IPv6 - Chance und Risiko für den Datenschutz im Internet*

Hannes Federrath, Universität Hamburg, Fachbereich Informatik

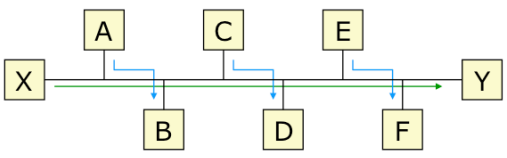
Vortrag beim IPv6-Symposium des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Museum für Kommunikation, Leipziger Straße 16 in 10117 Berlin, 22.11.2011

Meine Damen und Herren, Herr Schaar, vielen Dank für die Einladung. Ich möchte mich in meinem Vortrag zunächst nur auf technische Sachverhalte beschränken und lasse alle politischen Dinge außer Acht. Ich denke, es wird noch Gelegenheit in der Diskussion später geben, auch auf politische und strategische Fragen einzugehen.

Als ich mich auf meinen Vortrag vorbereitet habe, ist mir klar geworden, dass es eine gute Idee ist, zunächst einige Grundlagen im Bereich der Rechnernetze-Kommunikation darzulegen mit dem Ziel, manche Zusammenhänge besser zu verstehen. Dabei gehe ich natürlich insbesondere auf IPv6 ein und werde dann in einem zweiten Teil des Vortrags auf das eigentliche Thema, nämlich die Risiken und die Chancen von IPv6 eingehen, wobei ich hier, weil die Risiken, glaube ich, alle schon weitgehend und gut benannt sind, einfach auch ein paar Chancen erläutern möchte, die sich für den Datenschutz ergeben würden. Herr Schaar hat uns dies mit seinen einführenden Worten schon sehr schön motiviert.

Lassen Sie mich vielleicht als Erstes kurz erläutern, warum wir überhaupt Adressen in Kommunikationsnetzen brauchen. Sie sind nötig für das sog. Routing, also die Wegleitung einer Nachricht vom Sender zum Empfänger. Das Routing muss **einfach** sein, es soll stabil sein, es soll **robust** sein, es soll **fair** und **optimal** sein. Es soll nicht nur funktionieren, sondern eben auch ganz bestimmte Anforderungen erfüllen, die hier alle genannt sind.

Bei **Robustheit** sehen Sie sehr schön, dass wir es mit einem Sicherheitsziel zu tun haben. Hier geht es um die Verfügbarkeit von Kommunikation. Ist eine Route ausgefallen, dann soll es möglich sein, eine alternative Route zu wählen. Das bedeutet aber auch, dass die jeweiligen Ziele von Nachrichten explizit benannt sind und in aller Regel Routing-Informationen enthalten. Wir alle kennen das: Bei einer normalen Briefadresse existieren hierarchisch verschiedene Bereiche, die geografisch zugeordnet sind, und in einer bestimmten Reihenfolge auf einem Brief notiert werden. Im Grunde genommen funktioniert die Adressierung im Internet ähnlich. Die vorderen Bereiche der IP-Adresse bezeichnen größere Bereiche und die hinteren Teile der Adresse, dann im lokalen Bereich ganz bestimmte Geräte. Das ist deshalb auch wichtig, weil mit einer Vergrößerung der Adresse in IPv6 natürlich genau dieses Grundprinzip vom Groben zum Feinen noch stärker als in IPv4 zum Tragen kommt.



Optimalität: Wenn A, B, C, D, E, F gemeinsam voll auslasten können, sollten X und Y warten

Fairness: X und Y sollten jedoch nicht benachteiligt werden

Abbildung 1 – Kriterien Optimalität und Fairness beim Routing

* in: Peter Schaar (Hrsg.): Internetprotokoll Version 6 (IPv6) - Wo bleibt der Datenschutz? Tagungsband zum Symposium des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am 22. November 2011 in Berlin, 14-23. Die vollständigen Vortragsfolien sind im Internet unter http://www.informatik.uni-hamburg.de/SVS/publ/?search=ipv6 zu finden.

