



AN.ON — Anonymität.Online

**AN.ON - Starke Unbeobachtbarkeit und Anonymität im Internet
Teilvorhaben: Prototypentwicklung**

gefördert vom Bundesministerium für Wirtschaft und Technologie

Autor: Prof. Dr. Hannes Federrath

Abschlussbericht

Abschlussbericht

Zuwendungsempfänger:
Prof. Dr.-Ing. Hannes Federrath

Förderkennzeichen:
01 MS 918

Vorhabensbezeichnung:
AN.ON - Starke Unbeobachtbarkeit und Anonymität im Internet
Teilvorhaben: Prototypentwicklung

Laufzeit des Vorhabens:
1. Januar 2001 - 31. Dezember 2006

Berichtszeitraum:
1. Januar 2001 - 31. Dezember 2006

Datum:
31. Juli 2007

1 Überblick

1.1 Aufgabenstellung im Projekt

Ziele des im Jahr 2001 begonnenen Projekts waren der Entwurf, die Implementierung, die Validierung und das Nutzbarmachen eines prototypischen Systems zur anonymen und unbeobachtbaren Kommunikation im Internet, das sowohl gegen Betreiber als auch gegen starke externe Angreifer schützt, die Teile des Kommunikationsnetzes abhören können. Das System sollte zur Echtzeitkommunikation und für verschiedene Internetdienste geeignet sein, skalierbar sein und Abrechnungsmöglichkeiten vorsehen. Soweit nach Abschluss des Projekts Kapazitäten vorhanden wären, sollte die (quelloffene) Software weiter gepflegt werden. Andere Projekte könnten darauf aufbauen, Weiterentwicklungen im Rahmen von E-Commerce und E-Government wären möglich.

1.2 Voraussetzungen für das Vorhaben

Während der Projektlaufzeit haben die folgenden Mitarbeiterinnen und Mitarbeiter der TU Dresden, der FU Berlin und der Universität Regensburg im Projekt AN.ON mitgearbeitet: Im Bereich der Projektplanung und Entwicklung

- Oliver Berthold (TU Dresden, FU Berlin),
- Sebastian Clauß (TU Dresden),
- Stefan Köpsell (TU Dresden),
- Heinrich Langos (TU Dresden, FU Berlin),
- Andreas Pfitzmann (TU Dresden),
- Sandra Steinbrecher (TU Dresden, FU Berlin),

- Rolf Wendolsky (Universität Regensburg).

Im Bereich der Projektleitung und Kommunikation mit anderen Stellen:

- Hannes Federrath (TU Dresden, FU Berlin, Universität Regensburg)

Zur Unterstützung des Projekts waren etliche externe Partner eingebunden, u.a.:

- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
- eCONNEX AG,
- gaertner datensysteme GbR,
- NetUSE AG,
- secunet AG (Security Networks),
- SEDAT GmbH (security technologies),
- Sirrix GmbH.

1.3 Planung und Ablauf des Vorhabens

Zielsetzungen des Projekts waren die Entwicklung eines Konzeptes zur mehrseitig sicheren anonymen Nutzung des Internet und die Implementierung eines noch eingeschränkt nutzbaren Prototyps.

Tabelle 1 gibt eine Übersicht über die in der Laufzeit bearbeiteten fünf Arbeitsphasen.

Das Projekt wurde mit kleinen Verzögerungen abgewickelt. Der Schwerpunkt lag auf der Entwicklung einer performanten und zuverlässigen Serversoftware sowie eines Client-Programms, das sich durch eine möglichst einfache Benutzerführung auszeichnet und auch die Integration weiterer Dienste erlaubt (Phasen 1 bis 3). In den Phasen 4 und 5 lagen die Arbeitsschwerpunkte in der Implementierung von Funktionen zur Verfolgung illegaler Handlungen über das System sowie die kommerzielle Nutzbarmachung.

1.4 Ausgangspunkte in Wissenschaft und Technik

Grundlegende Konzepte zum Schutz vor Beobachtung in Rechnernetzen wurden bereits mehrere Jahre vor Beginn des Projektes erarbeitet. Tabelle 2 gibt einen Überblick über die historische Entwicklung der Techniken. Hervorzuheben sind insbesondere das Mix-Netz [5], das DC-Netz [8] sowie der Message-Service [9]. Diese Techniken wurden verbessert, verfeinert [28, 25, 24, 29] und für verschiedene Anwendungsfelder modifiziert:

- ISDN [26],

Tabelle 1: Arbeitspakete

Phase	Arbeitspaket
1 Entwicklung und Implementierung der Anonymitätsarchitektur	1.1 Analyse der existierenden Dienste/ Forschungsprojekte 1.2 Konzeption des Gesamtdienstes 1.3 Entwicklung des Client-Programms und des Mix-Proxy 1.4 Test der Prototypen 1.5 Dokumentation der Anwendungen und Ergebnisse
2 Erweiterung und Präzisierung der Anonymitätsarchitektur	2.1 Aufbau einer Zertifizierungsinfrastruktur 2.2 Entwicklung eines Ticketsystems 2.3 Entwicklung eines Informationsservices 2.4 Entwicklung eines Abrechnungsverfahrens 2.5 Dokumentation der Anwendungen und Ergebnisse
3 Entwicklung und Implementierung eines einsetzbaren Anonymitätsdienstes	3.1 Optimierung der Skalierbarkeit 3.2 Unterstützung verschiedener Internetdienste 3.3 Entwicklung von Anonymisierungsverfahren für die Anwendungsschicht 3.4 Implementierung einer selbsterklärenden Benutzungsschnittstelle 3.5 Dokumentation der Anwendungen und Ergebnisse
4 Strafverfolgung und Bezahlfunktion	4.1 Entwicklung von Konzepten zur datenschutzfreundlichen Strafverfolgung 4.2 Entwicklung von Bezahlfunktionen
5 Mix-Installationsprozedur	Vereinfachung der Mix-Installationsprozedur

- E-Mail-Kommunikation [10],
- Mobilkommunikation [17, 14],
- verbindungsorientierte Internetdienste [20],
- Internetdienste ohne strenge Realzeitforderungen [22].

Speziell für die Anonymisierung von Webzugriffen waren zu Projektbeginn waren folgende Systeme und Ansätze verfügbar:

- **Crowds:** Crowds war ein verteiltes System unter Nutzung von Kryptographie, bei dem die Nutzer sich in einer Anonymitätsgruppe zusammenschließen. Bei Crowds wird eine Webanfrage nicht direkt an den Server geschickt, sondern an einen zufällig ausgewählten anderen Crowds-Nutzer. Dessen Rechner entscheidet ebenfalls zufällig, ob die Anfrage direkt an den Server geschickt oder einem anderen Crowds-Nutzer zur Weiterleitung übermittelt wird. Crowds war nie ein aktives System, sondern eher eine Designstudie.

Tabelle 2: Historie grundlegender Konzepte

Year	Idea / PET system
1978	Public-key encryption [32]
1981	MIX, Pseudonyms [5]
1983	Blind signature schemes [6]
1985	Credentials [7]
1988	DC network [8]
1990	Privacy preserving value exchange [4]
1991	ISDN-Mixes [27]
1995	Blind message service [9]
1995	Mixmaster [10]
1996	MIXes in mobile communications [17]
1996	Onion Routing [20]
1997	Crowds Anonymizer [31]
1998	Stop-and-Go (SG) Mixes introduced [23]
1999	Zeroknowledge Freedom Anonymizer (service meanwhile closed)
2000	AN.ON/JAP Anonymizer [3]
2004	TOR [11]

- **Onion-Routing:** In Onion-Routing wurde ein vereinfachtes Mix-Prinzip eingesetzt, bei dem Echtzeitkommunikation möglich war, das aber keinen Schutz vor Verkehrsanalysen bot. Es wurde von der US Navy maßgeblich entwickelt, allerdings nie ernsthaft als Dienst angeboten, sondern blieb im Prototypstadium stecken. Inzwischen existiert jedoch ein „Next Generation Onion Routing Protocol“ namens TOR.
- **Freedom:** Freedom nutzte ebenfalls ein vereinfachtes Mix-Prinzip für die Realisierung von Echtzeitkommunikation und bot keinen Schutz vor Verkehrsanalysen. In Freedom konnten Benutzer pseudonym kommunizieren. Dies war das erste kommerzielle System (betrieben von einem Startup-Unternehmen während des Dot-Com-Hype) zum anonymen Internetzugriff. Freedom scheiterte jedoch an komplizierter Technik, unzureichender Dienstqualität und zu hohen Gewinnerwartungen der Risikokapitalgeber.
- **Anonymizer:** Anonymizer besitzt die Sicherheitsfunktionalität eines filternden Proxy-Services. Es werden u.a. aktive Inhalte (JavaScript, Java, ActiveX) gefiltert, um eine Enttarnung eines Nutzers zu erschweren. Anonymizer war der erste breit bekannte und auch kommerziell nutzbare Anonymisierer und ist bis heute nutzbar. Der Hauptnachteil des Systems besteht in der Beobachtungsmöglichkeit durch den Betreiber von Anonymizer.
- **Rewebber:** Rewebber war ein deutsches System mit der Funktionalität eines Proxy-Service (ähnlich Anonymizer). Neben der Anonymisierung von Webzugriffen (sog. Clientanonymität) wurde eine Funktion zum anonymen Publizieren von Webinhalten (sog. Serveranonymität) bereitgestellt.

Die genannten Systeme verfolgen zwar alle die gleichen Schutzziele, allerdings teilweise mit sehr unterschiedlichen Angreifermodellen, d.h. erheblichen Unterschieden in der unterstellten Stärke eines Angreifers. Mittlerweile sind alle genannten Systeme, bis auf Anonymizer, vom Markt verschwunden.

