Interview Prof. Andreas Pfitzmann

Zeit: 21.Juni 2010, 11:00 bis 12:30 Uhr
Ort: Dresden, Institut für Informatik, Büro Prof. Pfitzmann
Interviewer: Martin Rost

Status: Die Transkription wurde automatisch erstellt. Die Übereinstimmung zwischen Audio-Aufnahme und Transkript wurde für Kap. 3 geprüft.
Zeitpunkte dieser Bearbeitung: 2026-0726csh, 2026-0728mr
Kontakt: martin.rost@maroki.de

1. Quellen

- https://www.maroki.de/pub/video/pfitzmann/interview_pfitzmann_pub_v1.mp4
- https://www.maroki.de/pub/video/pfitzmann/interview_pfitzmann_pub_v1_transkript.pdf

2. Inhaltliche Gliederungsübersicht

Diese Übersicht fasst die zentralen inhaltlichen Stationen des Interviews mit Andreas Pfitzmann zusammen und dient als Orientierung für die anschließende wörtliche Transkription.

1. **Einstieg in Datenschutz und Informatik:** Pfitzmann schildert seinen persönlichen Weg zur Informatik, die Prägung durch die Volkszählungsdebatte 1983 und seine frühe Beschäftigung mit Datenschutz durch Technik.
2. **Frühe technische Datenschutzforschung:** Das Interview behandelt die Bedeutung von David Chaums Arbeiten zu Mixen, digitalen Pseudonymen und anonymen Kommunikationsstrukturen sowie die Rezeption dieser Ideen im deutschsprachigen Raum.
3. **Mehrseitige Sicherheit:** Pfitzmann erläutert das Konzept der Sicherheit für alle Beteiligten, die Aushandlung unterschiedlicher Interessen und den Zusammenhang mit technischem Datenschutz.
4. **Anonymität und praktische Umsetzung:** Ein Schwerpunkt liegt auf anonymen Kommunikationsdiensten, deren technischer Realisierung, den Grenzen früher Implementierungen und den gesellschaftlichen Reaktionen von Nutzerinnen und Nutzern, Polizei, Medien und Institutionen.
5. **Identitätsmanagement:** Das Gespräch beschreibt den Übergang von Datenvermeidung zu Teilidentitäten, digitalen Pseudonymen und der Frage, welche personenbezogenen Informationen in welchem Kontext tatsächlich erforderlich sind.
6. **Politische Wirkung technischer Datenschutzforschung:** Pfitzmann reflektiert Erfolge und Misserfolge politischer Einflussnahme, insbesondere bei

Kryptoregulierung, Steganografie, Vorratsdatenspeicherung und der Bedeutung einprägsamer Bilder in politischen Debatten.

7. **Datenschutz und Datensicherheit:** Das Interview grenzt Datenschutz als Schutz von Menschen vor übermäßigem Wissen anderer von Datensicherheit als Schutz von Daten ab und zeigt zugleich ihre technische Abhängigkeit voneinander.
8. **Systementwurf und Datenminimierung:** Pfitzmann beschreibt, wie er Systeme analysiert: über Zweck, benötigte Daten, weglassbare Komponenten, Speicherdauer, Erweiterbarkeit und Schutzmechanismen an Benutzungsschnittstellen.
9. **Ubiquitous Computing und Ambient Assisted Living:** Ein längerer Abschnitt behandelt die Risiken allgegenwärtiger Sensorik, automatisierter Auswertung und möglicher Machtverschiebungen durch umfassende Datenerfassung.
10. **Technischer Datenschutz 3.0:** Am Ende entwickelt Pfitzmann die Idee, künftig nicht nur Datenerfassung zu vermeiden oder Identitäten zu managen, sondern auch Kontexte von Kommunikationsakten technisch zu bewahren.
11. **Nachgang:** Der abschließende Nachtrag greift grundsätzliche Überlegungen zu offenen Netzen, rechtlicher Beherrschbarkeit, Wissenschaftskultur und Forschungsfreiheit auf.

3. Transkription, mit Zeitstempeln

(letzte Änderung: 27. Juli 2011)

Martin Rost: Prof. Pfitzmann, vielen Dank, dass ich zu einem Interview zu Ihnen kommen konnte. Wir sitzen hier in Dresden an der Technischen Universität, Lehrstuhl Datenschutz und Datensicherheit. Sie sind der Lehrstuhlinhaber. Bevor wir zu den Inhalten des Datenschutzes kommen, zu den sehr spannenden in technischer Hinsicht; und dafür sind Sie Spezialist, interessiert mich natürlich, wie Sie zum Datenschutz gekommen sind.

Andreas Pfitzmann: Oh, das ist irgendwo eine lange und eine kurze Geschichte. Die lange Geschichte ist, dass mich seit Ende meiner Schulzeit sehr bewegt hat: Was will ich in meinem Leben tun? Will ich mich mit Menschen beschäftigen? Ich habe damals darüber nachgedacht, Psychologie oder auch Theologie zu studieren. Will ich was aus meinen mathematisch-technischen Begabungen machen? Will ich mit Maschinen arbeiten? Und dann wurde mir damals so in der Abiturphase gesagt: Da gibt es ein Studienfach, was mit beidem etwas zu tun hat, die Informatik. Davon habe ich vorher noch nie gehört, das war damals neu. Da habe ich mich entschieden: Ja, das klingt gut. Es ist zwar mehr technisch-mathematisch, aber hat sicherlich mit dem Menschen und der Gesellschaft mehr zu tun als Physik oder Mathematik. Das studiere ich. Und es war mir während meines ganzen Studiums klar, dass ich diese technischen Dinge lernen möchte. Letztlich um dann irgendwie für Menschen oder für die Gesellschaft, irgendetwas Sinnvolles zu tun. Das ist die lange Geschichte.

Die kurze Geschichte geht dann so: Im Frühjahr 83 war ich gerade fertig mit meinem Studium. Ich habe im Herbst 82 mein Studium abgeschlossen, war ganz frisch

wissenschaftlicher Mitarbeiter an dem Lehrstuhl für Fehlertoleranz. Da hielt Frau Dr. Ruth Leuze, Landesbeauftragte für den Datenschutz in Baden-Württemberg, eine Vorlesung in Karlsruhe über Datenschutz. Dafür hatten die Studenten lange gekämpft. Das war am Anfang unseren Professoren gar nicht so recht, denn es hatte ja was mit Politik, mit Recht, also mit Dingen außerhalb der Informatik zu tun. Das war auch nicht sehr beworben, da waren vielleicht in der ersten Veranstaltung 20 Studenten. Und dann war ja für dieses Frühjahr die Volkszählung angesetzt. Das erste Mal waren wir 20, dann waren wir 40, dann platzte der Seminarraum aus allen Nähten, dann gingen wir in einen der größeren Hörsäle, der war das nächste Mal halbvoll und zum Schluss war er zum Bersten voll. Und es war für mich ein Aha-Erlebnis, wie starke Emotionen diese Volkszählung weckt. Wie sehr manche Bürger riesige Angst hatten, dass der Staat sie ausspionieren könnte, dass mit ihren Daten irgendetwas getan werden könnte, was gegen ihre Interessen ist. Vielleicht war bei vielen das Gefühl: "Menschenskind, 1983, das ist irgendwie 1984 Minus 1; also wir sind ganz dicht davor." Also es war eine riesige Bewegung und ich saß da mit innerlich offenem Mund. Und ziemlich in derselben Zeit ... ich bin damals regelmäßig in das Fakultätskolloquium gegangen ... hatten wir einen Vortrag von jemandem, der kam von der Fernmeldeindustrie. Der arbeitete an einem Projekt das hieß "Bigphone": breitbandiges Integriertes Fernmeldeortsnetz". Die Idee war: Wir vermitteln in Zukunft alle Dienste, also auch Fernsehen, auch Rundfunk. Was technisch den ungeheuren Charme hat, dass man jetzt aus einem unbegrenzten Angebot auswählen kann. Also die Übertragungsstrecke selbst ist nicht mehr das Limit, dass man nur eine bestimmte Anzahl an Fernsehkanälen übertragen kann, sondern man wählt aus. Und der Preis ist natürlich, dass diese Auswahl wahrnehmbar ist und auch registriert werden kann im Kommunikationsnetz. Bei dem klassischen Fernsehnetz kriegt das Netz nicht mit, wie viele Leute und welche Leute welchen Kanal sehen, welche Sendung, aber bei Bigphone würde man genau mitkriegen, welche Filme gesehen werden, wann umgeschaltet wird usw. Und da konnte man ganz genau verfolgen, welche Filme jemand sieht, ob er umschaltet, wenn gerade wenig Gewalt ist oder wenn viel Gewalt ist. Das war viel mehr unter die Haut gehend als die, mit Verlaub gesagt, doch eher etwas langweiligen Fragen in der Volkszählung. Also habe ich diesen Fernmeldetechniker gefragt, ob er denn mitkriegen würde, was gerade mit der Volkszählung los ist, und ob er jemals darüber nachgedacht hätte, was seine Arbeit als Ingenieur an diesem neuen Netz für Bezüge hat zum Datenschutz und ob er glaubt, dass dieses Netz irgendwann irgendwer akzeptieren würde. Und ich hatte Glück. Das war ein ganz ehrlicher Ingenieur, der mir sagte, er selbst hätte noch nie darüber nachgedacht, und er kennt auch niemanden, der darüber je nachgedacht hätte. Das hat dann zusammen mit der Vorlesung von der Ruth Leuze dazu geführt, dass ich angefangen habe, in der Kaffeerunde in unserem Institut über dieses Problem nachzudenken mit meinen Kollegen.

00:05:54

Martin Rost: und das Problem ist ja auch explodiert, die technische Entwicklung ist ja seitdem ja auch explodiert

Andreas Pfitzmann: Ja, uns war klar, wie viele technische getriebene Innovationen in der Infrastruktur kommen werden über die nächsten 10, 20, 30 Jahre. Ja und ich hatte auf einem Mal das Gefühl, Menscheskind, Andreas, das ist doch die Sache, wie du jetzt dein technisches Wissen und dein Interesse und dein Wunsch, auch wirklich für die Bedürfnisse der Menschen

etwas zu tun und nicht nur Geld zu verdienen, wie du das alles zusammenbringen kannst. So bin ich in den Datenschutz gekommen. Ich habe dann etwa 1 1/2 Jahre noch technischen Datenschutz ... so haben wir es damals genannt ... also Datenschutz durch Technik gemacht.

00:06:41

Martin Rost: In den 80er Jahren schon?

Andreas Pfitzmann: 83 war das, technischer Datenschutz

Martin Rost: Datenschutz durch Technik. Es gab einen großen Einfluss aus Amerika; einen theoretischen akademischen Einfluss.

Andreas Pfitzmann: Ja, also die ersten Monate habe ich völlig gearbeitet sozusagen aus dem Nichts. Ich habe mit Null angefangen, ich kannte nichts in der Richtung, und dann sagte mir auf der ersten Tagung, wo ich ein Papier untergebracht habe, ein Professor, Professor Fiedler: "Kennen Sie den Namen David Chaum?" Ich meinte, nein, kenne ich nicht, können sie mir den mal buchstabieren? Ich habe mir den Namen aufgeschrieben und bin in die Bibliothek gegangen und habe einen Artikel von David Chaum gefunden: "Communication of the ACM" von 1981 ... also noch ein paar Jahre früher, als David Chaum das Konzept *Mixe* und *Digitale Pseudonyme* entwickelt hat. Das fand ich interessant und spannend, ein klein bisschen natürlich auch enttäuschend: Oh, ich bin nicht der Erste. Ich bin sozusagen ein unabhängiger Zweiter, aber es hat uns einfach als Gruppe auch vorangebracht, weil David Chaum als Kryptograph ein anderes Herangehen an die Probleme hat, er wollte alles gerne mit Kryptographie lösen. Ich kam eher so von der Netzwerktechnik, von den Netzen; ich wollte die Probleme am liebsten gleich auf der physischen Ebene lösen. Aus heutiger Sicht würde man sagen: Sie mit Kryptographie lösen zu wollen, führt zu dem klareren Systementwurf. Oder dem flexibleren Systementwurf, und ist das, was sich durchgesetzt hat. Also wir lernten in der Literatur die erste grundlegende Arbeit von David Chaum kennen. Ich habe damals versucht, ihm einen Brief zu schreiben. Den habe ich auch geschrieben, auch abgeschickt, ist aber wohl nie angekommen. Ich hatte zunächst einmal keine Möglichkeit, ihn zu erreichen, ich hatte keine neuere Adresse und im Frühjahr 85 habe ich ihn dann auf einer Tagung getroffen, angesprochen. Er war überrascht, das jemand seinen Artikel nicht nur gelesen, sondern auch verstanden hatte, auch die schwierigeren Teile im Artikel. Er hat meine Gruppe und mich spontan eingeladen, ihn in Amsterdam zu besuchen. Er war damals von Amerika nach Amsterdam gewechselt, so dass der wesentliche Teil meiner Gruppe ... also Michael Waidner, Birgit Pfitzmann, teilweise ein oder zwei Studenten, ab dann des öfteren nach Amsterdam gefahren sind, und von David Chaum, der in dem Gebiet einfach ein paar Jahr Vorsprung hatte und einfach ein begnadeter Kryptograph ist, in kurzer Zeit sehr viel lernen konnten.