Die anderen genannten Kriterien möchte ich im Einzelnen nicht alle erläutern, aber damit Sie vielleicht einfach auch ein Gefühl dafür bekommen, dass eben nicht nur ein Aspekt eine Rolle spielt, sondern mehrere, habe ich für das Kriterium Optimalität noch ein Beispiel: **Optimalität** bedeutet, wenn hier beispielsweise Links, die ich mit A, B, C, D und E, F in der Abbildung 1 bezeichnet habe, gemeinsam die Leitung voll auslasten können, während X und Y vielleicht nur eine niedrige Last erzeugen, dann wäre eine optimale Routing-Entscheidung, dass X und Y warten und dafür zunächst die Pakete von A bis F transportiert werden. **Fairness** würde dann wiederum bedeuten, dass irgendwann auch X und Y „drankommen“, also nicht ewig warten müssen. Ich betone das auch deshalb, weil mit IPv6 sich manche Dinge geändert haben, die eben gerade hinsichtlich sog. **Quality-of-Service-Merkmale** eine neue Dimension darstellen. Man darf also bei IPv6 nicht nur den einen Aspekt isoliert betrachten, dass da viel größere Adressen mit natürlich viel besserer Identifizierbarkeit existieren, sondern muss weitere Merkmale im Auge behalten, die durchaus ihren Sinn haben können, wenn man das Internet, das ja seit vielen Jahren existiert, optimieren, also letztendlich verbessern will.

Zu den Adressen also dem wichtigsten Aspekt, der jetzt auch in dieser Diskussion eine Rolle spielen muss, möchte ich noch sagen: Wir haben in heutigen Kommunikationsnetzen nicht nur eine Adresse. Es gibt neben den IP-Adressen auch noch MAC-Adressen[1] und letztendlich auch sog. URLs[2]. Die URL enthält tatsächlich die IP-Adresse, aber eben auch weitere Merkmale, die eine Ressource im Internet eindeutig identifizieren. Wenn wir also über Datenschutz reden, und vor allem über Veränderungen, die über die Zeit durch Adressierung entstehen können, dann sollten wir nicht den Fehler machen, uns nur mit einer Ebene, oder wie Informatiker sagen, einer Schicht zu beschäftigen, sondern wir müssen alle Schichten eines Kommunikationsnetzes im Blick haben. Und es gibt in der reinen Lehre, ein Modell für den Aufbau von Kommunikationsnetzen mit insgesamt sieben Schichten. Sieben ist eine schöne Zahl. Sie wissen, die hat eine gewisse Magie. Das ist aber vermutlich nicht der Grund, warum tatsächlich sieben Schichten existieren, aber als dieses sog. OSI-Referenzmodell (siehe Abbildung 2), OSI steht für Open Systems Interconnection, entwickelt wurde, gab es das Internet überhaupt noch nicht.

