Eingereichter PRIMA-Beitrag

Strafverfolgung trotz Anonymität

Rechtliche Rahmenbedingungen und technische Umsetzung

Stefan Köpsell, Tobias Miosga
Technische Universität Dresden, Institut für Systemarchitektur
{sk13,tm461052}@inf.tu-dresden.de

Zusammenfassung

Die Erfahrungen mit dem Betrieb eines Dienstes zum anonymen und unbeobachtbaren Websurfen zeigen, daß ein solcher Dienst auch in geringem Umfang zum Begehen von Straftaten mißbraucht wird. Das vorliegende Papier beschäftigt sich mit der Frage, wie eine datenschutzgerechte Deanonymisierung in solchen konkreten Einzelfällen durchgeführt werden kann, ohne die Anonymität der anderen Teilnehmer zu gefährden oder eine „Massenüberwachung auf Knopfdruck" zu ermöglichen.

Ausgehend von den bestehenden Gesetzen werden die Rechte und Pflichten des Anonymisierungsdienstes dargestellt. Es werden konkrete Vorschläge für eine „Strafverfolgungsfunktion" erläutert, wobei ein Lösungsvorschlag detailliert beschrieben wird. Neben den rechtlichen Rahmenbedingungen ist dabei insbesondere das dem Anonymisierungsdienst zugrunde liegende technische Verfahren und das damit verbundene Vertrauensmodell zu berücksichtigen. Es handelt sich um ein verteiltes System, bei dem es keine zentrale Instanz gibt, die eine Deanonymisierung einzelner Kommunikationsverbindungen vornehmen könnte. Vielmehr ist dafür die Mitarbeit aller Server des Anonymisierungsdienstes notwendig. Es wird beschrieben, wie sich diese überzeugen können, daß eine Deanonymisierung auch tatsächlich im Zusammenhang mit dem Verdacht auf eine Straftat steht.

Einleitung

Seit Januar 2000 wird an der Technischen Universität Dresden in Zusammenarbeit mit der Universität Regensburg und dem Unabhängigen Landeszentrum für Datenschutz (ULD) Schleswig-Holstein ein Dienst zur anonymen und unbeobachtbaren Internetkommunikation entwickelt. Seit September 2000 findet ein öffentlicher Testbetrieb zur Evaluierung dieses Anonymisierungsdienstes statt. Jeder kann sich von den Projektwebseiten die benötigte Software herunterladen und dann kostenfrei ausprobieren, d. h. anonym im Web surfen.

Leider (oder natürlich?) haben die Erfahrungen mit dem Betrieb des Anonymisierungsdienstes [FeKL02, KöFH03] gezeigt, daß der Dienst auch in geringem Maße mißbraucht wird. Im Zeitraum Januar - Juni 2004 gab es beispielsweise 22 Anfragen von Strafverfolgungsbehörden (Polizei, Staatsanwalt, Richter) im Zusammenhang mit einem strafrechtlich relevanten Anfangsverdacht. Im gleichen Zeitraum wurden pro Monat ca. 200 Millionen URLs abgerufen, wobei ein Datenvolumen von ca. 4 TByte übertragen wurde. Es waren ca. 1500-2500 Nutzer gleichzeitig beim Dienst angemeldet.

Das vorliegende Papier beschäftigt sich mit der Frage, wie eine Deanonymisierung zum Zwecke der Strafverfolgung in konkreten Einzelfällen (richterliche Anordnung) möglich ist, ohne den Dienst an sich in Frage zu stellen.

Im nachfolgenden Kapitel werden zunächst die Grundlagen besprochen. Dabei werden die für das Verständnis des Papiers notwendigen technischen Details des Anonymisierungsdienstes erläutert. Ferner wird ein Überblick gegeben über die gesetzlichen Rahmenbedingungen sowohl allgemein für den Betrieb

des Dienstes als auch speziell für die Durchführung einer Deanonymisierung. Aufbauend auf diese Grundlagen wird in Kapitel 2 erläutert, wie eine möglichst datenschutzfreundliche Deanonymisierung durchgeführt werden kann.

1 Grundlagen

Dieses Kapitel beschäftigt sich mit den zum Verständnis des Papiers notwendigen technischen Details des Anonymisierungsdienstes. Des weiteren werden die rechtlichen Rahmenbedingungen erläutert, die für den Betrieb des Dienstes maßgebend sind. Dabei wird zum einen ausgeführt, daß der Dienst in seiner angebotenen Form vollkommen legal ist. Zum anderen wird erläutert, unter welchen Umständen eine Deanonymisierung gesetzlich vorgeschrieben ist. Darüber hinaus werden die bisher durch den Betrieb des Dienstes gewonnen Erfahrungen bezüglich Strafverfolgung beschrieben.

1.1 Technische Umsetzung des Anonymisierungsdienstes

Basis des Anonymisierungsdienstes ist das von David Chaum 1981 entwickelte Verfahren der *umkodierenden Mixe* [Chau81]. Diese Mixe sind dabei in Form von *Kaskaden* hintereinander geschaltet. Das Basisverfahren wurde um den Mechanismus der *symmetrisch verschlüsselten Kanäle* erweitert [PfPW89]. Nachfolgend werden (vereinfacht) lediglich die grundlegenden Mechanismen des Verfahrens vorgestellt, die für das Verständnis bezüglich Strafverfolgung notwendig sind.

