Internet-Technologie-Paradigmen und Implikationen für Privatheit und Öffentlichkeit

Matthias Bärwolff 2010
(Notizen im Rahmen der vierten Co:llaboratory-Inititative)

Die Frage nach Privatheit und Öffentlichkeit im Internet ist nicht zuletzt eine technische, das heißt, sie ist findet ihren konstituierenden Rahmen weitestgehend in den vorherrschenden technischen Gegebenheiten und Möglichkeiten. Jegliche normativen Erwägungen zu dieser Frage, erst recht der Entwurf von Szenarien, sollte die möglichen und wahrscheinlichen Entwicklungen in den technologischen Paradigmen des Internets zumindest in Erwägung ziehen.

Inhalt

Das Ende-zu-Ende-Paradigma

Das Internet kennt aus seinen Anfängen ein konstituierendes Paradigma, nämlich das von Ende-zu-Ende-Kommunikation über Protokolle die alleine in den Endpunkten sitzen und dabei auf einem internetweiten, nichtverlässlichen und extrem simplen Protokoll aufbauen welches in sämtlichen an der Kommunikation beteiligten Internetknoten – insbesondere auch den nur mittelbar beteiligten – sitzt. Das Ende-zu-Ende-Protokoll (häufig, aber nicht notwendigerweise TCP) und das internetweite "Internet Protocol" (IP) sind dabei so voneinander entkoppelt, dass beide prinzipiell austauschbar sind – weder ist IP auf TCP in irgendeiner Form angewiesen, noch ist TCP (abgesehen von der Überladung der IP-Adressen als Teil der Adressen für TCP-Verbindungen) grundsätzlich auf IP angewiesen.

Diese Architektur impliziert einen relativ breiten Raum für Privatheit gegenüber Öffentlichkeit, als dass intermediäre Knoten prinzipiell keinerlei Kenntnis der Ende-zu-Ende-Kommunikationsinhalte für ihre Arbeit benötigen, und Endpunkte völlig unabhängig von der Konstitution der intermediären Knoten jegliche Inhalte mit ihren Peers kommunizieren können – also auch verschlüsselte und signierte Inhalte. Zwar ist Verschlüsselung keine inherente Funktion des Internets, aber das Internet hält Endpunkte eben auch nicht davon ab, solcherart zu kommunizieren.[1]

… versus Anwendungsstrukturen

Nun kann zwar die Anwendungskommunikation im Internet eine unmittelbare Kommunikation zwischen zwei Endpunkten sein – direkt basierend auf eben der von TCP seit den späten 1970ern erbrachten Funktion – jedoch bildet solcherart Kommunikation die eigentlichen Anwendungsmuster wieder nur mittelbar ab. Selbst wenn sich eine verteilte Internet-Anwendung meist auf ein Zusammenspiel von TCP/IP-Verbindungen herunterbrechen lässt, übersteigt deren Komplexität die eines simplen Ende-zu-Ende-Schemas oft ganz erheblich. Schon die erste "Killerapplikation" des Internets, E-Mail, basierte auf einer verteilten Struktur, die eine asynchrone Kommunikation zwischen den Endpunkten der Applikation erst ermöglichte. In der Tat finden sich bei E-Mail praktisch alle grundlegenden Delegierungsmuster, die im Zeitalter von Googlemail und Facebook fast schon kanonisch für die Nutzung des Internets geworden sind.

---

[1] *Strikt ausgelegt, ist das Internet ja auch nur das allen Internetknoten gemeine IP-Protokoll. In der Tat gehörte theoretisch noch nicht einmal Routing zu den allermindesten Funktionen des Internets (und BGP behandelt ja bezeichnenderweise auch nur den kleinsten gemeinsamen Nenner aller Konnektivität, nämlich die Frage, ob zwischen Netzwerken solche besteht, nicht von welcher Güte diese ist).*

Der entscheidende Punkt dabei ist, dass viele Anwendungen ohne intermediäre Komponenten, die nicht der direkten Kontrolle der Endpunkte der Anwendung unterstehen, deutlich ineffizienter wären oder überhaupt nicht funktionieren würden. Was wäre das Web ohne DNS? Und was wäre "quasi-broadcast" Video-Streaming ohne CDNs wie Akamai? Und was wäre E-Mail ohne einen Proxy, der die asynchrone Kommunikation zweier Endpunkte überhaupt erst ermöglicht. Nicht nur ist bei all diesen Beispielen der Nutzen für die Endanwender unübersehbar, es ist in der Tat fast abwegig, sich ein Internet ohne solcherart Services vorzustellen.

