Erschien in: Dieter Klumpp, Herbert Kubicek, Alexander Roßnagel, Wolfgang Schulz (Hg.): Netzwelt – Wege, Werte, Wandel; Springer, Berlin Heidelberg 2010, 245–263

Identitätsmanagement in Netzwelten

Sandra Steinbrecher, Andreas Pfitzmann, Sebastian Clauß

1 Einführung

Viele Menschen verlagern immer mehr Aspekte ihres Lebens zumindest teilweise in die virtuellen und vernetzten Welten des Internet. In vielfältigen Netzwelten wird gekauft und verkauft, ein großes Spektrum an Themen diskutiert, Wissen mit anderen geteilt und erworben, miteinander gespielt und vieles mehr. Dies gilt sowohl für berufliche als auch private Belange vieler Menschen. Dabei kommt es häufig zu Interaktionen von einander vorher Unbekannten.

An die Systeme, die Interaktionen in Netzwelten technisch ermöglichen, werden wie an jedes technische System von Nutzern und Systemanbietern Sicherheitsanforderungen gestellt. Daneben haben Nutzer Erwartungen zum Verhalten ihrer Interaktionspartner. Diese Erwartungen betreffen auch Sicherheitsanforderungen. Technische Systeme sollten daher Nutzer darin unterstützen, mit potenziellen Interakteuren Sicherheitsanforderungen auszuhandeln und ihre Erfüllung einzuschätzen.

Die meisten Menschen möchten ihre Privatsphäre in Netzwelten genauso selbstverständlich gewahrt wissen wie in der physischen Welt. Wer ein Geschäft betritt, zeigt jedoch keine Identifikationsnummer vor, während er dies beim Besuch eines Internetshops etwa mit seiner IP-Adresse tut. Ein Schutz der Privatsphäre auf der Kommunikationsebene, also anonyme Kommunikation, ist durch verschiedene Anonymisierungsdienste möglich. Sie reichen von einfachen anonymisierenden Proxys bis zu sichereren Diensten wie JAP [BeFK_01] oder Tor [DiMS_04], die mehr oder weniger auf Chaums Mixen [Chau_81] basieren. Proxies erreichen nur Anonymität gegenüber dem Shop-Betreiber und externen Angreifern, während JAP und TOR Anonymität auch gegenüber den Betreibern des Anonymisierungsdienstes sicherstellen.

Wer in einem Geschäft die Beratung eines Verkäufers sucht, gibt ihm zumeist nur Informationen über die eigenen Vorlieben, die für den geplanten Kauf relevant sind, aber kein komplettes Persönlichkeitsprofil. Der Besucher eines Internetshops bietet ihm meist jedoch ein umfangreiches Persönlichkeitsprofil über vergangene Einkäufe bei ihm oder kooperierenden Shops. Dazu richten Dienstanbieter im Rahmen von Identitätsmanagement Nutzeraccounts ein und animieren die Nutzer, sich bei jedem Besuch des Shops einzuloggen bzw. versuchen, eben das automatisch zu erreichen.

Statt das Identitätsmanagement allein dem Dienstanbieter zu überlassen, um die Accounts seiner Nutzer zu verwalten, haben Nutzer zunehmend die Chance, nutzerkontrolliertes datenschutzfreundliches Identitätsmanagement (IDM) zu verwenden. Es hilft ihnen, die Datenmenge zu kontrollieren, die sie zu Dienstanbietern übertragen. Zugleich wird dem Dienstanbieter die Zurechenbarkeit von Aktionen zu Nutzern garantiert.

In diesem Beitrag stellen wir zunächst die üblichen Sicherheitsanforderungen vor, die Menschen an technische Systeme und ihre Interakteure in Netzwelten stellen, und beleuchten, wie nutzerkontrolliertes datenschutzfreundliches IDM helfen kann, die konkurrierenden Anforderungen verschiedener Interakteure und des Systembetreibers zu unterstützen. Insbesondere geben wir dabei einen Ausblick, welchen Herausforderungen sich dieser Forschungsbereich noch stellen muss.

2 Interaktionssysteme in Netzwelten

Interaktion bezeichnet nach der lateinischen Bedeutung eine Handlung („actio“) zwischen („inter“) Entitäten, die damit zu *Interakteuren* werden. Weiter gefasst ist Interaktion „die durch Kommunikation vermittelte gegenseitige Beeinflussung von Individuen oder Gruppen im Hinblick auf ihr Verhalten und Handeln, ihre Einstellungen und dergleichen, z.B. in einer Schulklasse. Dabei orientieren sich die Beteiligten an den wechselseitigen Erwartungen (z.B. Rollenvorstellungen, Situationsdefinitionen), oder das Handeln der einen Person löst das der anderen aus. Interaktion erfolgt demnach im Rahmen eines den Handlungspartnern vorgegebenen Gefüges aus stabilen Grundverhaltensmustern, Bedeutungssymbolen sowie Kommunikationstechniken“ [Bro_04]. Interakteure können demnach eine Erwartung an das Verhalten bzw. die Aktionen der anderen Interakteure haben: implizit (z.B. in Form von Grundverhaltensmustern) oder explizit (z.B. in Form eines Vertrags). Insbesondere die implizite, aber auch die explizite Erwartung, sowie die eigentliche Interaktion können dabei einer subjektiven Betrachtung durch die Interakteure und andere Nutzer unterliegen. In der physischen Welt hängt die Betrachtung einer Interaktion von dem erwähnten Gefüge aus verwendeten Verhaltensmustern, Bedeutungssymbolen und Kommunikationstechniken ab. Interaktion spielt sich in verschiedenen Facetten von Kommunikation (Worten, Gesten, Tonfall usw.) ab und besteht aus vielen feingranularen Aktionen, die vielseitig aufeinander bezogen sind.

