Wie Informatik Demokratie und Freiheit unterstützen kann

Münster, 16. Dezember 2011

Prof. Dr. Hannes Federrath

http://svs.informatik.uni-hamburg.de/

Fragen

- Wie ist heute die Welt der Informationssicherheit geordnet?
- Welche Techniken stehen uns zur Verfügung?
- Was hat das mit Demokratie und Freiheit zu tun?
- Welche Einsichten für die Technikgestaltung folgen daraus?

Gliederung

- Schutzziele der IT-Sicherheit
- Verfahren zum Schutz
- Fallbeispiele
  - Informationsfreiheit durch Anonymität
  - Unterstützung der Meinungsfreiheit in Diktaturen
  - Vorratsdatenspeicherung vs. gezielte Verbrechensbekämpfung
- Schlussbemerkungen

Schutzziele mehrseitiger IT-Sicherheit

- Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.

Kommunikationsgegenstand WAS? WORÜBER?	Kommunikationsumstände WANN?, WO?, WER?
Vertraulichkeit Verdecktheit	Anonymität Unbeobachtbarkeit
Integrität	Zurechenbarkeit Rechtsverbindlichkeit
Verfügbarkeit	Erreichbarkeit

Schutzziele mehrseitiger IT-Sicherheit

- Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.

Inhalte der Kommunikation	Kommunikationsumstände
Vertraulichkeit Verdecktheit	Anonymität Unbeobachtbarkeit

- Schutzziele — Vertraulichkeit
  - Schutz der Nachrichteninhalte
  - Schutz der Identität eines Nutzers während der Dienstnutzung
    - Beispiel: Beratungsdienste
  - Schutz der Kommunikationsbeziehungen der Nutzer
    - Nutzer kennen möglicherweise gegenseitig ihre Identität

Historische Entwicklung

Jahr	Idee / PET system
1978	Public-key encryption
1981	MIX, Pseudonyms
1983	Blind signature schemes
1985	Credentials
1988	DC network
1990	Privacy preserving value exchange
1991	ISDN-Mixes
1995	Blind message service
1995	Mixmaster
1996	MIXes in mobile communications
1996	Onion Routing
1997	Crowds Anonymizer
1998	Stop-and-Go (SG) Mixes
1999	Zeroknowledge Freedom Anonymizer
2000	AN.ON/JAP Anonymizer
2004	TOR

Grundverfahren
Anwendung

Beispiele für Bausteine datenschutzfördernder Technik

- Verschlüsselung
- Schutz von Kommunikationsbeziehungen
  - Schutz vor Outsidern
    - Proxies
  - Schutz vor Insidern und Outsidern
    - Broadcast
    - DC network
    - MIX network
- Schutz von Transaktionen
  - Pseudonyme
  - Credentials (an Pseudonyme gekettete Eigenschaften)

Broadcast

- Das war damals...

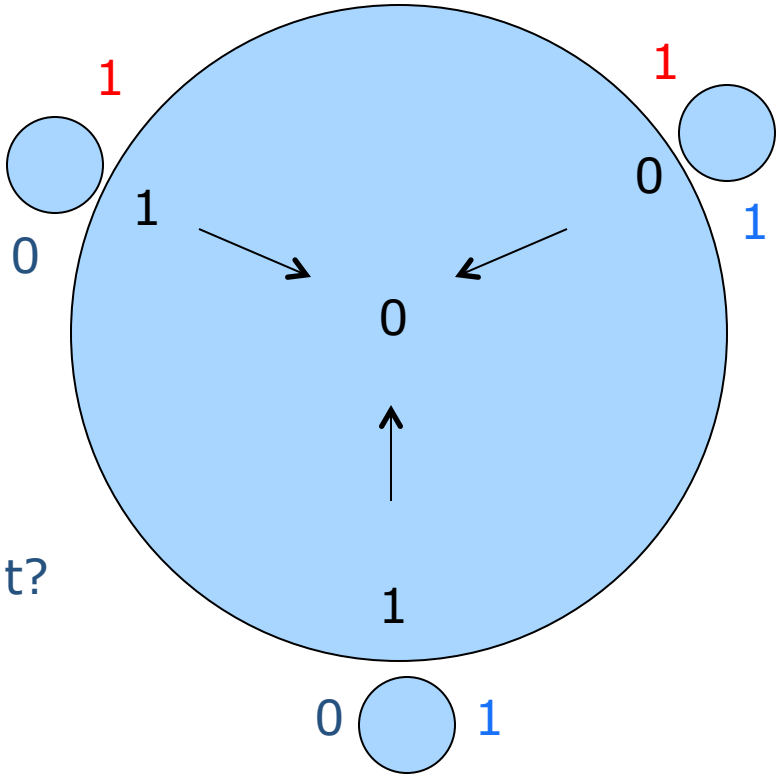
  - Zeitung lesen
  - Radio über Antenne hören
  - Fernsehen über Breitbandverteilkabel