Anonymizer und Rewebber schützen nur gegen „räumlich“ sehr begrenzte Angreifer und überhaupt nicht gegen den Betreiber des Anonymitätssdienstes selbst. Crowds, Onion-Routing und Freedom schützen prinzipiell auch gegen den Betreiber des Systems, aber nicht gegen Angreifer, die in der Lage sind, Verkehrsanalysen durchzuführen, d.h. eine Vielzahl von Kommunikationsleitungen zu überwachen.

Eine Analyse dieser Systeme findet man in [19, 3]. Keines der damals existierenden Systeme schützte sowohl vor seinem Betreiber als auch vor einem starken externen Angreifer, der in der Lage ist, Verkehrsanalysen durchzuführen.

Eigene theoretische Vorarbeiten im engeren Sinne waren insbesondere die in [28, 25, 24, 29, 26, 17, 27, 19, 2, 3, 15] publizierten Verfahren und Konzepte. Im DFG-Projekt „Effiziente und skalierbare Realisierung von unbeobachtbarer und anonymer Kommunikation im Internet“ wurden die Grundlagen erforscht, die im beantragten Vorhaben angewendet werden sollten. Im BMBF-Projekt „Schutz und Sicherheit in offenen Datennetzen“ (SSONET) wurde u.a. zur Gestaltung von Benutzungsoberflächen für Sicherheitsfunktionen und zur Aushandlung von Sicherheitsparametern gearbeitet [36].

Eigene praktische Vorarbeiten waren zwei Mix-Prototypen, die die Grundfunktionalität bereits erfüllten (Verbindungsauf- und -abbau, Proxyfunktion, kryptographische Funktionen), allerdings mit erheblichen Einschränkungen in der Dienstqualität (Performance, Durchsatz) und Sicherheit (noch keine Sicherheit gegen Verkehrsanalysen) [18, 35]. Zudem existierte ein „Anon Proxy“, der etwa die Funktionalität und Sicherheit von Anonymizer bzw. Rewebber bietet. Dieser diente dem Finden von Schwächen in Anonymisierungsdiensten [15]. Im Rahmen von Studien- und Diplomarbeiten wurden eine Reihe von praktischen Untersuchungen zur Internetsicherheit (Sniffing, Spoofing, Flooding, Trojanische Pferde) durchgeführt [12, 13, 37], die teilweise Fehler in Standardsoftware offen gelegt haben (vgl. hierzu [1]).

Mit dem Projektpartner Unabhängiges Landeszentrum für Datenschutz (ULD) in Schleswig-Holstein wurde im Rahmen des Projektes „Webzugriff anonym und unbeobachtbar“ (WAU, siehe <http://www.datenschutzzentrum.de/projekte/wau/index.htm>) bereits im Vorfeld zum AN.ON-Projekt kooperiert.

1.5 Zusammenarbeit mit anderen Stellen

Primär haben die Projektpartner Universität Regensburg und ULD zusammengearbeitet. Weitere enge Kooperationen bestanden mit

- der Humboldt-Universität Berlin, mit der insbesondere wirtschaftliche Fragestellungen erörtert wurden [33, 34], sowie
- der Rheinisch-Westfälischen Technischen Hochschule Aachen, wo ebenfalls technische Kompetenz zur Technik von Anonymisierungsdiensten angesiedelt ist.

In allen Phasen des Projektes fanden regelmäßige Treffen, zumeist bei einem der beteiligten Projektpartner, statt.

Darüber hinaus gab es einen regen Austausch mit den Betreibern von Mix-Rechnern, insbesondere der TU Dresden, der HU Berlin sowie dem Chaos Computer Club. Themen waren vor allem Fragen der Weiterentwicklung des Dienstes, an die Partner herangetragenen Anfragen und Beschwerden sowie die Erfahrungen aus dem Mixbetrieb.

In Einzelkontakten und Workshops kam es weiterhin zu konstruktiven Gesprächen mit Vertretern von Strafverfolgungsbehörden, z.B. BKA, LKÄ, Staatsanwaltschaften und Vertretern von Ministerien.

In der Endphase des Projektes wurde mit dem Bundeskriminalamt im Rahmen einer Diplomarbeit [30] kooperiert. Hierbei ging es um die Integration einer Präventionstechnologie zur Verhinderung des Abrufs von kinderpornographischen Inhalten.

2 Erzieltes Ergebnis

Im Projekt AN.ON wurde ein rechtskonformer Anonymisierungsdienst für den anonymen Internetzugriff entwickelt. Der Hauptnutzen des Dienstes besteht aus Endbenutzersicht in der Möglichkeit zum anonymen Web-Browsing.

Der Dienst ist nunmehr seit Projektbeginn ununterbrochen (abgesehen von wenigen Tagen im Jahr) im Einsatz und wurde seitdem ständig verbessert. Er gestattet es Internetsurfern, Webangebote zu nutzen, ohne dass es Dritten – nicht einmal dem Betreiber des Dienstes – möglich ist, Nutzerprofile zu erstellen. Nebennutzen des Dienstes ist eine Umgehung von Zensur im Internet.