Ja, so bin ich in das Gebiet gekommen, und dann haben sich nach kurzer Zeit auch andere für unsere Arbeit interessiert. Zunächst einmal vor allen Dingen Juristen, bei denen fiel mir das am stärksten auf. Da gab es natürlich sehr unterschiedliche Kommentare, also z.B. Datenschützer in der damaligen Zeit: "Was, Sie wollen die Daten verschlüsseln? Dann können wir ja überhaupt nicht mehr kontrollieren, wer was an wen schickt!" Also Datenschützer hatten in der damaligen Zeit das Gefühl: Also Datenschutz findet bitte nicht durch Technik statt, sondern durch Recht. Technik ist ja genau das, was gefährdet, wir brauchen das Recht,

um zu schützen. Na gut, mit dem stimmte ich nicht allzugut überein, aber es war schon einmal ein negatives Feedback und es ist immerhin ein Feedback und deutet irgendwo Interesse an. Dann gab es in der GI eine Fachgruppe, die sich so mit Rechtsinformatik, rechtliche Gestaltung von Informationstechnik beschäftigt.

00:10:43

Martin Rost: Nennen Sie mal Namen!

Andreas Pfitzmann: Das waren damals Herr Göbel, das war Herr Fiedler, Herr Redecker, die waren auch einfach interessiert, weil für die war neu, das wir jetzt manche Dinge direkt technisch unterstützen oder gar bauen wollten. Die haben uns zu vielen kleinen Workshops eingeladen, viel mit uns diskutiert und haben uns sehr geholfen, anzufangen zu verstehen, wie Juristen ticken. Ich will noch nicht behaupten, dass ich es schon ganz verstanden hätte, aber wir haben angefangen, das zu verstehen, und das war sozusagen die erste Disziplin außerhalb der Informatik, mit der wir ganz enge Kontakte hatten. Die Datenschützer selbst haben in den ersten Jahren noch nicht sehr reagiert. Ich weiß noch, dass ich dann so die ersten Papiere an die Frau Dr. Leuze geschickt habe mit einem Dankesbrief, wie toll ich es für mich fand, dass sie mich doch auf das Thema gebracht hat. Da kriegte ich dann einen lieben Brief zurück, aber da passierte nichts. Und es war dann erst sehr sehr viel später, dass Datenschützer sich wirklich für das interessiert haben, was wir machen, und haben sich darauf eingelassen.

00:12:02

Martin Rost: Ungefähr zeitlich?

Andreas Pfitzmann: Da sind wir jetzt ... schätze ich ... so 88/89/90/91 ... wo dann Leute wie Hansjürgen Garstka oder Helmut Bäumler in Kiel Leute wie mich einluden und sagten: "Ihr müsst mal bei uns Weiterbildung machen. Unsere Dienststelle aus Juristen muss jetzt was lernen über Technik und technische Möglichkeiten." Das war für mich eine große Überraschung; bin ich auch gerne hingefahren, habe gerne etwas beigebracht. Und was das Schöne natürlich ist, dann auch wiederum viel dazu gelernt, weil die Fragen, die man dann kriegt, vermitteln einem viel, wie z.B. die Fragen: Was interessiert die wirklich? Wie gut hat man erklärt usw.?

Ich habe viel von Juristen gelernt. Und es entstand dann auch ein lockerer Kontakt ... wahrscheinlich schon ein paar Jahre früher ... mit der Forschungsgruppe Provet ... also mit Professor Dr. Alexander Roßnagel. Und ich glaube, wenn ich jetzt über mein Leben so zurückgucke, dass wahrscheinlich Alexander Roßnagel der Jurist ist, mit dem ich am längsten und beständig immer wieder Austausch hatte.

00:13:20

Martin Rost: Die Chaumschen Papiere... Wie haben Sie das aufgenommen? Was haben Sie damit gemacht?

Andreas Pfitzmann: Wir haben dann zunächst einmal versucht, manche Dinge aus den Papieren aus unserer Sicht verständlicher aufzuschreiben. Und wir haben auch versucht, die Ingenieursperspektive, ein stückweit auch die juristische Perspektive, hineinzubringen und sozusagen die sehr sehr guten Ideen von David Chaum zu erweitern. Und zu überlegen, wie

könnte man sie implementieren und in den späteren Jahren dann auch wie man sie verbessern kann. Und ich denke, dass ist uns gelungen, da sind in der damaligen Zeit eine ganze Reihe von grundsätzlichen Artikeln entstanden. Aus heutiger Sicht muss man sagen, leider noch sehr viel auf deutsch; aus Wissenschaftler-Sicht muss man sagen, leider, weil das natürlich etwas ist, was jetzt unsere Kollegen aus Amerika oder Kollegen aus weltweit praktisch nicht lesen können. Als deutscher Staatsbürger muss ich sagen, glücklicherweise auf Deutsch, weil zumindest die Juristen und Politiker der damaligen Zeit mit englischen Artikel schlichtweg überfordert gewesen wären. D.h. dass wir viel am Anfang auch in Deutsch publiziert haben, hat geholfen, dass im deutschsprachigen Raum diese Auseinandersetzung Datenschutz und Technikgestaltung viel früher und intensiver gepflegt wurde, als ich das in irgendeinem anderen Sprachraum kenne. D.h. also, wenn man so in den Jahren von 85 sagen wir mal bis 90 lesen will, was in dem Bereich führende Literatur ist, dann ist die Literatur auf Deutsch, und nicht auf Englisch; erst in den späteren Jahren hat dann natürlich Englisch als Wissenschaftssprache auch in dem Feld das Rennen gemacht.

00:15:16

Martin Rost: "Mixe" von David Chaum, da haben Sie sich ja dran gemacht, mit Kollegen zusammen, die Dinger wirklich praktisch auf die Beine zu stellen, das wirklich umzusetzen, zu zeigen, dass das nicht nur Überlegungen sind, die vielleicht irgendwann in der Zukunft umgesetzt werden können, sondern die jetzt schon machbar sind.

Andreas Pfitzmann: Jetzt sind wir natürlich in den Jahren schon viel viel später. Mehrseitige Sicherheit ging los.

Martin Rost: Was heißt das? Mehrseitige Sicherheit; was ist die Kernidee?

Andreas Pfitzmann: Die Kernidee ist, dass wir uns um die Sicherheit von allen Beteiligten, man könnte fast allgemeiner noch sagen, von allen Betroffenen kümmern wollen. Wobei die Kernidee ist, schon möglichst nicht nur Betroffene zu haben, sondern die Betroffenen sozusagen in eine aktive Rolle zu bringen, dass sie Beteiligte sind und sich selbst in dem Prozess in dem Ablauf des Systems vertreten können und artikulieren können. Die Idee wäre also, dass man damit anfängt, wenn man ein System baut und konzipiert, erst einmal zu fragen: Was sind denn die unterschiedlichen Interessen? Das mal ordentlich analysiert und hinschreibt und dann natürlich dabei landen wird, dass es dabei typischerweise Interessengegensätze gibt. Bei Interessengegensätzen muss man jetzt gucken: Wie führen wir eine Aushandlung? Also wie lösen wir die Gegensätze auf? Weil ich kann natürlich als Ingenieur kein System bauen, was gegensätzlichen Anforderungen genügt, das geht nicht. Ich brauche eine widerspruchsfreie Anforderungsanalyse, sonst kann ich nichts bauen. Was natürlich auch umgekehrt bedeutet: Wenn diese Interessen aufgelöst werden müssen, dann muss die Interessenauflösung sozusagen schneller gehen als man typischerweise ein System bauen kann, d.h. also unsere Infrastruktur muss so gebaut werden, dass die verschiedensten Arten von Gewichtung der Interessen und Auflösung der Interessen unterstützt werden kann. Ja, also nach Ende der Aushandlung müsste klar sein, was gelten soll. Worauf hat man sich geeinigt? Und das müsste man dann auch gegen andere durchsetzen können. Also Datensicherheit und Datenschutz sollte ja nicht nur eine Absichtserklärung sein oder ein Versprechen was dann später auch beliebig vergessen, gebrochen und ignoriert werden kann.

Sondern wir hätten es schon gerne durchgesetzt. Und da würde man dann bei mehrseitiger Sicherheit sich auch wünschen, dass jeder seine Interessen durchsetzen kann gegen die anderen. Wenn man es zusammenfassen will, dann könnte man sagen, mehrseitige Sicherheit ist Sicherheit mit minimalen Annahmen über andere. Und jede Annahme über andere kann natürlich auch falsch sein. Also je weniger Annahmen ich über andere machen muss, desto besser sind die Chancen, dass ich keine falsche Annahme dabei habe und dass am Schluss, das, was ich mir wünsche, von dem System auch dann wirklich gewährleistet wird. Also soweit die mehrseitige Sicherheit, die in einem Kolleg der Gottlieb Daimler- und Karl Benz-Stiftung entwickelt wurde, zusammen von Günter Müller, Kai Rannenberg und mir, plus natürlich im Umfeld noch vielen weiteren Leuten, auch andere Disziplinen. Wir hatten damals dann auch viel zu tun mit Psychologen, das war dann die zweite Fachdisziplin nach den Juristen, mit denen ich engeren Kontakt kriegte und wo ich dann auch das Gefühl hatte, langsam fange ich an, sie zu verstehen und irgendwann sogar erfreut war, dass ich das Gefühl hatte, jetzt fühle ich mich von denen auch verstanden, wahrscheinlich hat es bei denen auch viel länger gedauert, dass sie sich verstanden fühlten von mir als ich das Gefühl hatte, ich würde sie verstehen.

Und dieses Konzept "Mehrseitige Sicherheit" ist aus meiner Sicht so eine Art Überbau oder Verallgemeinerung einerseits von der klassischen Sicherheit. Klassische Sicherheit war: Derjenige, der das System baut, entscheidet, wieviel und welche Art von Sicherheit da drin ist. Also typischerweise, wenn die Banken Systeme bauen, dann interessiert die Bank sich nur für die Sicherheit der Bank und nicht für die Sicherheit der Bankkunden. Und es dauert dann typischerweise 1 1/2 Jahrzehnte, bis die Bank merkt, dass, weil sie das System gebaut hat, und weil die Richter nach und nach verstehen, dass sie es auch hätten anders bauen können, dass sie dann auf einmal die Beweislast haben, dann die Prozesse verlieren. Und also ein System, was am Anfang sehr sicher für die Bank und sehr unsicher für die Kunden war, mittlerweile sehr sicher für die Kunden ist aber sehr unsicher für die Banken. Zumindest dann, wenn die Kunden sich einen fachlichen kompetenten Rechtsanwalt suchen. Also einerseits mehrseitige Sicherheit eine Verallgemeinerung von der klassischen Sicherheit; ich denke auch ein umfassendes Konzept, wo technischer Datenschutz seinen Platz findet, weil ich natürlich auch, wenn ich meine Anforderung an das System beschreibe, sinnvollerweise sage, welche Datenschutzeigenschaften ... welche Vertraulichkeitseigenschaften ... ich da beispielsweise gerne garantiert hätte. Natürlich auch welche Datenvermeidungsstrategien. Ja, so die mehrseitige Sicherheit.

00:22:37

Martin Rost: Anonymität?

Andreas Pfitzmann: ... entwickelt, also die mehrseitige Sicherheit entwickelt, sagen wir mal als Konzept so vielleicht von 95 bis 98. Anonymität ist auch sozusagen ein Schutzziel, was dann innerhalb mehrseitiger Sicherheit abgedeckt werden kann. Das hat uns von ganz Anfang an beschäftigt ... also Anonymität, wenn wir Netze bauen, Infrastrukturen bauen, war für uns ein primäres Ziel. Von 83 an. Weil wir erstens das Gefühl hatten, wenn Vertraulichkeit hart sein soll, dann dürfen die Inhalte nur denjenigen bekannt werden, die sie kennen sollen. Aber bei Kommunikation bedeutet das, dass mindestens ein anderer den Inhalt mitkriegt. Ich meine, wenn ich will, dass es niemand mitbekommt, brauche ich nicht zu kommunizieren.