Technische Interaktionssysteme können die verschiedenen Facetten und die Feingranularität von Interaktion bisher nicht ausreichend nachbilden. Im Folgenden muss angenommen werden, dass für Interaktionssysteme nur eine Menge klar abgrenzbarer Aktionen, aus denen sich Interaktionen zusammen setzen können, zur Verfügung steht. Die damit möglichen Aktionen eines Akteurs, die im Sinne von Interaktion auf einen Kontakt als potenziellen Interakteur ausgerichtet sind, werden vom Interaktionssystem in einem darunter liegenden Kommunikationssystem in Form von Nachrichten zwischen einem Absender und Adressaten abgebildet. Kommunikationssysteme wiederum nutzen die unteren Netzwerkebenen zur Übermittlung dieser Nachrichten als Signale von einem Sender zu einem Empfänger. Damit ergeben sich für ein Interaktionssystem drei Interaktionsebenen: Die *Kommunikationsebene* besteht aus allen sieben Schichten des ISO/OSI-Modells [Zim_80]; die *Interaktionsebene* als Anwendung liegt oberhalb der obersten der sieben Schichten (Anwendungsschicht) und wird nicht vom OSI-Modell erfasst; die *Signalebene* unterhalb der untersten der sieben Schichten (Bitübertragungsschicht) des OSI-Modells bildet den analogen Bereich.

So wie die Interaktionen müssen auch die Interakteure digital abgebildet werden. Menschen werden in informationstechnischen Systemen üblicherweise durch Mengen von maschinenlesbaren Daten repräsentiert, so genannte digitale Identitäten. Abhängig von der Situation und dem Kontext, in denen ein Mensch sich befindet, werden nur Teilmengen dieser Daten („Attribute“) zu seiner Repräsentation benötigt. Sie werden als (digitale) Teilidentitäten (engl. „(digital) partial identities“, pIDs) bezeichnet [PK_08].

Jeder pID wird auf der Interaktionsebene des Interaktionssystems ein Identifikator zugeordnet, unter dem Aktionen ausgeführt werden können und/oder die entsprechende pID durch eine Aktion kontaktierbar ist; dieser Identifikator wird im Folgenden als *Interaktionspseudonym* bezeichnet. Ebenso wird der pID auf Kommunikationsebene ein (nicht notwendigerweise gleicher) Identifikator zugeordnet, unter dem sie Nachrichten senden kann und/oder mit Nachrichten adressierbar ist; er wird im Folgenden als *Kommunikationspseudonym* bezeichnet.

3 Sicherheit in Netzwelten

3.1 Anforderungen an informationstechnische Systeme

An Aktionen haben der Akteur, seine Kontakte sowie andere Teilnehmer der Netzwelt Erwartungen, darunter Sicherheitsanforderungen, die das Interaktionssystem gewährleisten soll. Für informationstechnische Systeme wird meist eine Dreiteilung der Sicherheitsanforderungen vorgenommen [VoKe_83, ZSI_89]:

- Vertraulichkeit: Unbefugter Informationsgewinn im System soll verhindert werden.
- Integrität: Unbefugte Modifikation von Information im System soll verhindert werden.
- Verfügbarkeit: Unbefugte Beeinträchtigung der Funktionalität des Systems soll verhindert werden.

Diese Dreiteilung muss für konkrete Systeme in Form konkreter Sicherheitsanforderungen weiter präzisiert werden. Für ein Interaktionssystem heißt das, dass für die Sicherheitsanforderungen sowohl die Interaktions- als auch die Kommunikationsebene betrachtet werden müssen, da jede explizite Aktion im Interaktionssystem im darunter liegenden Kommunikationssystem abgebildet wird.

3.2 Anforderungen an Kommunikationssysteme

In einem Kommunikationssystem wird Kommunikation zwischen Kommunikationspartnern in Form von Nachrichten von Absendern zu Adressaten vermittelt. Die im System auftretenden Informationen, auf die sich die Sicherheitsanforderungen Vertraulichkeit und Integrität beziehen, setzen sich aus Inhalt und Kommunikationsumständen der Nachricht zusammen. Unter Kommunikationsumstände fallen der Absender und die Adressaten. Zusätzlich können die Kommunikationspartner weitere Umstände, die im Kommunikationssystem als Informationen auftreten, als schützenswert ansehen; dazu können etwa die Zeit zählen, zu der sie kommunizieren, oder der Ort, an dem sie sich befinden. Im Folgenden liegt der Fokus zunächst nur auf dem Identifikator der pID des Absenders bzw. des Adressaten als schützenswerte Umstände. Für Kommunikationssysteme lassen sich die drei obigen Sicherheitsanforderungen weiter präzisieren:

1. Die *Vertraulichkeitsanforderungen* umfassen:

   (a) *Anonymität* des Absenders bzw. der Adressaten von Nachrichten, d.h. sie sind innerhalb einer Menge möglicher Absender bzw. Adressaten nicht identifizierbar.

   (b) *Unbeobachtbarkeit* des Absenders oder der Adressaten von Nachrichten, d.h. jemand kann Absender oder Adressat der Nachrichten sein, ohne dass andere dies bemerken.

   (c) *Vertraulichkeit* des Inhalts von Nachrichten, d.h. niemand außer dem Absender und den Adressaten von Nachrichten erfährt etwas über deren Inhalt.

   (d) *Verdecktheit* des Inhalts von Nachrichten, d.h. niemand außer dem Absender und den Adressaten von Nachrichten bemerkt deren Existenz.

2. Die *Integritätsanforderungen* umfassen:

   (a) *Integrität* des Inhalts und der Kommunikationsumstände, d.h. niemand kann Nachrichten nach dem Absenden unbemerkt modifizieren.

   (b) *Zurechenbarkeit* des Absenders bzw. der Adressaten, d.h. ein Absender bzw. Adressat kann nicht erfolgreich abstreiten, Nachricht mit diesem Inhalt und den übermittelten Kommunikationsumständen gesendet bzw. erhalten zu haben.

(c) *Konsistenz* des Inhalts und des Absenders, d.h. alle Adressaten erhalten die gleichen Nachrichten mit dem gleichen Inhalt und den gleichen Kommunikationsumständen oder erkennen, dass dies nicht der Fall ist.

3. Die *Verfügbarkeitsanforderungen* umfassen:

   (a) *Verfügbarkeit* des Systems, das die Nachrichten vermittelt, d.h. Nutzer können Nachrichten senden oder empfangen, wenn sie es möchten.

   (b) *Erreichbarkeit* der Nutzer innerhalb des Systems, d.h. Nutzer können über Nachrichten erreicht werden oder auch nicht, entsprechend ihren Wünschen.