Zwischen dem Websurfer und der angefragten Webseite befinden sich mehrere Zwischenstationen (Chaumsche Mixe [5]). Die Datenpakete vieler gleichzeitig angemeldeter Nutzer werden in gleich aussehende Pakete verpackt und mehrfach verschlüsselt (umkodiert), in jedem Mix umsortiert und weitergeleitet. Dadurch werden die Aktionen einzelner Nutzer ununterscheidbar, und die Kommunikationsendpunkte werden für Außenstehende und sogar für die Mixbetreiber verschleiert.

Der im Projekt entwickelte Anonymisierungsdienst ist für alle Internet-Teilnehmer von Nutzen, zum Einen in der Rolle der Nachfragenden, zum Anderen in der Rolle der Anbietenden:

- Bürgerinnen und Bürger, die bei ihrer elektronischen Kommunikation ihr Recht auf Anonymität in Anspruch nehmen möchten,
- Firmen, die zur Wahrung ihrer Geschäftsgeheimnisse auf eine unbeobachtbare Kommunikation angewiesen sind (z.B. beim Abruf von Patentdatenbanken) oder die selbst Anonymisierungsdienste als generellen Service oder für spezielle Dienste anbieten wollen,
- Verwaltung und private Anbieter, die hinsichtlich elektronischer Dienstleistungen in besonderem Maße verpflichtet sind, datensparsame Techniken einzusetzen (z.B. § 3a BDSG; § 4 LDSG SH) und anzubieten (z.B. § 4 Abs. 6 TDDSG), z.B. bei Verfahren der Bürgerpartizipation, Online-Wahlen.

Das Projekt AN.ON mit seinem Anonymisierungsdienst, vor allem aber das Client-Programm JAP, wurden einer größeren Öffentlichkeit im In- und Ausland bekannt gemacht, z.B. über Presseerklärungen, Vorträge bei vielerlei Zielgruppen, Ausstellungen auf Messen wie der CeBIT und über die Projekt-Webseite.

In Spitzenzeiten sind auf den Servern des Dienstes bis zu 9000 Nutzer gleichzeitig online, und die Clientsoftware JAP wurde mehrere Millionen Mal heruntergeladen. Zehn verschiedene Organisationen (TU Dresden, Universität Regensburg, ULD, Chaos Computer Club, FoeBuD, Provider, Parteien und kommerzielle Unternehmen) betreiben mittlerweile AN.ON-Mixe, und deren Zahl wird mit der zwischenzeitlich vollzogenen Kommerzialisierung wohl noch weiter ansteigen (vgl. Erfolgskontrollbericht).

Im Rahmen des Probetriebes konnten zahlreiche praktische Erfahrungen aus technischer, ökonomischer und juristischer Sicht gewonnen werden [21, 16].

Alle wissenschaftlichen und technischen Ergebnisse wurde publiziert und der Fachwelt vorgestellt. Die Liste der im Projekt entstandenen Publikationen findet sich in Abschnitt 6.

3 Verwertungsplan

3.1 Wirtschaftliche Erfolgsaussichten

Die im Rahmen des Projektes geschaffenen Systeme, d.h. die Clientsoftware JAP sowie die Serversoftware, stehen einer breiten Öffentlichkeit zur Verfügung, indem der Quellcode und die Software, die Nutzer installieren können, über die Projekt-Webseite <http://www.anon-online.de> zum Download angeboten werden.

Dipl.-Wirtsch.-Inf. Rolf Wendolsky (ehemaliger Projektmitarbeiter an der Universität Regensburg) hat mit der Gründung eines Spin-off-Unternehmens die Kommerzialisierung des AN.ON-Dienstes in Angriff genommen. Einige der bisherigen Projektmitglieder haben die Absicht, dieses Vorhaben durch Beratung zu unterstützen. Es konnten bereits viele Betreiber gefunden werden, die definitiv bereit sind, ein oder mehrere Mixe in die Startphase des kommerziellen Dienstes einzubringen. Bei genügender Nachfrage werden diese Angebote deutlich ausgebaut. Der Geschäftsplan des Unternehmens (vgl. Erfolgskontrollbericht) setzt primär auf eine Bezahlung des Dienstes durch die Endverbraucher (Websurfer) und auf Unternehmen, Parteien und andere Organisationen als dessen Betreiber. Das neu gegründete Unternehmen wird die Softwareentwicklung, die Abrechnung und den Support als Mittler zwischen Endbenutzer und Betreibern übernehmen. Damit ist der Weiterbetrieb des Dienstes, die Weiterpflege Software und die Weiterentwicklung der Projektergebnisse gesichert.

Es ist geplant, dass die Nutzung des Dienstes auch kostenlos möglich sein soll, aber mit geringerer Geschwindigkeit und weniger Sicherheit durch kürzere und rein nationale Mixkaskaden. Die kostenlose Bereitstellung wird von der neuen Organisation zwar nicht monetär gefördert, aber mit personeller Hilfe bei Einrichtung und Verwaltung der von anderen Organisationen bereitgestellten Server unterstützt. Voraussetzung für den kostenlosen Betrieb sind gemeinnützige Organisationen, die zu diesen Zweck Geld investieren, wie es zur Zeit der Chaos Computer Club und der FoeBuD tun.