Was natürlich auch bedeutet, dass dieser andere den Inhalt immer weiter geben kann. Und bei Anonymität war für uns die große Forschungsfrage am Anfang: Können wir Netze so bauen, dass niemand mitbekommt, wer mit wem kommuniziert? Zunächst einmal kommt einem das völlig abstrus vor. Kann man das überhaupt bauen? Da würde man aus heutiger Sicht sagen: Ja, das verursacht einen spürbaren Aufwand, aber das kann man bauen. Und es ist natürlich als nächstes die Frage, ja, wer wird das denn überhaupt nutzen wollen, wenn ich kommuniziere, dann werde ich doch hoffentlich wissen wollen, mit wem ich kommuniziere. Aber die erste Frage ist: Muss man da unbedingt wissen, mit wem man kommuniziert, oder reicht es, beispielsweise eine Dienstbeschreibung oder Rollenbeschreibung zu haben und dann wende ich mich sozusagen an diesen Service; an diese Serviceadresse. Da könnten verschiedene dahinterstehen. Das ist im Übrigen gar nicht so fremd, also typischerweise wenn jemand die Telefonseelsorge anruft, dann weiß er eben auch nicht, mit welcher Person er jetzt verbunden wird, das ist eine Dienstbeschreibung. Und der zweite Aspekt dann bei Anonymität für uns war: Wenn wir einmal Anonymität haben auf der Kommunikationsebene, dann könnte man da, wo man gerne keine Anonymität hätte, ganz starke Verbindlichkeit, natürlich über digitale Signaturen, alle Nachrichten digital signieren und wenn man jetzt eine entsprechende Verzeichnisinfrastruktur drüber sog. Public-Key-Infrastruktur, dann könnte man auch, wenn dort wirklich die Namen, die zivilen Identitäten aufgeführt sind, mit sehr großer Sicherheit feststellen, von wem die Nachricht kommt. Kurzum, wir haben damals schon gesagt, dass, was da gerade gebaut wurde, das ISDN (Integrated Services Digital Network) ist ein sehr schlechter Kompromiss, weil, es weist letztlich nicht nach, von wem die Nachrichten wirklich kommen und ob sie wirklich unverändert sind. D.h. also für Integrität und Verbindlichkeit ist es eigentlich nicht gut genug. Aber es macht schon so viel an Anonymität kaputt, dass es da auch nicht gut ist; also es ist irgendwie etwas, was nichts wirklich gut leistet.

00:24:00

Martin Rost: Hat man Druck auf Sie ausgeübt, seitens der Industrie, der Sie auf die Füße traten, oder seien es die Sicherheitsbehörden? Oder hat man Sie gar nicht Ernst genommen?

Andreas Pfitzmann: Also man hat mir nicht in spürbarer oder harter Weise auf die Füße getreten. Also es gab schon den einen oder anderen Hochschullehrer in Karlsruhe, der meinte: "Herr Pfitzmann, es ist Ihnen aber schon bewusst, wie viele Forschungsgelder wir von der Deutschen Telekom kriegen oder von Siemens oder von Alcatel; und dass manches, was Sie schreiben, so aus der Sicht der Gesprächspartner so übertrieben, wie Sie es schreiben, aus meiner Sicht, so deutlich, wie Sie es schreiben, da nicht nur auf Wohlwollen stößt." Wir haben damals auch Papiere geschrieben, dass kryptographische Systeme öffentlich bekannt sein sollten, standardisiert werden sollten. Es war damals dann auch der Beginn der Kryptodebatte.

00:24:59

Martin Rost: Wo sind wir zeitlich damals wieder?

Andreas Pfitzmann: Damals ist jetzt so veröffentlicht 87, also vielleicht die Diskussion 86 beginnend. Damals haben wir den ersten Artikel im deutschsprachigen Raum darüber geschrieben. Ich denke, wir waren auch, jetzt verglichen mit den Amerikanern, wieder mal früher dran und haben da auch erwähnt die sogenannte Zentralstelle für das Chiffrierwesen. Das war damals eine Kryptoabteilung, im Wesentlichen um für den diplomatischen Dienst die

Kryptographie zu entwickeln und zu gewährleisten und natürlich auch die Kryptographie anderer Staaten zu brechen. Ich hatte mündlich gehört, dass es so etwas gibt, ich hatte da nie jemanden gesprochen. Ich glaube, die hatten auch kein Interesse daran, mit solchen Leuten wie mir zu reden. Und das erste Mal, diesen Begriff "Zentralstelle für das Chiffrierwesen" gedruckt gesehen, habe ich in dem Artikel, den wir selber geschrieben haben. Weil die suchten damals ganz und gar nicht das Licht der Öffentlichkeit. Und auch da gab es mal die Nachfrage von der ZFCH bei einem anderen Lehrstuhl in Harbor (?) in Karlsruhe, ob man diese Leute nicht irgendwie zum Schweigen bringen könnte. Aber mehr als diese Anfrage, auf die dann die Antwort zurück war: "Nein" - ich weiß jetzt nicht, ob die Antwort war: "Gott sei Dank nein" oder "Leider nein", aber die Antwort war in jedem Fall "Nein". Mehr habe ich an dieser Stelle nicht gespürt.

00:26:42

Martin Rost: D.h., man lässt Sie auch frei und nicht drangsaliert forschen?

Andreas Pfitzmann: Ja, das denke ich. Solange wir einfach geforscht haben, hatten wir, wie das bei Forschungen ist, und völlig normal, Leute, die sagten: "Was ihr macht, ist toll, wir stimmen zu!" Es gibt in jeder Forschung auch Leute, die sagen: "Nö, eure Annahmen, eure Prämissen akzeptieren wir nicht. Ihr solltet ganz andere Dinge tun." Aber das, was damals passierte, war einfach nur wissenschaftlicher Dialog, manchmal auch Streit, völlig normal.

00:27:14

Martin Rost: Aber Sie haben in Ihrem Team ja auch Ingenieure, d.h., Sie haben ja auch umgesetzt.

Andreas Pfitzmann: Damals überhaupt nicht.

Martin Rost: Dann später, hat sich da was geändert?

Andreas Pfitzmann: ... kann ich gerne dazu kommen. Also wir haben sagen wir mal bis 96/97 im Wesentlichen Schreibtischarbeiten gemacht. Das war für mich auch als Mensch etwas, was ich gerne gemacht habe, also sozusagen, Ideen, entweder von David Chaum genommen oder selbst entwickelt, und dann ziemlich haarklein durchbuchstabiert, wie könnte man die Technik entwickeln? Was kostet das? Jetzt nicht ausgedrückt in DM oder Euro, sondern: Was kostet das an Übertragungsvolumen, wie sieht es mit Verzögerungszeiten aus? Also sozusagen in Kosten ausgedrückt, wie Ingenieure halt Kosten ausdrücken. So dass klar war, in den ersten sagen wir mal gut 12/13 Jahren, dass Anonymität machbar ist, Kosten verursacht, klar. Und wenn man Anonymität nicht tut, das es dann eine politische oder juristische oder auch meinetwegen wirtschaftliche Entscheidung ist, dass man das nicht tut. Damit war ich als Mensch relativ zufrieden, weil ich denke, dass das die Aufgabe von einem Grundlagenwissenschaftler ist. Schauen, was ist an Wirklichkeiten da, wie könnte man umsetzen. Aber ich als Wissenschaftler bin nicht derjenige, der bestimmt, ob umgesetzt wird. Also Demokratie heißt, dass die Gesellschaft, das die Gemeinschaft und dann deren Repräsentanten entscheiden, was gemacht wird. So, denke ich, ist erst einmal meine Generation damit umgegangen, das war unser Forschungsansatz.

Und dann gab es so ab etwa 94/95/96 sehr stark über das Internet eine Bewegung, nicht nur Papiere zu schreiben, sondern zu sagen, wir können ausprobieren. Im Grunde ist das Internet von seiner Architektur her die große Spielwiese zum Ausprobieren. Zumindest war es ursprünglich mal so gedacht. Und manche Unsicherheiten kann man einfach auch nur so kommentieren: Es ist halt als Spielwiese konzipiert. Und es ist heute noch als Spielwiese konzipiert und man möge sich dann bitte nicht wundern, wenn es auch als Spielwiese genutzt wird. Also das kam dann in den Vordergrund, und Mitarbeiter von mir, die so vielleicht 8/10/12 Jahre jünger sind als ich, aufgewachsen sind in ihrem Studium mit "Wir probieren einfach mal aus", hatten dann sehr stark das Gefühl, wir wollen Anonymität, anonyme Kommunikation ausprobieren. Fand ich interessant, hab gesagt: Ja, okay, macht mal. Und dann haben sie auf eine Art angefangen, dass ich daneben saß und innerlich eine ganze Weile den Kopf geschüttelt habe. Nämlich, die haben nicht jetzt etwa das implementiert mit voller Stärke, was wir uns theoretisch ausgedacht haben, sondern sie haben erstmal so implementiert, dass die Performance noch halbwegs stimmt, und haben ihre Kompromisse bei der Anonymität gemacht. Das war für mich sehr ungewohnt, weil ich in meiner Arbeit am Schreibtisch natürlich das Ziel hatte: "Mach es möglichst sicher!" Also wir haben sehr früh wir haben es "Angreifermodelle" genannt, also sozusagen eine Beschreibung davon, was derjenige, der gegen die Schutzmechanismen arbeitet, wohl tun kann. Das nannten wir "Angreifermodell" Da haben wir sehr früh gesagt: "Wir gehen mal davon aus, alle Kanäle, alle Übertragungsstrecken werden von dem abgehört." Das war natürlich vielleicht 85 haben wir das das erste Mal gesagt .... das war natürlich Fiktion, das war eine Abschätzung, das war das absolute Horrorszenario. "Da haben wir viel Abstand, passiert nie." Heute muss man sagen: "Naja, das haben jetzt die Geheimdienste und die Polizeibehörden der Welt durchgesetzt, dass heute alle Übertragungsstrecken abgehört werden." Und natürlich die Konzepte, die wir damals am Schreibtisch gemacht haben, wären gegen diese Dinge nach wie vor sicher. Aber meine Mitarbeiter starteten also damals mit Angreifermodellen, die ich viel zu schwach fand, und ja ... aber sie sind gestartet -, und das brachte uns dann natürlich in Kontakt mit vielen Leuten und Organisationen und Institutionen, mit denen wir vorher keinen Kontakt hatten. Das geht sehr harmlos los. Da wurde dann unser Anonymitätsdienst genutzt, dass irgendein Schüler vermutlich sei es berechtigt oder aus Schabernack seiner Lehrerin in ihr Besucherbuch geschrieben hat: "Diese dumme Kuh kann keinen ordentlichen Unterricht machen." Und dann wandte sich natürlich die Dame an uns, sagte: "Ich will wissen, welcher Schüler das war." Wir haben natürlich gesagt: "Tut uns leid, können wir nicht rauskriegen, wir wissen es ja auch nicht." Ich weiß nicht, ob wir es geschrieben haben, aber haben es vermutlich alle gedacht, wahrscheinlich müsste sie jetzt eher die Energie reinstecken, mit ihren Schülern zu reden oder an ihrem Unterricht etwas zu ändern, als zu versuchen, über uns herauszufinden, wer denn jetzt die Kritik in ihr Gästebuch geschrieben hat.

00:33:11

Martin Rost: Das, was eben durchkam, das Besondere an diesem Anonymitätsdienst, war ja, dass das ja auch vor dem Betreiber des Dienstes schützt. Dass man das noch einmal sagt. Das war das eigentlich zu lösende Problem.