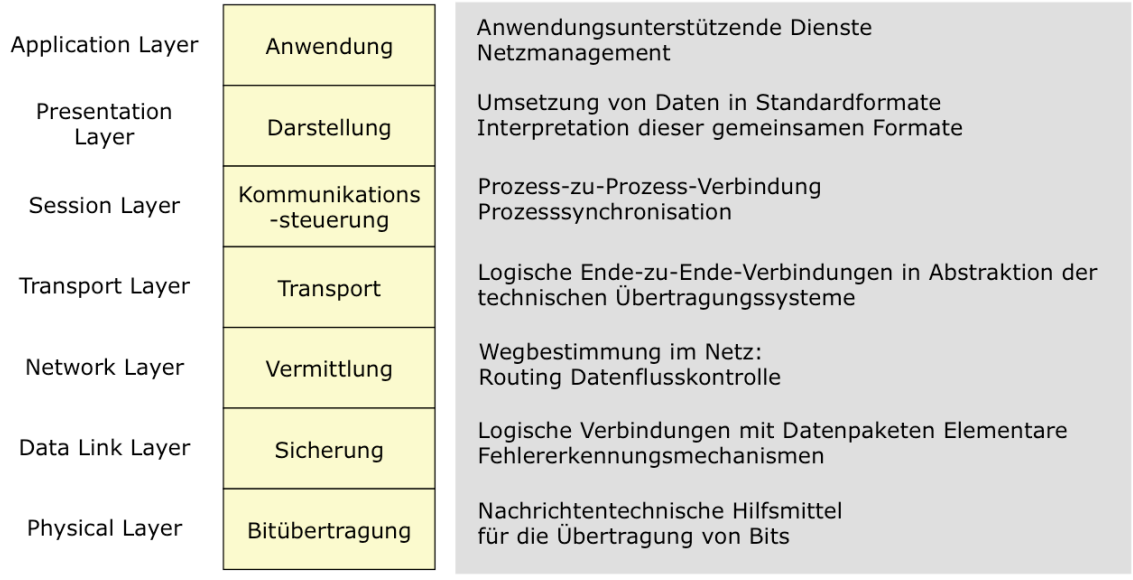


Abbildung 2 - OSI-Schichtenmodell

Sie finden in diesem OSI-Referenzmodell eine sehr schön strukturierte und hinsichtlich ihrer einzelnen Funktionalitäten auch wirklich klar abgegrenzte Einteilung der Funktionen eines Kommunikationsnetzes. Wir müssen uns die einzelnen Schichten jetzt hier nicht anschauen. Für uns entscheidend, weil wir ja über IP reden, ist die Schicht 3, die sog. Vermittlungs-

[1] Medium Access Control-Adresse, MAC-Adresse
[2] Uniform Resource Locator, URL; umgangssprachl. Internetadresse

schicht oder auf englisch auch Network-Layer genannt. Die Hauptaufgabe der Vermittlungsschicht ist das Routing, also die Datenflusskontrolle. Nun, diese sieben Schichten findet man nicht in jedem Gerät, das im Internet kommuniziert. Die Endgeräte, also unsere PCs, unsere Mobiltelefone, die zukünftigen Fernseher, vielleicht auch irgendwelche Sensoren, die innerhalb eines Autos verbaut werden, wenn wir ganz visionär denken und datenschutzunfreundlich vielleicht auch Sensoren, die im menschlichen Körper irgendwann existieren, diese **Endgeräte implementieren immer alle sieben Schichten. Router** dagegen **implementieren** in aller Regel **nur die untersten drei Schichten** des Kommunikationssystems (siehe Abbildung 3). In jedem Router wird für jedes IP-Paket anhand seiner IP-Adresse eine Routing-Entscheidung getroffen; alle darüberliegenden Daten in diesem Kommunikationsprotokoll interessieren letztendlich bei der Wegleitung überhaupt nicht.