3.2 Wissenschaftliche und technische Erfolgsaussichten

Die im Rahmen des Vorhabens entwickelten und realisierten Kommunikationsprotokolle, Architekturen und Algorithmen sind durch wissenschaftliche Veröffentlichungen dokumentiert, der Fachwelt zugänglich gemacht und zur Diskussion gestellt worden. Dasselbe gilt für die Dokumentation des Projektes aus datenschutzrechtlicher Sicht.

Durch das Schaffen einer Schnittstelle zum in den letzten Jahren primär in den USA entwickelten Anonymisierungsdienst TOR <http://tor.eff.org/> (Nachfolger von Onion Routing) wurde bezüglich des Projektes die internationale Wahrnehmung deutlich erhöht.

Da die internationale Standardisierung im Bereich anonymer Kommunikationsprotokolle nicht die Fortschritte gemacht hat, die am Anfang der Projektlaufzeit vermutet wurden, sind hier keine Ergebnisse vorzuweisen. Allerdings war es auch nicht die Absicht, innerhalb des Projektes Standards zu schaffen. Mit der Existenz zweier Lösungen (AN.ON und TOR) haben sich jedoch zwei Quasi-Standards herausgebildet, die konzeptionell so eng beieinander liegen, dass es denkbar ist, diese in der Zukunft in einen gemeinsamen Standard münden zu lassen. Zwar sind den maßgeblichen Personen, die international im Bereich der Themen Anonymität und anonyme Kommunikationsprotokolle tätig sind, die Arbeiten der Projekte bewusst, jedoch beschäftigen sich die Standardisierungsgremien bislang nicht mit dem Thema.

Die durch das AN.ON-Projekt vorgestellte Lösung ist neben TOR eine der Basiskomponenten zur Realisierung des im EU-Projekt PRIME (Privacy and Identity Management for Europe, <http://www.prime-project.eu/>) zu realisierenden Prototypen für das Identitätsmanagement.

4 Fortschritt bei anderen Stellen

Im wissenschaftlichen und technischen Bereich, insbesondere im Bereich der Privacy Enhancing Technologies (PET) waren auch Fortschritte bei anderen Stellen zu verzeichnen. Die Arbeiten im AN.ON-Projekt haben gewissermaßen die Arbeiten der sog. PET-Community mit geprägt.

Von besonderer Bedeutung ist die Entwicklung und Verbreitung des Anonymisierungsdienstes TOR, dessen Entwicklung sicherlich durch den Erfolg von AN.ON beflügelt wurde. Obwohl sich AN.ON und TOR konzeptionell stark ähneln, sind die Umsetzungen im Detail sehr verschieden. Darüber hinaus gibt es eine Reihe von Unterschieden zwischen Tor und AN.ON, was die Stärke der Anonymisierung und die Angreifermodele betrifft.

Innerhalb von Deutschland sind speziell Fortschritte bei der RWTH Aachen zu verzeichnen, die im Projekt PRIME die Arbeiten zur anonymen Kommunikation durchführen. Mit der dortigen Arbeitsgruppe besteht ein reger Informationsaustausch. Zu wirtschaftlichen Fragen gab es Arbeiten an der Humboldt-Universität Berlin, die in Kooperation mit dem AN.ON-Projekt abliefen, insbesondere zu Nutzerstrukturen des Anonymisierungsdienstes und der Bereitschaft, für die Nutzung zu zahlen.

Der Dialog mit Polizeibehörden und Staatsanwaltschaften diente auch der dortigen Verbesserung der Kompetenzen bei der Verfolgung von Straftaten im Internet (z.B. Ermittlungsansätze jenseits der IP-Adresse, die ja durch AN.ON nicht mehr sichtbar ist).

5 Veröffentlichungen des Ergebnisses

Das Projekt und seine Resultate wurden auf wissenschaftlichen Fachtagungen, in Vorträgen und auf Messen vorgestellt (u.a. auf den CeBIT-Messen in den Jahren 2001 bis 2003 am Stand der TU Dresden und 2001 bis 2006 am Stand des ULD).

Projektmitarbeiterinnen und -mitarbeiter hielten insgesamt mehr als 50 Vorträge zu AN.ON auf Veranstaltungen diverser Organisationen.

Das Konzept des AN.ON-Dienstes sowie die Fortschritte im Projekt waren weiterhin Bestandteil regelmäßiger Vorlesungen an der TU Dresden, FU Berlin und Universität Regensburg.

In der gesamten Projektlaufzeit wurde intensive Öffentlichkeitsarbeit betrieben. Die Veröffentlichung von Pressemeldungen und Informationsmaterial wurde hauptsächlich durch den Projektpartner ULD geleistet, unterstützt durch Zuarbeiten aus Dresden, Berlin und Regensburg.