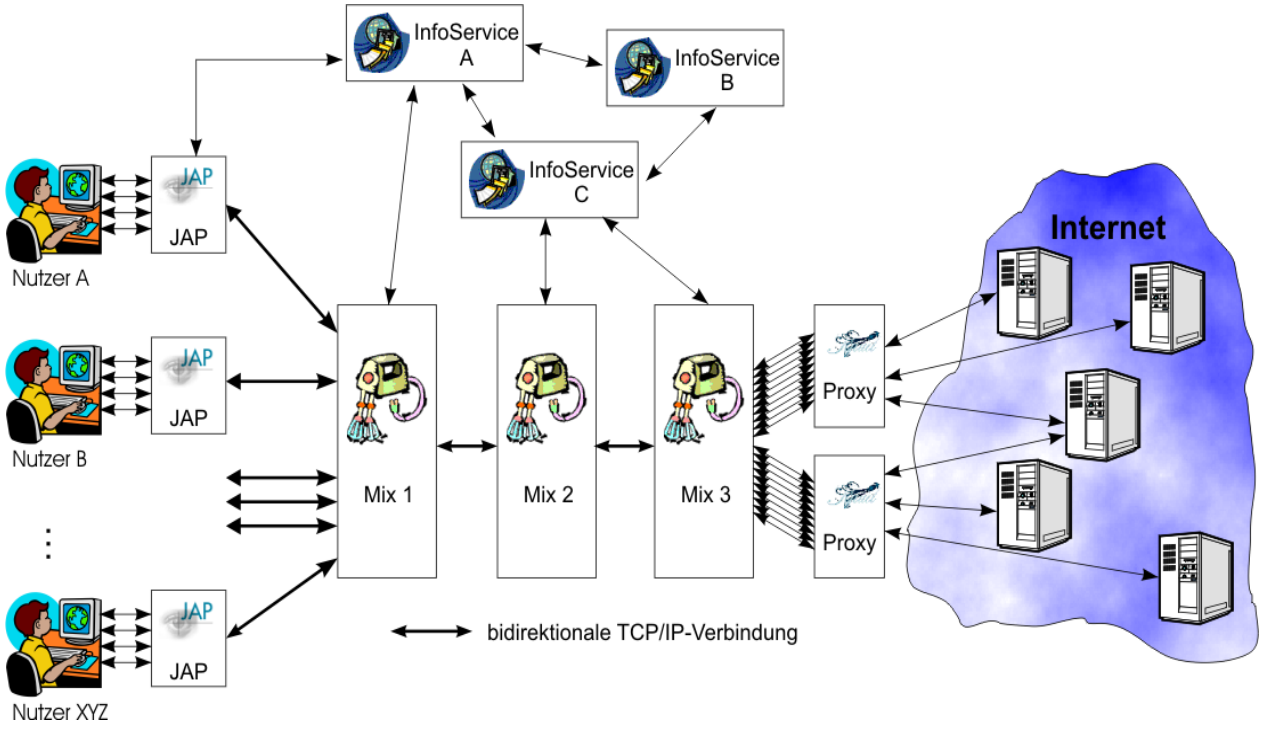

Abbildung 1: Architektur des Anonymisierungsdienstes AN.ON

Abbildung 1 gibt einen Überblick über das Gesamtsystem, das nachfolgend als AN.ON bezeichnet wird. Neben den für die eigentliche Anonymisierung zuständigen Mixen besteht es noch aus einem Client-Programm namens JAP, das jeder Nutzer auf seinem Rechner installieren muß. Der JAP nimmt die Anfragen des Webbrowsers entgegen, verschlüsselt sie gemäß Mixprotokoll und sendet sie an den ersten Mix einer vom Nutzer zuvor gewählten Kaskade. Ferner nimmt der JAP die über die Mixe zurückgesendete Ant-

wort des Webservers entgegen, entschlüsselt sie und sendet sie zur Darstellung an den Webbrowser weiter.

Ein dritter Bestandteil des Systems ist der sogenannte InfoService. Dabei handelt es sich im Wesentlichen um eine verteilte Datenbank, von der die Nutzer Informationen über vorhandene Mixkaskaden, deren Auslastung und das daraus resultierende Anonymitätsniveau abfragen können.

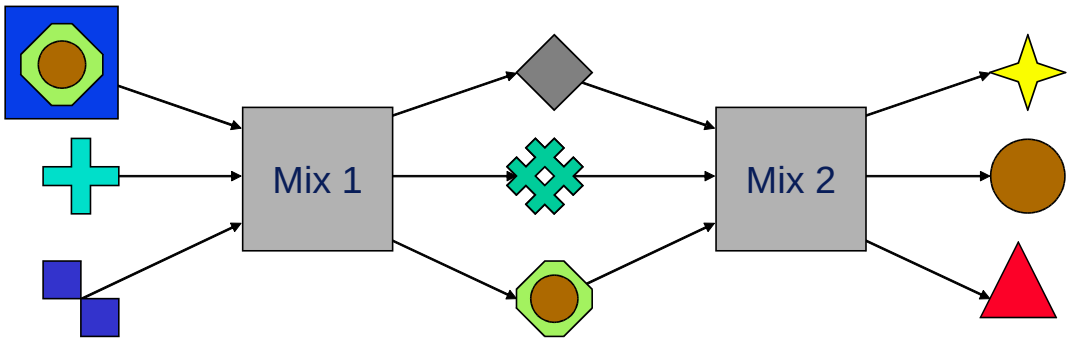

Abbildung 2: Das Mix-Verfahren: Umkodieren und Umsortieren als Basis der Unverkettbarkeit

Einen Mix kann man sich als einen Server im Internet vorstellen, der mehrfach verschlüsselte Nachrichten entgegennimmt, kryptographisch umkodiert (ent- bzw. verschlüsselt) und umsortiert wieder ausgibt (Abbildung 2). Alle Nachrichten (*Mixpakete*) sind dabei gleich lang. Ziel des Mix-Verfahrens ist es, die Zuordnung von ein- zu ausgehenden Nachrichten vor Außenstehenden (Angreifer) zu verbergen. Dies soll selbst dann der Fall sein, wenn der Angreifer in der Lage ist, die auf den Leitungen übertragenen Daten zu belauschen bzw. zu manipulieren (verändern, löschen, eigene hinzufügen).

Anonymität im Sinne der Mixe bedeutet nicht, daß Sender bzw. Empfänger sich unter einer „Tarnkappe“ verbergen. Es ist für einen Beobachter sehr wohl ersichtlich, wer alles Nachrichten zu einem Mix gesendet und wer alles Nachrichten von einem Mix empfangen hat. Durch die Unverkettbarkeit von ein- zu ausgehenden Nachrichten kennt der Beobachter jedoch nur die Menge aller Sender und die Menge aller Empfänger – die Kommunikationsbeziehung, d. h. wer an wen welche Nachrichten gesendet hat, bleibt für ihn jedoch verborgen.

Zur Gewährleistung der Anonymität gegenüber Außenstehenden würde bereits die Verwendung eines einzigen Mix ausreichen. Allerdings erfährt dieser eine Mix dann alle Kommunikationsbeziehungen. Die Nutzer müßten ihm daher vertrauen. Um diese Annahme abzuschwächen und gleichzeitig Schutz auch gegen die Betreiber des Systems zu erreichen, werden mehrere Mixe in Form einer statischen Kette, einer sogenannten Kaskade, hintereinander geschaltet. Ein Nutzer muß jetzt nur noch darauf vertrauen, daß nicht alle Mixe einer Kaskade zusammenarbeiten, d. h. für die Deanonymisierung einer gegeben Kommunikationsbeziehung ist es notwendig, daß *alle* Mixe ihr Wissen über die jeweilige Ein-/Ausgabezuordnung zusammenlegen, um so den kompletten Weg vom Sender zum Empfänger zu rekonstruieren. Um die Vertrauenswürdigkeit einer Kaskade zu erhöhen, sollten die einzelnen Mixe von möglichst unabhängigen Organisationen betrieben werden. Der Nutzer kann im JAP auswählen, welche Kaskade er verwenden möchte.

