von Kai Rannenberg, Christian Kahl und Katja Böttcher

Communities, Mobilität und Datenschutz

Innovative Konzepte zum Schutz der Privatsphäre im Projekt PICOS

Plattformen für Social Communities im Internet, wie Facebook, StudiVZ und XING, haben in den vergangenen Jahren rasant an Popularität gewonnen. Auf ihnen versammeln sich bereits heute Millionen von Nutzern weltweit. Sie verbinden sich über virtuelle Freundeslisten und tauschen sich über gemeinsame Interessen und Aktivitäten aus. Immer häufiger werden dazu auch mobile Endgeräte wie Handys verwendet, erlauben diese doch ständig in Kontakt mit der Community zu bleiben. Allerdings wollen viele Nutzer längst nicht jedem Mitglied einer Community alles preisgeben. Doch wie lässt sich die Privatsphäre in solchen Communities besser schützen? Dieser Frage geht das Forschungsprojekt PICOS nach.

Neben dem eigenen Profil, mit dem Nutzer sich durch die Angabe verschiedener Informationen beschreiben können, bieten Social Communities, die auch als Social Networks oder Soziale Netzwerke bezeichnet werden, vielfältige Kommunikationsmöglichkeiten – etwa um Nachrichten zu verschicken, mit anderen Nutzern zu chatten oder Kommentare auf deren Profilseiten zu hinterlassen. Auf diese Weise werden bestehende Beziehungen aus der Offline-Welt gepflegt, aber auch neue Kontakte geknüpft, sei es im privaten oder im beruflichen Umfeld. Communities vereinen damit viele bekannte Kommunikationsmöglichkeiten, wie E-Mail oder Instant Messenger (zum Beispiel ICQ, MSN Live Messenger), in sich.

Gleichzeitig bergen Communities aber auch Risiken für ihre Nutzer und bringen neue Herausforderungen mit sich. Insbesondere werden in Communities viele persönliche Daten preisgegeben, um sie mit Freunden innerhalb der Community zu teilen – angefangen von Name, Alter oder Wohnort über persönliche Interessen bis hin zu privaten Urlaubsfotos oder Videos, die Nutzer auf ihrer Profilseite bereitstellen können. Allerdings sind Freundschaften auch in Communities, ähnlich wie im realen Leben, nicht immer gleicher Art. So kann die virtuelle Freundesliste neben guten Freunden auch Bekannte, Nachbarn oder Arbeitskollegen beinhalten. Und nun mag man als einzelner Nutzer zwar seinen Namen oder seinen Wohnort mit all seinen virtuellen »Freunden« teilen, Informationen über den persönlichen Filmgeschmack oder die Fotos des letzten Urlaubs möchte man aber vielleicht nicht jedem zugänglich machen, zu dem man Kontakt hat.

Die meisten existierenden Communities bieten bislang nur wenige Möglichkeiten, den Zugriff auf die persönlichen Daten und Inhalte je nach Situation zu managen und bestimmte Bereiche nur für ausgewählte Nutzer zugänglich zu machen. Vor allem aber fehlen ganzheitliche Ansätze, die den Schutz persönlicher Daten und der Privatsphäre der Nutzer von Grund auf in Communities integrieren und dabei die gesamte Breite der gebotenen Kommunikationsfunktionen berücksichtigen.

Neue Interaktionsfelder mit mobilen Endgeräten

Nutzer in Communities verwenden zunehmend mobile Endgeräte wie Handys. Damit bieten sich für die Anbieter und Nutzer der Communities zusätzliche Möglichkeiten sowie neue Funktionen zur Kommuni-

kation und Interaktion. Durch die Nutzung von Orts- und Kontextinformationen lässt sich beispielsweise auf einer Karte anzeigen, welche Freunde mit ähnlichen Interessen sich in der Nähe befinden und an einem spontanen Treffen interessiert sein könnten.

Diese technischen Möglichkeiten bieten auch zusätzliche Chancen für Anbieter kommerzieller Dienste und Werbetreibende. So können potenzielle Kunden mit Werbung und Empfehlungen für Produkte oder Dienstleistungen, etwa Regenschirme oder Restaurants, erreicht werden, während diese noch unterwegs und zum Beispiel gerade in der Nähe des werbenden Geschäftes sind. Damit verknüpfen sich die Online-Welt und die reale Welt. Gleichzeitig kann diese Art von Werbung – ähnlich den Geschäftsmodellen von Google, Anzeigenblättern oder Vereinszeitschriften – eine entscheidende finanzielle Grundlage für den Betrieb von Communities werden, der ja mit Kosten verbunden und gegenwärtig oft nur über Anschubfinanzierungen gesichert ist.

