Autonome Namenssysteme und beständige Adressierung für selbstbestimmte digitale Telekommunikation

F2B6 7049 3EA0 926E 3F33
363E 23D1 ECB0 2200 3311

27. Januar 2019

Outline

Namen und Adressen offline

- *“Wie heißt Du?”*: wofür Namen und wie bekommt man einen?
- Tradition, Behörden. Gutdünken. Künstler- und Ordensname.
- Register. Nicknamen. Pseudo-, Anonymität. Situationsgebunden.
- Eigenschaften: aussprechbar, bedeutsam, lokal identifizierend.
- Nicht unbedingt eindeutig. Namen bezeichnen (m:n) **Entität**en. Person vs. Person**a**
- Von Behörden mitgeformt, verwendet. **Identität**.
- Namen und Namensgebung können Machtinstrumente sein: Werkzeuge der Unterdrückung, Klarnamens-“Pflichten”, . . .
- In vielen Kulturen bestehen Tabus rund um Namen.
- Wir gehen (für Telekommunikation) von der Existenz beiderseitig akzeptierter, beständiger, situationsangemessener Namen aus.
- Telekommunikation umfasst für uns Briefe, Anrufe etc.

Probleme von Namen und Adressierung

- Namen von Orten und Anschlüssen sind **Adressen**.
- Auch Koordinaten in Ortsbezeichner- und Adressrolle.
- Klassisch Domäne der ITU, Internationales **Post**-System, Telefonsysteme. **Telefon**buch. Telekommunikation heute **digital**.
- Im Folgenden: hinreichend qualifizierter Name einer Entität soll diese innerhalb eines Kreises möglicher Adressaten eindeutig bezeichnen (Skopus). Adresse soll weltweite Zustellung erlauben.
- Adresszuteilung, Identifizierung sowie Zustellungsmechanismen sind Hebel für Macht (Zensur, Diskriminierung). Klarnamen . . .
- Problemfelder, in diesem Vortrag nicht weiter behandelt:
- Anpassung an EDV-Systeme [McK], Bürokratisierung, Computergläubigkeit, Macht. Verwechslungen bei gleichem Namen + Geburtsdatum/ort. Ärger bei Namenswechsel. Adresshandel durch Meldeämter. Öffentliche Listung $\rightarrow$ Spam.

Namen und Adressierung online

- In diesem Vortrag: Beschränkung auf **computergestützte Telekommunikation** zwischen gleichberechtigten Entitäten
- Weniger: e-Commerce / B2C-Beziehungen oder e-Government / “digitalisierte” Verwaltungsvorgänge
- Name (zumindest lokal eindeutiger Bezeichner für eine Entität) und Adresse (zum Zustellen von Nachrichten)
- Typisches Beispiel: **Kontaktinfo** Dr. Pawel Blankoscheck <blankoscheck@informatik.uni-hamburg.de>
- Wunsch-Eigenschaften für Kontaktinfo: eindeutig, memorabel (sprechend), authentisch, adressierbar, erreichbar (verfügbar); nicht von einem proprietären System abhängig

Althergebrachte implizite falsche Annahmen

- Bezüglich Namen und Adressierung herrschen hartnäckige **falsche Annahmen** vor. Diese hemmen das Verständnis und machen digitale Netze weniger gut, als sie es sein könnten.
- “Um miteinander reden zu können, sind ein Dienst und ein Diensteanbieter **nötig**, dessen AGB der Kommunikation übergeordnet sind” (Telekom, WhatsApp)
- **“Es sind ein Dienst und ein Diensteanbieter nötig, um einen Anschluss-Bezeichner zu haben; der Anschluss ist auch die logische Adresse für die Kommunikationsebene und gehört eineindeutig einer Person”** (Telefonnummer, WhatsApp, DeNIC)
- “Es muss eine zentrale Autorität geben, die kraft ihrer Autorität an weitere Autoritäten delegiert, die Namen vergeben”.
- Woher erhält diese Autorität ihre Autorität? **Legitimation**

Gewachsene Strukturen und Korruption . . .

