proc. Workshop on Design Issues in Anonymity and Unobservability.* Berkeley, CA.

Kontaktinformation

Wolfgang Wörndl, Michael Koch
Technische Universität München, Fakultät für Informatik
Lehrstuhl für Angewandte Informatik / Kooperative Systeme
Arcisstr. 21
D-80290 München

Email: {woerndl,kochm}@informatik.tu-muenchen.de