Vor diesem Hintergrund arbeitet das Projekt PICOS, das 2008 mit Fördermitteln der europäischen Union gestartet wurde, daran, wie Datenschutz und Privatsphäre in Social Communities verbessert werden können, insbesondere in Social Communities, die auf mobile Nutzung ausgelegt sind [siehe auch »Fakten zu PICOS«, Seite 44]. Ziel von PICOS ist es vor allem, den Nutzern von Communities Möglichkeiten zu geben, ihre Privatsphäre und ihre persönlichen Daten besser zu schützen, als das bislang möglich ist. Da dies aber nicht allein durch technische Konzepte realisierbar ist, werden ebenso ökonomische, soziale und rechtliche Aspekte miteinbezogen. Nicht zuletzt aufgrund dieser Vielschichtigkeit geht es auch darum, Aufmerksamkeit auf das Thema zu lenken und für die damit verbundene Problematik zu sensibilisieren.

Mobil und flexibel: Kooperieren in wechselnden Konstellationen

Im Mittelpunkt der Forschungsarbeit stehen die Nutzer und ihre Interessen. Als beispielhafte Nutzergruppe haben wir zunächst Freizeitangler in das Projekt einbezogen: Sie sind in hohem Maße auf Mobilität angewiesen und nutzen bereits heute zunehmend spezielle Communities und Foren im Internet und über mobile Endgeräte, um sich auszutauschen, gemeinsame Aktivitäten zu planen und zuweilen auch Angelplätze zu empfehlen.

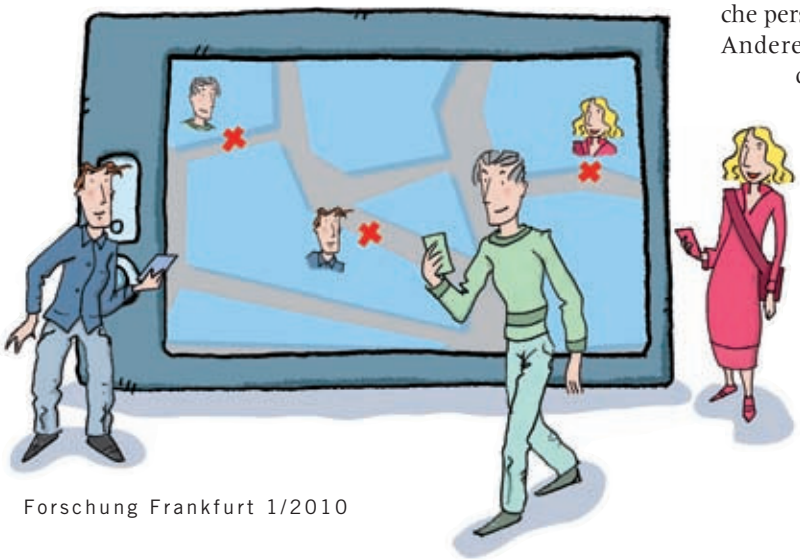
Angler müssen mobil sein und flexibel auf veränderte Umwelteinflüsse (etwa das Wetter) reagieren, wenn sie erfolgreich sein wollen. Beim Warten darauf, dass ein Fisch anbeißt, ist Austausch mit anderen Anglern willkommen, gegebenenfalls auch Besuch an der Angelstelle. Hängt dann ein prächtiger Fisch am Haken, geben Angler dies gern kund – am besten per Foto über Handys oder andere mobile Endgeräte.

Was sie aber nicht wollen ist, dass dann zu viele andere Leute kommen und die endlich anbeißenden Fische vertreiben. Analogien zu den in der Informationsgesellschaft immer häufiger vertretenen »Knowledge Workers« sind offensichtlich: Zu ihren Arbeitsinhalten gehört es, komplexe Informationen in verschiedenen Kontexten zu managen und in wechselnden Konstellationen zu kooperieren.