   (c) *Fairness* der Nutzer untereinander, d.h. alle Absender bzw. Adressaten haben die gleichen Möglichkeiten zum Senden bzw. zum Empfang von Nachrichten.

   (d) *Verbindlichkeit* der Nutzer, d.h. Nutzer können dafür verantwortlich gemacht werden, eingegangenen Verpflichtungen nachzukommen.[1]

Die Anforderungen 1. (a)-(c), 2. (a)-(b) sowie 3. (a) wurden bereits in [CC98] zusammen gefasst. Diese Anforderungen wurden in [WoPf_00] aufgegriffen und um die Anforderungen 1. (d), 3. (b) und 3. (d) ergänzt. Alle Sicherheitsanforderungen weisen eine Richtung auf, und zwar auf die Nutzer hin, gegenüber denen sie gelten sollen. Für alle Anforderungen außer 2. (c) und 3. (c) wird ebenfalls in [WoPf_00] näher ausgeführt, gegenüber wem sie gelten sollen. Insbesondere müssen sich beide Kommunikationspartner über den Inhalt einer Nachricht betreffende Anforderungen (d.h. Vertraulichkeit, Verdecktheit, Integrität und Verfügbarkeit) einig sein, damit sie umgesetzt werden können, weshalb diese Anforderungen als *gleichgerichtet* bezeichnet werden.

In [WoPf_00] wurde bereits in den Formulierungen der Sicherheitsanforderungen berücksichtigt, dass eine Nachricht von einem Absender nicht zwangsläufig nur an einen Adressaten gesendet wird, sondern auch mehrere haben kann. Die sich aus einem solchen Multicast ergebenden Sicherheitsanforderungen zwischen mehreren Adressaten wurden jedoch nicht formuliert. Aus diesem Grund wird hier Konsistenz als Sicherheitsanforderung 2. (c) unter Integrität ergänzt. Im Falle nur eines Adressaten ist diese Anforderung trivialer weise immer erfüllt. Da davon auszugehen ist, dass ein Kommunikationssystem von mehreren Absendern genutzt wird – sonst wäre Anonymität der Absender ohne Unbeobachtbarkeit gar nicht möglich –, wird Fairness des Sendens und Empfangs von Nachrichten der Absender und Adressaten jeweils untereinander unter Verfügbarkeit als weitere Sicherheitsanforderung 3. (c) ergänzt.

Das letzte Ziel 3. (d) – Verbindlichkeit – befindet sich bei Kommunikationssystemen bereits außerhalb des technischen Systems. Es muss – wie der englische Begriff „legal enforceability" dafür bereits sagt – juristisch behandelt werden. Verbindlichkeit hängt insbesondere davon ab, inwieweit die verwendeten technischen Maßnahmen zur Umsetzung der Sicherheitsanforderungen im geltenden Recht als ausreichend und rechtlich bindend angesehen werden.

3.3 Anforderungen an Interaktionssysteme

Das Interaktionssystem muss Akteure und ihre Aktionen, wie ausgeführt, gleichzeitig auf zwei Ebenen schützen:

1. *Interaktionsebene*: Ein Akteur führt eine Aktion aus bzw. ein Kontakt wird durch eine Aktion kontaktiert.
2. *Kommunikationsebene*: Ein Akteur sendet als Absender Nachrichten, die eine Aktion

1 Verantwortlichkeit heißt lediglich, dass derjenige bei Nichteinhaltung entsprechende rechtliche Konsequenzen tragen muss. Interakteure würden sich häufig wünschen, dass durch Verbindlichkeit derjenige sogar gezwungen werden könnte den Verpflichtungen nachzukommen. Dies ist aber im Zuge des Freiheitsrechts jedes einzelnen nicht durchsetzbar. Vielmehr ist ein rechtlicher Kompromiss gewünscht.

vermittelt, an Adressaten, die durch diese adressiert werden.

Auf beiden Ebenen treten Inhalte und Umstände der Kommunikation bzw. Interaktion auf. Da auf Kommunikationsebene die Aktionen als Nachrichten vermittelt werden, entspricht der Inhalt der Nachrichten dem der Aktion ergänzt um einen Parameter, um welche Aktion es sich handelt. Bei den Aktions- und Kommunikationsumständen werden wie bei den Kommunikationssystemen zunächst nur der zu einer Aktion bzw. Nachricht gehörende Akteur bzw. Absender und die zugehörigen Kontakte bzw. Adressaten betrachtet. Ihnen werden auf Kommunikationsebene Kommunikationspseudonyme und auf Interaktionsebene Interaktionspseudonyme zugeordnet, mit denen sie adressierbar bzw. kontaktierbar sind.

3.3.1 Anforderungen auf Kommunikationsebene

Das Interaktionssystem kann eine zentrale oder eine dezentrale Architektur haben oder Aspekte beider Architekturen beinhalten. Dementsprechend werden Kommunikationssysteme unterschiedlich genutzt.

Bei einer zentralen Architektur stellt das Interaktionssystem neben den Clients einen Server zur Verfügung, der die Aktionen der Akteure als Nachrichten entgegen nimmt. Sie können dort durch andere abgefragt werden (z.B. bei Webforen), oder der Server verteilt diese Nachrichten selbst (z.B. bei Mailinglisten).

Bei webbasierten Interaktionssystemen wird jedem Akteur meist ein Account zur Verfügung gestellt, unter dem er Aktionen ausführen kann. Auf ihn kann er in der Regel mit Login und Passwort zugreifen.

Bei einer dezentralen Architektur stellt das Interaktionssystem jedem Akteur einen Client zur Verfügung, mit dem der Akteur seine Aktionen ausführt. Die Nachrichten auf Kommunikationsebene kann der Client dann an andere Akteure verteilen (z.B. bei P2P-File-Sharing-Systemen).

Häufig werden jedoch auch Mischarchitekturen verwendet. Insbesondere werden in dezentralen Systemen häufig auch Clients zu Servern im Sinne von Zwischenstationen, die Nachrichten zwischen Kommunikationspartnern, deren Clients nicht direkt miteinander verbunden sind, weiterleiten.

