Michael Bartsch, Bernd Lutterbeck (Hrsg.): Neues Recht für neue Medien, Informationstechnik und Recht 7, Schriftenreihe der DGRI, Verlag Dr. Otto Schmidt, Köln 1998, 319-328.

Anonymität, Authentizität und Identifizierung im Internet

Hannes Federrath, Andreas Pfitzmann
TU Dresden, Fakultät Informatik, 01062 Dresden

1 Einleitung

Der Nutzer des heutigen Internet begegnet zunehmend der Fragestellung, wie sicher das globale Kommunikationsmedium Internet überhaupt ist. Eine Pauschalaussage hierzu läßt sich nicht treffen. Allein durch die gegenläufigen Anforderungen Anonymität, Authentizität und Identifizierbarkeit wird deutlich, daß Sicherheitsaussagen stets im Zusammenhang mit den Umständen der Kommunikation gesehen werden müssen, d.h. welche Sicherheitseigenschaften (Schutzziele) für wen, gegen wen, für welches Anwendungsfeld etc. gelten. Trotz ihrer Gegenläufigkeit schließen sich Schutzziele nicht unbedingt gegenseitig aus. Es ist technisch durchaus möglich, Anonymität und zugleich Authentizität zu realisieren. Den technischen Hintergrund sowie Arbeiten zu den Rahmenbedingungen für Sicherheit liefert z.B. [MüPf_97].

2 Begriffe: Anonymität, Authentizität und Identifizierung

Anonymität: Eine Instanz, d.h. ein Rechenprozeß oder eine Person, ist dann anonym, wenn ein Angreifer keine Möglichkeit hat, Ereignisse (z.B. Kommunikation), an denen die Instanz beteiligt ist, so miteinander zu verketten, daß ihre Identität offengelegt wird. Hierzu untersucht er z.B. zeitliche Korrelationen, ausgetauschtes Datenvolumen oder Ursprungsorte eines Kommunikationsereignisses.

Authentisierung bezeichnet einen Prozeß, bei dem Instanzen (und ggf. auch ihre Nachrichten oder „Willenserklärungen“) auf Authentizität (Echtheit) überprüft werden. Durch eine erfolgreiche Authentisierung erhält die Instanz schließlich die Berechtigung, eine Funktion (z.B. Zugriff auf Daten) auszuführen.

Identifizierung dient dazu, die Identität von Instanzen festzustellen. In der Regel besitzt jede Instanz nur eine Identität, kann aber mehrere Pseudonyme besitzen.

3 Anonymität im Internet — bisher eine Illusion

Anonymität im heutigen Internet *ist* eine Illusion. Jeder mittelmäßig fähige Angreifer ist in der Lage, Teilnehmer im Internet zu überwachen. An jedem Knotenpunkt im Internet fallen Daten darüber an, von welchem Rechner die vorbeikommenden Datenpakete stammen und zu welchen sie geschickt werden. Diese ***Verkehrsdaten*** geben Aufschluß über das Verkehrsverhalten der Internetnutzer.

Die folgenden Beispiele zeigen für Electronic Mail und World Wide Web, wie solche Verkehrsdaten aussehen.

```
>tail syslog
Oct 15 16:32:06 tcs sendmail: from=<feder@tcs.inf.tu-dresden.de>, size=1150, class=0
Oct 15 16:32:06 tcs sendmail: to=<hf2@irz.inf.tu-dresden.de>, delay=00:00:01, stat=Sent
Oct 15 16:32:07 tcs sendmail: to=<federrath@inf.tu-dresden.de>, delay=00:00:03, stat=Sent
```

Electronic Mail: Log-Dateien zeigen Kommunikationsbeziehungen

Die Auswertung einer solchen Log-Datei ergibt, daß der Nutzer mit der Mailadresse feder@tcs.inf.tu-dresden.de am 15. Oktober um 16 Uhr 32 Minuten eine Nachricht mit einer Länge von 1150 Byte an die Empfängeradressen hf2@irz.inf.tu-dresden.de und federrath@inf.tu-dresden.de gesendet hat. Ebenso ist der Empfang von Nachrichten dokumentierbar.