Partielle Identitäten und »Privacy Policies«

Daher wurde in PICOS in einem ersten wesentlichen Schritt zunächst erhoben, welche Anforderungen von Community-Nutzern an Datenschutz und Privatsphäre gestellt werden. Um die ermittelten Anforderungen verallgemeinern zu können, wurden neben den Anglern auch zwei weitere Communities befragt: Zum einen eine Community aus dem Online-Computer-Spiele-Bereich und zum anderen eine Community selbstständiger Taxifahrer. Die Gruppen haben dabei zum Teil unterschiedliche, aber auch durchaus ähnliche Anforderungen, wie sich in unseren Untersuchungen gezeigt hat. So sind Angler beispielsweise sehr daran interessiert, sich mit bestehenden Kontakten aus der realen Welt auszutauschen, etwa in Form der Bilder vom letzten Angel-Trip. Sie wollen aber eben nicht alle dieser Informationen an jeden weitergeben. Online-Spieler hingegen haben ein Interesse daran, andere Spieler kennenzulernen und sind dabei generell etwas offener im Umgang mit ihren Daten.

Ziel ist es, den Nutzern Werkzeuge an die Hand zu geben, um auf einfache Art und Weise ihre Privatsphäre zu schützen. Eines dieser Konzepte sind die sogenannten »partiellen Identitäten«. Damit kann ein Nutzer verschiedene Pseudonyme anlegen, mit denen er in einer Community auftritt. Zu jedem Pseudonym gehört ein Profil, dem der Nutzer unterschiedliche persönliche Daten von sich mitteilen kann. Andere Nutzer können dadurch immer nur den Teil der Informationen sehen, den der Nutzer unter diesem Profil zugänglich gemacht hat. So kann ein Nutzer etwa zwei unterschiedliche Identitäten für Privatleben und Beruf anlegen und privaten Freunden beispielsweise die letzten Urlaubsfotos bereitstellen, ohne dass Arbeitskollegen den Zusammenhang erkennen. Theoretisch ist das einfach, aber praktisch durchaus anspruchsvoll, speziell, wenn man öfter die Rolle



Fakten zu PICOS

PICOS steht für »Privacy and Identity Management for Community Services«. Das 2008 gestartete Forschungsprojekt mit einer Gesamtdauer von 36 Monaten und einem Volumen von knapp sechs Millionen Euro wird von der Europäischen Union gefördert.

Koordiniert wird das Projekt von Prof. Dr. Kai Rannenberg und einem Team der Professur für Mobile Business & Multilateral Security an der Goethe-Universität. Zu den insgesamt elf beteiligten europäischen Partnern gehören darüber hinaus: Hewlett-Packard Laboratories Bristol (UK), Hewlett-Packard Centre de Competence France (Frankreich), Universidad de Málaga (Spanien), Center for Usability Research & Engineering (Österreich), Katholieke Universiteit Leuven – Interdisciplinary Centre for Law and ICT (Belgien), IT-Objects GmbH (Deutschland), Atos Origin (Spanien), Deutsche Telekom AG (Deutschland), Leibniz-Institut für Meeresforschung (Deutschland), Masaryk University Brno (Tschechien).

www.picos-project.eu info@picos-project.eu

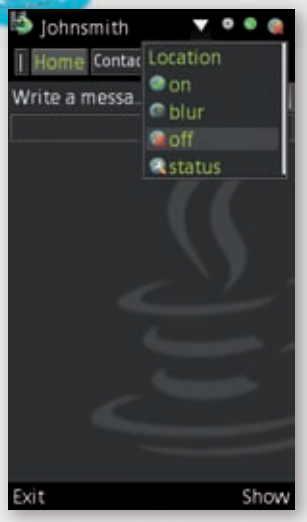
wechselt: im Beispiel der Angler etwa von einem einsam auf anbeißende Fische Wartenden, der gern preisgibt, wo man ihn besuchen kann, zu dem, der über einen schönen Fang berichten kann, dies aber auf keinen Fall allen preisgeben möchte und dies dann besser unter einer anderen Identität »verkündet«.