- Verteilung (Broadcast) + implizite Adressierung
  - Technik zum Schutz des Empfängers
  - Alle Teilnehmer erhalten alles
  - Lokale Auswahl
  - Es bleibt verborgen, welchen Inhalt der Nutzer konsumiert

DC network (Chaum, 1988)

- Jeder für sich:
  1. Jeder wirft mit jeden eine Münze
  2. Berechnet das xor der beiden Bits
  3. Wenn bezahlt, dann xor mit 1 (Komplement des Ergebnisses aus Schritt 2)
  4. Ergebnis veröffentlichen

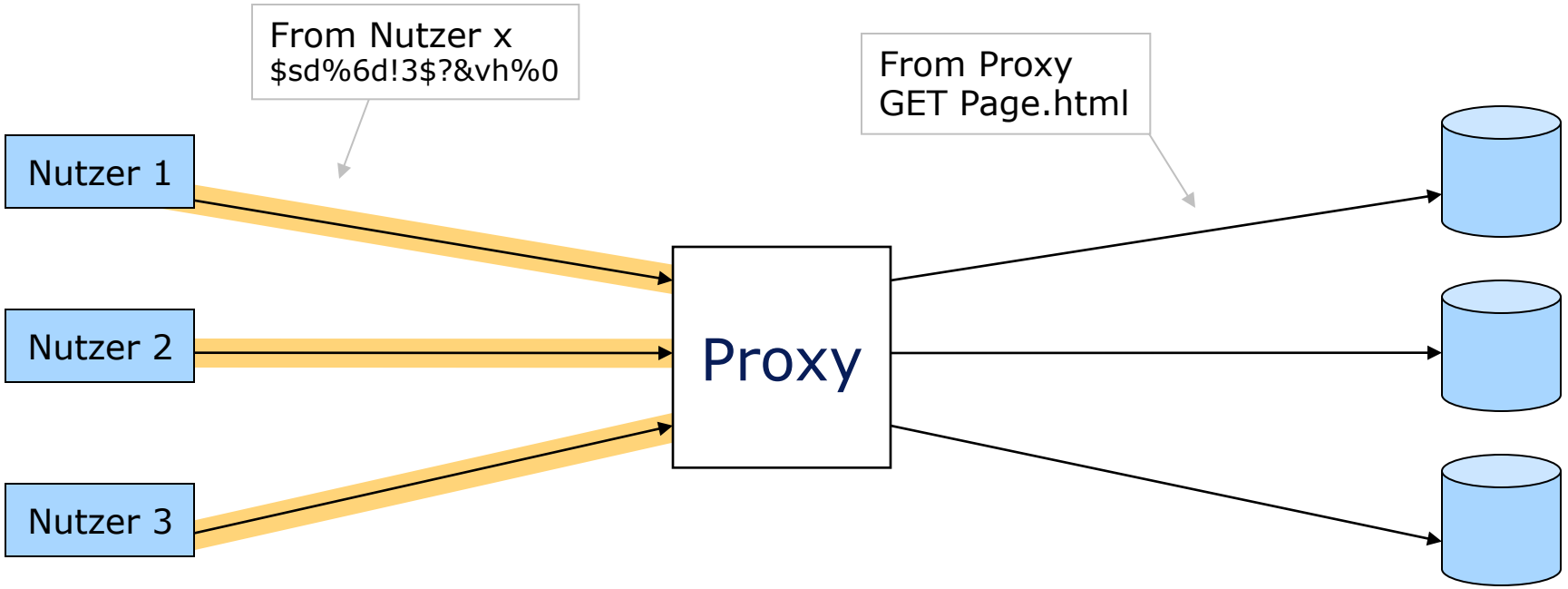
- Alle zusammen:
  1. Berechnen das xor der drei (lokalen) Ergebnisse
  2. Wenn globales Ergebnis 0, hat jmd. anderes bezahlt



Wer hat bezahlt?