Unabhängig von der Architektur deckt sich der Akteur bei expliziten Aktionen mit dem Absender des zugrunde liegenden Kommunikationssystems, das die die Aktion vermittelnden Nachrichten auf Kommunikationsebene des Interaktionssystems sendet. Bei der zentralen Architektur folgt allerdings eine weitere Verwendung des Kommunikationssystems, wenn die vom Absender erhaltene Nachricht an die Nutzer weiter verteilt wird. Dadurch wird der Server dann ebenfalls als Zwischenstation zum Absender, nicht jedoch zum Akteur. Muss die Nachricht durch einen Nutzer explizit abgefragt werden, wird auch dieser Nutzer zum Absender der entsprechenden Abfrage, nicht jedoch zum Akteur im Sinne des Interaktionssystems.

Für Kommunikationssysteme wurden Sicherheitsanforderungen bereits in Abschnitt 3.2 vorgestellt.

3.3.2 Anforderungen auf Interaktionsebene

In Kommunikationssystemen werden nur Sicherheitsanforderungen bezüglich einzelner Nachrichten betrachtet. In Interaktionssystemen tritt jedoch nicht nur uni- oder bidirektionale Kommunikation auf, sondern auch Verkettungen von Aktionen in Form von Interaktionen oder in Form von unter dem gleichen Interaktionspseudonym begangenen Aktionen.

Bei den Aktionen innerhalb von Interaktionen treten folgende Unterschiede zwischen Interaktionsebene und Kommunikationsebene auf:

Interaktionsebene: Bei der Initiierung von Interaktion werden mögliche Kontakte durch die

Parameter bestimmt, die bei der Aktion angegeben werden. Die Parameter können sich aus Inhalt und/oder Umständen der zugehörigen Nachricht zusammensetzen (z.B. gibt der Parameter „Interakteur“ einen Umstand an; der Parameter „Thema“ hingegen bezieht sich sowohl explizit auf den Inhalt der Aktion als auch implizit auf mögliche Kontakte, und damit einen Umstand der Nachricht). Ob ein Kontakt zustande kommt, hängt von den kontaktierten potenziellen Interakteuren ab; sie entscheiden selbst, ob sie den Kontakt wahrnehmen und mit einer Reaktion in die Interaktion eintreten wollen. Im Gegensatz zum Adressaten einer Nachricht ist ein Kontakt also nicht notwendigerweise fremdbestimmt. Erst durch die Reaktion auf eine erfolgte Aktion wird ein Kontakt selbst aktiv als Akteur. Seine Reaktion hat als Kontakt mindestens die Akteure, die bisher an der Interaktion beteiligt waren sowie ggf. weitere Nutzer, die sich von der Interaktion als Kontakt angesprochen fühlen. Die explizite Beendigung einer Interaktion hat auf Interaktionsebene als Kontakt die bisherigen Interakteure in dieser Interaktion. Damit ergibt sich folgende neue Verfügbarkeitsanforderung der Nutzer an das Interaktionssystem:

> *Kontaktierbarkeit* der gewünschten Kontakte; d.h. ein Nutzer kann von anderen Nutzern kontaktiert werden, wenn er dies auch wünscht.

Kommunikationsebene: Der Adressat ist je nach Architektur entweder der Server, der die Nachricht an die Clients verteilt oder zur Abfrage durch diese zur Verfügung stellt, oder direkt die Clients der anderen Nutzer. Kontaktierbarkeit auf Interaktionsebene erfordert, dass auf Kommunikationsebene Erreichbarkeit gewährleistet ist. Erreichbarkeit ist damit notwendige, nicht jedoch hinreichende Bedingung für Kontaktierbarkeit, da Kontaktierbarkeit eine Aktion des Kontakts erfordert, Erreichbarkeit jedoch nicht.

3.3.3 Anforderungen bzgl. Verknüpfung digitaler und physischer Identität

Mit der Anmeldung bei einem Interaktionssystem erhält ein Nutzer das Recht, unter dem vereinbarten Interaktionspseudonym Aktionen auszuführen; mit der Abmeldung wird ihm dieses Recht entzogen.

Seine Wiedererkennung erfolgt durch das Interaktionspseudonym und geeignete Authentisierung bzw. Identifizierungsmaßnahmen für dieses, auf deren Basis seine Autorisierung für Aktionen möglich ist. Die unter dem Interaktionspseudonym begangenen Aktionen sind diesem zurechenbar und die physische Identität des Inhabers, soweit erforderlich, aufdeckbar. Dann kann er für seine Aktionen verantwortlich gemacht werden. Dadurch wird die eindeutige Verkettbarkeit von Aktionen, an denen ein Nutzer als Akteur oder Kontakt beteiligt ist, mindestens innerhalb des Interaktionssystems hergestellt. Es ergeben sich folgende zusätzliche Sicherheitsanforderungen:

- *Pseudonymität* einer Aktion, d.h. ein Akteur kann Aktionen unter diesem Pseudonym ausführen, ohne dass er dafür seinen Namen in der physischen Welt, d.h. seine physische Identität, preisgeben muss.
- *Autorisierbarkeit* einer Aktion, d.h. Pseudonyme sind innerhalb des Interaktionssystems eindeutig als Identifikator verwendbar und es ist möglich, einen Akteur basierend darauf zu authentisieren und ihm zu erlauben, diese Aktion durchzuführen.
- *Eindeutige Verkettbarkeit* von Elementen (Aktionen, Pseudonymen); d.h. diese Elemente stehen mit hoher Wahrscheinlichkeit zueinander in Beziehung.
- *Unverkettbarkeit* von Elementen (Aktionen, Pseudonymen); d.h. ein potenzieller Angreifer kann nicht hinreichend unterscheiden, ob diese Elemente zueinander in Beziehung stehen oder nicht.

Nach [PK_08] sind Verkettbarkeit und Unverkettbarkeit genau gegensätzliche Sicherheitsanforderungen. Verkettbarkeit bedeutet, dass ein potenzieller Angreifer hinreichend unterscheiden kann, ob diese Elemente zueinander in Beziehung stehen oder nicht.
Bei obiger Definition von eindeutiger Verkettbarkeit wird jedoch nur der Fall des in-Beziehung -

stehens betrachtet.