Bei dem ursprünglichen, von Chaum veröffentlichten Mix-Verfahren wird pro Nachricht und Mix mindestens eine asymmetrische Kryptooperation für das Umkodieren benötigt. Asymmetrische Kryptographie hat generell einen wesentlich höheren Rechenaufwand verglichen mit symmetrischer Kryptographie. Um die Leistungsfähigkeit des Anonymisierungsdienstes zu erhöhen, wird deshalb das Verfahren der symmetrisch verschlüsselten Kanäle verwendet. Dabei wird zunächst ein asymmetrisch (oder ge-

nauer: hybrid) verschlüsseltes Kanalaufbaupaket übertragen. Dieses enthält einen Schlüssel eines symmetrischen Kryptoverfahrens, daß zur Umkodierung der weiteren über den Kanal übertragenen Daten verwendet wird. Jedes Datenpaket enthält dabei eine Kanalnummer, so daß der Mix weiß, welcher Schlüssel zu verwenden ist.

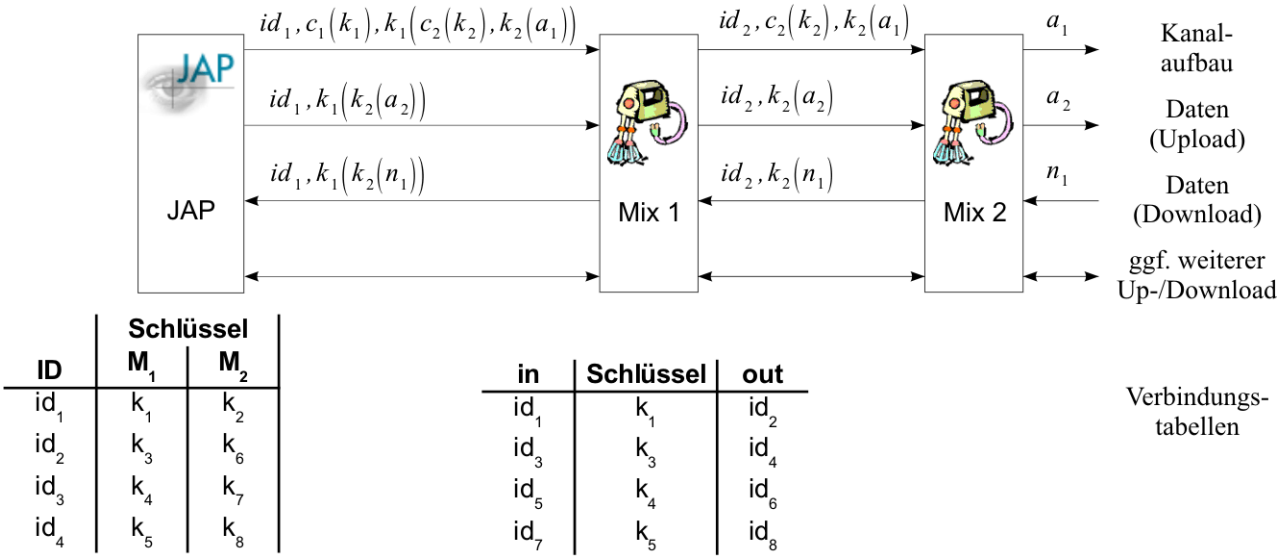

Abbildung 3: Beispiel für Kanalaufbau und Datenübertragung

Das nachfolgende Beispiel soll den prinzipiellen Ablauf verdeutlichen (siehe auch Abbildung 3). Gegeben sei eine Mixkaskade aus den zwei Mixen M_1 und M_2, die jeweils ein Schlüsselpaar eines asymmetrischen Kryptosystems erzeugt haben. c_1, c_2 seien die zugehörigen öffentlichen Verschlüsselungsschlüssel. Ferner seien $a_1 \ldots a_n$ die Bestandteile einer Anfrage a.
Das Kanalaufbaupaket wird nun gebildet, indem der JAP eine zufällige (lokal eindeutige) Kanalnummer id_1 und zufällige Schlüssel k_1, k_2 generiert und an den ersten Mix folgendes sendet:

$$JAP \rightarrow M_1: \; id_1, c_1(k_1), k_1(c_2(k_2), k_2(a_1))$$

Der erste Mix entschlüsselt das Paket, speichert in seiner Verbindungstabelle id_1, k_1 und eine neue lokal eindeutige, zufällig generierte Kanalnummer id_2. Das entschlüsselte Paket sendet er an den zweiten Mix weiter, wobei er id_1 durch id_2 ersetzt:

$$M_1 \rightarrow M_2: \; id_2, c_2(k_2), k_2(a_1)$$

Der zweite Mix speichert nach Entschlüsselung in seiner Verbindungstabelle id_2, k_2 und die Adresse des Empfängers. Ferner sendet er a_1 an diesen.

Zur Übermittlung der weiteren Bestandteile a_i der Anfrage muß der JAP diese nur noch symmetrisch mit k_1 und k_2 verschlüsseln:

$$JAP \rightarrow M_1: \quad id_1, k_1(k_2(a_i))$$
$$M_1 \rightarrow M_2: \quad id_2, k_2(a_i)$$
$$M_2 \rightarrow Empfänger: \quad a_i$$

Soll vom Empfänger eine Antwort n bestehend aus den Bestandteilen $n_1 \ldots n_l$ über den vorhandenen Kanal zurück an den JAP übertragen werden, so werden diese Daten von den einzelnen Mixen der Reihe nach verschlüsselt. Da der JAP alle Schlüssel kennt, kann er das empfangene, mehrfach verschlüsselte Paket entschlüsseln:

$$\begin{aligned} &Empfänger \rightarrow M_2: && n_1 \\ &M_2 \rightarrow M_1: && id_2, k_2(n_1) \\ &M_1 \rightarrow JAP: && id_1, k_1(k_2(n_1)) \end{aligned}$$

Das dem Anonymisierungsdienst zugrundeliegende Protokoll sieht eine Möglichkeit zum Austausch von Steuerinformationen zwischen benachbarten Mixen bzw. dem JAP und dem ersten Mix vor. Diese Informationen werden in sogenannten *Steuerkanälen* übertragen. Ein Steuerkanal faßt dabei mehrere logisch zusammengehörige Steuernachrichten (Pakete) zusammen. Diese Nachrichten werden auf der selben TCP/IP Verbindung übertragen, auf der auch die Mixpakete übertragen werden. Sie besitzen einen ähnlichen Aufbau wie diese und lassen sich von ihnen durch einen reservierten Bereich von Kanalnummern unterscheiden. Der Datenteil eines solchen Steuerpakets enthält die zu übertragende Steuernachricht. Steuerkanäle sind grundsätzlich verbindungsverschlüsselt und integritätsgesichert.