Das Paradigma verteilter Anwendungskommunikation

Wenn das Delegieren von Anwendungsfunktionen an Intermediäre ein offenbar sinnvolles (sprich, effizientes, nützliches oder schlicht notwendiges) Muster darstellt, dann stellt sich die Frage nach Privatheit und Öffentlichkeit in einem gänzlich anderem Licht als beim simplen TCP/IP-Ende-zu-Ende-Kommunikationsfall. Meine grundlegende These ist daher die folgende:

> *In naher Zukunft wird das ursprüngliche TCP/IP-Kommunikationsparadigma des Internets – Applikationsenden kommunizieren weitgehend frei von Intermediären, die auf der selben konzeptionellen Ebene agieren – durch eines abgelöst werden, bei dem solcherart Intermediäre für die meisten Applikationen von immanenter Bedeutung sind. Dies hat weitreichende Implikationen für ein adäquates Verständnis von Privatheit und Öffentlichkeit im Internet.*

Ende-zu-Ende-Verschlüsselung versus explizite Effizienz

Für Endanwender bedeutet dies zunächst vor allem eines: Sie muss sich im Klaren sein, dass private Daten, die bei der Verwendung von Internetanwendungen anfallen, in die Hände von potenziell nicht-vertrauenswürdigen Intermediären fallen können, teilweise ganz explizit und offensichtlich – siehe etwa Facebook, Twitter oder auch Googlemail. Selbst wenn die Daten, die ein Nutzer dort einstellt, nicht für beliebige andere Nutzer zugänglich sind (sein sollen), hat der beteiligte Intermediär logischerweise Zugang zu diesen Daten.

Ende-zu-Ende-Verschlüsselung von Daten ist der einzig wirksame Schutz vor solcherart Zugriffen Dritter. Das entscheidende Problem bei solcher Verschlüsselung ist jedoch,

dass die potenziell zuträglichen und sinnvollen Funktionen, die ein Intermediär für die Anwendungsendpunkte übernehmen kann, dadurch stark eingeschränkt sind. Viele Funktionen, insbesondere solche, die sich auf mehr als zwei Endpunkte beziehen und zentralisierte Dienstleistungen erbringen, basieren darauf, zumindest Lesezugriff auf die von den Enden erbrachten Daten zu haben. Ob Broadcast-Video-Delivery oder das Einblenden von Werbung im Googlemail-Webinterface, all solche Funktionen sind nicht möglich, wenn Sender und Empfänger die Daten ihrer Kommunikation Ende-zu-Ende-verschlüsseln.

Die schlussendliche Frage lautet also bei allen Anwendungen, die eine explizite Beteiligung von Intermediären erfordern, welches Maß an Vertrauen bringt der Endanwender den Intermediären entgegen – insbesondere dort, wo es sich um informelle Nutzungssituationen handelt, etwa bei der für den Privat(!)-Gebrauch kostenfreien Nutzung von Diensten im Internet.

Ende-zu-Ende-Verschlüsselung versus implizite Effizienz

In den bisher betrachteten Fällen rufen die Endpunkten einer Applikation die Intermediäre explizit, also intentional, auf – ein Vorgang der in letzter Konsequenz zumindest potenziell unter der Kontrolle des Endanwenders steht. Ein Nutzer kann sich zum Beispiel aussuchen, welchen DNS-Server er für die Auflösung von Domainnamen verwenden möchte; selbes gilt im Prinzip für E-Mail. Ein qualitativ anders gearteter Fall ergibt sich jedoch, wenn Intermediäre "implizit" mit den Daten einer Ende-zu-Ende-Kommunikation in Berührung kommen – sei es durch ihre topologische Lage oder durch ihre kontingente Beteiligung als möglicher Knoten zwischen den Endpunkten. In diesem Falle gelten die oben gemachten Erwägungen zu Verschlüsselung in ganz ähnlicher Form. Auch hier kann der Endanwender sich vor potenziellen Zugriffen auf ihre Daten nur durch Ende-zu-Ende-Verschlüsselung schützen. Denn selbst wenn einen Router weder die Absenderadresse noch der Inhalt von IP-Paketen etwas anzugehen brauchten um seiner Hauptaufgabe nachzukommen, so hat er doch naturgemäß vollständigen Zugriff auf all diese Daten.

Aber auch hier ist es möglich, dass Intermediäre eine den Zwecken der Endpunkten zuträgliche Rolle spielen können, insbesondere da diese für die Endpunkte praktisch transparent ablaufen kann, was einerseits Kosten für jene spart und andererseits eine gewisse Flexibilität in der Gestaltung der Übernahme von Funktionen durch den fraglichen

Intermediär erlaubt.[2] Ein Beispiel ist die Priorisierung von verzögerungssensiblen gegenüber nicht-verzögerungssensiblen Anwendungen. So geschehen etwa in der Frühzeit des Internets im US-amerikanischen NSFNET in den 1980er Jahren: Als das Backbone-Netzwerk an seine Kapazitätsgrenzen stieß und Telnet-Sessions zum wachsenden Unmut der Nutzer nur noch mit deutlicher Verzögerung funktionierten, wurden die verwendeten Fuzzball-Router so umprogrammiert, dass sie IP-Pakete, die mutmaßlich zu einer Telnet-Sitzung gehörten, priorisierten, vor allem gegenüber solchen Paketen, die mutmaßlich zu einem FTP-Datentransfer gehörten. Für die Nutzer ergab sich nur ein sichtbarer Effekt: ihre Anwendungen liefen, sehr zu ihrer Freude, deutlich flüssiger als zuvor.[3] Ohne diese Episode und mögliche aktuelle Anwendungsfelder solcherart Interventionen zu bewerten, bleibt doch festzuhalten, dass es zumindest das Potenzial für ökonomisch effiziente implizite und für die Anwendungsendpunkte weitgehend transparente Intervention von intermediären Kommunikationsknoten gibt. Zumal die Grenze zwischen "expliziter Invokation" eines Intermediärs durch die Anwendungsenden und "transparenter Intervention" seitens eines Intermediärs für die allermeisten Anwender recht fließend ist: beides sind für sie Vorgänge, auf die sie im Anwendungs-Interface häufig nur bedingt Einfluss haben.