Unverkettbarkeit von Aktionen kann oft nur eine Anforderung gegenüber nicht beim Interaktionssystem angemeldeten Nutzern sein. Die unter einem Interaktionspseudonym ausgeführten Aktionen sind gegenüber dem Dienstanbieter und gegenüber beim Dienst angemeldeten Nutzern eindeutig verkettbar. Ist Unverkettbarkeit auch gegenüber diesen gewünscht, muss sich jeder Akteur unter verschiedenen unverkettbaren Interaktionspseudonymen beim Interaktionssystem anmelden können, oder er muss in die Lage versetzt werden, eines seiner Pseudonyme in ein anderes umzuwandeln, ohne dass die anderen Akteure diese verketten können.

3.3.4 Anforderungen an die Akteure

In Kommunikationssystemen ist es üblich, dass sowohl Kommunikationspartner als auch nicht an der Kommunikation Beteiligte als potenzielle Angreifer gesehen werden. Nach [WoPf_00] müssen sich beide Kommunikationspartner über die gleichgerichteten Sicherheitsanforderungen (d.h. Vertraulichkeit, Verdecktheit, Integrität und Verfügbarkeit) einig sein, damit diese auch umgesetzt werden können.

Wenn Kommunikationssysteme Nachrichten zwischen sich vertrauenden Kommunikationspartnern vermitteln, ist dies leichter zu erreichen als in Interaktionssystemen, wo Interaktionen zwischen sich noch unbekannten Akteuren entstehen können. Akteure in Internetcommunities haben bzgl. der gleichgerichteten Sicherheitsanforderungen neben den Anforderungen an das Interaktionssystem auch Erwartungen an das Verhalten der anderen Interakteure. Neben der Tatsache, dass das Interaktionssystem alles tun soll, um diese Anforderungen technisch sicherzustellen, müssen auch die Akteure versuchen, die Anforderungen semantisch zu garantieren. In der Informationstheorie versteht man unter der Semantik einer Information die Bedeutung dieser Information. In diesem Sinne bedeutet semantische Erfüllung der gleichgerichteten Sicherheitsanforderungen [BHLP_07]:

1. *Semantische Vertraulichkeit/Verdecktheit* einer Aktion seitens der Akteure erfordert *Diskretion* der Akteure bzgl. der Aktion; d.h. niemand außerhalb der berechtigten Akteure erfährt von diesen etwas über den Inhalt bzw. die Existenz der Aktion.
2. *Semantische Integrität* einer Aktion erfordert *Zulässigkeit* der durch einen Akteur durchgeführten Aktion. Ein Akteur handelt subjektiv zulässig für einen Betrachter (Akteur, Kontakt oder Außenstehender), wenn er dessen Erwartungen an die Aktion entspricht.
3. *Semantische Verfügbarkeit* einer Aktion seitens der Akteure erfordert *Aktionsbereitschaft* eines Akteurs zur Durchführung der Aktion; d.h. die Aktion wird durchgeführt, wenn andere Akteure sich dies wünschen.

Diskretion und Aktionsbereitschaft sind meist objektiv beurteilbar; für die Zulässigkeit von Aktionen gilt dies meist nicht: Die Einteilung von Aktionen in zulässige und nicht zulässige ist neben der Subjektivität des Betrachters auch von anderen Faktoren abhängig, z.B. dem Zeitpunkt der Beurteilung. Bei fehlendem Hintergrundwissen kann diese Einteilung sogar unmöglich sein.

4 Identitätsmanagement in Netzwelten

Identitätsmanagement kann Nutzern helfen, die in Interaktionen mit anderen verwendeten Teilidentitäten übersichtlich zu verwalten und auf Interaktionsebene im Sinne mehrseitiger Sicherheit einen kontrollierbaren Ausgleich zwischen den eigenen Sicherheitsanforderungen und denen der anderen Interakteure zu erreichen. Aufgrund der Unsicherheit, ob die Anforderung der Diskretion durch andere Nutzer erfüllt wird, müssen die Daten, die Einzelne an andere übertragen, minimiert und kontrolliert werden.

Gleichzeitig wünschen Interakteure sich, dass die Integrität übertragener Daten gesichert wird. IDM-Systeme müssen deshalb Bausteine anbieten, die die Erfüllung von sowohl Integritäts- als

auch Vertraulichkeitsanforderungen unterstützen, um mehrseitige Sicherheit zu erreichen.

Das EU Projekt FIDIS unterscheidet drei Kategorien von IDM-Systemen (vgl. [BaMe_05]):

1. zum Account-Management (insbesondere Implementierung von AAA-Infrastrukturen).
2. zum Profiling von Nutzerdaten durch Organisationen, z.B. Data Warehouses, zwecks Unterstützung personalisierter Dienste oder der Analyse von Nutzerverhalten.
3. zum nutzerkontrollierten kontextabhängigen Rollen- und Pseudonymmanagement.

IDM-Systeme der ersten beiden Typen werden meist zentral implementiert. Ihr Hauptziel ist die vertrauenswürdige Identifikation von Personen oder vertrauenswürdige Zuschreibung von Eigenschaften zu diesen, um Zurechenbarkeit zu erreichen. Pseudonymität wird hingegen meist vernachlässigt, da alle mit partiellen Identitäten assoziierten Daten serverseitig gespeichert werden. Die einfachste Umsetzung ist ein stand-alone-System mit einer Datenbank zur Speicherung der partiellen Identitäten, das von diesem Server und den dem Nutzer angebotenen Anwendungen genutzt wird. Im Folgenden wird v.a. auf die neuen Trends zum nutzerkontrollierten Identitätsmanagement eingegangen.

4.1 Nutzerkontrolliertes datenschutzfreundliches Identitätsmanagement

Grundsätzlich soll ein nutzerkontrolliertes Identitätsmanagement einem Nutzer die Kontrolle über die Herausgabe seiner personenbezogenen Daten ermöglichen. Es sollen sowohl kontrollierte Pseudonymität des Nutzers als auch Verlässlichkeit der übermittelten Daten erreicht werden. Dieser Abschnitt gibt einen Überblick über die wesentlichen Prinzipien und Technologien solcher IDM-Systeme. Mehr Details dazu können in [ClKo_01, CPHH_02] nachgelesen werden.