1.2 Rechtliche Rahmenbedingungen

Die nachfolgenden Ausführungen sollen das Verständnis der Autoren bezüglich der rechtlichen Rahmenbedingungen erläutern. Dabei sei darauf hingewiesen, daß die Erläuterungen sicher nicht den Normen für juristische Aufsätze genügen, da keiner der Autoren einen entsprechenden Hintergrund hat. Vielmehr geht es darum, zu vermitteln, was ausgehend von der Literatur zum Thema und Konsultation der Juristen des Projektpartners Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein als Grundlage für die technische Umsetzung der „Strafverfolgungsfunktion“ angenommen wurde. Auch wenn absolute Aussagen im juristischen Umfeld generell schwierig sind, so existieren zumindest zwei richterliche Beschlüsse, die man durchaus als herrschende Meinung ansehen kann. Die Verweise auf die Gesetze und die juristische Fachliteratur ermöglichen es dem Leser darüber hinaus, sich gegebenenfalls eine eigene Meinung zu bilden.

Neben allgemein gültigen Gesetzen und Verordnungen wie z. B. dem Grundgesetz (GG), dem Außenwirtschaftsgesetz (AWG), dem Gesetz zur Beschränkung des Brief-, Post-, und Fernmeldegeheimnisses (G10-Gesetz), der Strafprozessordnung (StPO) oder dem Bundesdatenschutzgesetz (BDSG) etc. bestimmen insbesondere auch bereichsspezifische Vorschriften den rechtlichen Rahmen. Dazu zählen im Bereich der „Neuen Medien“ bzw. der Tele- und Internetkommunikation z. B. das Telekommunikationsgesetz (TKG), der Mediendienste-Staatsvertrag (MDStV), das Teledienstegesetz (TDG), die Telekommunikationsüberwachungsverordnung (TKÜV), die Telekommunikations-Datenschutzverordnung (TDSV), das Teledienstedatenschutzgesetz (TDDSG) etc.

Aus rechtlicher Sicht ist es zunächst wichtig zu entscheiden, um welche Art von Dienst es sich bei dem Anonymisierungsdienst handelt (Mediendienst, Telekommunikationsdienst bzw. Teledienst) und unter welchen rechtlichen Regelungsrahmen er folglich fällt.

Telekommunikationsdienste sind nach § 3 Nr. 24 TKG in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdiensten in Rundfunknetzen. Teledienste hingegen sind nach § 2 Abs. 1 TDG elektronische Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bildern oder Tönen bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt. Hierzu gehören u. a. sowohl der Bereich der Individualkommunikati-

on (§ 2 Abs. 2 Nr. 1 TDG), wie auch Angebote zur Information oder Kommunikation, soweit nicht die redaktionelle Gestaltung zur Meinungsbildung für die Allgemeinheit im Vordergrund steht (§ 2 Abs. 2 Nr. 2 TDG), als auch Angebote zur Nutzung des Internet oder weiterer Netze (§ 2 Abs. 2 Nr. 3 TDG). Mediendienste schließlich sind Angebote und die Nutzungen von an die Allgemeinheit gerichteten Informations- und Kommunikationsdiensten (§ 2 Abs. 1 MDStV), worunter insbesondere redaktionell betreute Dienste verstanden werden.

Unter welchen Begriff ein Anonymisierungsdienst fällt, ist umstritten. Als gesichert dürfte dabei nur gelten, daß es sich nicht um einen Mediendienst im Sinne § 2 MDStv handelt, da es an jeglicher irgendwie gearteter redaktionellen Aufarbeitung von Inhalten fehlt.

„Die Zuordnung von Anonymisierungsdiensten zum TDG oder TKG ist in der Literatur umstritten." [Raa03]. Während z. B. in [Raa03] resümiert wird, daß „auch für den AN.ON-Dienst von einer Einordnung sowohl als Telekommunikations- als auch als Teledienst auszugehen" ist, wird in [Gol3, FeGo04] davon ausgegangen, daß es sich um einen reinen Teledienst handelt. Beide Auffassungen bestätigen jedoch die Wirksamkeit der im TDDSG getroffenen Regelungen, insbesondere der im § 3 festgeschriebenen Grundsätze, nach denen gilt: „Personenbezogene Daten dürfen vom Diensteanbieter zur Durchführung von Telediensten nur erhoben, verarbeitet und genutzt werden, soweit dieses Gesetz oder eine andere Rechtsvorschrift es erlaubt oder der Nutzer eingewilligt hat" (Absatz 1). Außerdem zu beachten ist die nach § 4 Absatz 6 geltende Verpflichtung, die „Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist." Der Anonymisierungsdienst stellt praktisch eine mögliche technische Umsetzung dieses Gebots da.

Gleichwohl gelten für den Dienst natürlich die allgemeinen Vorschriften der Strafprozessordnung. Bezüglich der Anordnung von Überwachungsmaßnahmen der Telekommunikation sind dabei insbesondere die §§ 100 a, b und §§ 100 g, h zu beachten [Ger04, FeGo04]. Im Falle von §§ 100 g, h StPO ist „der Auskunftsanspruch allerdings auf solche Daten beschränkt, die ... nach bestehenden Regelungen zulässigerweise erhoben und gespeichert werden und insoweit bereits vorliegen" [FeGo04]. Da die Mixe gemäß den Vorgaben des TDDSG jedoch keine Daten speichern, wird ein entsprechender Beschluß nicht zum gewünschten Ergebnis führen. Zwar wird in [Ger04] davon ausgegangen, daß sehr wohl Daten gespeichert werden – nämlich die für die Realisierung des Dienstes technisch notwendige, kurzzeitige Erfassung von Datenstrukturen im Hauptspeicher der Mix-Server – jedoch wird dieser Auffassung in [FeGo04] widersprochen.

Für die Anordnung einer Überwachungsmaßnahme kommen somit ausschließlich die §§ 100 a, b StPO in Frage. Auf Grundlage dieser Paragraphen kann die Aufzeichnung personenbezogener Daten über die Nutzer für die Zukunft angeordnet werden. Dabei muß jedoch der Verdacht auf eine Straftat gemäß eines definierten Straftatenkatalogs vorliegen. Außerdem bedarf es grundsätzlich einer richterlichen Anordnung (§ 100 a Abs. 1 StPO). Diese ist auf maximal drei Monate befristet, kann aber jeweils um drei Monate verlängert werden (§ 100 a Abs. 2 StPO). Bei Gefahr im Verzug kann ausnahmsweise die Anordnung auch durch die Staatsanwaltschaft erfolgen. Diese ist dann jedoch höchstens drei Tage gültig und muß anschließend von einem Richter bestätigt werden.