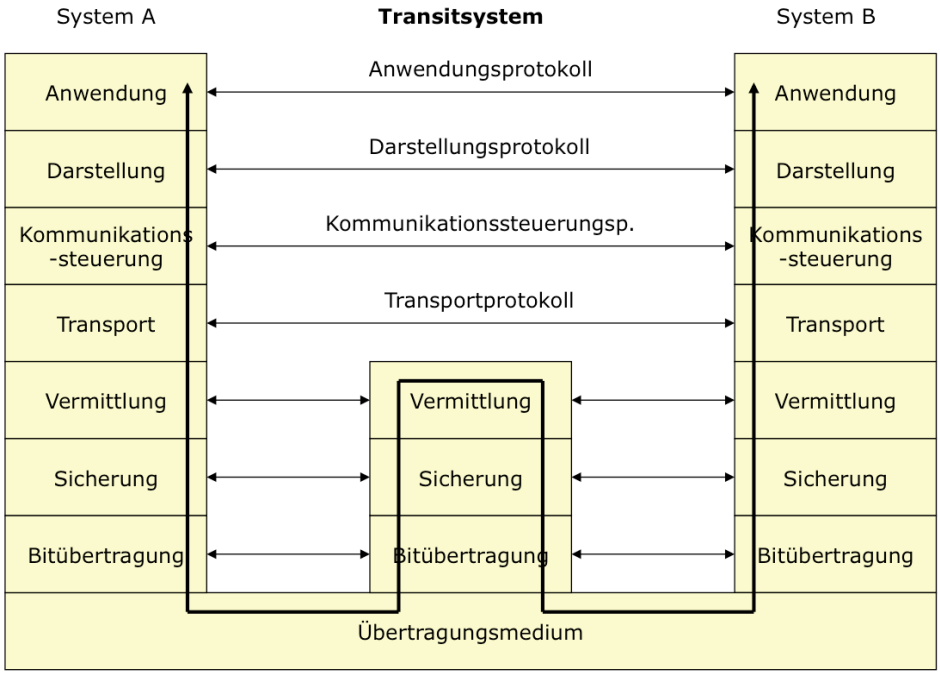


Abbildung 3 – Kommunikation im OSI-Schichtenmodell

Das OSI-Referenzmodell ist für Nicht-Informatiker schwer vorstellbar. Es ist deshalb vielleicht eine gute Idee, menschliche Kommunikation in einem Schichtenmodell beispielhaft darzustellen. Ein solches Schichtenmodell für normale menschliche Kommunikation (siehe Abbildung 4) könnte etwa so aussehen, dass jeder Mensch Gedanken produziert, auf der höchsten Ebene im Gehirn und dann in Sprache, sozusagen auf einer niedrigeren Schicht dieses Modells, ausdrückt. Es findet dann ein Dialog mittels Sprache statt und die eigentliche Datenübertragung geschieht über Laute, die über die Luft übermittelt werden. Wenn Sie dieses Modell, auf die elektronische Kommunikation übertragen wird klar, warum Kommunikation in einzelnen Schichten abläuft. Wenn wir die sieben Schichten des OSI-Referenzmodells (siehe Abbildung 3) nehmen, dann haben wir ganz unten elektrische Signale (Schicht 1), die in bestimmte Bitfolgen codiert werden (Schicht 2), die in Pakete verpackt werden (Schicht 3). Diese Pakete können zusammenhängen und werden, eine Schicht höher, jetzt sind wir oberhalb von IP, als Verbindung (Schicht 4) transportiert, und auf der allerhöchsten Ebene, der Schicht 7, gibt es eben dann Inhalte, die als Ganzes repräsentiert werden und die tatsächlich dann im Browser, im E-Mail-Programm oder als Audiosignale in einem Voice-over-IP-System nutzbar sind.

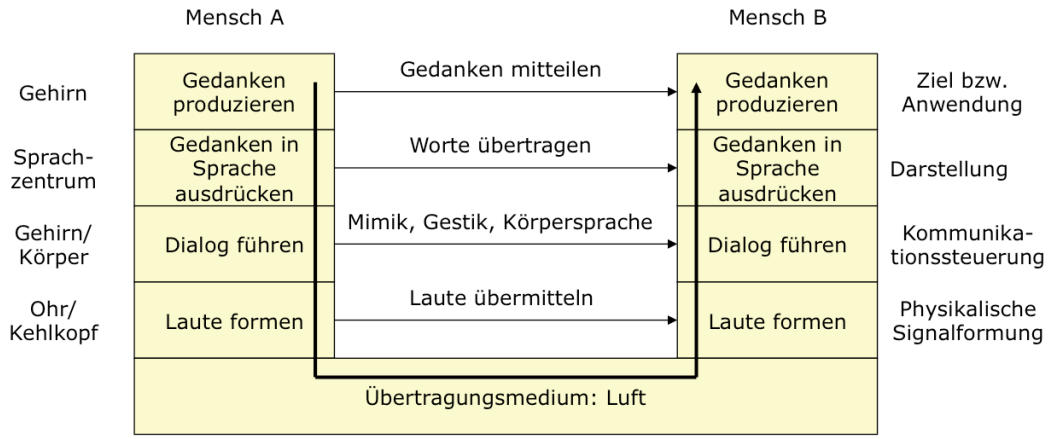


Abbildung 4 - Schichtenmodell der menschlichen Kommunikation

Im Internet finden wir heute genau die Schichten 1, 2, 3, 4 und 7. Die Schichten 5 und 6 des OSI-Referenzmodelss werden dort als Teil der Schicht 7 modelliert. Soviel vielleicht zu den Grundlagen der Kommunikation in Rechnernetzen. IP bettet sich also gewissermaßen ein in viele andere Protokolle.