Personenbezogene Daten werden in solchen IDM-Systemen grundsätzlich unter Kontrolle des Nutzers gespeichert. Der Nutzer kann entscheiden, ob, an wen und für welchen Zweck er ihn betreffende Daten herausgeben möchte. Um dies zu erreichen ist ein zugrunde liegendes Netz erforderlich, das anonyme Kommunikation ermöglicht. Zusätzlich müssen Pseudonyme verwendet werden, die eine Kontrolle der Verkettbarkeit der herausgegebenen Daten ermöglichen.

Digitale Pseudonyme können als öffentliche Schlüssel eines digitalen Signaturverfahrens realisiert werden. Der Pseudonyminhaber besitzt dabei den zugehörigen geheimen Schlüssel. Durch eine mit dem geheimen Schlüssel erzeugte digitale Signatur kann die Zurechenbarkeit einer Nachricht zu einem digitalen Pseudonym nachgewiesen werden. Beispielsweise ist ein öffentlicher PGP-Schlüssel ein digitales Pseudonym.

Um Unverkettbarkeit zwischen mehreren Pseudonymen eines Nutzers beibehalten zu können ist es notwendig, zertifizierte Attribute zwischen Pseudonymen transferieren zu können. Ein Nutzer sollte ein Attribut unter einem seiner Pseudonyme von einer dritten Partei zertifiziert bekommen können, es dann aber auch unter jedem anderen seiner Pseudonyme vorzeigen können, ohne dabei einen Zusammenhang mit dem ersten Pseudonym herstellen zu müssen. Um dies zu erreichen, müssen die Attribute in Form von *pseudonymen umrechenbaren Credentials* vorliegen. Das bedeutet, dass das Attribut durch eine dritte Instanz zertifiziert ist, das Zertifikat aber mit Hilfe kryptographischer Methoden unter verschiedenen Pseudonymen (für Empfänger und Dritte unverkettbar) vorgezeigt werden kann.

Ein Credentialsystem mit solchen Eigenschaften wurde erstmals von David Chaum [Chau_86] veröffentlicht. Weitere verbesserte Systeme wurden u.a. von Brands [Bran_99] und Camenisch/Lysyanskaya [CaLy_00] entwickelt.

Um Attribute in Form von pseudonymen Credentials verlässlich benutzen zu können, wird außerdem eine Public-Key-Infrastruktur mit entsprechenden Schlüsselservern benötigt, da die credential-ausstellenden Instanzen mit Hilfe einer Zertifizierungsinfrastruktur beglaubigt und die zum Verifizieren der Credentials benötigten Schlüssel zertifiziert und veröffentlicht werden

müssen.

Ein nutzerkontrolliertes Identitätsmanagement kann durch zusätzliche Infrastruktur unterstützt werden. Treuhänder für Werteaustausch (Wertetreuhänder) oder Treuhänder zur vertrauenswürdigen Verwaltung von Identitätsdaten (Identitätstreuhänder) können Datensparsamkeit und Rechtssicherheit unterstützen. Weiterhin kann es dritte Parteien geben, die sich auf datenschutzfreundliche Bezahlung oder Lieferung von Gütern spezialisieren.

Privacy Emergency Response Teams (PERT) können analog zu den bereits bestehenden Computer Emergency Response Teams (CERT) Informationen über Sicherheits- und Datenschutzrisiken an IDM-Systeme der Nutzer weitergeben, um dort entsprechende Entscheidungen über die Herausgabe personenbezogener Daten zu beeinflussen.

Das IDM-System soll dazu beitragen, dass jeder Nutzer die Herausgabe personenbezogener Daten an Kommunikationspartner in elektronischen Kommunikationsvorgängen minimieren kann. Es muss demzufolge sichergestellt werden, dass nur genau die dafür vorgesehenen Daten herausgegeben werden. Hierbei ist eine Messung der Anonymität (oder des Gegenteils: der Identifizierbarkeit) für den Nutzer wichtig. Der Nutzer kann dadurch Informationen erhalten, inwieweit ein Kommunikationspartner ihn identifizieren kann, oder allgemeiner: inwieweit es möglich ist, eine digitale Identität des Nutzers mit seiner physischen Identität zu verketten.

4.2 Nutzerkontrolliertes Identitätsmanagement für beliebige Interaktionssysteme

Ein IDM-System der dritten Kategorie existiert für allgemeine Interaktionssysteme bisher nicht. Der Nutzer-Dienst-orientierte Ansatz eignet sich höchstens für das Identitätsmanagement gegenüber Dienstanbietern, nicht jedoch gegenüber einzelnen Interakteuren. Diese Thematik wird im Projekt PrimeLife[2] adressiert. Ein solches IDM-System steht vor weiteren Sicherheitsanforderungen und benötigt in Ergänzung zu obigen Bausteinen aus Abschnitt 4.1 weitere Bausteine. Einen Überblick, welche Bausteine im Falle im von Communitysystemen als Interaktionssysteme zusätzlich nötig sind, haben wir in [BHLP_06, BHLP_07] gegeben:

- *Wahl und Entwicklung einer Interaktionsumgebung*: Die Minimierung der über Pseudonyme verfügbaren Informationen wirft im Zusammenhang mit Communities das funktionale Problem auf, dass es schwieriger wird, interessierte neue Interakteure zu finden. Hier können Reputations- oder Empfehlungssysteme helfen.
- *Awareness*: Spielen bei Kontaktierbarkeit und Aktionsbereitschaft Zeitaspekte eine Rolle, so sind Awareness-Informationen in Internetcommunities von großer Bedeutung. Beispiele sind Gruppen-Awareness (Informationen über die Gruppe, in der ein Nutzer interagiert), Kontext-Awareness (Informationen über die Umgebung eines Nutzers wie Zeit oder Ort) und informelle Awareness (weitere implizite Informationen). Awareness-Informationen sind zum einen Daten, die sicherheitsrelevante Entscheidungen beeinflussen (z.B. Aushandlungen im Sinne mehrseitiger Sicherheit). Zum anderen enthalten sie selbst häufig auch Daten anderer Nutzer, die diese als schützenswert ansehen könnten.
- *Unterscheidung von Kontexten*: Communities beschäftigen sich meist nicht nur mit einem Thema oder Kontext, sondern kombinieren mehrere. Damit müssen Nutzer ihre Awareness bzgl. Trennung dieser Kontexte unter dem Gesichtspunkt der Kontrolle ihrer Anonymität erhöhen, indem sie unterschiedliche Pseudonyme innerhalb der gleichen Community verwenden, um dadurch entsprechende Kontexte zu separieren. Dies ist ein entscheidender Unterschied zum klassischen Identitätsmanagement gegenüber Diensten, wo nur Dienst und Kontext bei der Pseudonymwahl zu berücksichtigen sind. Hier interagiert ein

2 Privacy and Identity Management in Europe for Life (www.primelife.eu), gefördert von der europäischen Union im 7. Rahmenprogramm.