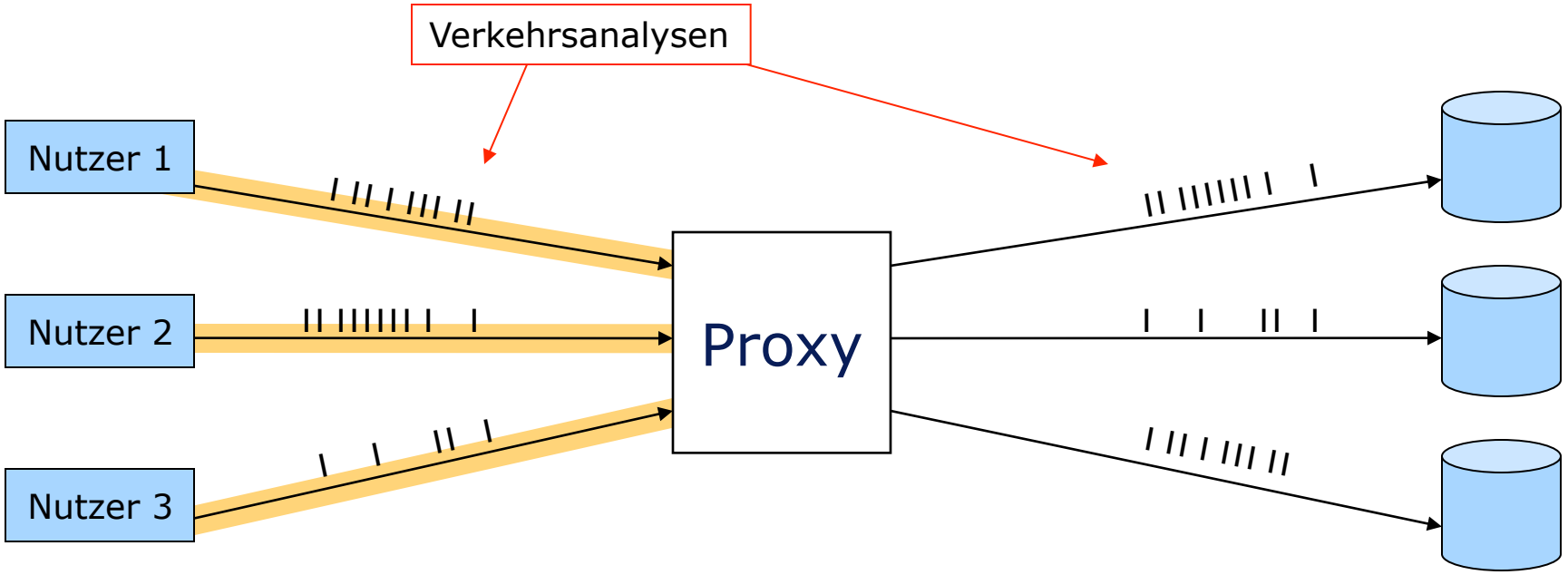
Proxies: Outsider

- Erreichbare Sicherheit (Outsider)
  - Beobachter nach Proxy und Serverbereiber:
    - erfahren nichts über den wirklichen Absender eines Requests
  - Beobachter vor Proxy:
    - Schutz des Senders, wenn Verbindung zu Proxy verschlüsselt



Proxies: Outsider

- Erreichbare Sicherheit (Outsider)
  - Aber: Trotz Verschlüsselung:
    - kein Schutz gegen Verkehrsanalysen
      - Verkettung über Nachrichtenlängen
      - zeitliche Verkettung



Mix-Netz (Chaum, 1981)