Eine IP-Adresse, Herr Schaar hat es schon gesagt, hat bei IPv4 eine 32 Bit und ist sehr bekannt in der Schreibweise mit 4 von Zahlen zwischen 0 und 255. Bei IPv6 hat die Adresse nun 128 Bit, ist also deutlich angewachsen. Betrachtet man den Aufbau des IP-Headers so kann man feststellen, dass die Header von IPv4-Datenpaketen deutlich komplizierter sind als bei IPv6. IPv6 bringt also Komplexitätsreduktion. Aus Sicherheits-, vielleicht auch aus Datenschutzsicht, ist Komplexitätsreduktion immer eine gute Idee und zu befürworten. Aber es gibt in IPv6 auch Erweiterungs-Header, die wieder alles komplex und kompliziert machen können. Über die möchte ich aber im Folgenden nicht reden.

Wir stellen ein erstes Zwischenfazit: Es hat sich eigentlich wenig geändert, die Komplexität ist gesunken, die Adressen sind größer geworden und es gibt noch weitere Vorteile, die IPv6 sozusagen automatisch mitbringt. Da ist zunächst eine viel **bessere Unterstützung von Quality-of-Service-Anforderungen** zu erwähnen. Manche Datenpakete müssen schnell durchs Netz gehen, andere Datenpakete dürfen ruhig etwas langsamer unterwegs sein. Eine Priorisierung gab es zwar auch schon bei IPv4, aber bei IPv6 ist diese Priorisierung jetzt tatsächlich vollständig implementiert und auch anwendbar. Bei IPv4 war das nicht der Fall. Version 6 bringt hier auf jeden Fall qualitativ einen großen Vorteil, aber auch einen anderen Nachteil, der die **Netzneutralität** betrifft. Denn jetzt sind plötzlich Datenpakete nicht mehr gleich. Eine weitere, auf jeden Fall vorteilhafte Seite von IPv6 ist das **Vorhandensein von Sicherheitsfunktionen**. Bei IPv6 gibt es Funktionen zur Verschlüsselung und zur Authentifizierung von Datenpaketen.

Schaut man sich die 7 Schichten unter dem Sicherheitsaspekt an, dann stellt man fest, dass auf allen Schichten, bis auf die Vermittlungsschicht, also eben die IP-Schicht, bereits in IPv4 Sicherheitsfunktionen nutzbar waren, also existierten. Hier (in der Vermittlungsschicht) allerdings war ein schwarzes Loch. IPv4 hat nichts implementiert. IPv6 schließt also eine Lücke im Bereich Vertraulichkeit und Integritätssicherung. Aber: Tatsächlich ist IPSec[3] der Standard, der fester Bestandteil von IPv6 ist, auch schon mit IPv4 nutzbar gewesen. Faktisch reden wir also über einen Ist-Zustand, in dem IPSec bereits Standard ist, IPv6 aber noch nicht. Würden wir also irgendwann die größeren Adressen bekommen, würden wir ausgehend vom Ist-Zustand nur Nachteile bekommen aber keine Vorteile aus Sicherheitssicht. Denn mit IPv6 kommen nicht etwa neue aktualisierte Standards im Bereich der Sicherheit, alles bleibt eigentlich beim Alten, denn IPSec lässt sich auch mit IPv4 nutzen.