- Im **Internet**: ICANN (Internet Corp. for Assigned Names and Numbers) (Organisationsstruktur: [ICAb] – *kein* Organ der UNO)
- Was unterscheidet ICANN von Hänschen's Namensregister (z.B. OpenNIC, backplane)?
- ICANN delegiert an NICs für geopolitische Entitäten wie ".dd", ".de", ".uk", ".to", ".io" und nationale, supranationale, private etc. Organisationen. Rechtliches Rahmenwerk?
- "The Internet Architecture Board [IETF-Kommittee] has spoken out strongly against **alternate roots** in RFC 2826." (2000) [wal] [pou]
- Also: "Experimentieren ist OK, aber wer unser authoritatives Namenssystem antastet, ist ein Spalter!" [icaa] [uni]
- Diese Äußerung hat bestimmt nichts zu tun mit $185.000 für neue "gTLDs" privater Pächter, z.B. ".website", ".сайт" = ".xn—80aswg", ".autos" oder ".deloitte" [new]

Weitere Probleme mit zentralen Stellen

- Wer legitimiert, kann (i.d.R.) auch Legitimation **entziehen**.
- Die Anlässe dazu sind vielfältig und manchmal banal
- Anforderungen and Betreiber sind willkürlich und unbeständig
- Beispiel: scihub (Durchsetzung der Geschäftsinteressen eines weitgehend parasitären Oligopols), .iq (Besitzer verhaftet) [iqd]
- Wie “offiziell” ist das Ganze? (Internet-Domains): erfolgreiche Domain-Klagen vor vielen Gerichten, Nutzung von Domains durch staatliche Stellen für offizielle Zwecke weltweit en vogue.
- Wie “offiziell” ist das Ganze? (Telefonnummern): Rufnummernmitnahme, Schnüffelgesetze (Anschlussinhaber-Identifikation, ETSI, ...)
- Wie “offiziell” ist das Ganze? (Telemediengesetz, Telekommunikationsgesetz ...)

Kaputte Systeme. Beispiel: E-Mail

- E-Mail: allgegenwärtig, aber extrem wackelig.
- Status quo höchst problematisch! **Points of failure**: unsichere Protokolle, zentrale Autoritäten, Admins, wacklige Server, Spam-Blockaden gegen wacklige Server.
- Kontakt-Information soll dauerhaft sein, ist aber von einem abenteuerlichen Vasallensystem abhängig:
- Erreichbarkeit von Gnaden des Administrators, abhängig von dessen Kompetenz und der Beständigkeit seiner Institution
- Erreichbarkeit von Gnaden des streng hierarchischen DNS-Systems, von Gnaden der ICANN, von Gnaden der USA
- Im Internet: zunächst einmal IP-Adressen. Mit IPv6 könnte sogar jedes Gerät und damit jede Nutzer*in eine eigene besitzen.
- Aber: Erreichbarkeit von Gnaden des IPv(4/6)-Routing, von Gnaden der Präfix-Zuteilung

Wovon hängt Erreichbarkeit per E-Mail ab?

- mailto: <blankoscheck@informatik.uni-hamburg.de>
- DNS-Anfrage (nicht authentifiziert (!), nicht privat (!)) an Resolver (RFC 1034) [DNSb] [how],
- Rekursives DNS-Resolving, beginnend bei Root-Server, jedesmal volle Query (außer bei Caching)
- Ergebnis: (nicht signiertes, aber siehe DNSSEC [rfcb], das aber die anderen Fehler erbt – und [DNSa]) Zuordnung zu ... einer IPv4/6-Adresse! (wieder ICANN)
- Sowohl bei C2S als auch S2S greift schließlich (hoffentlich) TLS ... authentifizert durch korruptes, zentrales CA-System
- E-Mail-Protokoll SMTP. ABSENDER SIND NAHEZU TRIVIAL FÄLSCHBAR. [rfca] Daraus resultiertendes Spam-Problem.
- Authentifizierung durch Server (Credentials bei Server, Server kann Nachrichten fälschen) – Abhilfe schafft **GPG**.