„Entscheidend ist, dass eine Überwachung einer Kommunikationsbeziehung rechtlich ausschließlich im Einzelfall und bei Vorliegen eines richterlichen Beschlusses auf der Grundlage dieser Vorschriften zulässig sein kann. Die Anordnung einer Massenüberwachung aller Nutzer des Anonymisierungsdienstes kann auf Grund dieser Vorschriften nicht erfolgen" [WWW_1].

Zusammenfassend wird also davon ausgegangen, daß:

- der Betrieb des Anonymisierungsdienstes in seiner angebotenen Form im Einklang mit den geltenden gesetzlichen Regelungen steht,

- eine Vorratsspeicherung von Nutzungsdaten bezüglich des Dienstes zum Zwecke der Strafverfolgung nicht vorgeschrieben ist; vielmehr im Gegenteil die Speicherung dieser Daten rechtswidrig wäre,
- im Einzelfall eine Überwachung einer Kommunikationsbeziehung durch richterlichen bzw. staatsanwaltschaftlichen Beschluß angeordnet werden kann.

1.3 Erfahrungen aus dem Betrieb des Dienstes

Wie bereits in der Einleitung erwähnt, läßt die Mißbrauchsstatistik den Schluß zu, daß der Anonymisierungsdienst nicht in besonderem Maße zur Begehung strafbarer Handlungen benutzt wird. Anfragen von Strafverfolgungsbehörden (hauptsächlich Polizei, selten Richter oder Staatsanwalt) betrafen stets die Herausgabe von Daten, die der Identifizierung des Absenders einer über den Anonymisierungsdienst übertragenen Nachricht dienen könnten. Dabei wurden als Merkmale die IP-Adresse des letzten Mix der Kaskade und die betreffende Uhrzeit genannt. Da keine Logdateien geführt werden, konnten in keinem Fall sachdienliche Hinweise gegeben werden. Diese negativen Bescheide wurden ausnahmslos akzeptiert.

Die mißbräuchliche Nutzung selbst betraf größtenteils Beleidigungen, die anonym in Chats, Newsgroups und Foren geäußert wurden, sowie die Erschleichung von Leistungen unter Angabe von gefälschten Kreditkarten bzw. Bankverbindungsdaten.

Einzige Ausnahme des oben beschriebenen Musters bildet der sogenannte BKA-Fall [Gol03a, Kra04]. Dabei erging auf Betreiben des BKA eine richterliche Anordnung vom Amtsgericht Frankfurt/Main, die AN.ON verpflichtete, Daten zu speichern, die zur Identifizierung des Initiators von Verbindungen zu einer bestimmten Ziel-IP-Adresse hilfreich sind. Da diese Anordnung auf falscher gesetzlicher Grundlage (§§ 100 g, h StPO) erfolgte, wurde Widerspruch eingelegt. Dies hat jedoch keine aufschiebende Wirkung, so daß zunächst die zur Deanonymisierung notwendigen Daten gespeichert wurden. Nach Aussetzung der Anordnung und noch bevor die endgültige Aufhebung durch das zuständige Landgericht Frankfurt/Main erfolgte (Az.: 5/6 Qs 47/03), erwirkte das BKA eine Durchsuchungsanordnung, mit dem Ziel die bis dahin angefallen Daten zu beschlagnahmen. Auf diese Weise gelangte das BKA in den Besitz eines Datensatzes, wobei dies auf rechtsmißbräuchliche Weise geschah, wie das Landgericht Frankfurt/Main später bestätigte (Az.: 5/8 Qs 26/03). Der Versuch, über die zuständigen Datenschutzbeauftragten eine Löschung der zu Unrecht erworbenen Informationen zu erreichen, erwies sich als schwierig, da zunächst sowohl das BKA als auch das in die Beschlagnahme involvierte sächsische LKA behaupteten, die Daten nie erhalten zu haben.

2 Umsetzung

Dieses Kapitel beschreibt ausgehend von einer Anforderungsanalyse die Umsetzung der „Strafverfolgungsfunktion“. Dabei werden zunächst aus der Literatur bekannte Ansätze diskutiert. Anschließend werden verschiedene mögliche Lösungen vorgeschlagen und bewertet.

2.1 Anforderungen

Ausgehend von den im vorangehenden Kapitel beschriebenen Rahmenbedingungen aus rechtlicher Sicht und dem Systemdesign sowie den durch den Betrieb des Anonymisierungsdienstes gesammelten Erfahrungen bezüglich Strafverfolgung ergeben sich folgende Anforderungen an die Deanonymisierung:

- **A1**: gemäß §§ 100 a, b StPO muß eine Deanonymisierung im Einzelfall auf entsprechende Anordnung unter Angabe der zu überwachenden Kennung ex nunc (von jetzt an) möglich sein

- **A2**: die Anonymität der nicht überwachten Teilnehmer muß gewahrt bleiben, d. h. daß bei n Teilnehmern und Durchführung einer Überwachung die Kardinalität der verbleibenden Anonymitätsmenge $n-1$ beträgt
- **A3**: das Vertrauensmodell des Anonymisierungsdienstes muß erhalten bleiben, d. h. die Deanonymisierung erfordert die Mitarbeit *aller* Mixe einer Kaskade
- **A4**: es sollen Audit-Daten gespeichert werden, um die Häufigkeit von durchgeführten Deanonymisierungen durch externe Stellen kontrollieren zu können

2.2 Trivialer Ansatz – Speichern von Logdateien[1]

Ein einfacher Lösungsversuch besteht darin, daß die Mixe die jeweilige Ein-/Ausgabezuordnung aus ihren Verbindungstabellen in einer Logdatei speichern. An Hand dieser Protokolle kann dann (insbesondere wenn gewünscht auch rückwirkend) jede beliebige Kommunikationsbeziehung schrittweise beginnend vom ersten bzw. letzten Mix einer Kaskade aufgedeckt werden.

Ohne näher auf technische Details dieser Idee einzugehen, verbietet sie sich schon deshalb, weil sie den Dienst ad absurdum führen würde. Der Zugriff und die Verwendung dieser Protokolldaten wären nicht kontrollierbar. Sind sie einmal vorhanden, so werden Begehrlichkeiten geweckt. Dies belegen die Erfahrungen mit dem BKA-Fall bzw. dem Fall des finnischen Remailers anon.penet.fi [WWW_2]. Der Dienst könnte keinerlei Zusicherungen bezüglich der Anonymität seiner Nutzer machen, da es jederzeit möglich ist, an Hand der Logdateien die Kommunikationsbeziehungen aller Nutzer aufzudecken und somit auf einfachste Weise eine Massenüberwachung zu ermöglichen.