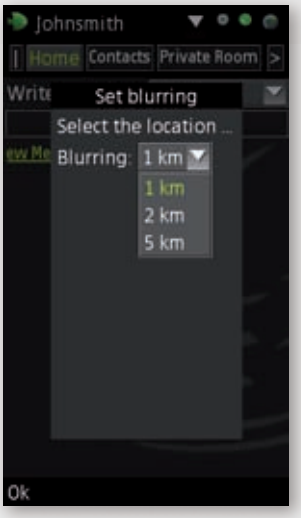
Darüber hinaus lässt sich der Zugriff anderer Nutzer auf die eigenen persönlichen Daten über die Einrichtung von »Privacy Policies« in weiteren Details regeln. Sie ermöglichen festzulegen, welche Daten unter welchen Bedingungen anderen Nutzern zugänglich sind. Zum Beispiel kann ein Angler festlegen, die neuesten Informationen über die Güte eines Angelplatzes zunächst nur den engsten und ältesten Freunden mitzuteilen. Um speziell die Information über den aktuellen Standort des Nutzers zu schützen, haben wir zusätzlich das »Blurring-Konzept« integriert, es sorgt dafür, dass der eigene Standort bei Bedarf nur ungenau in einer Karte dargestellt wird. Alternativ sieht das Konzept außerdem vor, Informationen zum Standort nur bestimmten anderen Nutzern oder gar nicht freizugeben.

Der »Privacy Advisor«, eine Art persönlicher Ratgeber, steht Nutzern bei all diesen Einstellungen zur Seite. Er hilft ihnen beim Umgang mit persönlichen Daten und warnt sie durch entsprechende Hinweise, wenn sie im Begriff sind, sensible Informationen preiszugeben. Damit soll bei den Nutzern einerseits Bewusstsein für die Problematik in spezifischen Fällen vermittelt werden, gleichzeitig Hilfe, wie sie die Werkzeuge, die wir ihnen an die Hand geben, sinnvoll nutzen können.

Diese Konzepte wirken vor allem in Kombination miteinander und dadurch, dass sie in einer Communi-

Der PICOS Prototyp als Handy-Anwendung: Über die Menüleiste lassen sich die wichtigsten Funktionen schnell erreichen.





Oben links lässt sich per Klick auf den Namen eine andere partielle Identität auswählen. Mit den Symbolen oben rechts kann direkt auf verschiedene Einstellungen zum Schutz der persönlichen Daten zugegriffen werden. Links:»„Privacy Policies« regeln den Zugriff auf persönliche Daten (zum Beispiel Profildaten) und helfen bei der der Einschränkung des Zugriffs auf bestimmte Nutzer. Mitte/rechts: Einstellen von »Blurring« der eigenen Position auf einen bestimmten Umkreis (zum Beispiel 1 km). Die Position des Nutzers wird dann entsprechend undeutlich in der Karte dargestellt, so dass der genaue Standort für andere verborgen bleibt.

ty akzeptiert und integriert angeboten werden. Dafür haben wir im nächsten Schritt eine technische Plattform entwickelt, auf der diese Konzepte prototypisch für die Angler-Community umgesetzt werden. Die Community-Mitglieder können live einige der entwickelten Konzepte nutzen. Gleichzeitig haben wir die Möglichkeit zu evaluieren, ob die Konzepte, die wir aufbauend auf den Anforderungen der Angler entwickelt haben, in ihrer Umsetzung die Bedürfnisse der Angler erfüllen.

Nach dem ersten Testlauf im Dezember 2009 lässt sich bereits sagen, dass das Feedback der Nutzer positiv war und die erarbeiteten Konzepte gut aufgenommen wurden. Im Laufe des Jahres werden die Tests fortgesetzt und auf die Community der Online-Gamer ausgeweitet.

Umsetzung in der Praxis

Unsere Arbeit in PICOS schafft wichtige Voraussetzungen, um den Daten- und Privatsphärenschutz in mobilen Communities zu verbessern. Die entwickelten Konzepte geben insbesondere den Community-Nutzern selbst Möglichkeiten, bewusster mit persönlichen Daten in Communities umzugehen. Gleichzeitig zeigt die praktische Umsetzung und deren Test mit End-Nutzern, wie derartige Konzepte in der Praxis Anwendung finden und in Communities integriert werden können.

In wissenschaftlichen Publikationen und durch Präsentationen auf Konferenzen, Workshops und Messen, wie zu Beginn des Jahres auf dem Mobile World Congress in Barcelona, der weltweiten Leitveranstaltung im Bereich Mobilkommunikation, lenken wir immer wieder die Aufmerksamkeit auf die wichtige Frage, wie die Privatsphäre in hoch kommunikativen und mobilen Communities geschützt werden kann und präsentieren unsere PICOS-Ergebnisse. Bereits im Zuge des Projektes finden die entwickelten Konzepte ihren Weg in die Praxis und in bestehende Communities und Technikplattformen der entsprechenden Projektpartner. Dazu zählen das »IFM Geomar Institut« in Kiel, dessen Meeresforscher sich unter anderem in engem Kontakt zu existierenden Angler-Communities befinden, weil sie sich von Anglern berichten lassen, welche Fische wann und wo aktuell vorkommen. Die in PICOS vertretenen Industriepartner, wie die Deutsche Telekom, Hewlett-Packard oder ATOS Origin, können über die Integration von PICOS-Konzepten in Produkte und Dienstleistungen zusätzlich für eine nachhaltige Verwendung der Konzepte auch in der Praxis sorgen. ◆