Dem Thema „Strafverfolgung und Datenschutz“ wurde im Mai 2004 ein besonderer Workshop gewidmet, der gemeinsam von ULD und Innenministerium Schleswig-Holstein organisiert wurde und einen Austausch zwischen Vertretern von Polizei, Justiz, Datenschutzinstitutionen, Wissenschaft, Internet-Providern und dem Projekt AN.ON ermöglichte. Dort wurde – neben den juristischen Themen – auch dem Bereich Technik viel Raum gegeben und Wissen vermittelt.

Als gemeinsame Abschlussveranstaltung mit dem Projektpartner ULD fand im November 2006 ein Workshop in Berlin mit dem Thema „Anonymität.Online: Technik - Szenarien - Geschäftsmodelle“ (<http://anon.inf.tu-dresden.de/bmwi2006/index.html>) statt. Neben den Projektergebnissen wurde über die Verwertungsmöglichkeiten der Projektergebnisse berichtet und diskutiert. Anwesend waren aktive und ehemalige Projektmitarbeiter, Vertreter von Medien, Verbraucherschutzorganisationen, Internet Providern und Strafverfolgungsbehörden.

6 Liste der Veröffentlichungen (Teilprojekt Prototypentwicklung AN.ON)

Rolf Wendolsky, Dominik Herrmann, Hannes Federrath: Performance Comparison of low-latency Anonymisation Services from a User Perspective. in: Proc. 7th Workshop on Privacy Enhancing Technologies, University of Ottawa, Canada, Springer-Verlag, Heidelberg, 2007.

Hannes Federrath: Technische Grundlagen von Auskunftsansprüchen. Zeitschrift für Urheber- und Medienrecht ZUM 50/6 (2006) 434-438.

- Stefan Köpsell, Rolf Wendolsky, Hannes Federrath: Revocable Anonymity. in: Günter Müller (Ed.): Proc. Emerging Trends in Information and Communication Security: International Conference, ETRICS 2006, Freiburg, Germany, June 6-9, 2006, LNCS 3995, Springer-Verlag, Heidelberg 2006, 206-220.
- Hannes Federrath: Privacy Enhanced Technologies: Methods, Markets, Misuse. Proc. 2nd International Conference on Trust, Privacy, and Security in Digital Business (TrustBus '05). LNCS 3592, Springer-Verlag, Heidelberg 2005, 1-9.
- Andreas Pfitzmann, Marit Hansen: Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology http://dud.inf.tu-dresden.de/Anon_Terminology.shtml, 2005
- Hannes Federrath, Claudia Golembiewski: Speicherung von Nutzungsdaten durch Anonymisierungsdienste im Internet. Datenschutz und Datensicherheit DuD 28/8 (2004) 486-490.
- Hannes Federrath: Das AN.ON-System – Starke Anonymität und Unbeobachtbarkeit im Internet. in: Helmut Bäumler, Albert von Mutius (Hrsg.): Anonymität im Internet. Vieweg-Verlag, Wiesbaden 2003, 172-178.
- Hannes Federrath, Marit Hansen (als Gastherausgeber): Schwerpunktheft Anonymität und Pseudonymität in Anwendungen. Datenschutz und Datensicherheit DuD 27/5 (2003).
- Stefan Köpsell, Hannes Federrath, Marit Hansen: Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes. Datenschutz und Datensicherheit DuD 27/3 (2003) 139-142.
- Oliver Berthold: Analyse moderner Mixschemata in offenen Umgebungen. DACH Security IT Security & IT Management, Patrick Horster (Ed.) Proceeding of DACH Security, 25.-26.03.03, Erfurt, Germany, ISBN 3-00-010941-2, 2003.
- Oliver Berthold, Claudia Golembiewski, Sandra Steinbrecher: Erfahrungen mit dem Betrieb eines Anonymisierungsdienstes, in: IT-Sicherheit im verteilten Chaos, Tagungsband zum 8. Deutschen IT-Sicherheitskongress des Bundesamts für Sicherheit in der Informationstechnik (BSI), SecuMedia Verlags GmbH, Ingelheim 2003, S. 203.
- Claudia Golembiewski, Marit Hansen, Sandra Steinbrecher: Experiences Running a Web Anonymising Service. in: Proc. 14th International Workshop on Database and Expert Systems Applications (DEXA 2003), Workshop on Trust and Privacy in Digital Business at DEXA'2003, 1.-5.09.2003, Prague, Czech Republic, 482.
- Hannes Federrath, Marit Hansen (als Gastherausgeber): Schwerpunktheft Anonymität. Datenschutz und Datensicherheit DuD 27/3 (2003).
- Hannes Federrath, Stefan Köpsell, Heinrich Langos: Anonyme und unbeobachtbare Kommunikation im Internet. Proc. GI-Jahrestagung 2002, Informatik bewegt. Lecture Notes in Informatics (P-19), Köllen Verlag, Bonn 2002, 481-488.
- Oliver Berthold, Heinrich Langos: Dummy Traffic Against Long Term Intersection Attacks. in: Proc. 2nd Workshop on Privacy Enhancing Technologies, San Francisco, CA, USA, April 2002.