Im übrigen verstößt das Aufzeichnen der Logdaten gegen § 6 TDDSG, da diese Daten weder zur Diensterbringung noch zu Abrechnungszwecken benötigt werden. Zu beachten ist auch, daß zur Herausgabe der gespeicherten Daten lediglich eine Anordnung nach §§ 100 g, h StPO erforderlich wäre. Somit entfällt insbesondere das nach §§ 100 a, b StPO notwendige Vorliegen einer Katalogstraftat.

Das Speichern von Logdateien ist aus den genannten Gründen in keinem Fall eine Lösung.

2.3 Bekannte Verfahren als Lösungsansätze

In [Golle04] wird ein Verfahren beschrieben, mit dem die Mixe im Falle eines Mißbrauchs gegenüber Dritten beweisen können, daß sie nicht Urheber der betreffenden Nachrichten sind. Das vorgeschlagene Verfahren beruht auf blinden Signaturen. Es ermöglicht jedoch keine Identifizierung des tatsächlichen Senders.

Das in [BeFK01] beschriebene Ticketverfahren basiert ebenfalls auf blinden Signaturen und dient dem Schutz gegen sogenannte $n-1$ -Angriffe (Flooding-Angriffe). Ein Nutzer registriert sich zunächst unter einem Pseudonym beim Anonymisierungsdienst und erhält dann sogenannte Tickets (Credentials), die es ihm erlauben, Nachrichten über den Dienst zu versenden. Dazu überträgt der Sender mit jedem Mixpaket ein gültiges Ticket.

Das Verfahren bietet in seiner ursprünglichen Form keine Möglichkeit der Zuordnung der gesendeten Nachrichten zum jeweiligen Nutzer(-pseudonym). In [ClDí03] wird dieser Mechanismus dahingehend erweitert. Es ist jedoch zu erwarten, daß eine Zwangsregistrierung vor Benutzung des Dienstes wenig Akzeptanz finden würde. Dementsprechend klein wäre die erreichte Anonymität(smenge). Gleichzeitig dürfte es sehr schwierig sein, eine derartige Registrierung in einem offenen Netz wie dem Internet zu realisieren.

[1] Eine weitere „einfache“ Lösung wäre natürlich, den Dienst technisch so zu realisieren, daß jeglicher Mißbrauch ausgeschlossen ist. Allerdings sind momentan keine Verfahren bekannt, die dies leisten – und es scheint fraglich, ob es jemals möglich ist, Kommunikation so zu formalisieren, daß eine maschinelle Einteilung in „erlaubt“ und „verboten“ möglich ist.

In [BaNe99] wird beschrieben, wie die Bezahlung des Anonymisierungsdienstes realisiert werden kann, indem mit jedem Mixpaket ein digitale Münze eines anonymen digitalen Zahlungssystems gesendet wird. Besitzt das verwendete Zahlungssystem ferner die Fairneß-Eigenschaft[2], so könnte diese ausgenutzt werden, um den Absender einer Nachricht zu identifizieren. Allerdings existiert in der Praxis zur Zeit kein solches Zahlungssystem, so daß dieses Verfahren im Moment keine Lösung darstellt.

Natürlich wäre es auch vorstellbar, gänzlich auf eine Möglichkeit der Deanonymisierung in der Kommunikationsschicht zu verzichten und statt dessen Verfahren zur Identifizierung in höheren Schichten zu realisieren, beispielsweise unter Benutzung von digitalen Pseudonymen, Credentials und Identitätsmanagementsystemen. Zum einen sind derartige Mechanismen in der Praxis aber zur Zeit wenig verbreitet, zum anderen ist es fraglich, ob Firmen wie eBay etc. bereit sind, in die Sicherung ihrer Anwendungen zu investieren. Dieser Vorschlag ist daher maximal als Ziel zukünftiger Entwicklungen zu verstehen, löst aber nicht die mit dem heute existierenden Anonymisierungsdienst verbundenen Probleme.

2.4 Grundlegende Lösungsidee

Die nachfolgend vorgeschlagenen Verfahren basieren alle auf der Idee, daß die Deanonymisierung schrittweise von Mix zu Mix durchgeführt wird. Erkennen erster bzw. letzter Mix einer Kaskade einen Zugriff, der laut Anordnung zu protokollieren ist, so teilen sie dem benachbarten Mix dies mit. Dieser informiert dann seinen Nachbar und so weiter. Dabei werden jeweils zusätzlich alle notwendigen Daten übertragen, die es jedem Mix erlauben, sich davon zu überzeugen, daß die durchgeführte Deanonymisierung auch wirklich gemäß den in der Anordnung gemachten Angaben erfolgt. Dazu ist es notwendig, daß jeder Mix einen entsprechenden (richterlichen) Beschluß erhält. Andernfalls müßten alle Mixe dem ersten bzw. letzten Mix vertrauen. Dies widerspricht jedoch dem Vertrauensmodell des Dienstes (siehe auch Anforderung A3).

Für die Beweisführung sind folgende zwei Teilprobleme zu lösen:

- **P1**: erkennt ein Mix M, gegebenenfalls nach Verarbeitung eines Mixpaketes p (Umkodierung), daß eine der zu überwachenden Kennungen auf p zutrifft, so muß er dem benachbarten Mix M_B dies beweisen, z. B. indem er zeigt, daß die Umkodierung korrekt durchgeführt wurde
- **P2**: M_B muß sich sicher sein, tatsächlich p an M gesendet (bzw. p von M empfangen) zu haben

Generell ist anzumerken, daß als Ergebnis einer Deanonymisierung die Kommunikationsbeziehungen nicht bis zu einer Person zurückverfolgt werden können .Vielmehr entstehen Indizien (z. B. IP-Adressen), die mit Hilfe weiterer Parteien (insbesondere Access-Provider) Rückschlüsse auf die (bürgerliche) Identität eines Senders bzw. Empfängers zulassen.

2.5 Deanonymisierung der Sender

Voraussetzung für die Deanonymisierung des Senders ist, daß alle Mixe eine Überwachungsanordnung erhalten haben, in der die Kennzeichen der zu überwachenden Nachrichten genannt sind. Typischerweise handelt es sich dabei um die Adresse des Empfängers.