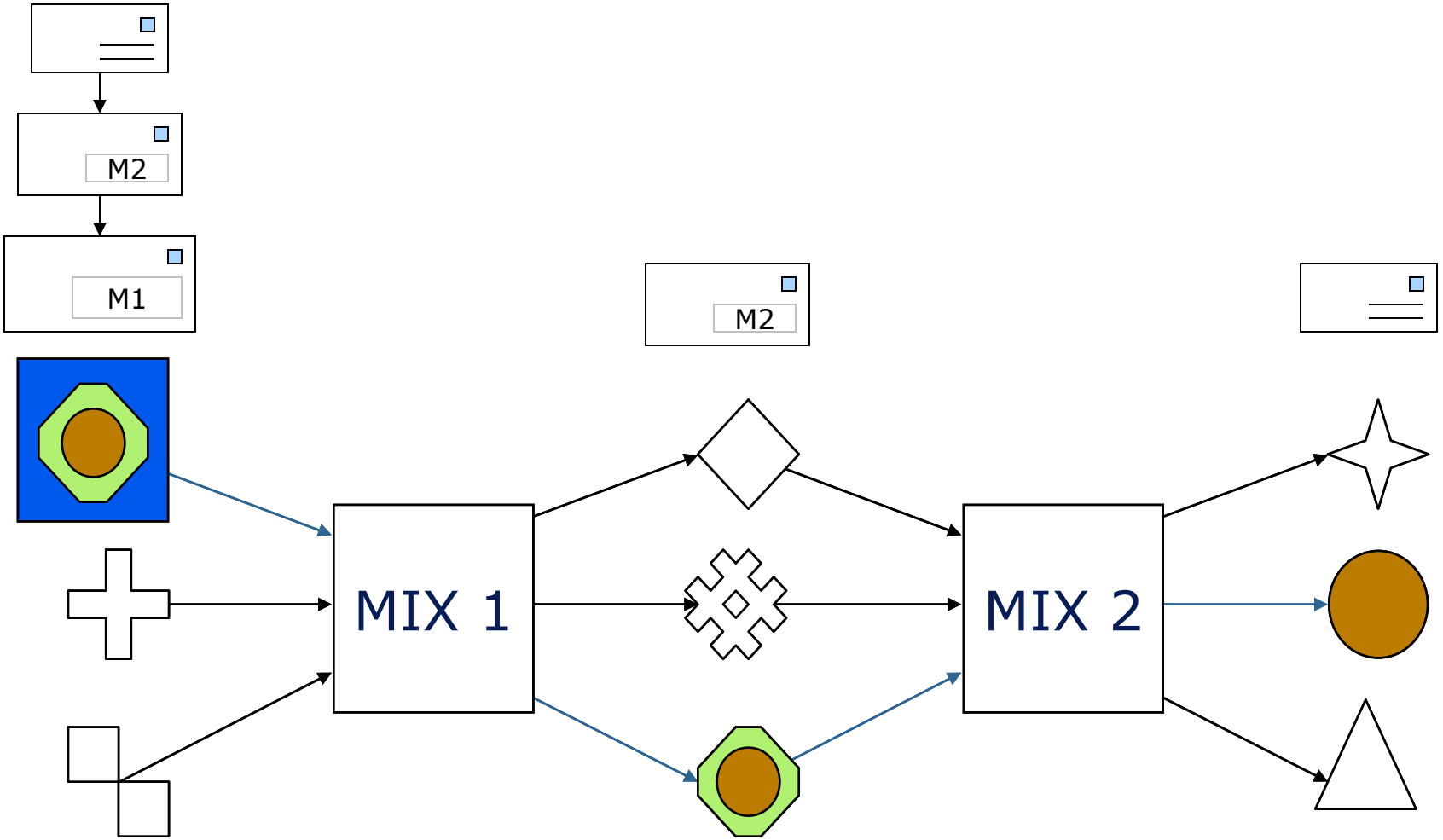
- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation

- Grundfunktionen:
  - Nachrichten in einem »Schub« sammeln,
  - Wiederholungen ignorieren,
  - Nachrichten umkodieren,
  - umsortieren,
  - gemeinsam ausgeben
  - Alle Nachrichten haben die gleiche Länge.
  - Mehr als einen Mix und unterschiedliche Betreiber verwenden
  - Wenigstens ein Mix darf nicht angreifen.

- Schutzziel:
  - Unverkettbarkeit von Sender und Empfänger

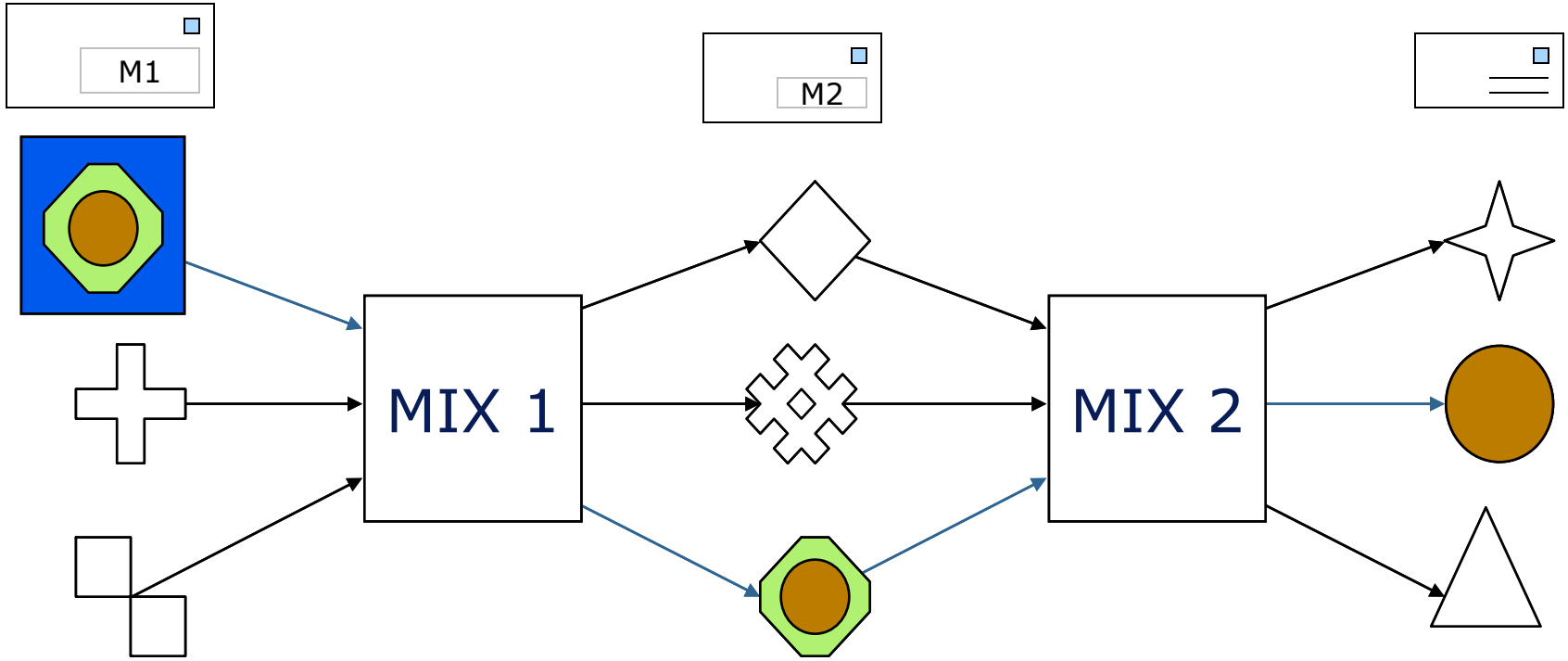
Mix-Netz (Chaum, 1981)

- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation



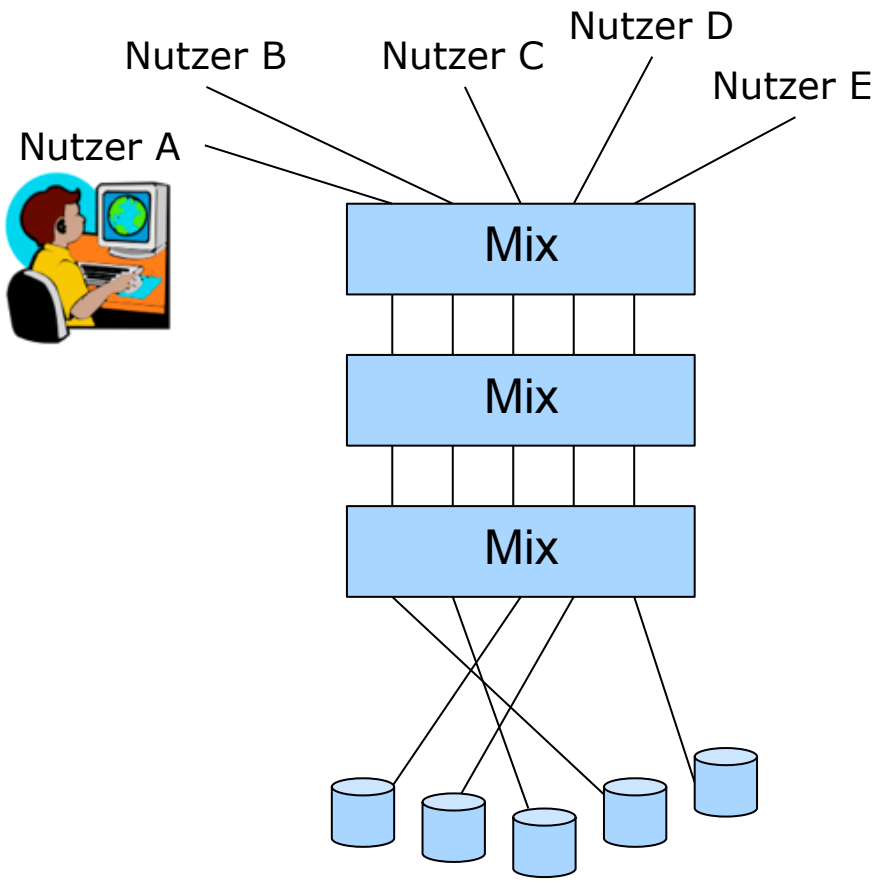
Mix-Netz (Chaum, 1981)

- Stärke der Mixe:
  - Auch die Betreiber der Mixe erfahren nichts mehr über die Kommunikationsbeziehung zwischen Sender und Empfänger.
- Notwendige Bedingungen:
  - Mehr als einen Mix und unterschiedliche Betreiber verwenden
  - Wenigstens ein Mix darf nicht angreifen.