Akteur jedoch innerhalb der gleichen Community, die zum Dienst korrespondieren würde, oft mit unterschiedlichen Interakteuren, die wiederum anders als der Dienst, der unter einem festen Pseudonym auftritt, auch verschiedene Pseudonyme verwenden können. In [BDFL_05] wird Nutzerunterstützung für die Separierung von Kontexten in einer E-Learning Umgebung vorgestellt.

- *Zugang*: Basierend auf dem Eintritt in eine Internetcommunity werden meist Zugangsdaten ausgegeben, mit denen sich die Nutzer bei Aktionen im folgenden authentisieren und basierend darauf Autorisationen zu den angestrebten Aktionen erhalten. Übliche technische Realisierungen sind access control lists oder rollenbasierte Zugriffskontrolle.
  Da Identitätsmanagement jedoch einen dynamischen Wechsel von Pseudonymen abhängig vom Kontext erlaubt, können diese Realisierungen aufgrund ihrer Notwendigkeit zur festen Rollenvergabe hier nicht angewendet werden. Um Unverkettbarkeit der Pseudonyme des gleichen Nutzers zu gewährleisten, kann ein von Capabilities inspirierter, aber auf pseudonymen Credentials basierender Ansatz verwendet werden, wie er in [FBWB_06] für eine E-Learning Umgebung vorgeschlagen wird.
- *Aushandlung und Durchsetzung von Policies*: Im Identitätsmanagement für das Nutzer-Dienst-Szenario gelten meist feste Policies bzgl. Sicherheitsanforderungen seitens des Dienstbetreibers (z.B. welche Daten des Nutzers erforderlich sind oder welches Authentisierungs- oder Verschlüsselungssystem für eine Aktion verwendet wird). Nach der EU Direktive zum Datenschutzrecht [ECDir_95] ist der Dienstbetreiber verpflichtet eine Privacy Policy herauszugeben, wenn personenbezogene Daten erhoben werden. Im Gegensatz dazu gilt diese rechtliche Anforderung für Privatpersonen nicht. Meist divergieren die Anforderungen von eher gleichberechtigten Interakteuren wesentlich mehr – können sich aber besser an die Aktionen des Interakteurs anpassen. Dadurch kann die Aushandlung von Kompromissen wesentlich komplexer werden. Hier tut sich eine neue Forschungsfrage auf, welche Aushandlungsschritte dabei mit Policies erfasst werden können.
- *Workflows*: Viele Menschen wünschen sich vorgegebene Workflows für ihre Aktionen. Während bei der Interaktion mit Diensten die Workflows durch diese meist fest vorgegeben sind, müssen sie zwischen gleichberechtigten Interakteuren oft ausgehandelt werden. Wenn ein Interakteur dem anderen einen Workflow vorschlägt,
  gefährdet er unter Umständen schon seine Anonymität, da er unter verschiedenen Pseudonymen wiedererkennbar werden könnte. Deshalb sollte ein IDM-System für Communities seinen Nutzern bereits feste Workflows anbieten, die ihnen Anonymität innerhalb all derer erlauben, die die gleichen Workflows verwenden. Zusätzlich ist es zum Zwecke der Funktionalitätssteigerung sinnvoll, dass Nutzer selbst Workflows erstellen, existierende kombinieren und ihre selbst erstellten Workflows anderen Nutzern zur Verwendung anbieten können. Diese Wiederverwendung erhöht wiederum ihre Anonymität. Gleichzeitig muss dabei beachtet werden, dass der Workflow keine Anonymität gefährdenden Daten enthält.
- *Trust Management*: Vertrauen ist bei der Interaktion Unbekannter von entscheidender Bedeutung. Reputation von Nutzern erlaubt anderen Nutzern geeignete Interakteure auszuwählen, die sich mit hoher Wahrscheinlichkeit an einer Interaktion beteiligen und sich dabei auch korrekt und diskret verhalten. Dabei sind zwei Arten von Reputation zu unterscheiden: Implizite Reputation ist jeweils an ein einzelnes Pseudonym gebunden, die dieses im Laufe der Zeit durch sein Verhalten in Interaktionen erworben hat. Dies kann ein Nutzer sein, der vielfach innerhalb der Community gute Ratschläge gibt. Wenn ein Nutzer aber gleichzeitig eine akzeptable Anonymität seines Pseudonyms wahren möchte, muss er zwischen der implizit aufgebauten Reputation und der Unverkettbarkeit seiner Handlungen abwägen. Dies mag ein Grund sein, explizite Reputation eines Pseudonyms zu etablieren, die mit Hilfe eines Reputationssystems auf Basis von Erfahrungen anderer Nutzer mit

diesem Pseudonym berechnet wird. Explizite Reputation erlaubt einem Nutzer, anonym innerhalb aller Nutzer mit der gleichen Reputation zu sein, so lange seine Interaktionsgeschichte nicht öffentlich ist. Wenn Pseudonyme jedoch in vielen Interaktionen und über eine lange Zeit genutzt werden, wird die Anzahl der Pseudonyme mit der gleichen Reputation recht klein werden. Datenschutzfreundliche Reputationssysteme [Stei_06] versuchen diesem Problem zu begegnen.

Die Praxis wird zeigen, für welche Arten von Interaktionssystemen IDM-Systeme noch weitergehender ausgebaut werden müssen.