Der Ablauf zur Lösung von Teilproblem P1 ist wie folgt:

- findet der letzte Mix M_n in der Anfrage a, die er nach Entschlüsselung des vom vorletzten Mix M_{n-1} empfangenen Kanalaufbaupaketes $p = id_n, c_n(k_n), k_n(a)$ erhält, ein Kennzeichen gemäß der Überwachungsanordnung so:
  1. speichert er verschlüsselt das Mixpaket p und den aktuellen Zeitpunkt. Dies dient zum einen der Beweissicherung und zum anderen für die Veröffentlichung einer Statistik über durchgeführte Überwachungsmaßnahmen (Anforderung A4)

[2] Digitale Münzsysteme, bei denen eine Deanonymisierung im Verdachtsfall möglich ist, werden als fair bezeichnet.

2. sendet er über einen Steuerkanal an M_{n-1} das Mixpaket p und den Schlüssel k_n

- der vorletzte Mix M_{n-1}:
  1. entschlüsselt die Anfrage a aus p mittels k_n und überprüft ob ein Kennzeichen gemäß Überwachungsanordnung enthalten ist
  2. überprüft ob die Verschlüsselung des von Mix M_n gesendeten Schlüssels k_n mit dem öffentlichen Schlüssel c_n identisch ist mit dem im Mixpaket p enthaltenen Bitstring $c_n(k_n)$
  3. speichert p, k_n und die aktuelle Zeit aus den oben genannten Gründen (vorausgesetzt die ersten beiden Überprüfungen waren erfolgreich)
  4. sendet über einen Steuerkanal an den vorangehenden Mix M_{n-2} den von M_n erhaltenen Schlüssel k_n, den Schlüssel k_{n-1} und das zuvor von M_{n-2} erhaltene Mixpaket $p' = id_{n-1}, c_{n-1}(k_{n-1}), k_{n-1}(c_n(k_n), k_n(a))$ (M_{n-2} kann p' aus p mit Hilfe des in seiner Verbindungstabelle gespeicherten Schlüssels k_{n-1} rekonstruieren.)
- die Mixe $M_{n-2}, \ldots, M_1$ verfahren sinngemäß, d. h. sie überprüfen jeweils, ob die Anfrage a ein zu überwachendes Kennzeichen enthält und ob aus dem erhaltenen Paket bei korrekter Umkodierung die Anfrage a entsteht. Beides ist möglich, da die geheimen symmetrischen Schlüssel offengelegt wurden. Der erste Mix speichert zusätzlich verschlüsselt die IP-Adresse des Senders.

Für die Lösung von Teilproblems P2 gibt es zwei verschiedene Möglichkeiten:

- jeder Mix $M_i \in \{M_1, \ldots, M_{n-1}\}$ speichert für die Dauer eines Kanals jeweils einen Hashwert h des Kanalaufbaupaketes. Er überprüft dann, ob die Hashfunktion angewendet auf das von M_{i+1} erhaltene Mixpaket den Wert h ergibt.
- jeder Mix $M_i \in \{M_1, \ldots, M_{n-1}\}$ sendet zusammen mit jedem Kanalaufbaupaket p jeweils einen Authentikationskode $Mac_{M_i}(p)$. Im Falle einer Deanonymisierung wird dieser dann mit gesendet. Jeder Mix kann sich durch Überprüfen des Authentikationskodes davon überzeugen, daß p tatsächlich von ihm gesendet wurde.

Beide Lösungen unterscheiden sich bezüglich des zusätzlichen lokalen Speicheraufwandes vs. des zusätzlichen Übertragungsvolumens. Dabei ist insbesondere zu beachten, daß im ersten Fall lediglich Fixkosten entstehen, während im zweiten Fall laufende Kosten für die Datenübertragung anfallen.

2.6 Deanonymisierung der Empfänger

Soll aufgedeckt werden, zu welchen Empfängern ein bestimmter Sender Kommunikationsbeziehungen unterhält, so ist das Vorgehen ähnlich dem im Abschnitt 2.5 geschilderten. Die zu überwachende Kennung wird dabei typischerweise die IP-Adresse des Senders sein.

Die Lösung von Teilproblem P1 gestaltet sich insofern schwierig, da der erste Mix M_1 den nachfolgenden Mixen nicht beweisen kann, daß er ein zu überwachendes Mixpaket auch tatsächlich von der in der Anordnung genannten IP-Adresse erhalten hat. Die Internetprotokolle sehen momentan keinen allgemeinen Mechanismus zur beweisbaren Überprüfung des Absenders vor[3]. Die Mixe $M_{2,}\ldots, M_n$ müßten also darauf vertrauen, daß sich M_1 korrekt verhält. Dies widerspricht aber Anforderung A3.

Als Lösung wird vorgeschlagen, bei dem vom Sender benutzten Internet Service Provider (ISP) ein sicheres Gerät zu installieren, auf das nur die Strafverfolgungsbehörde Zugriff hat. Dieses Gerät überwacht den Netzwerkverkehr des Senders und fügt an alle Mixpakete eine digitale Signatur an. Der erste Mix erhält dann mit der Überwachungsanordnung zusätzlich noch den Signaturtestschlüssel t. Die Mixe $M_2, \ldots, M_n$ erhalten ausschließlich diesen Testschlüssel und nicht mehr das eigentliche Überwachungskennzeichen, was aus Datenschutzsicht positiv zu werten ist.

[3] Sollten sich Technologien wie z. B. TCPA durchsetzen, die sichere und überprüfbare Endgeräte versprechen, so bleibt zu untersuchen, wie diese Verfahren zur besseren Identifizierung von Sender/Empfänger verwendet werden können.

Teilproblem P2 ist einfacher zu lösen als bei der Deanonymisierung des Senders, da bereits vor durchlaufen des Anonymisierungsdienstes klar ist, welche Pakete zu überwachen sind. Daher ist eine zusätzliche Speicherung der Hashwerte übertragener Pakete nicht erforderlich.