Andreas Pfitzmann: Ja, was es schon gab vorher, sogenannte Anon-Proxies, wo es einen Rechner gab, zu dem wurde hingesendet und der hat dann Adressen ersetzt und hat es

weitergesendet. Und dieser eine Rechner wusste dann natürlich ganz genau, was von wem an wen geht, so dass man, also ich wechsele jetzt mal die Perspektive, wenn ich Geheimdienstchef wäre, dann wäre völlig klar, dass ich so einen Anon-Proxy anbieten würde. Weil billiger kann ich die Information - wer hält was für geheimhaltungsbedürftig und wer will nicht beobachtet werden, wenn er mit wem kommuniziert.... also billiger kann ich an die Information nicht kommen. Und bei unserem System war es halt so, dass wir nicht über einen Zwischenknoten gegangen sind, sondern über mehrere, die dann auch unterschiedliche Betreiber haben, also einen früher Betreiber von so einem Mix war ja auch das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein, so dass dann mehrere Betreiber miteinander kooperieren müssen, um rauszukriegen, wer kommuniziert mit wem. So, das hatten wir von Anfang an dabei, aber ich könnte jetzt über viele Schwächen der zumindest ersten Varianten unserer Software berichten, wie man diese Verkettung damals auch hätte tun können, ohne dass diese Betreiber kooperieren. Das war für mich der Anlass, warum ich da am Anfang so sehr den Kopf geschüttelt habe. Aber Hannes Federrath, Stefan Köpsell und andere haben gesagt: "Andreas, lass es uns doch mal machen." Und ein Stück weit scheint das, trotz der aus meiner Sicht vorhandenen Schwächen, auch wirklich gewirkt zu haben. Weil ja jetzt nicht nur die Lehrerin, sondern auch die Polizei kam natürlich hin und wieder zu uns, mit irgendwelchen Ermittlungsverfahren, und hat gesagt: "Wir würden gerne wissen ...." Okay. Dann war unsere Standardantwort natürlich: "Es tut uns leid, wir ..." entweder wissen es nicht, wir haben keine Aufzeichnung, oder aber dann kam natürlich oftmals die Anfrage: "Aber dann zeichnen Sie bitte für die Zukunft auf." Dann ist die Frage, auf welcher Rechtsgrundlage sind wir dazu verpflichtet oder sind wir dazu zumindest berechtigt usw. usf.? Also wir hatten dann ab dem Punkt, wo wir auch praktisch ein System betrieben haben, auf einmal sehr viel Kontakt zu Polizei weniger Geheimdienste natürlich dann auch Medien und Presse.

Weil ich glaube, dass für Medien und Presse natürlich so ein laufendes System dann auch mit den kleinen Skandalen und Skandälchen viel plastischer ist und viel greifbarer. Und ich glaube, dass dieses System, an dem wir viel gelernt haben, auch natürlich noch einmal viele Benutzer dazu gebracht hat, viel über Anonymität zu lernen. Also es war sozusagen eine große ... und ist nach wie vor eine große Awareness-Kampagne.

00:36:25

Martin Rost: Die Anonymitätssoftware dieser Dienst wurde auch genutzt z.B. auch von der Polizei, wahrscheinlich auch von Großindustrievertretern wenn sie sicherstellen wollten, dass ihre Konkurrenz z.B. nicht weiß, für was sie sich interessieren. D.h. Sie haben eigentlich auch Fürsprecher in Bereichen, wo man nicht unbedingt Fürsprecher für Anonymität so erst einmal spontan vermuten würde, bei Ermittlungsbehörden zum Beispiel. Und trotzdem habe ich im Moment immer noch nicht den Eindruck, dass es eigentlich selbstverständlich sein muss, dass es eine Anonymitätsinfrastruktur für Kommunikation geben muss, um z.B. nur ein Beispiel zu nennen, politische Wahlen über das Netz machen zu können.

Andreas Pfitzmann: Also zunächst einmal ..., dass es ein Bedürfnis für Anonymität gerade auch bei Polizei, Geheimdiensten und auch bei der Industrie gibt, kann ich bestätigen. Wir hatten mal eine Zeit, da wurde so wurde uns gesagt über unseren Dienst nicht nur Kinderpornografie verbreitet, sondern es hat sich wohl auch ein Ring von Pädophilen über

unseren Dienst zum Missbrauch an Kindern verabredet. Und das ist natürlich ein Punkt, wo wir als Forscher angeboten haben: Wir fahren unseren Dienst runter. An der Stelle muss ich einfach sagen: Forschungsfreiheit ist eine schöne Sache. Aber irgendwo möchte ich mich als Forscher nicht auf meine Freiheit berufen, wenn es darum geht, dass Kinder missbraucht werden. Und die Antwort, die ich damals bekam, war: "Um Himmelswillen, fahren Sie Ihren Dienst nicht runter! Ihr Dienst muss weiterlaufen. Und zwar jetzt nicht nur, weil wir sonst die Leute warnen und sie merken, dass wir ihnen mit der Entwicklung und Strafverfolgung auf den Fersen sind. Sondern auch: Wir brauchen Ihren Dienst selbst! Weil wir sozusagen Ihren Dienst nutzen, um nach illegalen Inhalten im Internet zu suchen. Denn wenn wir mit einer IP-Adresse des BKA ankommen, dann ist natürlich klar, dass uns die Webseiten nur Inhalte anzeigen, die rechtlich okay sind." Also an der Stelle einfach der Hinweis: Das, was ein Webserver als Antwort gibt, kann auch davon abhängig sein, mit welcher IP-Adresse die Abfrage gemacht wird. Also uns wurde ziemlich klar gesagt: "Wir wollen nicht, dass Ihr Euren Dienst abschaltet. Wir brauchen Euren Dienst."

00:39:02

Martin Rost: Ich erinnere mich an die Geschichte mit China; dass man aus China heraus im Internet forschen können wollte und dass deshalb westliche Unternehmen auch auf AN.ON bzw. den JAP zugriffen.

Andreas Pfitzmann: Wir können das jetzt noch weiter machen: Ich denke, es war für Firmen wichtig. Und es war für Freiheitsbewegungen im Iran wichtig. Dieser Dienst brachte uns mit vielen Akteuren in Kontakt; wir kriegten teilweise Nachrichten aus China und dem Iran: "Danke, dass ihr diesen Dienst betreibt." Wir kriegten also nicht nur Mails von Lehrerinnen, die sich jetzt kritisiert fühlten von ihren Schülern. Wir haben natürlich auch zur Kenntnis nehmen müssen, dass dieser Dienst auch missbraucht wurde. Also ich muss für mich einfach sagen: Es geht schon unter die Haut, wenn man erfährt, dass etwas, was man betreibt, oder wo man mit dran gebaut hat, benutzt wird, um den Missbrauch an Kindern zu organisieren; das lässt einen nicht ruhig. Nach allem, was wir statistisch wissen, muss man allerdings sagen: Unser Dienst hat keineswegs eine höhere Kriminalitätsrate als das Internet als Ganzes. Also wir hatten ja in den ersten Jahren nicht gewusst: Wird unser Dienst ein Sammelbecken von Leuten, die letztlich mit dem Gesetz, und damit dann auch irgendwann mit der Polizei, in Konflikt kommen? Das ist nicht der Fall. Wir haben schon einige spektakuläre Fälle, wo unser Dienst auch für kriminelle Dinge benutzt wurde.

Aber das ist bei Millionen von Downloads und wahrscheinlich von mehreren Hunderttausend Benutzern nie gleichzeitig, aber sozusagen verteilt über dies Jahrzehnt seines Bestehens sind die Nachfragen der Polizei keineswegs ein Beleg dafür, dass es bei uns häufiger zu Konflikten mit dem Gesetz kommt. Und insoweit haben sich unsere Befürchtungen, die wir am Anfang hatten ... "Machen wir da jetzt einen Dienst und müssen wir ihn dann so vor unserem inneren Gewissen nach einem halben Jahr wieder abschalten? Einfach weil wir im Wesentlichen nur Kriminelle in ihrem Tun unterschützen?" Das hat sich nach allem, was wir wissen, nicht bewahrheitet.

00:41:28

Martin Rost: Jetzt können wir mal die Perspektive weitern, ist mein Vorschlag: Erst haben wir Infrastruktur gemacht, danach folgte ja eine Phase zum Thema Identitätsmanagement, das man erst einmal einige Schichten höher legen kann.

Andreas Pfitzmann: Ja. Also wir haben jetzt sozusagen geredet über, ich möchte es mal so nennen, *Datenvermeidung*. Und sogar nicht nur Vermeidung der *Speicherung*, sondern sogar Datenvermeidung im Sinne von Vermeidung der *Erfassbarkeit*. Das war das Thema, mit dem ich in die Forschung gestartet bin. Das läuft auch weiter. Es ist nach wie vor ein Thema unter der Perspektive: Wie weit kann man da kommen? Wie effizient kann man da werden? Aber es ist auch klar, dass es einfach viele Dienste gibt, bei denen Datenvermeidung das Problem nicht vollständig lösen kann, weil ja irgendwelche Daten kommuniziert werden sollen, weil man ja auch von Kommunikationspartnern wiedererkannt werden will, etwa um eine Transaktion fortzusetzen oder einen Dialog fortzusetzen. Und das führte sozusagen zu Arbeiten, da könnte man jetzt sagen, eine Art zweite Generation von Forschungsaktivitäten. Das ist hier in der Gruppe hauptsächlich verbunden mit dem Schlagwort: *Identitätenmanagement*. Also die Idee, dass jeder Mensch nicht nur *eine* Identität hat, und immer sozusagen unter seiner gesamte Identität auftritt also meinetwegen Personalausweisnummer, Geburtsdatum, Wohnort, Interessen, Ausbildungsabschlüsse, Blutgruppe, und was weiß ich alles; also immer unter seiner Gesamtidentität -, sondern dass man sagt: "Nein! Wir wollen in unterschiedlichen Zusammenhängen mit unterschiedlichen Teilidentitäten - so nennen wir das -, auftreten!" Also wenn es darum geht, dass ich an einem Forum teilnehme, in dem wir uns über die neuesten Witze austauschen, dann sind meine Blutgruppe und wahrscheinlich auch mein höchster Bildungsabschluss vollkommend irrelevant. Da kommt es höchstens darauf an: Waren die letzten zehn Witze, die er öffentlich gemacht hat, lustig oder waren sie es nicht? Und da könnte man sich mit sehr wenigen personenbezogenen Daten eine Teilidentität schaffen, die im Wesentlichen nur zu sichern hätte, dass jetzt niemand anders unter meinem Namen schlechte Witze posten kann. Ich bräuchte dann im Wesentlichen ein digitales Pseudonym sprich einen Testschlüssel von dem digitalen Signatursystem dann würde ich anonym auf einer anonymen Infrastruktur meine Witze posten, würde sie jeweils mit diesem digitalen Pseudonym signieren, damit klar ist, sie kommen von mir. Damit nicht jemand anders meinen guten Namen kaputt machen kann, dass meine Witze doch irgendwie ganz nett und unterhaltsam sind.

Zwischen dem "immer alles unter seiner vollen zivilen Identität zu tun" und jetzt dem anderen Beispiel mit den Witzen ... Letzteres war sozusagen das schöne andere Extrem, wo man praktisch keinerlei personenbezogene Daten braucht. Da geht in der digitalen Welt ein Auseinanderhalten, was in der gegenständlichen Welt so zumindest nicht gut geht. Und dass das Auseinanderhalten in der digitalen Welt gut geht, finde ich auch sehr sehr wichtig. Denn in der digitalen Welt ist Vergessen praktisch nicht zu organisieren. In der Oper oder im Fußballverein usw., da werden Leute mein Gesicht nach und nach vergessen, außer ich habe mich fürchterlich daneben benommen, oder sie tierisch beeindruckt. Aber in der digitalen Welt, wenn man es mal miteinander verketten und zusammenbringen kann, dann ist das nicht mehr aus der Welt zu schaffen. Und insoweit ergänzt sich sehr gut diese erste Generation anonymer Kommunikation mit dem zweiten Schritt Identitätenmanagement: Sozusagen nur das an Informationen dem Kommunikationspartner geben oder auch den Partnern, wenn man mit einer Gruppe kommuniziert, was in diesem Lebensbereich dieser Situation relevant ist.

00:47:57

Martin Rost: Ihre Arbeit ist eindeutig auch politisch. Und Sie wollen auch politisch wirken. Können Sie Beispiele dafür nennen, dass Sie erfolgreich auch politisch gewirkt haben?

Andreas Pfitzmann: Die erste Frage ist: Was heißt erfolgreiches politisches Wirken? Wenn ich es als Grundlagenforscher nehme, dann heißt es: Man hat Dinge rausbekommen in der Grundlagenforschung, die neue Möglichkeiten schaffen. Und ob man diese neuen Möglichkeiten realisieren will, darüber wird politisch diskutiert und auch entschieden. Oftmals heißt entschieden "Durch Nichtstun reagiert."... aber okay ... Also in diesem Sinne würde ich sagen: "Ja, sehr erfolgreich." Übrigens nicht wir alleine. Das war eine ganze Gruppe von Leuten: David Chaum, unsere Gruppe, inzwischen auch an vielen anderen Plätzen, sei es im deutschsprachigen Raum oder auch international. Leute, die gute Arbeit machen. Ja, die Entwicklungen im Bereich technischer Datenschutz werden wahrgenommen und werden politisch diskutiert. Das war die Sicht des Grundlagenforschers.