Einer Mailadresse einen Nutzernamen zuordnen, ist sehr leicht. Man möchte z.B. wissen, wer hinter dem Empfänger hf2@irz.inf.tu-dresden.de steckt, und erhält als Antwort „Hannes Federrath“:

```
>finger hf2@irz.inf.tu-dresden.de
[irz.inf.tu-dresden.de]
Hannes Federrath (hf2) is not presently logged in.
Last seen at irz.inf.tu-dresden.de on Wed Oct  1 13:34:17 1997
```

Finger: Die Zuordnung zu Personen fällt nicht schwer

Auch im World Wide Web entstehen Log-Dateien, über die feststellbar ist, wer zu welcher Zeit auf welche Daten eines World-Wide-Web-Servers zugreift:

```
wwwtcs.inf.tu-dresden.de>tail access_log
amadeus.inf.tu-dresden.de - - [15/Oct/1997:11:50:01 +0200] "GET
/lvbeschr/winter/TechnDS.html HTTP/1.0" 304 - "http://wwwtcs.inf.tu-dresden.de/IKT/"
"Mozilla/3.01 (X11; I; SunOS 5.5.1 sun4u)"
```

World Wide Web: Log-Dateien zeigen Interessensdaten

Hier hat der Rechner amadeus.inf.tu-dresden.de vom Server die URL (Uniform Ressource Locator) http://wwwtcs.inf.tu-dresden.de/lvbeschr/winter/TechnDS.html aufgerufen, und zwar von der Seite http://wwwtcs.inf.tu-dresden.de/IKT/. Will man wissen, welche Person der Aufrufer der Seite ist, kann beispielsweise wieder mit finger nachgefragt werden:

```
ithif19 logs 17 >finger @amadeus.inf.tu-dresden.de
[amadeus.inf.tu-dresden.de]
Login       Name               TTY         Idle    When    Where
feder    Hannes Federrath      console           Wed 11:56
```

Finger: Die Ermittlung eines Rechnerbenutzers ist kein Problem

4 Auswege

Trotz dieser Beobachtungsmöglichkeiten ist Anonymität im heutigen Internet machbar, wenn die technischen Möglichkeiten genutzt werden. Konzepte zur Realisierung von Anonymität und Unbeobachtbarkeit [Chau_81, Pfit_90] sind für die wichtigsten Internetdienste (Electronic Mail, World Wide Web, File Transfer u.a.) vorhanden und teilweise bereits implementiert, siehe z.B.

- http://www.anonymizer.com/,
- http://www.itd.nrl.navy.mil/ITD/5540/projects/onion-routing/ oder
- http://www.obscura.com/~loki/remailer-essay.html.

Damit können Internetnutzer schon heute unbeobachtbar und anonym im Netz „surfen“ und Daten austauschen, vorausgesetzt, sie verfügen über entsprechendes Wissen, wie sie sich schützen können. Einfache Lösungen, wie Proxydienste und Firewalls genügen hier jedoch nicht! Von der breiten Masse der Nutzer bleiben diese Möglichkeiten jedoch noch ungenutzt.

Gleichwohl ist trotz der Nutzung von Anonymitätsverfahren im Extremfall ein ***„Aufdecken“ des Nutzerverhaltens*** möglich. Damit stehen im Bedarfsfall Daten zur gezielten Überwachung von einzelnen Teilnehmern zur Verfügung. — Eine „orwellsche“ Überwachbarkeit der Massen im großen Stil wird durch die Verfahren jedoch verhindert. Somit ist ein demokratischer Staat durchaus in der Lage, seine Sicherheitsaufgaben vernünftig zu erfüllen und entgeht gleichzeitig dem Vorwurf, Massenüberwachung zu wollen.

Technisch wird dieses „Aufdecken“ realisiert, indem die Anonymitätsdienste des Netzes im Bedarfsfall aufgefordert werden, geheime Daten zur Verfügung zu stellen, die im regulären Betrieb verarbeitet wurden. Es müssen für die Aufdeckbarkeit in der Regel keine zusätzlichen Speicherfunktionen implementiert sein. Ist das Anonymitätsverfahren „gut“, führt die Herausgabe solcher Daten zur Deanonymisierung einer verdächtigen Person, wobei der Schutz der anderen Teilnehmer weitgehend unbeeinträchtigt bleibt. Solche Aufdeckungsmöglichkeiten wurden u.a. in [Chau_81] und [Pfit_90] erörtert.