Fallbeispiele

- Informationsfreiheit durch Anonymität
- Unterstützung der Meinungsfreiheit in Diktaturen
- Vorratsdatenspeicherung vs. gezielte Verbrechensbekämpfung



Recht auf informationelle Selbstbestimmung

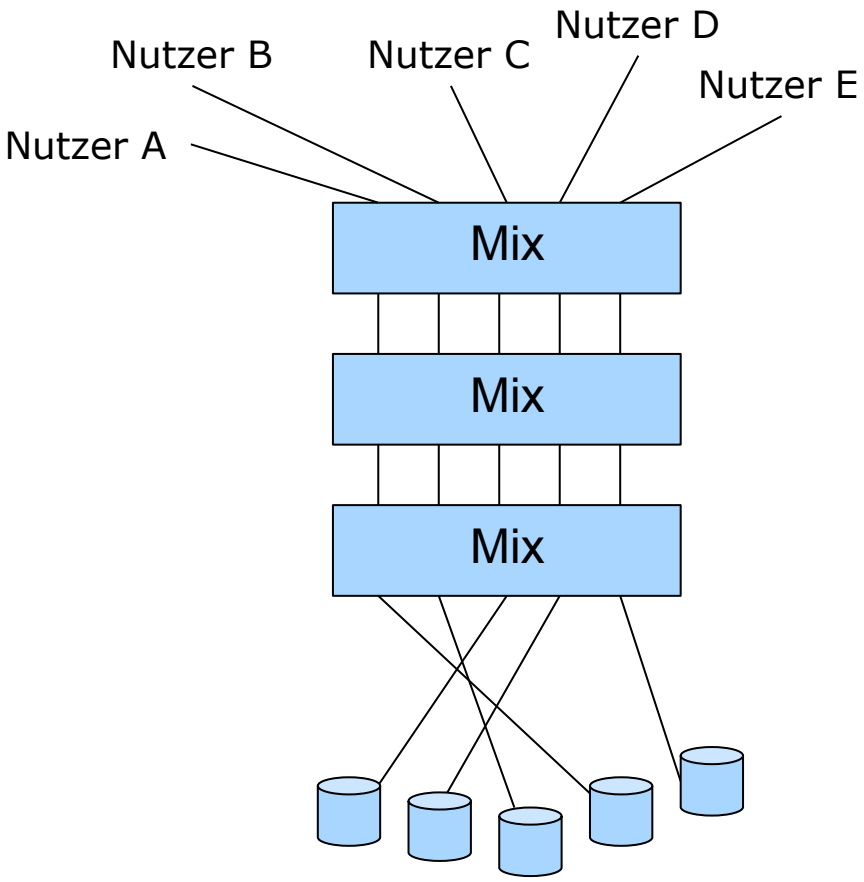
»Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den *Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten* voraus. …

Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. *Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.«*

aus dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 1. BvR 209/83 Abschnitt C II.1, S. 43

AN.ON – http://www.anon-online.de

- Implementierung eines Dienstes zum anonymen Internetzugriff
- Schaffen einer praktikablen Lösung für anonyme und unbeobachtbare Basiskommunikation
  - beruht auf Erweiterungen des Mix-Verfahrens von Chaum
  - Schutz auch vor dem Betreiber des Dienstes (Schutz vor Insidern)
- Schutz des Einzelnen vor Überwachung und Profilierung seiner Internetaktivitäten auch durch private Organisationen



Nicht immer nur der Staat hat die Überwachungsmöglichkeiten

- Beispiele
  - Payback, Google, Facebook

- Die Wirtschaft und private Organisationen sammeln heute mehr Daten denn je
  - freiwillige Preisgabe
  - Verbesserung des Service (Customer Relationship Management)
  - illegal (weil kaum nachweisbar und unauffällig) oder in rechtlicher Grauzone (z.B. international handelnde Unternehmen)
- Was kann der Einzelne tun?
  - Zurückhaltung, Skepsis bei Datenweitergabe, technische Schutzmöglichkeiten nutzen (z.B. Verschlüsselung, Anonymisierer)

Juristische Sicht

- Telemediengesetz (TMG, vormals Teledienstedatenschutzgesetz TDDSG)
  - § 13 Abs. 6 TMG: Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

AN.ON/JAP

Förderer: BMWi, Projektpartner: TU Dresden, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, FU Berlin, HU Berlin, Universität Regensburg, Medizinische Universität Lübeck, Chaos Computer Club, Ulmer Akademie für Datenschutz und IT-Sicherheit, RWTH Aachen, New York University

Ziele:

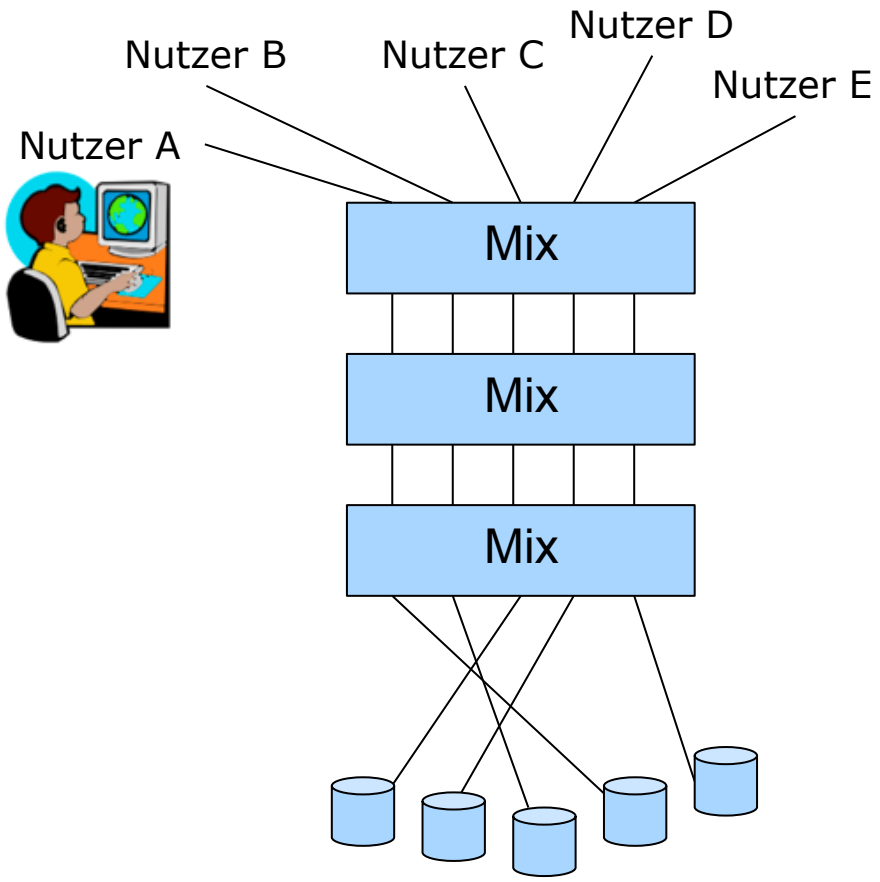
Schaffen einer praktikablen Lösung für anonyme und unbeobachtbare Basiskommunikation

Schutz auch vor dem Betreiber des Dienstes (Schutz vor Insidern)