Wenn Sie jetzt mich fragen als politisch denkenden Bürger: "Wie sehr sind dann politische Entscheidungen so gefallen, wie ich mir das gewünscht hätte oder wie ich es mir wünsche als politisch denkender Bürger?"... Und wenn jetzt Erfolg bedeutet: Es fällt wirklich eine Entscheidung, und sie fällt in die Richtung, wie ich mir das wünsche? Dann war unser Erfolg sehr gemischt.

Es gab einzelne Fälle, wo wir Erfolg hatten. In den meisten Fällen passierte gar nichts. Und in wenigen Fällen passierten Dinge explizit gegen unseren Rat. Jetzt kann man natürlich oder muss man wahrscheinlich auch als politisch denkender Bürger sagen: Das ist doch eigentlich eine sehr gesunde Situation. Weil es wäre ja in einer gewissen Art schon sehr verwunderlich, wenn sich ein Einzelner hinstellen könnte, und sagen könnte: "Sie haben meinen Ratschlag immer angenommen, und alles ist so gekommen, wie ich es mir gewünscht hätte." Also irgendwo hätte ich fast das Gefühl, wenn das jemand sagt, dann muss er schon ziemlich dumm sein oder von sich selbst eingenommen.

Also wann haben wir als Forscher das Ergebnis bekommen, was wir uns gewünscht haben? Da ist das prominenteste Beispiel, was wir haben: das Thema *Kryptoregulierung*. Also so etwa ab dem Jahr 86 wurde intensiv diskutiert, ob man die Verwendung von Kryptographie - also Export-Implementierung vielleicht sogar - reguliert, weil die Kryptographie da soweit war, dass sie in den Massenmarkt kommen konnte. Man hatte natürlich Angst, dass die Kryptographie dann auch verwendet wird von Schurkenstaaten, von fremden Geheimdiensten, von Terroristen. Und insbesondere in den USA, aber auch in anderen Industrienationen wurde diskutiert: "Können wir nicht versuchen, dass bei Kryptographie immer irgendwo ein Schlüssel hinterlegt wird, so dass irgendjemand in der Lage ist, den Klartext mitzulesen?" Die Schlagworte aus den USA kommend waren Clipper-Chip und Key-Recovery, und dann also erst einmal Key-Escrow mit dem Clipper-Chip und später Key-Recovery. Hier haben wir ... also meine Gruppe damals noch in Karlsruhe und dann später auch an anderen Stellen, in Hildesheim und in Dresden sehr früh sehr grundlegende Papiere geschrieben, warum wir glauben, dass die Kryptographie und die Förderung von Kryptographie, gerade auch von Public-Key-Kryptographie, der Zivilgesellschaft mehr nützt, als der Versuch einer Regulierung Terroristen und Verbrecher schadet. Weil typischerweise Terroristen und

Verbrecher brauchen gar keine Public-Key-Kryptographie, die können ihre Schlüssel auch anders austauschen. Und das One-Time-Pad ... das ist ein Kryptoverfahren, was durch keinen Supercomputer der Welt zu brechen ist ... das ist einfach schon längst erfunden. Das steht in allen Lehrbüchern, das kennen alle Leute, die es wissen wollen. [Hält einen USB-Stick hoch]. Auf so einen USB-Stick kriegt man die Volkszählungsdaten von 1983 fünfmal drauf. Jetzt sind wir gerade beim One-Time-Pad, hier kriege ich so viel Schlüsselmaterial auf das One-Time-Pad, dass ich einfach auf Lebenszeit mit jemanden telefonieren kann; selbst Bildschirmsprechen viele Stunden. Also Kryptoregulierung wird, so meine Überzeugung, ich denke, es gibt sehr gute Argumente dafür ... organisierte Kriminalität und Terroristen praktisch nicht schaden, aber der Zivilgesellschaft. Dieses Argument ist ziemlich alt, steht schon in den ersten Papieren und hat, unter uns gesagt, praktisch nichts bewirkt. Weil ich das Gefühl habe, dass in politischen Diskussionen Argumente sehr sehr wenig bewirken. Wir sind dann damals also so 92/93 mal wieder die Key-Escrow/Key-Recovery-Debatte aus den USA richtig hoch geschwappt ist, in ein neues Forschungsfeld gegangen: Die *Steganografie*.

Steganografie ist eine alte Kunst, wie man geheime Daten in größeren Datenmengen, die normal erscheinen, verstecken kann. Das heißt: Man bettet geheime Daten verschlüsselt in Bilder ein und die Bilder selbst sehen danach dann praktisch genauso aus und sind sehr unauffällig. Das haben wir entwickelt und da auch die Forschung vorangetrieben. Es gab Jahre, von denen ich denke, dass wir da zumindest in Europa die beste Forschungsgruppe hatten im Bereich Steganografie. Und wir haben das auch vorführen können, teilweise auch, wie wir Daten einbetten können in Videokonferenzen. Wir haben richtig schön einen Demonstrator gebaut, wo man dann Dinge sehen konnte. Das haben wir auch vorgeführt, beispielsweise im Hessischen Landtag, da ist jedes Jahr ein großes Treffen der Datenschützer. Sie hatten uns eingeladen, ich glaube es war 98, und wir wollten das vorführen. Dann hieß es, im Plenarsaal gibt es aber leider keine Leinwand. Wir haben darauf bestanden, dass wir eine Leinwand brauchen. Wir haben es dann geschafft, dass da an einem Nachmittag wirklich ein Dübel gesetzt wurde, an die Stirnwand des Hessischen Landtages, damit dort eine Leinwand aufgehängt werden konnte, und wir demonstrieren konnten, wie das aussieht: "Bilder zeigen". Der Erfolg war durchschlagend. Was ich mir als Grundlagenforscher gewünscht hätte, ist, dass hinterher irgend jemand gekommen wäre und gesagt hätte: "Und was ist hinter den Bildern, die Ihr zeigt? Wie macht Ihr das genau?" Und das gern erläutert hätte. Niemand kam. Das wollte niemand wissen. Das haben sie uns alles geglaubt. Konnten sie auch. Okay wir haben nicht geblufft, es war real, was zu sehen war. Aber eigentlich hätte man es kritisch hinterfragen müssen, was niemand getan hat. Und die Bilder waren sehr sehr eindrucksvoll. Da fühlten sich Leute richtig berührt. Also da hat ein Staatssekretär aus dem Bayerischen Innenministerium uns als Unterstützer des Terrorismus bezeichnet. Da hat ein Bundesjustizminister gesagt: "Ja wenn das so ist, dann macht ganz offensichtlich Kryptoregulierung keinen Sinn." Also die Bilder haben wirklich beeindruckt.

Was will ich daraus lernen? Naja, es gibt manche Disziplinen, da ist es sehr einfach, Bilder zu haben. Im Bereich Steganografie, wenn man eben Bilder einbettet, ist das sehr schön zu zeigen. Und leider ... in vielen anderen Feldern ist es nicht klar, oder ist es nicht einfach, die Botschaft, die man hat für die Politik, als Bild darzustellen.

Seitdem bewegt mich die Frage immer wieder: Wir können wir das, was uns ganz wichtig ist, also unsere Botschaft, so verdichten und so darstellen, dass sie im Grunde innerhalb weniger Sekunden fassbar wird. Weil ich den Eindruck habe, dass die politische Aufmerksamkeit, das gilt für die Massenmedien, das gilt aber auch für die Aufmerksamkeit von Politikern im Grunde in Sekunden zu messen ist. Nicht in Minuten, nicht in Stunden. Also... da war ein Erfolg: Da hat dann die Bundesrepublik entschieden: Wir stimmen innerhalb der OECD gegen die von den USA eingebrachte bindende Richtlinie, dass alle Kryptografie, die in den Industriestaaten also dem Club der OECD gebaut und vertrieben wird, sozusagen eine Hintertür enthalten muss, also: Key-Recovery. Das ist wahrscheinlich der größte Erfolg, den wir hier als politisch agierende Bürger, vor dem Hintergrund, dass wir natürlich als Wissenschaftler die Grundlagenarbeit gemacht haben, den wir dort hatten.

Ich will auch reden über den größten Misserfolg: Der größte Misserfolg, den wir haben, ist, dass es uns nicht gelungen ist, Politiker zu überzeugen, dass die sogenannte *Vorratsdatenspeicherung* von Kommunikationsdaten ein großer Unsinn ist. Da gilt inhaltlich etwas sehr Ähnliches wie bei der Kryptodebatte. Die Leute, die in kleinen geschlossenen Gruppen etwas tun wollen, um Terrorakte zu planen oder auch um meinetwegen einzelne Fotos im Bereich Kinderpornografie auszutauschen. Ich brauche nicht ein Höchstleistungskommunikationsmedium, es reicht ein relativ bescheidendes Übertragungsvolumen und eine relativ bescheidene Realzeitanforderung. Und das ist etwas, was jeder, der möchte, selbst dann, wenn es in vielen Staaten Vorratsdatenspeicherung gibt und die dort auch durchsetzbar ist, immer noch erreichen kann. Indem er Strukturen nutzt, Server in Ländern, wo es keine Vorratsdatenspeicherung gibt.

Oder wir entwickeln zur Zeit auch, basierend auf dem "DC+"-Netz, einen Anonymisierungsdienst der nächsten Generation, wo es Vorratsdatenspeicherung einfach überhaupt nicht mehr geben wird. Weil es nichts gibt, was man sinnvollerweise auf Vorrat speichern könnte. Also da haben wir denke ich sehr gute wissenschaftliche Argumente, warum es nichts bringt. Es ist uns nicht gelungen, das auf einem Bild zu verdichten. Und es ist dann einfach das passiert, was die Amerikaner über die OECD wollten: Sie hätten es innenpolitisch nie durchgekriegt mit dem Key-Recovery. Sie wollten es außenpolitisch machen über die OECD. und die Data-Retention hätte vermutlich auch kein Nationalstaat durchgekriegt. Deswegen hatte man es über eine EU-Richtlinie gemacht. Und das haben wir nicht verhindern können. Da muss man jetzt mal schauen, wird diese Richtlinie vielleicht irgendwann überprüft? Vielleicht ist da auch noch nicht alles vorbei. Aber das ist aus meiner Sicht der Punkt, wo ich jetzt als Bürger sage: "Nein, wie wir argumentiert haben und wie wir auch glauben, sehr gute Argumente zu haben, das hat sich nicht durchgesetzt." Und das kann jetzt natürlich auch wiederum mit Bildern zu tun haben. Und zwar Bilder jetzt anders gemeint. Jeder, der Verbrechensaufklärung machen will, wird den politischen Entscheidungsträgern Bilder zeigen von entführten und zerstückelten Kindern, von missbrauchten Kindern. Und er wird über diese Bilder einen emotionalen Druck aufbauen, dass da etwas getan werden muss. Verständlich. Wenn man da etwas tun kann, sollte man da auch etwas tun, dass ist völlig klar. Aber der Druck ist emotional so stark, dass zumindest aus meiner Sicht einfach der Verstand aussetzt und diese Leute jedes Maß verlieren, ob denn die Maßnahmen, die jetzt vorgeschlagen werden, was man gegen diesen Missbrauch von Kindern und gegen dieses Kidnapping von Kindern usw. tun kann, ob das denn wirklich wirkt.

Unser größter Erfolg war: Wir hatten Bilder und die Bilder hatten gewonnen. Und unser größter Misserfolg war: Da hatten andere Bilder, und diese Bilder haben gewonnen. Die Schlussfolgerung ist, dass ich fast das Gefühl habe, in der politischen Diskussion kommt es auf Argumente kaum an. *Es sind die Bilder, die entscheiden.*

Und von mir aus noch eine dritte Klasse von Bildern: die einstürzenden Twin Towers. Diese Bilder hat jeder von uns in seinem Kopf gespeichert. Sie sind da. Wir empfinden es als eine Riesenkatastrophe. Wenn man nüchtern hingucken würde, 5000 irgendwas Tote, nicht mal, weniger

01:00:19

Martin Rost: Ich glaube 3600.