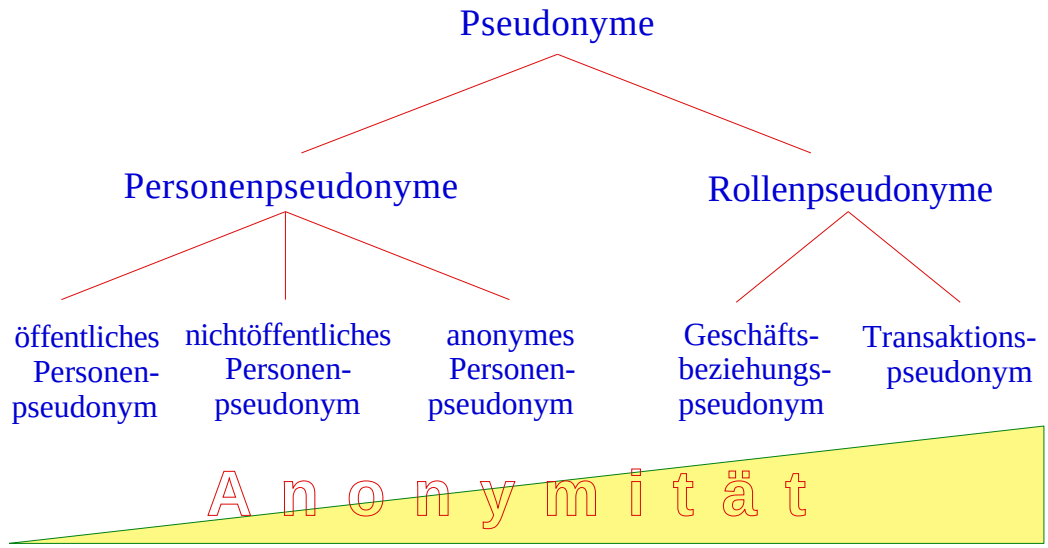
5 Authentizität und Identifizierung

Ob Daten „richtig“ sind, d.h., ob Daten eine adäquate Beschreibung der Wirklichkeit darstellen, ist *innerhalb* des technischen Systems nicht feststellbar. Es ist lediglich überprüfbar, ob die

Daten bei ihrem Transport durch das Netz oder bei ihrer Speicherung unverfälscht geblieben sind. Mit Hilfe kryptographischer Methoden ist weiterhin prüfbar, ob Nachrichten von einer bestimmten Instanz (z.B. Person oder Personengruppe) stammen. Message Authentication Codes (MACs) und Digitale Signaturen finden hierzu Verwendung.

Pseudonymitätskonzepte [Chau_81, Chau_85] erlauben es dem Nutzer, Anonymität und Authentizität in Einklang miteinander zu bringen, vorausgesetzt, die technischen Möglichkeiten werden ausgeschöpft. Eine Übersicht hierzu findet sich z.B. in [PWP_90]. Man unterscheidet Personen- und Rollenpseudonyme, die bezüglich ihrer Anonymität skalierbar sind. Einige dieser Pseudonyme erlauben im Streitfall eine Identifizierung des Pseudonymbenutzers. Damit sind auch Rechtsgeschäfte durchaus pseudonym realisierbar.

In [PWP_90] wurden die verschieden Arten von Pseudonymen grob eingeteilt (siehe folgende Abbildung aus [PWP_90]).



Pseudonyme sind skalierbar in ihrem Personenbezug

Ein Pseudonym wird als ***Personenpseudonym*** bezeichnet, wenn sein Besitzer es für viele verschiedene Geschäftsbeziehungen über lange Zeit hinweg verwendet, es somit einen Namensersatz darstellt. Hinsichtlich der Verkettungsmöglichkeiten eines Personenpseudonyms mit seinem Besitzer stellt es ein potentielles Personenkennzeichen dar. Es können drei Arten von Personenpseudonymen unterschieden werden: Bei öffentlichen Personenpseudonymen ist die Zuordnung zu einer Person im allgemeinen bekannt (z.B. Telefonnummern), bei nichtöffentlichen Personenpseudonymen ist diese Zuordnung nur wenigen Stellen bekannt (z.B. nicht im Teilnehmerverzeichnis aufgeführte Telefonnummern) und bei anonymen Personenpseudonymen ist diese Zuordnung nur dem Besitzer bekannt.

In einem Streitfall ist man zumindest bei den öffentlichen und nichtöffentlichen Personenpseudonymen in der Lage, die Verkettung zwischen der Identität und dem Pseudonym herzu-

stellen. Damit kann eine Person trotz Pseudonymverwendung verfolgt werden, falls dies erforderlich ist.