[3] Internet Protocol Security, IPSec

Wir wissen, bei IPv4 ist der Adressvorrat mit 32 Bit recht begrenzt und es ist eine Tatsache, die als unumstößlich gilt, dass der Adressvorrat von IPv4 bereits heute zu klein ist, um jedes Gerät jederzeit mit einer eindeutigen Kennung zu versehen, wohlgemerkt auf IP-Ebene. IPv6 löst dieses Problem. Damit ist aber nicht die Aussage verbunden, dass diese Adresse auf Lebenszeit dieses Gerätes immer gleich bleiben muss. Sie kann natürlich gewechselt werden. Aber zumindest die Ende-zu-Ende-Adressierung sehr vieler Endgeräte gelingt künftig nur mit IPv6. Das ist gut und ein großer Vorteil. Weiterhin, wie bereits erwähnt, kann die eingebaute Priorisierung von Datenpaketen die Netzneutralität gefährden. Das muss man kritisch sehen, darf es aber gleichzeitig nicht überkritisch sehen, denn es handelt sich hier um eine technische Priorisierung, keine ökonomische. Natürlich kann man aus technischen Mechanismen ökonomische Mechanismen generieren. Aber auf technischer Ebene ist es richtig und gut, dass eine Priorisierung vorgenommen wird, um eben letztendlich auch eine effiziente Datenübermittlung im Internet zu ermöglichen.

Dann ist weiterhin festzustellen, dass die Medium Access Control-Adresse, oder kurz MAC-Adresse, bei der es sich um eine Schicht 2-Adresse handelt, gerne als Teil der IP-Adresse in Version 6 aufgefasst wird und es auch tatsächlich entsprechende Vorschläge gibt. Das ist aus Datenschutzsicht eine schlechte Idee. Es gibt keinen technischen Grund für eine solche datenschutzunfreundliche Lösung. Dieser Vorschlag ermöglicht innerhalb eines lokalen Netzes gewissermaßen „Huckepack“ die Identifizierung eines Gerätes mittels der IP-Adresse. Das bringt technische Vorteile, aber nur Nachteile aus Datenschutzsicht. Und es ist nicht zwingend erforderlich, dass man das so macht. Man hat darauf reagiert in der Standardisierung und hat mit den sog. Privacy Extentions Vorschläge gemacht, die es ermöglichen, die MAC-Adresse zufällig zu erzeugen und regelmäßig zu wechseln. D. h. auch hier gibt es technische Vorkehrungen, die lediglich eingesetzt werden müssen und keine Verschlechterung gegenüber dem Ist-Zustand im Datenschutz bedeuten müssen.

Nun kennen Sie vermutlich Schutzfunktionen wie Network Address Translation (NAT) und Proxies, die innerhalb von IPv4 eingesetzt werden, bei denen sich die Frage stellt, ob sie auch mit IPv6 nutzbar sind. Bei **Network Address Translation (NAT)** handelt es sich um eine Adressersetzung auf Schicht 3, also auf IP-Schicht des OSI-Referenzmodells. **Proxies** ersetzen auf Schicht 7, also auf Anwendungsschicht des OSI-Referenzmodells. Beides kommt etwa auf die gleiche Art daher und die Wirkung aus Datenschutzsicht ist auch relativ ähnlich, wenn auch die technische Umsetzung doch teilweise dramatisch unterschiedlich ist. In beiden Fällen ist ein Gerät, das sich hinter einem Router befindet, nicht mehr eindeutig identifizierbar, da alle Geräte hinter diesem Router mit ein und derselben Kennung ins Internet kommunizieren. Nachteil: Es ist nicht mehr möglich, Geräte direkt zu adressieren, sondern nur über komplizierte und ressourcenmäßig sehr aufwändige Mechanismen. Trotzdem gibt es keinen Grund, sowohl Network Address Translation als auch Proxie ein für allemal zu vergessen, da beide Techniken, das prophezeie ich heute, auch weiterhin mit IPv6 eingesetzt werden, und zwar aus Gründen der Sicherheit, vielleicht auch aus Datenschutzsicht. Man sollte diese Mechanismen in jedem Fall weiterhin fördern, weil sie viele Vorteile bieten um zu verhindern, dass eine Netzinfrastruktur, die man vielleicht nicht offenlegen möchte, nach außen verborgen bleibt. Viele Firmen und Organisationen werden nicht nur aus Datenschutzsicht, sondern insbesondere aus IT-Sicherheitssicht weiterhin Network Address Translation und Proxies einsetzen, dessen bin ich mir sicher.