Andreas Pfitzmann: 3600 ... ein Bruchteil dessen, was wir an Toten jedes Jahr im Straßenverkehr haben. Das heißt: Wenn ich eigentlich meine Bevölkerung schützen will, dann muss ich nicht gegen diese Terroristen kämpfen, sondern muss ich mich fragen, wie wir unseren Straßenverkehr anders organisieren. Wenn ich gucke: Warum sind die Twin Towers eingestürzt? Vermeintlich wegen diesen Flugzeugen... klar ohne die Flugzeuge wären sie an diesem Tag auch nicht eingestürzt, in dem Sinne: ja! Aber nach allem, was wir heute wissen: Die Twin Tower wären viele Stunden später eingestürzt, falls sie denn überhaupt eingestürzt wären, wenn die Brandschutzvorkehrungen an den Stahlskeletten der Twin Tower so gewesen wäre, wie die Vorschriften waren. Das heißt, also eigentlich haben die Terroristen nicht wohlgebaute, wohlunterhaltende Gebäude zum Einsturz gebracht. Sondern da waren Gebäude einfach nicht so betrieben und nicht in einem Zustand, dass sie so hätten sein dürfen. Und diese Form von Kritik, dass man einfach sagt: "Okay, und jetzt geht es nicht los mit einem Kampf gegen den Terrorismus. Jetzt schauen wir uns mal die Bausubstanz an und machen entsprechende Brandschutzvorkehrungen." Das habe ich aus den USA nie gehört. Es ist vermutlich billiger und für Politiker auch prestigeträchtiger zu sagen, wir machen jetzt einen "War On Terror" als "Wir kümmern uns mal um den Brandschutz in unseren öffentlichen Gebäuden oder auch um den in wirtschaftlich genutzten Gebäuden". Also insoweit: Die Macht der Bilder ist ungeheuer groß.

Und an der Stelle auch vielleicht noch die Bemerkung: Die Bilder, die wir sehen, die neue Multimediawelt, auch viele Bilder, die ja inzwischen von Amateuren gemacht werden, und die dann weiter verbreitet werden... Einerseits finde ich es gut, dass Information nicht mehr unterdrückt werden kann. Aber wir sollten als Gesellschaft noch gucken: Wie lernen wir einen sinnvollen Umgang mit diesen Bildern, so dass nicht uns diese Bilder jede Rationalität und jeden Verstand rauben und uns einfach drängen, Dinge zu tun, die einfach irrational sind und nicht wirklich hilfreich.

01:02:38

Martin Rost: Wie würden Sie den Unterschied zwischen Datensicherheit und Datenschutz ... wo würden Sie den ziehen? Wie würden Sie das Verhältnis zueinander bestimmen?

Andreas Pfitzmann: Na, die flapsige Antwort ist natürlich: Datenschutz ist in erster Näherung Schutz *vor* Daten und Datensicherheit ist in erster Näherung der Schutz *von* Daten. Aber okay, gucken wir genauer hin.

Bei Datenschutz möchte ich Menschen schützen ... Individuen. Zumindest ist das für mich sehr stark die Motivation. Ich kann mir auch vorstellen, dass es im Datenschutz auch Leute gibt, die sagen: "Naja, die Individuen sind es nicht nur, ich möchte eigentlich auch Gruppen schützen, ich möchte auch Gruppeninteressen schützen usw." Aber für mich, zumindest in meiner Motivation, wie ich rein kam in das Feld, ist der Schutz des Individuums vor... ja übermäßigem Wissen anderer über dieses Individuum, mit der Möglichkeit, dieses Individuum dann zu verfolgen, zu manipulieren usw. eine wesentliche Motivation.

Datensicherheit ist auf eine viel größere Menge an Daten bezogen. Also bei Datenschutz geht es um Daten, die sich auf Menschen, ihr Leben, ihre Beziehung beziehen. Während Datensicherheit ... das können alle möglichen Daten sein. Das können Daten sein ... was weiß ich ... über das Liebesleben der Schildkröten. Wo ich jetzt nicht eine Datenschutzrelevanz sehen würde. Es sei denn, wir wollen den Schildkröten auch Persönlichkeitsrechte zugestehen und ihr Recht auf Privatsphäre. Was sicherlich eine interessante juristische Forschungsfrage wäre, aber vielleicht gibt es noch wichtigere Fragen als die. So wäre da meine Abgrenzung. Es ist klar, dass auch wenn ich zunächst mal alles sehr gut auseinanderhalten kann. Wenn ich dann Systeme baue, ich Datenschutz nur dann halbwegs implementieren kann, wenn ich ordentliche Datensicherheit habe. Weil ich baue typischerweise für personenbezogene Daten keine andere Infrastruktur auf als das, was ich sowieso benutze. Ich habe typischerweise auch für personenbezogene Daten keine anderen Sicherheitsmechanismen, als das was ich für jede Art von irgendwo sensiblen, sensitiven oder wertvollen Daten habe. Kurzum: Ich brauche eigentlich beides.

01:05:10

Martin Rost: Wenn Sie über Systeme nachdenken ... Sie sollen bestehende Systeme analysieren oder Sie möchten neue Systeme entwerfen ... Sie möchten sie gut entwerfen... In welchen Kategorien denken Sie über solche Systeme nach?

Andreas Pfitzmann: Zunächst einmal möchte ich verstehen und gesagt kriegen, was die Bedürfnisse sind. Was ist der Nutzen des Systems für wen? Was soll das System leisten?

Martin Rost: Die Datenschützer würden nach dem Zweck fragen. Was soll das System?

Andreas Pfitzmann: Ja. Und dann würde ich gucken, was alles an Daten brauche ich für diesen Zweck nicht? Und oftmals ist es so, man wird ja gar nicht gefragt, man soll ein neues System konstruieren, sondern es wird einem eigentlich ein schon konstruiertes System vorgestellt. Oder zumindest ein Grobkonzept für so ein System. Und wenn ich jetzt überlege: Was kann ich also alles weglassen? Dann ist es meistens nicht, dass ich mir jetzt was ausdenke: Was kann ich weglassen? Sondern da ist ein konkreter Systementwurf da, und ich frage mich: Was kann ich davon weglassen? Die nächste Frage ist: Wenn dann klar ist, was sozusagen alles weglassbar ist: Wo kann ich die Erfassungsmöglichkeit verhindern? Wo kann ich vielleicht auch Speicherdauer da, wo gespeichert werden muss verkürzen? Dann habe ich irgendwann so etwas wie einen Systementwurf, mit einem Minimum an Daten. Einem Minimum auch an Speicherdauer. Und dann ist die nächste Frage natürlich noch: Ist es irgendwo akzeptabel, dass das System ein bisschen weniger kann als das, was ihr wollt? Oder dual dazu die Frage: Soll das System, was wir jetzt konzipieren, erweiterbar sein? In welche Richtung? Also sozusagen: Wie viel Spiel nach unten und nach oben habe ich? Um dann

ausdrücken zu können, wenn ich dieses Spiel nutzen kann, was an weiteren Daten könnte ich weglassen? Wenn ich sozusagen ein bisschen runter gehen kann. Oder aber, wenn es erweiterbar sein soll... Muss ich da eventuell schon jetzt sozusagen weitere Daten oder Schnittstellen hinzufügen? Das ist meine Art zu fragen und wahrscheinlich habe ich dann sozusagen Schutzziele eher im Hinterkopf. Also Schutzziele würden dann für mich relevant oder werden mir bewusst, wenn wir uns dann vorstellen: Und wie sehen etwa Benutzungsschnittstellen des Systems aus? Also bei einem mehrseitig sicheren System hätten ja alle Beteiligten ihre Perspektive auf das System, typischerweise auch ihr Gerät mit dessen Hilfe sie dann mit dem Gesamtsystem, oder den anderen Geräten in diesem System, interagieren. Und da kommt für mich dann sehr stark auch eine Schutzzielperspektive ins Spiel, dass ich sage: "Okay, an dieser Schnittstelle muss nicht nur die Funktionalität ausgedrückt werden, sondern da muss ich jetzt auch in irgendeiner Form eine Auswahl haben. Welche Schutzmechanismen werden denn jetzt benutzt? Wie erkenne ich Leute wieder oder auch nicht usw.?" Also da spielt es dann eine Rolle.

01:08:35

Martin Rost: Nun haben wir es aber mit Ambient Assisted Living zu tun, mit ubiquitärem Computing. Und dort ist ja die Idee, dass man eigentlich bitte alles erfassen möchte vom Menschen, insbesondere beim AAL. Dort kommen Sie mit ihrem Vorschlag "Können wir das auch minimal fahren und können wir vielleicht etwas weglassen?", Da stößt man auf taube Ohren. das ganze Gegenteil ist der Fall. Und was machen Sie dann in solchen Situationen?

Andreas Pfitzmann: Ja. Da haben wir jetzt ... wenn man so will ... einen ganz ganz alten Konflikt, aber jetzt noch einmal richtig auf die Spitze getrieben. Als ich 83 anfing mich mit Netzen zu beschäftigen, war die große Frage, die mich umgetrieben hat: Wie können wir die Datenerfassungsmöglichkeit minimieren oder vielleicht sogar ausschließen? Weil damals war klar: Wenn Daten mal erfasst sind - oder wenn es darum geht, welche Art von Gewissheit kann ich mir erschaffen? Wenn Daten mal erfasst werden konnten, dann kann ich hinterher nie mehr nachweisen, dass sie nicht erfasst wurden. Oder dass, falls sie erfasst wurden, dass sie inzwischen aber wirklich in allen vorhandenen Exemplaren gelöscht wurden. Das war der Startpunkt von unserer Arbeit. Und die Motivation damals war: Wozu brauchen wir das? Weil einfach klar ist, dass dieses exponentielle Wachstum von Speicherkapazitäten und Verarbeitetung und auch Kommunikationskapazitäten dazu führt, dass Speicherung und Verarbeitung, auch Kommunikation, so billig wird, dass die Kosten irrelevant werden. Was also bedeutet: Man ist immer in der Versuchung, auf Vorrat Dinge weiterhin zu speichern. Oder auch im Rahmen der durch die Datenerfassung gegebenen Möglichkeiten auf Vorrat zu erfassen, weil es kostet ja praktisch nichts. Und man weiß nie, wofür man das später noch einmal gebrauchen kann. Man kann im übrigen abstrakter auch noch sagen: Auch für die Daten, die wir dann wirklich erfassen, das Verständnis von Daten, die Auswertungsmöglichkeit von Daten wird ja auch laufend besser. Also auch an der Stelle bei Daten, wo wir mal akzeptiert haben "wir erfassen sie", auch die würde man normalerweise nicht wegschmeißen. Nicht nur unter dem Aspekt "wir wissen doch gar nicht, wozu wir sie mal brauchen können" sondern "wir wissen eventuell auch zum Erfassungszeitpunkt auch in den ersten Jahren gar nicht, welchen Informationswert diese Daten wirklich haben". Weil Data-Mining-Algorithmen usw. einfach verbessert werden.

Das heißt also, unsere Früherkenntnis war: Wenn ich jetzt Vertraulichkeit wirklich als eine harte Eigenschaft will - und ich denke, dass ist in relevanten Teilen, wenn es jetzt um Macht, Machtausübung, Machtkontrolle geht - dass es dann schon hart sein muss. Also wenn ich - was weiß ich - von einem Geheimdienst unter Druck gesetzt werde, mit Behauptungen "Wir wissen folgendes über Sie: ...", dann möchte ich schon wissen: Was wissen die jetzt wirklich und wo bluffen die? Oder wenn Familien bedroht werden: Ich möchte schon wissen: Was wissen die jetzt wirklich über die Familie über Aufenthaltsorte usw.? Das heißt also: So eine weiche Vertraulichkeit... "Naja, ich hoffe mal, dass die das nicht wissen usw.", das wird mir eben nicht das Rückgrat stärken, dann "Nein!" zu sagen. Sondern in dem Moment, wo Vertraulichkeit nicht wirklich hart ist, nicht wirklich belastbar, werden Menschen einknicken. Was für mich sehr früh zu der Überzeugung geführt hat: Also wir müssen schon versuchen, dass die Datenerfassung vermieden wird. Und das war damals 1983 und in den Folgejahren ein ziemlich realistischer Ansatz, weil in Rechensysteme und in Datennetze die Daten hineinkamen, und nur die Daten, die halt von Menschen eingegeben wurden. Oder die halt im Rahmen von Vermittlungsprozessen entstanden sind.

01:13:01

Martin Rost: Und AAL ist das perfekte Gegenteil!