Bei anonymen Personenpseudonymen besteht innerhalb des Kommunikationsnetzes keine direkte Möglichkeit zur Verkettung mit einer Identität. Da sich jedoch bei jeder Pseudonymbenutzung personenbezogene Daten ansammeln, besitzt man nach einer gewissen Zeit genug Informationen zur Deanonymisierung des anonymen Personenpseudonyms. Über Kontextinformationen, z.B. die zeitlich oder örtlich verkettete Beobachtung einer verdächtigen Person bei nicht anonymen Handlungen (u.U. auch außerhalb des Kommunikationsnetzes) kann ein Bezug zur Identität der Person hergestellt werden.

Rollenpseudonyme sind im Gegensatz zu Personenpseudonymen nicht einer Person, sondern *nur* ihrer momentan ausgeübten Rolle zugeordnet. Geschäftsbeziehungspseudonyme sind solche Rollenpseudonyme, die für viele Transaktionen verwendet werden, z.B. eine Kontonummer bei den vielen Buchungen eines Kontos. Transaktionspseudonyme hingegen werden nur für eine Transaktion verwendet, z.B. Kennwörter bei anonym aufgegebenen Chiffreanzeigen. Bei Verwendung von Rollenpseudonymen können verschiedene Parteien über den Pseudonymträger gesammelte Information zumindest nicht einfach über die Gleichheit von Pseudonymen, sondern allenfalls über Korrelation von Zeiten, Geldbeträgen etc. verketten. Aber trotzdem besteht bei Geschäftsbeziehungspseudonymen die Gefahr, daß bei intensiv genutzten Beziehungen der Partner genügend pseudonymbezogene Information zur Deanonymisierung erhält. Aus der Sicht des Datenschutzes sollten daher, wenn immer möglich, Transaktionspseudonyme verwendet werden.

6 Authentizität und pseudonymes Handeln im Internet

Da im heutigen Internet die Authentizität von Nachrichten und Absendern praktisch nicht gewährleistet ist, kann sich jeder Internetnutzer beliebige Kennzeichen erzeugen, unter denen er erreichbar ist und handelt damit de facto pseudonym.

Die Basismechanismen des Internet sind nicht darauf ausgerichtet, Angriffe auf die ***Authentizität von Nachrichten*** und ihrem Absender zu verhindern. Ein herausragendes Beispiel hierfür ist Electronic Mail, bei dem das Fälschen des Absenders und damit z.B. das Versenden einer Mail unter dem Namen einer anderen Person ein Kinderspiel ist [DaFS_96, Fox_95].

Durch zusätzliche Sicherungsfunktionen sollen die Internetnutzer dazu befähigt werden, sich selbst zu schützen. Oft steht dabei die Vertraulichkeit der Daten (Verschlüsselung) im Vordergrund, jedoch bieten die meisten Mechanismen ebenfalls Möglichkeiten zur authentisierten Kommunikation. Beispiele hierfür sind:

- ***PGP*** (http://www.pgp.com/ und http://www.ifi.uio.no/pgp/) – die bekannte Software Pretty Good Privacy und

- ***PEM*** (http://www.semper.org/sirene/outsideworld/security.html#prot.pem) – Privacy Enhanced Mail zur Sicherung von Electronic Mail im Internet,

- ***S-HTTP*** – Secure Hypertext Transfer Protocol zur Sicherung von Zugriffen im World Wide Web und

- ***SSL*** (http://home.netscape.com/newsref/std/SSL.html) – Secure Socket Layer zur Sicherung von Internetverbindungen, insbesondere im World Wide Web, jedoch auch für andere verbindungsorientierte Dienste verwendbar.

Authentisierte Kommunikation schränkt jedoch nicht unbedingt die Möglichkeiten zur pseudonymen Kommunikation ein. Vielmehr können Interaktionen zwischen Nutzern und Anbietern pseudonym laufen, solange sich beide Parteien an die vereinbarten Regeln halten.

Im Streitfall muß es jedoch Mechanismen zur Klärung eines Konflikts geben. Es existieren zwei grundsätzliche Möglichkeiten:

1. Im Streitfall erfolgt Pseudonymaufdeckung und anschließend ***Schadensregulierung*** wie im nichtanonymen Fall einer Interaktion. Die Pseudonymaufdeckung kann erfolgen

   a) durch eine ***Verkehrsanalyse*** im Netz. Hierbei wird nicht eigentlich das Pseudonym aufgedeckt, sondern es erfolgt die Zuordnung einer pseudonym gesendeten Nachricht zu ihrem Absender.

   b) durch eigens entwickelte ***Aufdeckungsfunktionen***. Im einfachsten Fall besitzt eine vertrauenswürdige Dritte Instanz im Netz die Zuordnung zwischen Identität und Pseudonym und wird im Bedarfsfall aufgefordert, diese preiszugeben.