Zooko's Dreieck

- Ziele: Namen sollen **sicher***, **dezentral**, **bedeutsam** sein (jeweils mehr oder weniger, nicht absolut)
- z.B. PGP-Fingerprint: +sicher, +dezentral, -bedeutsam
- z.B. Amtl. Personenvz.: +sicher, -dezentral, +bedeutsam
- z.B. Handelsregister: +sicher, -dezentral, +bedeutsam
- z.B. ICANN-Domain: -sicher*, -dezentral, +bedeutsam
- z.B. Jabber-Adresse: -sicher, +dezentral, +bedeutsam
- z.B. OnionV3-Adresse: +sicher, +dezentral, -bedeutsam
- z.B. Namecoin: +sicher, +dezentral, +bedeutsam
- Keine Lösung: "**Identitätsprovider**", Föderation kleiner Server mit jeweils eigener Login-Verwaltung. Identität $\neq$ account.
- Staatlich verbriefte Identitäten nur als ein Baustein unter vielen sinnvoll, oft nicht anwendbar.
- Keine schöne Lösung, schafft neue Probleme: **Blockchain**

Total dezentrale Kontaktdaten, Teil 1 der Lösung

- Lösungsansatz für das CA-/Hierarchical-Trust-Problem:
- Alle Teilnehmenden, technisch verkörpert durch private Schlüssel, sind per se höchste Autoritäten (souverän und autonom): wem ich vertraue (auch in Sachen des Vertrauens) sollte meine Sache sein  , nicht die einer externen "Autorität"  .
- Web of Trust statt Hierarchie. **Public Key** Fingerprint zum Namen!
- Gehen wir von PGP aus. Schlüsseldatei **enthält** aktuelle Adresse.
- Öffentliche Verzeichnisse bzw. Weiterreichung. Fingerprint auf die Visitenkarte, nicht E-Mail-Adresse oder Telefonnummer. *Die steht tagesaktuell am Key!* (Einzige Schwierigkeit: Key-Management)
- Eigenschaften von PGP-Mail (vertraulich, authentisch) gibt's obendrein. Phishing und Spam sind damit eigentlich tot.
- Lässt robuste Adressierung offen, aber dafür gibt es **pkey-adressierbare** Knotennamen, siehe nächste Folie

Noch einen Schritt weiter: nicht-kaputte Adressierung

- **Variante 1**: F2F- oder P2P-Netz (z.B. GNUNet [ea]) zwischen autonomen Knoten, durch öffentliche Schlüssel adressierbar
- Weiterleitung an nächsten Nachbarn bzgl. XOR-Metrik (je mehr gleiche Binärstellen, um so näher) und Zurückschicken vermeiden (GNUNet R^5RS baut darauf auf, siehe auch cjdns [Del])
- Erwartete Routenlänge je nach Netztopologie erträglich!
- Vom Internet prinzipiell unabhängige Routing-Infrastruktur.
- **Variante 2**: Onion-Adressen [Kad]. nach Hashwert des Keys auf “zufällige” Knoten verteilte Einträge, die eine logische Adressierung des Servers ermöglichen, unabhängig von dessen Standort und Netzwerkadresse.
- Beides zusammen, um Sicherheits- / Verlässlichkeitsvorteile zu kombinieren.

Neue Grundlagen für das Internet - das GNS

- GNUNet: eine komplette neue Infrastruktur für das Internet
- u.A. für uns interessant (hoffentlich): das Namenssystem GNS
- Installation von GNUnet erforderlich – cross-platform, aber die Bedienbarkeit lässt noch **stark zu wünschen** übrig.
- Gnu-Namenssystem GNS: DNS-Ersatz, ähnliche Funktion, aber gegensätzliche Philosophie.
- Einträge verteilt gespeichert und sind nicht unter Kontrolle der antwortenden Knoten. Diese können sie nicht fälschen und kennen auch den Inhalt und Absender der Anfrage nicht.
- Einträge sind signiert durch Ersteller des Eintrags, gelten in Bezug auf dessen Zone. Adressierung ist direkt über Public Key oder indirekt durch Verkettung möglich.
- Web of Trust somit **direkt für Adressierung** nutzbar.