Andreas Pfitzmann: Und jetzt kommt genau das Gegenteil. Oder man sagt: das perfekte Gegenteil! Wir geben sozusagen unseren Rechnern, die immer kleiner geworden sind und leistungsfähiger, sozusagen noch ihre eigenen Augen, Ohren, Hände, um die Welt zu erfassen, zu begreifen, auszuwerten. Wir bauen auch erst einmal, wenn wir so Räume ausstatten im Bereich ubiquitäres Computing eine Infrastruktur, wo wir dann noch gar nicht wissen, was wird dann später in diesen Räumen gemacht. Also wir sind in der Hinsicht bestrebt, was Sensoren angeht, universell genug zu sein, dass damit alles geht. Wir nehmen im übrigen jetzt auch noch Dinge auf, gerade im Bereich Multimedia, wo wir noch weniger wissen, was der eigentliche Informationsgehalt ist. Also, was weiß ich... Wenn sie 1983 von mir E-Mails aufgezeichnet hätten, da hätte man sicherlich auch rausgekriegt: "Okay, was weiß der? Was kommuniziert der? Was macht der an typischen Interpunktions- oder Grammatik- oder Rechtschreibfehlern?" Okay, ja da stand schon mehr Info in dem Text, als nur das, wovon der Text handelt. Also man kann ein bisschen schließen darüber: Wie ist vielleicht seine Schulbildung? Vielleicht, wenn das jetzt sehr variiert, kann man noch ein bisschen was daraus schließen: Wie wichtig es jetzt ist? Wie in Zeitnot ist er jetzt gerade usw.? Aber wenn wir jetzt Räume haben, die etwas machen, was im Grunde diesen Videokameras entspricht, die jetzt gerade aufzeichnen. Was zeichnen die denn gerade auf? Sie zeichnen auf, klar: Was ich rede. Wie ich rede. Wie ich das was ich sage mit Gestik und Mimik unterstreiche. Je nachdem was die Auflösung ist, zeichnen die vielleicht sogar auf, Augenhintergrund, wenn ich jetzt direkt in die Kamera gucke. Vielleicht Temperaturverteilung im Gesicht, wenn ich entsprechende mit Bildverarbeitung und Farbverschiebung reingehen würde. Und vielleicht könnte ein Arzt, wenn er diese Videos sieht und vergrößert und analysiert, sagen: "Okay, ich sehe dem Menschen jetzt an, dass er vielleicht herzinfarktgefährdet ist. Oder vielleicht Risikopatient ist im Bereich psychische Krankheiten." Wir wissen es nicht. Und das heißt also, wenn wir jetzt hier multimediale oder viele modale Größen erfassen, dann geht es absolut ins Uferlose wie man glaubt, später sie vielleicht auswerten zu können. Wie manche Leute momentan Stein

und Bein schwören, dass sie sich schützen würden, wo ich einfach sagen muss: Daten in Infrastrukturen zu glauben dass man über Jahre oder Jahrzehnte schützen kann, das ist einfach albern. Also man muss einfach nur einmal gucken: Wie häufig muss ich meine Systeme patchen? Und dann weiß ich, wie viele Tage und Wochen ich denn glauben kann, dass ich meine Daten schütze, bevor die erste Möglichkeit besteht, dass jemand sich in mein System hackt.

01:16:29

Martin Rost: Ich möchte noch einmal auf dieses Arztbeispiel kommen, der vielleicht über eine Temperaturverteilung im Gesicht zu einer Analyse vordringen könnte, dass dieser Mensch einem besonderen gesundheitlichen Risiko ausgesetzt sein kann. Er behauptet das, es wird wissenschaftlich belegt, dass es so sei. Daraufhin setzt die Versicherung ihre Police fest, so dass aus dieser Analyse schon das Recht auf informationelle Selbstbestimmung beschränkt wird, weil eine Versicherung über den Preis für die Gesundheitspolice schon so etwas wie ein normales Leben vorformt. Also, das Präventionsproblem, das sich darin ausdrückt.

Andreas Pfitzmann: Also es ist mir jetzt zu schnell. Oder ich würde mich lieber zurückhalten, das jetzt sofort abschließend bewerten zu wollen. Wenn ich jetzt sozusagen hier vor der Kamera sitze und nehme an, diese Videos würden auch unter dem Aspekt ausgewertet, und das Ziel der Auswertung wäre, dass mir mein Hausarzt sagt: "Also Herr Pfitzmann--- Sie müssen unbedingt mal in die Praxis kommen. Wir müssen mit Ihnen ein paar Tests machen. Es sieht so aus, als ob Sie momentan gefährdet werden, ich würde Sie gern innerhalb der nächsten 24 Stunden sehen." Dann würde ich natürlich sagen: Gott sei Dank, dass diese Auswertungen gemacht würden. Ich gehe dahin, selbst wenn es Fehlalarm war. Lieber 10 Mal so einen Fehlalarm, als dann erst irgendwo im Krankenhaus wieder zu sich kommen.

01:18:12

Martin Rost: Krankenversicherung?

Andreas Pfitzmann: Natürlich, wenn... und das ist jetzt das Dilemma mit dieser Art von Daten... wenn nicht ich der Erste bin, der diese Diagnose erfährt, oder mein Arzt, der im übrigen einer gewissen Schweigepflicht unterliegt. Sondern, die Gefahr ist sehr groß, dass Krankenversicherungen so etwas nutzen. Dass vielleicht auch Geheimdienste so etwas nutzen, um zu überlegen, "Hmmm wie: Ust der jetzt gerade in einer Stresssituation? Können wir den jetzt gerade besonders leicht anwerben, weil in einer Stresssituation und in einer Lebenskrise?" Also wenn ich sozusagen bei diesem Ubiquitous Computing wüsste, dass mit diesen Daten nichts Negatives gemacht wird, dann würde ich natürlich auch akzeptieren, dass viele der Auswertungen mir als Mensch auch wirklich nützen können. Aber: Meine Erfahrung sagt mir, und im Grunde genommen sagt uns das die Geschichte, dass es in der Gesellschaft immer Interessensgegensätze gab. Und dass natürlich die Fähigkeit, an Daten zu kommen und Daten auszuwerten, bedeutet: Macht auszuüben. Und damit ist natürlich so etwas wie Ubiquitous Computing und die entsprechenden Datensammlungen etwas, was aus meiner Sicht zumindest für jede Gesellschaft ein großes Stabilitätsproblem aufwirft. Wie würde ich mir eigentlich eine Gesellschaft wünschen? Ich würde mir eine Gesellschaft wünschen, in der, wenn da mal irgend etwas passiert, dann wird nicht überreagiert. Man hat eine gewisse Gelassenheit. Also nicht, dass man sagt: Laissez faire, wir kümmern uns um nichts. Aber bitte

nicht überreagieren. So, wenn wir jetzt dieses Ubiquitous Computing haben, wenn wir Leute beobachten können, wenn wir alle möglichen Auswertungen fahren können, ohne dass das die Betroffenen mitkriegen...

01:20:27

Martin Rost: Automatisiert.

Andreas Pfitzmann: Automatisiert für alle. So dann stellen wir uns bitte vor den 11.09.2001. Ein amerikanischer Präsident, der zwar sich erst einmal in die Büsche geschlagen hat und 24 Stunden überhaupt nicht zu sehen war, aber dann um so entschiedener hinterher Handlungsfähigkeit demonstrieren will und der einfach sagt: "Wir werten jetzt alles in jeder Hinsicht aus. Und jeder, der irgendwo anders ist, wird erst einmal präventiv beobachtet oder weggeschlossen. Und dann schauen wir nach und nach alle Leute, die im Normalen sind, die lassen wir dann auch wieder ins normale Leben rein usw." Da muss ich einfach nur sagen: Katastrophe!

Also was ich mir eigentlich wünsche als Techniker ist, dass die Technik, an der ich mitbaue, helfen möge, dass die Gesellschaft eher stabiler und robuster wird. Und ich bin sehr vorsichtig, Technik zu bauen oder in Infrastrukturen zu bauen, wo das Potential zur Destabilisierung der Gesellschaft mit Händen zu greifen ist. Weil mir einfach die Geschichte sagt: Die Vorstellung, dass eine Gesellschaft im Management komplexer Systeme immer die Ruhe bewahrt und immer das Maß... das war noch nie so. Und ich habe keinen Glauben, dass ich denke, das wird jetzt die nächsten Jahre oder Jahrzehnte in belastbarer, in verlässlicher Weise entstehen. Und deswegen wäre ich an der Stelle lieber etwas vorsichtiger, lieber etwas behutsamer. Und insoweit wenn wir jetzt über Datenschutz reden, bezogen auf Anonymität und Datenvermeidung auf Identitätenmanagement ist natürlich Ubiquitous Computing ein Riesenproblem. Und möglicherweise, nach einer gründlichen Analyse, könnte man vielleicht zu dem Ergebnis kommen: Nein, das machen wir nicht!

01:22:37

Martin Rost: Das kann man so sagen "will man nicht". Es gibt aber keine Instanz, die darüber entscheiden kann. Und zweitens: Es findet statt. Es laufen gerade Vorstudien, jede Menge und ganz toll bezahlt, da ist ganz viel Geld drin, das lockt. Auch die Vorstellung, dass man das gesamte Pflegesystem, in diesem Wohlfahrtstaat wie bisher nicht aufrechterhalten kann. Dass die Versicherungspolicen dramatisch in die Höhe gehen müssen, wenn man das so fortsetzt. Das gilt für das gesamte medizinische System. Sondern dass auch dort eine stärkere Technisierung stattfinden muss, um überhaupt noch ein gewisses Niveau zu erlauben. Und mit dieser Vorstellung wird gerade ganz viel geforscht in diesem Bereich. Also im Moment sieht es so aus, als wenn genau jetzt diese Systeme gangbar gemacht werden sollen. Was kann man tun?

Andreas Pfitzmann: Ja, was Kleines und vielleicht was Größeres. Das kleinere ist, dass ich versuchen kann, diese Systeme, wenn es um Pflege geht beispielsweise so auszulegen, dass ich jetzt ein Pflegesystem habe, in dem alle Räume, alle unsere Wohnräume, vielleicht auch unsere öffentlichen Plätze, so mit Sensorik ausgestattet werden, dass ich alles verfolgen kann, was in dieser Gesellschaft passiert. Sondern, ich gehe jetzt ins Extrem, wenn ich potentiell

beaufsichtigt werden muss oder pflegebedürftig bin, dass dann ein Pflegeroboter in dem Raum ist, in dem ich auch bin. Oder nehmen wir an, ich bin noch bewegungsfähig, der mir hinterherläuft und darauf wartet, dass ich vielleicht umfalle, und sich dann um mich kümmert. Also, bitte, wenn ich Hilfe brauche, dann nicht so tun, als ob jetzt alle Menschen in jeder Hinsicht Hilfe brauchen. Wenn jetzt aber Ubiquitous Computing gemacht wird... was könnten Motivationen sein, es zu tun? Offensichtlich geht es nicht um Pflege. Weil das ginge mit weniger. Ist es Gedankenlosigkeit? Ist es dass die Geheimdienste sagten: "okay, wir machen jetzt Guck und Horch voll automatisiert und überall, weil Personalkapazität ist teuer, Computer sind billig?" Also wird uns dann eventuell ein Pflegesystem annonciert. Aber wirklich gebaut wird ein Überwachungssystem, mit dem man dann natürlich auch Pflege organisieren kann, klar.

Ich springe mal zurück zum Jahre 83. 83 wurde geredet über Bildschirmtext. Das war so ein uraltes System, wo im Grunde der Fernseher zu einem Art Terminal werden sollte, wo man interaktiv Daten abrufen konnte. Dieses System... wenn ich es als Ingenieur bauen würde, um möglichst genau Leute zu überwachen... würde man exakt so bauen: Keinen lokalen Speicher, möglichst kleinen Bildschirm. Damit ich jedes Scrollen, jedes, was der Mensch vor dem Ding tut, genau nach verfolgen kann. War jetzt Bildschirmtextsystem ein Systementwurf, um Leute möglichst genau beobachten zu können? Oder aber einfach ein sehr wenig durchdachter Entwurf, mit sehr unvollkommender Technik? Also ist Ubiquitous Computing ein sehr unbedachter Entwurf mit "die Sache nicht zu Ende gedacht"? Oder wird da uns was verkauft mit ganz anderen Zielen, als die die genannt werden? Ich weiß es nicht. Ich würde jetzt eher in Richtung dieser mobilen Geräte, den mobilen Begleitern, arbeiten. Also was weiß ich, manches davon gibt es ja schon. Wir haben ja schon heute unsere Handys, die im Grunde unseren Herzschlag erfassen können, wenn wir sie in der Brusttasche haben. Und die, wenn da irgendetwas Komisches passiert, einen Arzt informieren. Gibt es ja alles, gedanklich zumindest gibt es das. Es gibt auch Prototypen, es ginge auch anders. Dann stellt sich natürlich die Frage: Wenn man es nicht stoppen kann, kann man es noch für weitere gute Zwecke nutzen? Und dann muss ich jetzt noch einmal weit weit ausholen.