Ich möchte weiterhin in dem Zusammenhang noch erwähnen, dass trotz der Verwendung solcher Techniken eine **Identifizierbarkeit durch starke Angreifer** gegeben ist. Zunächst ist klar, dass ein Proxy sowieso beobachten kann. Er kennt ja sowohl die Quelle als auch das Ziel; somit ist vor dem Proxy kein Schutz möglich. Aber nehmen wir Network Address Translation: Auch hier ist es möglich, die Clients zu identifizieren. Es gibt ein Papier aus 2002 von Steve Bellovin, dem „Papst der Firewalls“. Er hat gezeigt, dass es anhand bestimmter Datenfelder innerhalb des IP-Headers möglich ist, eine solche Identifizierung einzelner Clients vorzunehmen. Sein Papier hat ursprünglich nicht darauf abgezielt, die Identifizierbarkeit zu ermöglichen, sondern lediglich zählbar zu machen, wie viele Hosts sich eigentlich hinter einem Gateway, also hinter einem solchen Router befinden. Aber man kann die

Ideen praktisch adaptieren und trotz Network Address Translation im Grunde genommen eine eindeutige Identifizierung erreichen. Gegen starke Angreifer schützen Proxies und NAT leider nicht.

Auch eine dynamische Adressvergabe, wie sie Internet-Service-Provider heute in IPv4 praktizieren, ist in Zukunft mit IPv6 möglich. Die Voraussetzung dafür ist, dass Internet-Service-Provider sensibel sind für die Problematik und auch weiterhin dynamisch Adressen vergeben wollen. Dies erzeugt überhaupt keinen zusätzlichen Aufwand. Es bringt nur Nutzen, zumindest aus Datenschutzsicht. Ich denke, man kann einwenden, dass die Strafverfolgung nicht leichter wird gegenüber dem Ist-Zustand. Das mag sein, aber gegenüber dem Ist-Zustand bringt auch bei IPv6 eine dynamische Adressvergabe kaum Performanceverluste, kaum Veränderungen hinsichtlich der Beobachtbarkeit und somit letztendlich nur Vorteile aufgrund des effizienteren und schnelleren Routings. Deswegen kann man IPv6 durchaus positiv sehen, wenn es richtig eingesetzt wird.

Lassen Sie mich zum Schluss kommen. IPv6 birgt einige Chancen aus Datenschutzsicht. Ein Vorteil ist, dass IPSec fester Bestandteil von IPv6 geworden ist. Es wird in Zukunft kein Gerät mehr geben, bei dem Verschlüsselung und Authentifizierung nicht mehr implementierbar ist. Wir haben damit zumindest ein riesengroßes Vertraulichkeitsproblem auf der Ebene der Inhalte gelöst. Es ist weiterhin so, dass jedes Gerät mehrere Adressen erhalten könnte. Der riesige Adressvorrat von IPv6 zwingt niemanden dazu, einem Gerät nur eine einzige Adresse zu geben. Ein Gerät könnte theoretisch, denken Sie an den Vergleich mit dem riesigen Erdball und der Menge an Adressen pro geografischem Gebiet, jedem Gerät viele Adressen zuweisen. Wenn ich als Informatiker von vielen Adressen rede, dann meine ich damit viele Tausend, vielleicht sogar viele Millionen Adressen. Das ermöglicht etwas, dass tatsächlich auch schon theoretisch untersucht wurde aber praktisch noch nicht implementiert ist, nämlich die Realisierung sog. Transaktionspseudonyme.