Freie, autonome, selbstbestimmte Telekommunikation

- ... ist mit heutigen Mitteln **realisierbar**, aber mit künstlichen Schwierigkeiten verbunden. Menschenwürde-kompatible Telekommunikation als einziges akzeptables Zukunftsmodell (vs. **Manipulation**, **Massentracking**, **Werbung**, **Zensur**, “**KI**”, **. . .**)
- Wenn Alice mit Bob kommunizieren muss, dann sollte das **unabhängig** des Wohlwollens dritter möglich sein, insbesondere ohne Wissen und Zustimmung der Netzbetreiber. Vermittelnde Systeme müssen nur unspezifisch kooperieren und Datenpakete weiterleiten. Jeder Eingriff oberhalb dieser Ebene ist abzulehnen.
- Der heilige Gral ist erreichbar: logische Adressierung und Netzwerk-Endgeräte-Adressen sind vollständig **entkoppelbar**!
- Allerdings werden Adressierung und Erreichbarkeit in gängigen Protokollen immer noch (teils absichtlich) falsch gedacht.

Freie, autonome, selbstbestimmte Telekommunikation

- Falsche Annahme: “Subscriber identity”, also persönliche Identifizierung, sei technische Voraussetzung für mobile Telekommunikation.
- Geräte-ID (IMEI) ist erst recht nicht erforderlich. Beides sind Artefakte eines verfehlten, hochproblematischen Standards.
- Mobile Vernetzung ohne individuelles Tracking ist technisch möglich, lediglich politisch nicht gewollt. Abrechnung ist mit kryptographisch übermittelten Einmal-Tokens zu realisieren.
- “Aber ich muss doch erreichbar sein, also muss ich bei einem Anbieter sein”? **Nein**: Erreichbarkeit benötigt lediglich eine Internetverbindung und eines der genannten Overlay-Netze. Mobilität braucht Anbieter, aber . . .
- . . . sogar die Infrastruktur könnte ehrenamtlich betrieben werden, nach dem Modell von Freifunk. Das würde in jeder Hinsicht (für uns Nutzer*innen) besser funktionieren als das derzeitige Modell.

Freie, autonome, selbstbestimmte Telekommunikation

- Mehr Trugvorstellungen, mit denen wir aufräumen können:
- “Aber ich muss doch erreichbar sein, *somit* über Telefonnummer trackbar”? Nein, kompletter Trugschluss (siehe vorige Folien)
- “Aber ich möchte doch telefonieren/Videokonferenz/Gruppenchat machen und brauche deswegen kommerzielle, zentralisierte Dienste”? Komplett falsch (siehe vorige Folien und vielfältige Projekte, die *alle* nur das Internet und P2P-Protokolle brauchen)
- Internet ist *immer* ausreichend, jedweder Extra-Dienst ist unnötig und eine Begriffsverzerrung. Es genügen drei Voraussetzungen:
  1. Allgemeine, neutrale Weiterleitung von Datenpaketen, am besten von und für die Allgemeinheit betrieben
  2. Freie Protokolle, die aus Eigeninteresse betrieben werden.
  3. Geräte in Nutzer*innenhand

Was steht dem im Weg?

- Netzanbieter sollen Infrastruktur bereitstellen und Pakete von A nach B bringen. Das ist **Netzneutralität**. “Mehr” ist Betrug, weil es keinen Mehrwert liefert. Stattdessen sehen wir künstliche Einschränkungen, die “Zusatzangebote” flankieren.
- Das ist in der EU zwar illegal, aber die Deutsche Telekom AG verstößt vorsätzlich gegen das Gesetz. Das kann sie sich leisten – u.A. weil die Strafe maximal EUR 500.000 beträgt. [fG]
- Der “*War on general purpose computation*” – uns sollen nur noch “Appliances” für vorgegebene Zwecke statt universeller Computer in die Hand gegeben werden [Doc] (“Digitalisierung” statt freier Vernetzung und mündigem Umgang mit Technologie ...)
- Wo freier Zugang fehlt, sind Workarounds möglich: getunnelte Overlay-Netze, Sneaker-Nets. “Rüstungswettlauf” und “Katz und Maus”, in Diktaturen für den Staat entschieden (China). **Das muss um jeden Preis vermieden werden!**