Hannes Federrath: AN.ON – Privacy Protection on the Internet. ERCIM News No. 49, April 2002, 11.

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.

Oliver Berthold, Andreas Pfitzmann, Ronny Standtke: The Disadvantages of Free MIX Routes and How to Overcome Them. in: Hannes Federrath (Ed.): Designing Privacy Enhancing Technologies. Proc. Workshop on Design Issues in Anonymity and Unobservability, LNCS 2009, Springer-Verlag, Heidelberg 2001, 30-45.

Oliver Berthold, Sebastian Clauß, Stefan Köpsell, Andreas Pfitzmann: Efficiency Improvements of the Private Message Service. in: Information Hiding 4th International Workshop, IH 2001 Pittsburg, PA, USA, April 2001 Proceedings, LNCS 2137, Springer-Verlag Berlin, 112-125.

Oliver Berthold, Hannes Federrath, Stefan Köpsell: Web MIXes: A system for anonymous and unobservable Internet access. in: Hannes Federrath (Ed.): Designing Privacy Enhancing Technologies. Proc. Workshop on Design Issues in Anonymity and Unobservability, LNCS 2009, Springer-Verlag, Heidelberg 2001, 115-129.

Hannes Federrath (Ed.): Designing Privacy Enhancing Technologies. Proc. Workshop on Design Issues in Anonymity and Unobservability, LNCS 2009, Springer-Verlag, Heidelberg 2001.

Literatur

- [1] Martin Bartosch: Lotus notes client: Security advisory, 23.März 1999. <http://securityportal.com/list-archive/bugtraq/1999/Mar/0154.html>.
- [2] Oliver Berthold: Effiziente Realisierung von Dummy Traffic zur Gewährleistung von Unbeobachtbarkeit im Internet. Diplomarbeit, TU Dresden, Institut für Theoretische Informatik, Dezember 1999.
- [3] Oliver Berthold, Hannes Federrath, Marit Köhntopp: Project “Anonymity and Unobservability in the Internet”. In: Proc. Workshop on Freedom and Privacy by Design / Conference on Freedom and Privacy 2000, Toronto/Canada, April 4–7, 2000. Association for Computing Machinery, ACM, ISBN 1-58113-256-5, 2000, 57–65.
- [4] Holger Bürk, Andreas Pfitzmann: Value exchange systems enabling security and unobservability. *Computers & Security* 9/8 (1990) 715–721.
- [5] David Chaum: Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms. *Communications of the ACM* 24/2 (1981) 84–88.
- [6] David Chaum: Blind Signatures for Untraceable Payments. In: Ronald L. Rivest, A. Sherman, David Chaum (Hg.): Proc. CRYPTO '82. Plenum Press, New York, 1983, 199–203.

- [7] David Chaum: Security without Identification: Transaction Systems to Make Big Brother Obsolete. *Communications of the ACM* 28/10 .
- [8] David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. *Journal of Cryptology* 1 (1988) 65–75.
- [9] David A. Cooper, Kenneth P. Birman: Preserving privacy in a network of mobile computers. In: 1995 IEEE Symposium on Research in Security and Privacy. IEEE Computer Society Press, Los Alamitos, 1995, 26–38. <http://cs-tr.cs.cornell.edu:80/Dienst/UI/1.0/Display/ncstrl.cornell/TR85-1490>.
- [10] Lance Cottrell: Mixmaster & Remailer Attacks, 1995. <http://www.obscura.com/~loki/reamailer-essay.html>.
- [11] R. Dingledine, N. Mathewson, P. Syverson: Tor: The second-generation onion router. In: Proceedings of the 13th USENIX Security Symposium. Aug. 2004. URL citeseer.ist.psu.edu/dingledine04tor.html.
- [12] Michael Doberenz, Michael Popp: Sicherheitslücken und Angriffe im Intra- und Internet. Studienarbeit, TU Dresden, Institut für Theoretische Informatik, Dez. 1998.
- [13] Michael Doberenz, Michael Popp: Sicherheitsprobleme durch aktive Inhalte im Internet. Diplomarbeit, TU Dresden, Institut für Theoretische Informatik, Nov. 1999.
- [14] Fasbender, Kesdogan, Kubitz: Variable and Scalable Security: Protection of Location Information in Mobile IP. In: Proc. IEEE VTC. Atlanta, USA, Mai 1996.
- [15] Hannes Federrath: Flaw in anonymity systems found, Febr. 2000. <http://www.inf.tu-dresden.de/~hf2/anon/aproxies/indexe.html>.
- [16] Hannes Federrath: Privacy enhanced technologies: Methods, markets, misuse. In: Proc. 2nd International Conference on Trust, Privacy, and Security in Digital Business (TrustBus '05), Lecture Notes in Computer Science 3592. Springer-Verlag, Berlin, 2005, 1–9. <http://www-sec.uni-regensburg.de/2005/Fed2005TrustBus05InvitedPaper.pdf>.
- [17] Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: Mixes in Mobile Communication Systems: Location Management with Privacy. In: Ross J. Anderson (Hg.): Proc. 1st Workshop on Information Hiding, Lecture Notes in Computer Science 1174. Springer-Verlag, Berlin, 1996, 121–135.
- [18] Hannes Federrath, Kai Martius: Anonymität und Authentizität im World Wide Web. In: ITG-Fachtagung „Internet - frischer Wind in der Telekommunikation“, ITG-Fachbericht 153. VDE-Verlag, 1998, 91–101.
- [19] Hannes Federrath, Andreas Pfitzmann: Neue Anonymitätstechniken. *Datenschutz und Datensicherheit DuD* 22/11 (1989) 628–632.