Als ich anfing mit Datenschutz, also mit Datenschutz durch Technik, 83 in den ersten Jahren, haben wir natürlich überlegt: Können wir viele Dinge sehr viel datenschutzfreundlicher machen?" Die Antwort war: ja! Es war uns aber irgendwie klar, dass es natürlich jetzt nicht den kompletten Schwenk geben wird. Zumindest war das nicht zu erwarten, dass die Gesellschaft komplett auf maximale Anonymität und maximale Datenvermeidung umstellt. Weil manche Leute wollen das nicht. Manche Dinge werden dann vielleicht auch teurer. Warum haben wir es gemacht? Weil wir glauben, dass es neben dem zu wissen "es geht im Prinzip" dass es gewisse Herangehensweisen an Technik stärkt. Und dass es uns in einem wahnsinnig dynamischen Prozess Zeit kauft. Also: der wahnsinnig dynamische Prozess ist: Die Rechenleistung, Speicherleistung, Kommunikationsleistung verdoppeln sich im Schnitt so etwa alle 18 Monate. Manchmal geht es ein bisschen schneller, manchmal geht es ein bißchen langsamer. Aber alle Verdopplung alle 18 Monate ist ein ganz guter Wert. Der aus heutiger Sicht rückblickend so etwas für 55 Jahre schon.

01:28:27

Martin Rost: … in Speicher und Geschwindigkeit?

Andreas Pfitzmann: Ja, alles bei gleichem Preis. Was natürlich auch bedeuten kann... ich könnte jetzt auch sagen: Alle 18 Monate kriege ich die gleiche Leistung zum halben Preis. Um mal anschaulich zu machen, was das bedeutet, eine Verdoppelung zum gleichen Preis. Man stelle sich vor: Autos in 1 1/2 Jahren, doppelt so schnell zum gleichen Preis. Da würde aber spätestens nach 20 Monaten der Gesetzgeber aktiv und sagen: "Nee, nee, nee so nicht!" Oder machen wir es anders: Halber Preis! Ein Auto, gleiches Auto, in 18 Monaten halber Preis. Das würde man vielleicht 36 Monate durchhalten und dann würde die Bundesregierung schreien: "Alarm! Womit erwirtschaftet dann die deutsche Industrie überhaupt noch ihre Exportgewinne, wenn das Zeug so billig wird? Da müssen wir eingreifen." Nur bei der Informationstechnik glaubt man, dass man es im Wesentlichen laufen lassen kann; nicht eingreifen muss. Und dass jetzt nicht um den Faktor 2 oder 4, sondern seit etwa 55 Jahren. Um es noch deutlicher zu machen: 15 Jahre bedeutet 10 mal Verdoppelung, bedeutet im Grunde der Faktor 1000! 30 Jahre bedeutet der Faktor 1 Million! Das heißt also: Hier ist ein Wachstumsprozess in der Technik, der aus Sicht von 83 schon mehrere Jahrzehnte lief. Und wo auch zu erwarten war, dass er mindest noch zwei Jahrzehnte laufen würde. Aus heutiger Sicht wissen wir: Er ist gut 2 1/2 Jahrzehnte auf jeden Fall gelaufen. Ich denke, er wird auch noch mindestens 1 bis 1 1/2 Jahrzehnte so weiterlaufen. Dieser Prozess ist etwas, was wir in der menschlichen Geschichte auf der technischen Ebene noch nie hatten.

Und eine ganz naive Vorstellung von mir ist: Wenn irgend etwas wahnsinnig schnell geht, viel zu schnell, dann ist es wahrscheinlich eine gute Sache, wenn die Gesellschaft etwas mehr Zeit gewinnt, sich darauf einzustellen. Man kann wenn da Wachstumsprozesse sind, um so viele Millionen, Milliarden usw. als Faktor, nicht erwarten, dass man das stoppen kann. Man kann nicht erwarten, dass man es völlig unter Kontrolle hält. Ich glaube zu erwarten, dass wir jetzt mit Datenvermeidung oder mit Identitätenmanagement das alles in den Griff kriegen, das wäre sehr naiv. Wir werden es vielleicht, wenn es gut läuft, in manchen Teilen in den Griff kriegen oder vielleicht auch als Ganzes etwas abfedern können. Die Gesellschaft wird etwas mehr Zeit haben; das wäre schon einmal viel.

01:31:36

Martin Rost: Das heißt jetzt: Mit Ihren Aktivitäten hat diese Gesellschaft Zeit bekommen, über das Datenschutzproblem nachdenken zu können.

Andreas Pfitzmann: Ja. Und hoffentlich auch einzusehen, dass, wenn es mit dem Datenschutz, gesehen als Vertraulichkeit, also das heißt, Datenschutz besteht darin, dass gewisse Daten nicht erfasst werden, oder dass, falls sie denn erfasst werden, sie wirklich vertraulich bleiben, dass wenn das technisch nicht mehr klappt oder nicht durchgesetzt werden kann, dass man dann in der Gesellschaft sehr viel mehr Toleranz und sehr viel mehr "Wir nutzen es nicht aus." braucht. Datenvermeidung und Identitätenmanagement haben uns etwas Zeit gegeben und vielleicht ist es für manche Sektoren auch weiterhin ein Hilfsmittel. Aber ich gehe schon davon aus, das Ubiquitous Computing, auch in der negativen Variante mit sozusagen Sensoren überall oder nahezu überall, wahrscheinlich kommt. Jetzt ist die Frage: Können wir damit noch irgendetwas tun für Datenschutz?

Und wenn ich überlege: Was kann ich für Datenschutz tun, wenn Vertraulichkeit nicht mehr wirklich geht? Weil einfach Erfassung überall, Speicherung nahezu kostenlos,

Kommunikation kostenlos, Kopien allüberall, ich kann kein Löschen mehr durchsetzen, Was kann ich dann noch tun?

Und nun ist das Einzige, was mir bisher eingefallen ist: Vielleicht kann man aus der Not eine Tugend machen, dass ich sage: Was ich jetzt in dieser Welt mit Rechnern allüberall sicherstellen kann ist, dass Äußerungen von Menschen, also dass Kommunikationsakte, nicht mehr aus ihrem Kontext gerissen werden können. Ich mache ein Beispiel: Was könnte mir als Hochschullehrer schaden? Nehmen wir an, ich wäre in einem Diskutierclub und kriege, wie in Diskutierclubs üblich, die Aufgabe, irgendeine Position zu vertreten, die jetzt möglicherweise überhaupt nicht meine Position ist. Jetzt machen wir es politisch noch richtig interessant: Also ich kriege die Aufgabe: Rechtfertigen Sie doch mal die Rassenlehre der Nazis und auch die entsprechenden Taten der Nazis so gut wie sie es können! Jetzt geschieht alles im Debattierclub. Sportlich gesehen: Wie gut kann man diese Position vertreten? Also ich engagiere mich wirklich für die Sache, finde ein paar gut oder weniger gute Argumente, trage die aber auf jeden Fall sehr überzeugend vor, wie ich kann. Wenn mir das gut gelingt, wird man den Bildern auch ansehen, oder weitestgehend ansehen: Der ist ja wirklich überzeugt davon. Denn wie will ich etwas überzeugend vortragen, wenn ich nicht selbst auch zumindest so tue, so gut ich halt kann, dass ich davon überzeugt bin. So jetzt haben sie ein Plädoyer von mir von 15 Minuten Argumentation, die Rassenlehre der Nazis mit allen Konsequenzen ist prima. So, jetzt schneiden sie den kleinen Vorspann weg, dass wir in irgendeinem Debattierclub sind, wo ich irgendeine Position zu vertreten kriege, die ich mir nicht selber ausgesucht habe. Und wir schneiden auch den Abspann wenn, wo wir dann noch miteinander sagen: "Ja, okay, war jetzt ein toller Argumentenaustausch. Aber nebenbei: Wir wissen, dass es ein Spiel ist und das es keiner von uns wirklich ernst meint; das schneiden wir auch weg." Wir stellen das ganze von mir aus unter Youtube. Und vielleicht machen noch irgendwelche Forensiker eine Analyse, dass sie feststellen, da ist kein Schnitt drin, also diese 15 Minuten sind wirklich am Block. Da ist auch keine andere Sprache unterlegt, das ist wirklich authentisch Andreas Pfitzmann, zu diesem Thema, so. Das wäre das Ende meiner Reputation.

Und was jetzt diese ubiquitäre Welt könnte ist, dass man sagt: "Okay, es gibt ja diesen Vorspann. Und diesen Nachspann. Und die Daten über: Wo haben wir uns getroffen? Zu welchem Zweck haben wir uns getroffen?" Das gibt es ja noch in x Exemplaren. Also müsste ich dafür sorgen können, technisch, dass wer immer sich dieses Video anschaut die Information erhält: hier ging es um einen Debattierclub. Hier hält nicht Andreas Pfitzmann eine Rede über das, was er wirklich denkt, glaubt, für richtig hält. So, nennen wir das mal "*kontextuelle Integrität"*. Das heißt also: Die Integrität des Kontextes wird gewahrt und kann nicht verfälscht werden oder kann nicht eliminiert werden oder unterdrückt werden. Das ist eine Eigenschaft, die sicherlich eine datenschutzfreundliche, eine dem Datenschutz fördernde Eigenschaft ist. Sie ist im übrigen nicht neu. Also solche Ideen, dass jetzt nicht Informationen falsch interpretiert werden können durch Kontextwechsel, das ist keineswegs neu. Das war für den Datenschutz, schon bevor ich damit angefangen habe zu lesen, als Problem bekannt. Diese Sorte von Problemen könnte dieses Ubiquitous Computing helfen zu lösen. So dass, wenn ich über die Zukunft nachdenke, dann bin ich nicht so naiv, dass ich glaube, dass man diese ganz großen Trends - Rechnen, Speichern, Übertragen - wird immer billiger und findet auch immer weitgehender statt - dass man das stoppen kann. Aber vielleicht kann man in manchen Sektoren gewisse Bereiche erhalten, wo man wirklich vertraulich kommunizieren

kann. Und für die Gemeinschaft und Gesellschaft als Großes dann Räume sichern, wo die Kontexte von Informationsakten wirklich gesichert werden. Und das wäre für mich dann sozusagen "technischer Datenschutz 3.0" also nicht mehr "1.0 Vermeidung", "2.0 Identitätenmanagement", sondern "3.0 Kontexte wahren".

01:37:59

Martin Rost: Professor Pfitzmann, vielen Dank für das Gespräch.

Nachgang...

Andreas Pfitzmann: Ich denke mal, Steinmüller hat ja noch Aufsätze gemacht, dass offene Netze, im Sinne von: Netze für beliebige Dienste, rechtlich prinzipiell nicht mehr zu beherrschen sind. Das war so einer seiner Grundlagenartikel, wo er einfach sagte: Um die Zulässigkeit zu beurteilen, brauche ich die konkreten Dienste. Und deswegen kann ich über ein offenes Netz, wo ich die Dienste eben noch nicht habe, sondern für beliebige Dienste als Jurist nichts sagen. So sein Argument damals. Und im Grunde ist ja das Internet jetzt wirklich die Implementierung davon, was man früher Mal unter dem ISDN verstanden hatte. Das ISDN sollte ja sozusagen ein Vehikel sein für diese offenen Netze. Was es nur sehr eingeschränkt geworden ist. Und das Internet ist dann das geworden, was ISDN mal werden sollte. Also low cost, sehr flexibel und verbindet alles mögliche. Und im Grunde wäre dann Steinmüllers Resignation an der Stelle auch wirklich inhaltlich gut zu begründen, dass er einfach sagt: Mit dem jetzt vorhandenen Rechtsinstrumentarium ist das nicht mehr zu beherrschen oder da kommt man nicht mehr weiter.

Jetzt kommt wieder ein bisschen Kulturpessimismus von meiner Seite rein: Es ist so, dass wir uns mit der Hochschulreform nicht so viel....Evaluation, Trallala Trallal machen, dass es diese Positionen oder Forschungsräume, über die wir jetzt reden, gar nicht mehr gibt. Weil die guten Leute einfach sagen: Ich werde Anwalt und ich verdien wirklich Kohle. Ich ärgere mich doch nicht mit der Uni-Verwaltung rum, mit der jährlichen oder alle dreijährlichen Evaluation. Aber wenn alle 50 nur low risk machen und Mainstream. [Achselzucken].