Weiterführende Links und Literatur

PICOS Community Requirements beschreibt die Anforderungen der exemplarischen Communities und deren Erhebung: http://www.picos-project.eu/PICOS_D2_4_Requirements_v1_0_Final_Public.pdf

PICOS Platform Architecture and Design beschreibt die Community-Plattform Architektur, einschließlich innovativer PICOS-Konzepte für Privatsphären und Datenschutz: http://www.picos-project.eu/PICOS_D4_1_Architecture_v1_4_Final_Public.pdf

PICOS Community Application Prototype beschreibt die prototypische Community-Anwendung, die auf Basis der Architektur entwickelt und implementiert wurde: http://picos-project.eu/PICOS_D6_1_Community_Application_Prototype_v1_Final_Public.pdf

Crespo, A., Mendez, R., Liesebach, K. *Climbing towards trust and privacy management in social mobile communities* W3C Workshop on the Future of Social Networking Proceedings, W3C, Barcelona, Spain, 2009. http://www.w3.org/2008/09/msnws/papers/W3C_Position Paper_PICOS.pdf

Weiss, S. *Privacy Threat Model for Data Portability in Social Network Applications, Proceedings of the 14th Americas Conference on Information Systems (AMCIS)* Toronto, Canada, 2008.

Die Autoren

Das PICOS-Team (von links nach rechts): Markus Tschersich, Prof. Dr. Kai Rannenberg, Katja Böttcher, Christian Kahl und Stephan Heim.

Prof. Dr. Kai Rannenberg, 45, ist seit 2002 Inhaber der T-Mobile Stiftungsprofessur für Mobile Business & Multilateral Security an der Goethe-Universität. Nach dem Studium der Informatik in Berlin und der Promotion in Freiburg war er unter anderem für Microsoft Research in Cambridge im Bereich »Personal Security Devices & Privacy Technologies« tätig. Er ist zudem aktiv beteiligt an Standardisierungsprozessen im Informations- und Telekommunikationsbereich bei der Internationalen Standardisierungsorganisation ISO/IEC. Darüber hinaus engagiert sich Rannenberg in verschiedenen europäischen Initiativen zum Daten- und Privatsphärenschutz. Mit seiner Professur ist er seit mehreren Jahren in zahlreichen nationalen und europäischen Forschungsprojekten vertreten, dazu gehört neben PICOS auch PRIME und PrimeLife. In diesen Projekten geht es um die Erforschung von Möglichkeiten, Privatsphäre und Datenschutz in verschiedenen Kontexten und vor dem Hintergrund unterschiedlicher Anwendungsszenarios zu verbessern. PICOS und PrimeLife bauen auf dem Projekt PRIME auf.

Christian Kahl, 28, arbeitet seit 2007 als wissenschaftlicher Mitarbeiter und Doktorand im Team von Prof. Rannenberg. Der Diplom-Wirtschaftsinformatiker hat in Essen unter anderem mit den Schwerpunkten E-Business und Marketing studiert und forscht heute im Bereich (mobiler) Sozialer Netzwerke. Der Schwerpunkt seiner Arbeit liegt dabei insbesondere auf neuen Konzepten zu Marketing und Geschäftsmodellen für derartige Netzwerke im Internet und für mobile Geräte.

Katja Böttcher, 29, gehört seit 2008 als wissenschaftliche Mitarbeiterin und Doktorandin zum Team von Prof. Rannenberg. Sie studierte Diplom-Medien-Informatik in Dresden und war dort nach ihrem Studium bereits im EU-Projekt PRIME tätig. In ihrer Forschung fokussiert sie aktuelle Fragestellungen zu Daten- und Privatsphärenschutz kollaborativer sozialer Netzwerke im Unternehmenskontext mit speziellem Fokus auf Teamarbeit im Web 2.0.

Kai.Rannenberg@m-chair.net
Christian.Kahl@m-chair.net
Katja.Boettcher@m-chair.net