5 Ausblick

Nur nutzerkontrolliertes Identitätsmanagement ist in der Lage, die auftretenden Anforderungen verschiedener Akteure bei Interaktionen im Internet in gegenseitigem Einvernehmen zu erfüllen. Diese Ansicht hat sich inzwischen auch außerhalb des Wissenschaftsbereichs in der Wirtschaft durchgesetzt wie u.a. der Vorstoß von Microsoft mit MS Cardspace[3] zeigt.

Es bleibt allerdings abzuwarten, inwiefern Betreiber von Diensten auch willens sind, solche IDM-Systeme zu integrieren, und inwiefern Nutzer sie auch verstehen und benutzen lernen. Nicht zuletzt stellt sich hierbei die Frage, wie Nutzer auch unabhängig von Diensten bei der Interaktion miteinander im Internet lernen, sorgsam mit ihren Identitätsdaten umzugehen.

6 Literatur

[BaMe_05] Matthias Bauer and Martin Meints (Editors). Structured Overview on Prototypes and Concepts of Identity Management Systems; FIDIS Del. 3.1. Available from http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview on IMS.pdf, 2005.

[BeFK_01] Oliver Berthold, Hannes Federrath, and Stefan Köpsell. Web mixes: A system for anonymous and unobservable internet access. In Hannes Federrath,editor, Designing Privacy Enhancing Technologies (PET'00), LNCS 2009, pages 115–129, New York, NY, USA, 2001. Springer-Verlag.

[BDFL_05] Katrin Borcea, Hilko Donker, Elke Franz, Katja Liesebach, Andreas Pfitzmann, and Hagen Wahrig. Intra-application partitioning of personal data. In Proceedings of Workshop on Privacy-Enhanced Personalization (PEP 2005), Edinburgh, UK, 2005.

[BHLP_06] Katrin Borcea-Pfitzmann, Marit Hansen, Katja Liesebach, Andreas Pfitzmann, and Sandra Steinbrecher. What user-controlled identity management should learn from communities. Information Security Technical Report, 11(3):119–128, 2006.

[BHLP_07] Katrin Borcea-Pfitzmann, Marit Hansen, Katja Liesebach, Andreas Pfitzmann, and Sandra Steinbrecher. Managing one's identities in organisational and social settings. DuD, Datenschutz und Datensicherheit, 31(9):671–675, 2007.

[Bran_99] Stefan A. Brands. Rethinking Public Key Infrastructures and Digital Certificates - Building in Privacy. Dissertation, Netherlands, 1999. 2nd Edition: The MIT Press; August 2000.

[Bro04] Der Brockhaus in Text und Bild 2004. Bibliographisches Institut F. A. Brockhaus AG, Mannheim, 2004.

[CaLy_01] Jan Camenisch and Anna Lysyanskaya. An efficient system for nontransferable anonymous credentials with optional anonymity revocation. In EUROCRYPT '01: Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, pages 93–118, London, UK, 2001. Springer-Verlag.

[CC_98] Common criteria for information technology security evaluation - part 2: Security functional requirements. Version 15408-2 FDIS, ISO/IEC SC27 N2162, 15 November 1998.

[Chau_81] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 4(2):84–88, February 1981.

[Chau_86] David Chaum. Showing credentials without identification. Signatures transferred between unconditionally unlinkable pseudonyms. In Advances in Cryptology - EUROCRYPT '85, Workshop on the Theory and Application of of Cryptographic Techniques, pages 241–244, New York, NY, USA, 1986. Springer-Verlag.

3 http://msdn.microsoft.com/en-us/library/ms733090.aspx

[ClKo_01] Sebastian Clauß and Marit Köhntopp. Identity management and its support of multilateral security. Computer Networks, 37(2):205–219, October 2001.

[CPHH_02] Sebastian Clauß, Andreas Pfitzmann, Marit Hansen, and Els Van Herreweghen. Privacy-enhancing identity management. The IPTS Report, 67:8–16, September 2002.

[DiMS_04] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second generation onion router. In Proceedings of the 13th USENIX Security Symposium, August 2004.

[ECDir_95] Directive 95/46 EC. Official Journal L281,23/11/1995 pp. 31-50.

[FBWB_06] Elke Franz, Alexander Böttcher, Hagen Wahrig, and Katrin Borcea-Pfitzmann. Access control in a privacy-aware elearning environment. In Proceedings of AReS 2006, Workshop on Security in eLearning (SEL), Vienna, 2006.

[PK_08] Andreas Pfitzmann and Marit Köhntopp. Anonymity, unobservability, and pseudonymity - a proposal for terminology. Version 0.8 in: Hannes Federrath (Ed.): Designing Privacy Enhancing Technologies; Proc. Workshop on Design Issues in Anonymity and Unobservability, Lecture Notes in Computer Science 2009, 2001, pp. 1-9, Andreas Pfitzmann and Marit Hansen: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology. Version 0.30 in: Rene Balzer, Stefan Köpsell, Horst Lazarek (Hg.): Fachterminologie Datenschutz und Datensicherheit Deutsch - Russisch - Englisch; FGI - Forschungsgesellschaft Informatik, Technische Universität Wien, Wien, Februar 2008, 111-144. Version 0.31 available from http://dud.inf.tu-dresden.de/literatur/Anon Terminology v0.31.pdf, 2008.

[Stei_06] Sandra Steinbrecher. Design options for privacy-respecting reputation systems within centralised internet communities. In Proceedings of IFIP Sec 2006, 21st IFIP International Information Security Conference: Security and Privacy in Dynamic Environments, May 2006.

[VoKe_83] Victor L. Voydock and Stephen T. Kent. Security mechanisms in high-level network protocols. ACM Computing Survey, 15(2):135–171, 1983.

[WoPf_00] Gritta Wolf and Andreas Pfitzmann. Properties of protection goals and their integration into a user interface. Computer Networks, 32(6):685–699, 2000.

[Zim_80] Hubert Zimmermann. OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection. IEEE Transactions on Communications, 28(4):425–432, April 1980.

[ZSI_89] Zentralstelle für Sicherheit in der Informationstechnik (Hrsg.). ITSicherheitskriterien; Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT). 1. Fassung vom 11.1.1989; Köln, Bundesanzeiger, 1989.