2. ***Schadensverhinderung*** durch Einbeziehung eines „digitalen“ Treuhänders zur koordinierten Interaktion zwischen den bezeiligten Instanzen (z.B. Ware gegen Geld).

Die Pseudonymaufdeckung nach 1.*a)* ist etwas aufwendiger, führt allerdings zu geringeren Mißbrauchsmöglichkeiten als 1.*b)*, da eine solche bezüglich der Geheimhaltung von Daten vertrauenswürdige Dritte Instanz ein bevorzugtes Angriffsziel sein könnte. Im Fall 2. muß der Treuhänder selbst eine vertrauenswürdige Instanz sein. Außerdem sind die Mißbrauchsmöglichkeiten durch ihn größer, da er direkt in den Werte- bzw. Warenaustausch einbezogen ist. Dafür ist er jedoch vollständig kontrollierbar, denn er muß nichts geheimhalten, sondern nur die Integrität des Austauschs sichern. Hierbei wird angenommen, daß die Anonymität der Teilnehmer über einen entsprechenden Dienst (siehe Abschnitt 4) gesichert wird. Außerdem werden Transaktionspseudonyme verwendet.

7 Mehrseitige Sicherheit als umfassendes Schutzkonzept

Wie die vorangegangenen Ausführungen zeigen, sind die Möglichkeiten zum Schutz der Kommunikation noch nicht ausgeschöpft. Es existieren Konzepte, die das Vertrauen des Nut-

zers in zentrale Einrichtungen (Betreiber, vertrauenswürdige Dritte, Treuhänder etc.) erfordern. Häufig wird dieses Vertrauen implizit vorausgesetzt. Durch die zunehmende Sensibilisierung wächst jedoch das Interesse an Schutzkonzepten, die dieses Vertrauen nicht unbedingt fordern.

Es ist nicht das primäre Interesse eines Betreibers, beispielsweise Daten über seine Teilnehmer zu sammeln, um diese anschließend mißbräuchlich zu verwenden. Im Gegenteil: Je weniger Daten ein Betreiber zur Diensterbringung benötigt, umso weniger Kosten fallen für deren Verarbeitung und Schutz an. Damit wird das Ziel einer Betrachtungsweise und Methodik klar, die „Mehrseitige Sicherheit“ genannt wird.

Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen *aller* Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.

Die technische Basis für die Realisierung mehrseitiger Sicherheit sind

- sichere Endgeräte, d.h. Endgeräte, die sicher vor Ausforschung und gegen Angriffe durch alle anderen Beteiligten sind,
- Kryptosysteme und kryptographische Protokolle sowie
- ein Kommunikationsnetz, das den Nachrichtenaustausch effizient und für alle Beteiligten ermöglicht.

Die Bausteine mehrseitiger Sicherheit werden z.B. in [MüPf_97, S.83ff] erläutert.

Die Realisierung von mehrseitiger Sicherheit führt nicht zwangsläufig dazu, daß die Interessen aller Beteiligten erfüllt werden. Möglicherweise offenbart sie sogar gegensätzliche, unvereinbare Interessen, die den Beteiligten bisher nicht bewußt waren, da Schutzziele explizit formuliert werden. Sie führt jedoch zwangsläufig dazu, daß die Partner einer mehrseitig sicheren Kommunikationsbeziehung in einem geklärten Kräfteverhältnis miteinander interagieren.

8 Literatur

Chau_81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84-88.

Chau_85 David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete. Communications of the ACM 28/10 (1985) 1030-1044.

DaFS_96 Herbert Damker, Hannes Federrath, Michael J. Schneider: Maskerade-Angriffe im Internet. Eine Demonstration für Unsicherheit. Datenschutz und Datensicherung DuD 20/5 (1996), 286-294.

Fox_95 Dirk Fox: Schlüsseldienst - Private Kommunikation mit PEM und PGP, c't 9/95.

MüPf_97 Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Addison-Wesley-Longman, 1997.

Pfit_90 Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. IFB 234, Springer-Verlag, Heidelberg 1990.

PWP_90 Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.