Stellen Sie sich vor, Sie besitzen eben diesen riesigen Adressvorrat und benutzen für die Kommunikation mit Ihrer Bank eine IP-Adresse, mit Ihrem E-Mail-Provider eine andere IP-Adresse. Wenn Sie im Internet zu einer bestimmten URL surfen, verwenden Sie einfach wieder eine andere IP-Adresse. Die Verkettbarkeit über viele Anbieter hinweg, die heute mittels IP-Adressen möglich ist, wird damit aufgehoben. Diese Chance hätten wir bei IPv4 niemals. Bei IPv6 erhalten Sie gewissermaßen den Adresswechsel direkt eingebaut aufgrund dieses riesigen Vorrats. Betrachtet man also aus dieser Perspektive IPv6, dann kann man nur Vorteile erkennen. Man muss sich darüber im Klaren sein, dass es dennoch weiterhin einen Präfix geben wird, d.h. man kann nicht die komplette Adresse jemals beliebig und sozusagen zufällig wählen, sondern es wird auch weiterhin einen Präfix geben müssen, der die Wegleitung zum jeweiligen Aufenthaltsort ermöglicht. Aber dieses Präfix, kann z. B. so gewählt sein, dass es immer sehr viele Teilnehmer gibt, die genau mit dem gleichen Präfix kommunizieren. Wenn viele Menschen in einer Stadt wie Berlin einen identischen Teil der Adresse nutzen, nämlich den Teil, der den Ort betrifft, dann ist der restliche Teil erst in Berlin interessant und außerhalb Berlins „verdeckbar“. Dieser verdeckte Teil erhöht den Datenschutz, zumindest wenn man sich außerhalb von Berlin befindet. Befindet man sich dann am Ort, und wird dort die Wegleitung fortgesetzt, dann muss natürlich der jeweilige feingranulare Teil aufgedeckt werden und für das Routing zur Verfügung stehen. Auf diese Weise verhindern wir sozusagen eine omnipräsente Sicht der Verteilung von Teilnehmern über den gesamten Versorgungsbereich eines Netzes. Derartige Ideen lassen sich mit IPv6 ziemlich effizient implementieren. Bisher hat das aber noch niemand implementiert.

Als Letztes möchte ich noch erwähnen, dass es tatsächlich auch innerhalb von IPv6 Mechanismen gibt für sog. Multicast. Multicast ist eine abgeschwächte Form des Broadcast. Das bedeutet, ich kann mit einem Paket nicht nur ein Ziel, sondern viele Ziele erreichen. Multicast bzw. Broadcast sind datenschutzfreundliche Technologien in dem Sinne, dass der Sender nichts wissen muss über das Ziel. Das Ziel muss lediglich die Broadcast-Adresse wissen, auf die es hört. Das bedeutet, ich kann damit einen Empfänger mit Hilfe dieser Broadcast- bzw. Multicast-Technologien relativ gut verschleiern. Sein Aufenthaltsort und seine Identität lässt

sich damit gut verbergen und es ist sogar möglich, in diesem Zusammenhang bekannte Techniken, die schon seit wenigstens 20 Jahren publiziert sind, auch in IPv6 einzusetzen. Erwähnen möchte ich in dem Zusammenhang Techniken von David Chaum wie Mixe aber auch DC-Netze. Dies sind spezielle Schutztechniken, die dem Schutz des Endteilnehmers dienen. Diese Techniken auf IP-Ebene zu implementieren, gelingt mit IPv6 sehr effizient. Bei Implementierungen in IPv4, wie sie heute mit TOR[4] und JAP[5] existieren, bleibt in aller Regel nichts anderes übrig, als auf Anwendungsschicht, also Schicht 7 zu implementieren, was in aller Regel weniger effizient geht. Wir gewinnen mit IPv6 zwar aus Sicherheitssicht gegenüber dem Ist-Zustand nichts, aber wir gewinnen Performance. Jetzt ließen sich endlich solche Anonymitätstechniken auch halbwegs performant einsetzen. Jeder, der schon mal über TOR gesurft hat, dürfte wissen, wovon ich spreche.

Vielen Dank.

[4] http://www.torproject.org
[5] http://anon-online.de