Ausblick (1)

- **Viel Licht in der Theorie, viel Schatten in der Praxis.**
- Schatten entsteht durch festgefahrene Denkmuster – und durch massive Manipulation der Rahmenbedingungen durch einen nach Entmündigung dürstenden politisch-industriellen Komplex – und durch nicht mit ausreichendem Nachdruck eingeforderte Rechte.
- Viele Ausgestaltungen – synchron (Telefonie) oder asynchron (Nachrichten nachsenden) – für all das gibt es entweder schon schöne Software, oder es liegt an uns, diese zu entwickeln und die frohe Botschaft der FLOSS-Philosophie zu verkünden!
- Etwas breiter gefasst, ist mit ähnlichen Verfahren kryptographisch sichere Content-Adressierung von Dateien möglich (Freenet) – z.B. können unsere Hyperlinks im Anhang verloren gehen und im Museum landen (archive.org), Content-adressierbare Dateien aber erst bei Wegfall der letzten Kopie. Zweischneidiges Schwert!

Ausblick (2)

- Neue Schwierigkeiten: **Schlüsselmanagement**, Popularisierung der Idee, Netzwerkeffekt.
- Die kryptographischen, technischen und ergonomischen Herausforderungen (Protokolle, Schlüsselmanagement, Benutzerfreundlichkeit . . .) sind einer **positiven Herangehensweise** zugänglich.
- Die sozialen hoffentlich auch!

- Caleb James Delisle, *cjdns*, https://github.com/cjdelisle/cjdns, Accessed: 2018-12.
- *DNSCurve by djb*, https://dnscurve.org/, Accessed: 2018-11.
- *Wikipedia: Domain name system*, https://en.wikipedia.org/wiki/Domain_Name_System, Accessed: 2018-11.
- Cory Doctorow, *The war on general purpose computation (28c3 keynote)*, https://media.ccc.de/v/28c3-4848-en-the_coming_war_on_general_computation, Accessed: 2018-12.
- Christian Grothoff et al., *GNUnet*, https://gnunet.org, Accessed: 2018-12.
- Friedhelm Greis für Golem, *Telekom setzt stream on unverändert fort*, https://www.golem.de/news/streit-mit-bundesnetzagentur-telekom-setzt-stream-c html, Accessed: 2018-12.


Serverfault: how DNS works, https://serverfault.com/questions/355414/how-is-dns-lookup-order-determined, Accessed: 2018-11.


ICANN wiki altroots, https://icannwiki.org/Alternative_Roots, Accessed: 2018-11.


Wikipedia: ICANN, https://en.wikipedia.org/wiki/ICANN, Accessed: 2018-12.


Iraq, its domain and the 'terrorist-funding' owner, https://www.theregister.co.uk/2003/04/09/iraq_its_domain/, Accessed: 2018-12.


George Kadianakis, *Tor's Fall Harvest: the Next Generation of Onion Services*, https://blog.torproject.org/tors-fall-harvest-next-generation-onion-services, Accessed: 2018-12.


Patrick McKenzie, *Falsehoods programmers believe about names*, https://www.kalzumeus.com/2010/06/17/falsehoods-programmers-believe-about-names/, Accessed: 2018-11.


ICANN new gTLDs, https://newgtlds.icann.org/en/, Accessed: 2018-11.


TCP/IP inventor on self-proclaimed ICANN monopoly, https://www.silicon.co.uk/workspace/open-root-and-the-grandfather-of-the-internet-9749 Accessed: 2018-11.


IEEE IETF RFC 5321: SMTP, https://tools.ietf.org/html/rfc5321, Accessed: 2018-11.


IETF RFC 4033: DNSSEC, https://tools.ietf.org/html/rfc4033, Accessed: 2018-11.

 *ICANN unique authoritative root*, `https://www.icann.org/resources/pages/unique-authoritative-root-2012-02-25-en`, Accessed: 2018-11.

 *Wikipedia: Alternative roots*, `https://en.wikipedia.org/wiki/Alternative_DNS_root`, Accessed: 2018-11.