Privatheit und Effizienz

Wie kann nun ein System – in unserem Falle die technologische Infrastruktur des Internets und die konkrete Form der Anwendungen – gestaltet werden, so dass beidem genügender Raum gegeben wird: Privatheit (in Form eines gewissen Maßes an Kontrolle über private Daten) und Effizienz (in Form einer sinnvollen Balance zwischen absoluter Privatheit und einem effizienten Maß an Öffentlichkeit privater Daten, sei es durch explizite Ermächtigung Dritter oder deren transparente Intervention)? Hierzu lassen sich folgende normative Thesen skizzieren:

> *→ Es muss für Endanwender immer die Möglichkeit geben, das Internet so zu nutzen, dass, sämtliche Funktionen über Best-Effort-IP-Service[4] hinaus in den Endpunkten und damit unter direkter Kontrolle der beteiligten Endanwender liegt. Dies bezieht sich einerseits auf die Anwendungen selbst – kontingente Intermediäre sind hier explizit nicht Teil der verteilten Anwendungsstruktur – und andererseits auf die zu kommunizierenden Daten – diese werden nach dem Ermessen der*

---

[2]Transparenz ist hier im informatischen Sinne gemeint – also nicht wie in "offen", sondern wie in "dass ein bestimmter Teil eines Systems zwar vorhanden und in Betrieb, aber ansonsten 'unsichtbar' ist und daher vom Benutzer nicht als vorhanden wahrgenommen wird."

[3]Siehe für eine detaillierte Behandlung dieser und anderer Episoden Bärwolffs Doktorarbeit (zu finden unter bärwolff.de; im PDF am besten im Index of Interesting Asides nachschlagen).

[4]Zum Begriff Best Effort siehe Bärwolffs Doktorarbeit, wieder über den Index of Interesting Asides.

beteiligten Endpunkte verschlüsselt, so dass Intermediäre darauf keinen Zugriff haben. Dieser Forderung folgend sollten Anwendungen zumindest potenziell Ende-zu-Ende-basiert umsetzbar sein, und entsprechende Standards sollten dem nicht unnötig im Wege stehen.

→ Ebenso muss es aber auch möglich sein, Anwendungen so zu gestalten, dass Intermediären – sowohl explizit aufgerufenen als auch transparent intervenierenden – eine explizite unterstützende Rolle in der Ausgestaltung der Funktionalitäten zufällt. Weder sollte also Ende-zu-Ende-Verschlüsselung von Daten obligatorisch (technisch oder rechtlich) sein, noch sollte die potenzielle Rolle von Intermediären unnötig eingeschränkt werden durch rechtliche Vorgaben oder Standards in dieser Hinsicht.

Um im zweitgenannten Punkt das insgesamt eher abträgliche Potenzial von "Lemons-Market-Effekten"[5] zu verringern sind zwei Optionen denkbar, beide bislang kaum bis garnicht implementiert:

→ Erstens wäre "strukturelles Multihoming" von Anwendungsendpunkten eine gangbare Option um der Gefahr vorzubeugen, dass einzelne kontingente Intermediäre Zugriff auf die komplette Kommunikation der fraglichen Anwendung haben. Technisch lässt sich dieses Problem auf Basis von existierender IP-Technologie lösen (siehe etwa die Arbeit der Mutipath TCP Working Group der IETF), die entsprechende Ausstattung von Endgeräten mit mehreren parallelen Netzzugängen (oder entsprechenden Software-Radio-Lösungen) wäre eine wünschenswerte Entwicklung, ebenso wie die Möglichkeit für Endnutzer, ihren Internetzugang (bei insgesamt gleicher Bandbreitennutzung) auf mehrere Zugänge aufzuteilen ohne dass dadurch erhebliche Mehrkosten entstehen.

→ Zweitens wäre es vorstellbar, eine Art "don't intervene in any way, rather put me on the slow lane if you have to"-Bit (oder das logische opt-in-Gegenstück dazu) im IP-Header zu implementieren. Dies würde einen entsprechenden Industrie-Konsensus erfordern, der nicht ohne weiteres abzusehen ist, dennoch aber nicht unvorstellbar ist. Entsprechende öffentliche Diskussionen der relevanten Stakeholder hierzu wären wünschenswert.

---

[5] *Um das klassische Gebrauchtwagenmarktversagen auf unser Problemfeld anzuwenden: I cannot trust nor control whether an ISP messes with (as in inspect, sell on, etc.) my data, so I better not let him do so in the first place, thus falling back to end-to-end application implementation and full encryption, in turn reducing the overall value to be had from the application.*