- [20] David M. Goldschlag, Michael G. Reed, Paul F. Syverson: Hiding routing information. In: Ross J. Anderson (Hg.): Proc. 1st Workshop on Information Hiding, Lecture Notes in Computer Science 1174. Springer-Verlag, Berlin, 1996, 137–150.
- [21] Claudia Golembiewski, Marit Hansen, Sandra Steinbrecher: Experiences running a web anonymising service. In: Proc. 14th Intl. Workshop on Database and Expert Systems Applications (DEXA'03). IEEE Computer Society, Prague, Czech Republic, 1.–5.Sept. 2003, 482–486.
- [22] Dogan Kesdogan, Roland Büschkes, Otto Spaniol: Stop-and-Go-MIXes Providing Probabilistic Anonymity in an Open System. In: Günter Müller, Kai Rannenberg (Hg.): Multilateral Security in Communications, 3: Technology, Infrastructure, Economy. Addison-Wesley, München, 1999, 365–380.
- [23] Dogan Kesdogan, Jan Egner, Roland Büschkes: Stop-and-Go-MIXes Providing Probabilistic Security in an Open System. In: David Aucsmith (Hg.): Proc. 2nd Workshop on Information Hiding, Lecture Notes in Computer Science 1525. Springer-Verlag, Berlin, 1998, 83–98. <http://www.cl.cam.ac.uk/~fapp2/ihw98/ihw98-sgmix.pdf>.
- [24] Andreas Pfitzmann: Dienstintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. IFB 234. Springer-Verlag, Berlin, 1990.
- [25] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Datenschutz garantierende offene Kommunikationsnetze. Informatik-Spektrum 11/3 (1988) 118–142.
- [26] 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. Datenschutz und Datensicherheit DuD 13/12 (1989) 605–622.
- [27] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-Mixes: Untraceable Communication with Very Small Bandwidth Overhead. In: Proc. Kommunikation in verteilten Systemen (KiVS), IFB 267. Springer-Verlag, Berlin, Febr. 1991, 451–463.
- [28] Andreas Pfitzmann, Michael Waidner: Networks without user observability. Computers & Security 6/2 (1987) 158–166.
- [29] Birgit Pfitzmann, Andreas Pfitzmann: How to break the direct RSA-implementation of MIXes. In: Advances in Cryptology – Eurocrypt '89, Lecture Notes in Computer Science 434. Springer-Verlag, Berlin, 1989, 373–381.
- [30] Wolfgang Pöpl: Integration eines Datenscanners in den Anonymisierungsdienst AN.ON. Diplomarbeit, Universität Regensburg, Institut für Wirtschaftsinformatik, Sept. 2006.
- [31] Michael K. Reiter, Aviel D. Rubin: Crowds: Anonymity for Web Transactions. DIMACS Technical Report 97/15 .

- [32] R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM* 21/2 (1978) 120–126. Reprinted: 26/1 (1983) 96-99.
- [33] Sarah Spiekermann: Die Konsumenten der Anonymität – Wer nutzt Anonymisierungsdienste? *Datenschutz und Datensicherheit DuD* 27/3 (2003) 150–154.
- [34] Sarah Spiekermann: The desire for privacy: Insights into the views and nature of the early adopters of privacy services. *International Journal of Technology and Human Interaction* 1/1 .
- [35] Ronny Standtke: Benutzer- und Entwicklungsumgebung zur anonymen Kommunikation. Diplomarbeit, TU Dresden, Institut für Theoretische Informatik, Februar 1999.
- [36] Gritta Wolf, Hannes Federrath, Andreas Pfitzmann, Alexander Schill: Endbenutzer- und Entwicklerunterstützung bei der Durchsetzung mehrseitiger Sicherheit. In: Patrick Horster (Hg.): *Sicherheitsinfrastrukturen. Grundlagen, Realisierungen, Rechtliche Aspekte, Anwendungen. Proceedings des Workshops, Hamburg, 9.-10. März 1999, DuD Fachbeiträge. Vieweg-Verlag, Wiesbaden, 1999, 17–30.*
- [37] Andreas Zschocke: Analyse und Katalogisierung von Angriffen über spezielle Ports. Studienarbeit, TU Dresden, Institut für Theoretische Informatik, Juli 1999.