Konkret funktioniert die Deanonymisierung wie folgt:

- empfängt Mix M_1 ein zu überwachendes Mixpaket $p = id_1, c_1(k_1), k_1(c_2(k_2), k_2(\ldots))$ zusammen mit der vom Überwachungsgerät generierten Signatur $Sig(p)$, so:
  1. prüft M_1 mittels des Testschlüssels t ob die Signatur gültig ist
  2. sendet er über einen Steuerkanal p, $Sig(p)$, k_1 und id_2 an den nachfolgenden Mix M_2
  3. sendet er an M_2 das gemäß Mixprotokoll bearbeitete Paket $p' = id_2, c_2(k_2), k_2(\ldots)$
  4. speichert er p, $Sig(p)$ und die aktuelle Zeit (siehe oben)
- Mix M_2:
  1. prüft mittels des Testschlüssels t ob die Signatur $Sig(p)$ gültig ist
  2. überprüft mittels k_1 und c_1, ob das von Mix M_1 erhaltene Paket p' eine korrekte Umkodierung von p ist
  3. sendet über einen Steuerkanal p, $Sig(p)$, k_1, k_2 und id_3 an M_3
  4. sendet an M_3 das gemäß Mixprotokoll bearbeitete Paket p''
  5. speichert p, $Sig(p)$, k_1 und die aktuelle Zeit
- die Mixe $M_3, \ldots, M_n$ verfahren sinngemäß, d. h. sie überprüfen ob die Signatur $Sig(p)$ gültig ist und ob durch korrekte Umkodierung aus p das erhaltene Mixpaket entsteht. Dies ist möglich, da jeweils die geheimen symmetrischen Schlüssel offengelegt wurden. Der letzte Mix M_n speichert zusätzlich verschlüsselt das erhaltene Mixpaket.

2.7 Anmerkungen zur Implementierung

Die Implementierung sollte (soweit technisch möglich) die Einhaltung von gesetzlich vorgeschriebenen Regeln überprüfen. Dazu zählt insbesondere die maximale Dauer einer Überwachungsmaßnahme.

Beim AN.ON System steht zur Konfiguration der Mixe ein Programm mit graphischer Benutzungsschnittstelle zur Verfügung. Dieses wird so erweitert, daß die in der Überwachungsanordnung angegebenen Daten leicht eingetragen werden können. Der Nutzer muß dabei insbesondere auswählen, ob es sich um eine richterliche oder eine staatsanwaltschaftliche Anordnung handelt. Dementsprechend wird die maximale Dauer auf drei Monate bzw. drei Tage eingestellt. Die Eingabe von kürzeren Zeiträumen ist möglich. Der Mix beendet auf Grund dieser Angaben die Überwachung automatisch.

Fazit

Ausgehend von den rechtlichen und technischen Rahmenbedingungen wurde ein effizientes Verfahren der datenschutzgerechten Deanonymisierung im Einzelfall vorgestellt. Dabei wurde insbesondere das dem Anonymisierungsdienst zugrundeliegende Vertrauensmodell berücksichtigt. Es bleibt abzuwarten, inwieweit sich das Verfahren in der Praxis bewährt. Insbesondere stellt sich die Frage, ob es gelingt, die Strafverfolgungsbehörden davon zu überzeugen, daß jeder Mix eine Überwachungsanordnung erhalten muß, da andernfalls die Maßnahme „ins Leere“ läuft.

Zu untersuchen bleibt, inwieweit das vorgestellte Verfahren kompatibel mit internationalem Recht ist, d. h. der Fall, daß eine Mixkaskade aus Mixen besteht, die unter unterschiedliche Rechtssprechung fallen. Des weiteren sollte untersucht werden, ob es (juristisch und technisch) möglich ist, daß auch der erste (bzw. letzte) Mix nicht erfahren, welche Daten (IP-Adressen) letztlich das Ergebnis der Deanonymisierung sind.

Literatur

BaNe99 Matthias Baumgart, Heike Neumann: Bezahlen von Mix-Netz-Diensten. Verläßliche IT-Systeme - VIS 1999, Vieweg-Verlag, 1999.

BeFK01 Oliver Berthold, Hannes Federrath, Stefan Köpsell: Praktischer Schutz vor Flooding-Angriffen bei Chaumschen Mixen, in: Patrick Horster (Hrsg.): Kommunikationssicherheit im Zeichen des Internet. DuD-Fachbeiträge, Vieweg, Wiesbaden, 2001, 235-249.

Chau81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84-88.

ClDí03 Joris Claessens, Claudia Díaz, et al.: APES, Anonymity and Privacy in Electronic Services, Deliverable 10, Technologies for controlled anonymity, 2003, https://www.cosic.esat.kuleuven.ac.be/apes/docs/APES_d10.pdf

FeGo04 Hannes Federrath, Claudia Golembiewski: Speicherung von Nutzungsdaten durch Anonymiserungsdienste im Internet. Welche strafprozessualen Vorschriften zur Überwachung der Telekommunikation sind auf Anonymiserungsdienste anwendbar?, in: Datenschutz und Datensicherheit (DuD), 28/8 (2004), 486

FeKL02 Hannes Federrath, Stefan Köpsell, Heinrich Langos: Anonyme und unbeobachtbare Kommunikation Internet. Proc. GI-Jahrestagung 2002, Informatik bewegt. Lecture Notes in Informatics (P-19), Köllen Verlag, Bonn 2002, 481-488.

Ger04 Marco Gercke: Die Protokollierung von Nutzerdaten. Zu den Ermittlungsmaßnahmen gegen JAP nach § 100 g/h StPO, in: Datenschutz und Datensicherheit (DuD), 28/4 (2004), 210

Gol03 Claudia Golembiewski: Das Recht auf Anonymität im Internet - Gesetzliche Grundlagen und praktische Umsetzung, in: Datenschutz und Datensicherheit (DuD), 27/3 (2003), 129

Gol03a Claudia Golembiewski: AN.ON: Der Staatsanwalt hat geklingelt, in: Datenschutz und Datensicherheit (DuD), 27/10 (2003), 596

Golle04 Philippe Golle: Reputable Mix Networks, in Proceedings of Privacy Enhancing Technologies workshop (PET 2004), 2004, erscheint in LNCS, Springer

KöFH03 Stefan Köpsell, Hannes Federrath, Marit Hansen: Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes, in: Datenschutz und Datensicherheit (DuD), 27/3 (2003), 139

Kra04 Henry Krasemann: Besprechung des Beschlusses des Landgerichts Frankfurt am Main vom 15.09.2003 (Az.: 5/6 Qs 47/03) und des Beschlusses des Landgerichts Frankfurt am Main vom 21.10.2003 (Az.: 5/8 Qs 26/03), http://www.jurpc.de/aufsatz/20040140.htm

PfPW89 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2•64 + 16)-kbit/s-Teilnehmeranschluß, in: Datenschutz und Datensicherheit (DuD), 13/12 (1989), 605

Raa03 Oliver Raabe: Die rechtliche Einordnung zweier Web-Anonymisierungsdienste, in: Datenschutz und Datensicherheit (DuD), 27/3 (2003), 134

WWW_1 AN.ON Projekt: Erklärung des Projektes zum künftigen Verhalten gegenüber Strafverfolgungsbehörden, http://anon.inf.tu-dresden.de/strafverfolgung/policy.pdf

WWW_2 Sabine Helmers: A Brief History of anon.penet.fi - The Legendary Anonymous Remailer, http://www.december.com/cmc/mag/1997/sep/helmers.html