www.anon-online.de

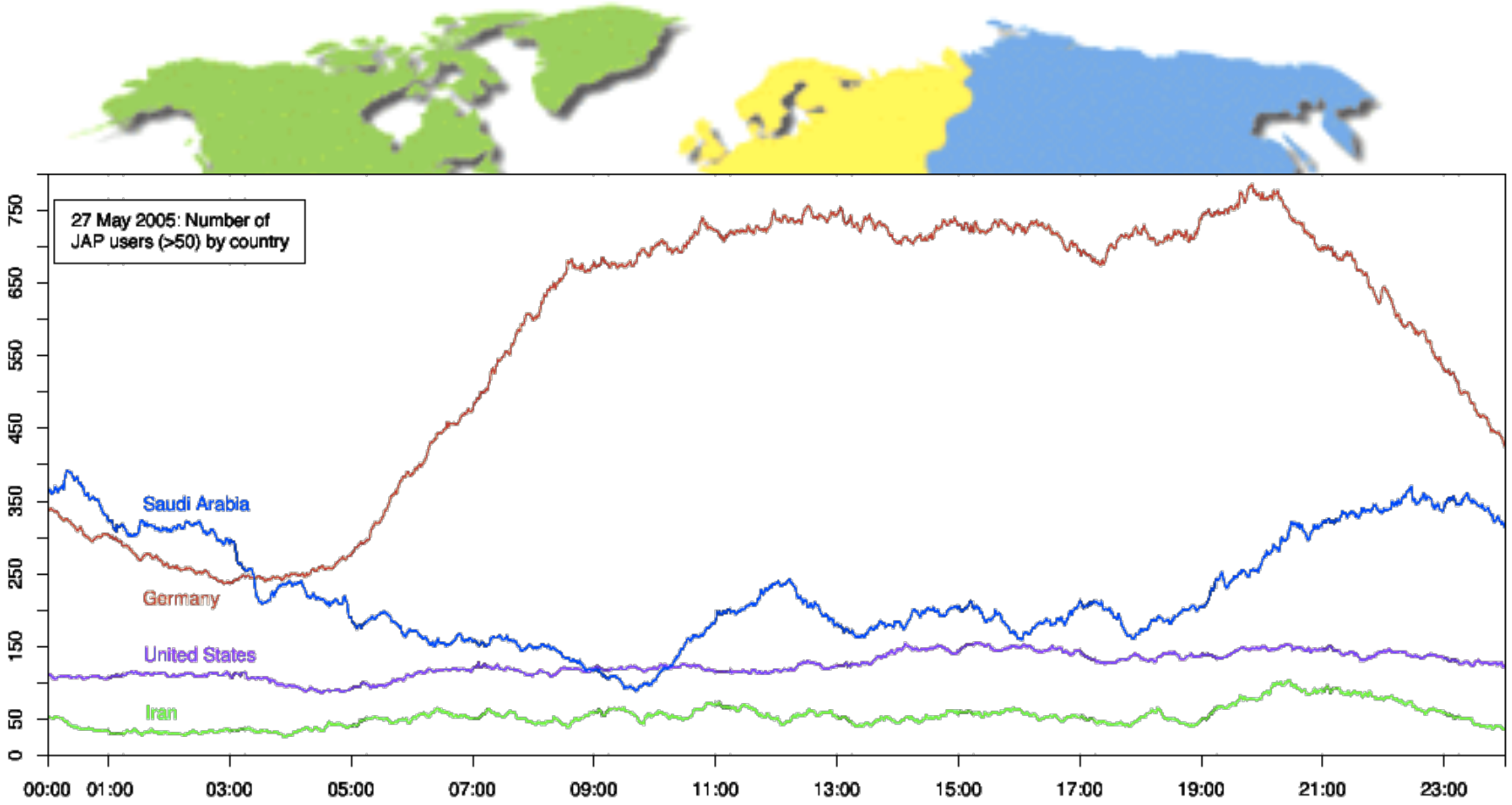
Fallbeispiele

- Informationsfreiheit durch Anonymität
- Unterstützung der Meinungsfreiheit in Diktaturen
- Vorratsdatenspeicherung vs. gezielte Verbrechensbekämpfung



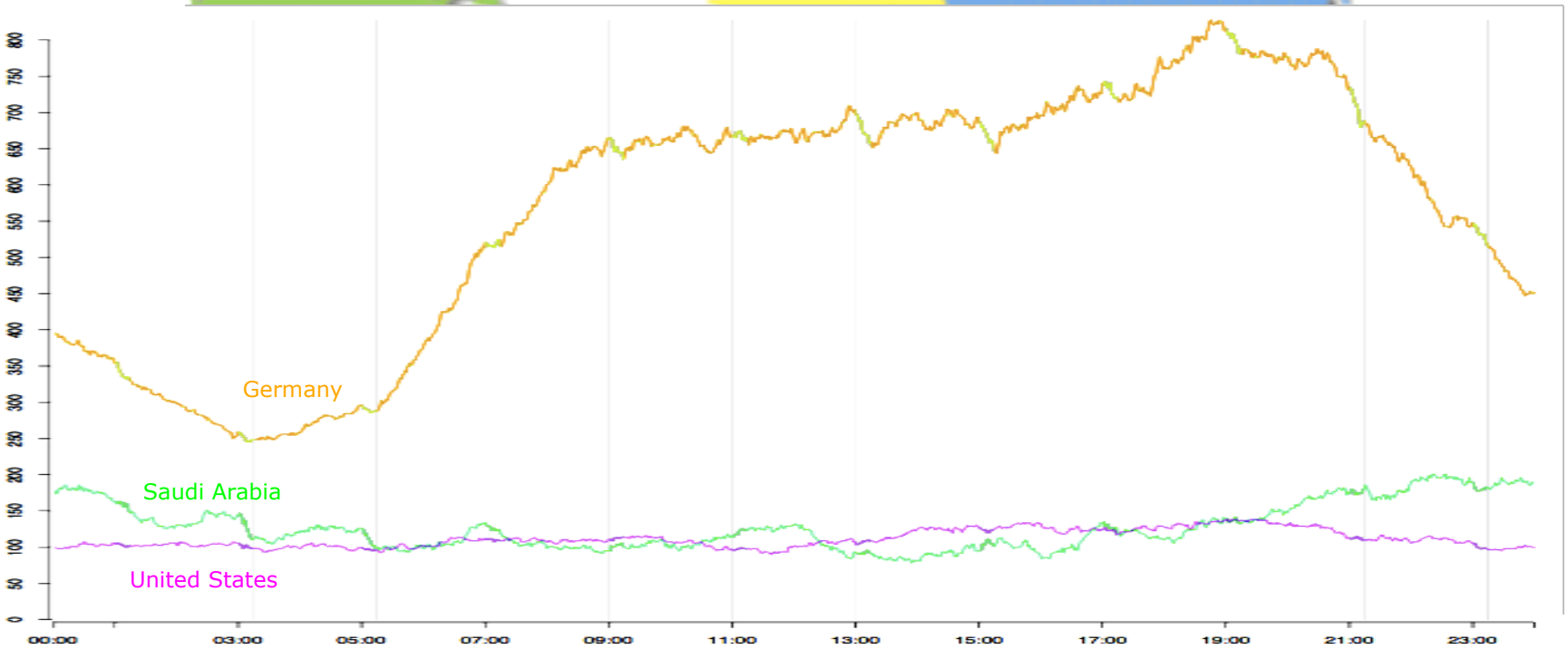
Wo kommen die JAP-Nutzer her?

- Dayline of May 27, 2005



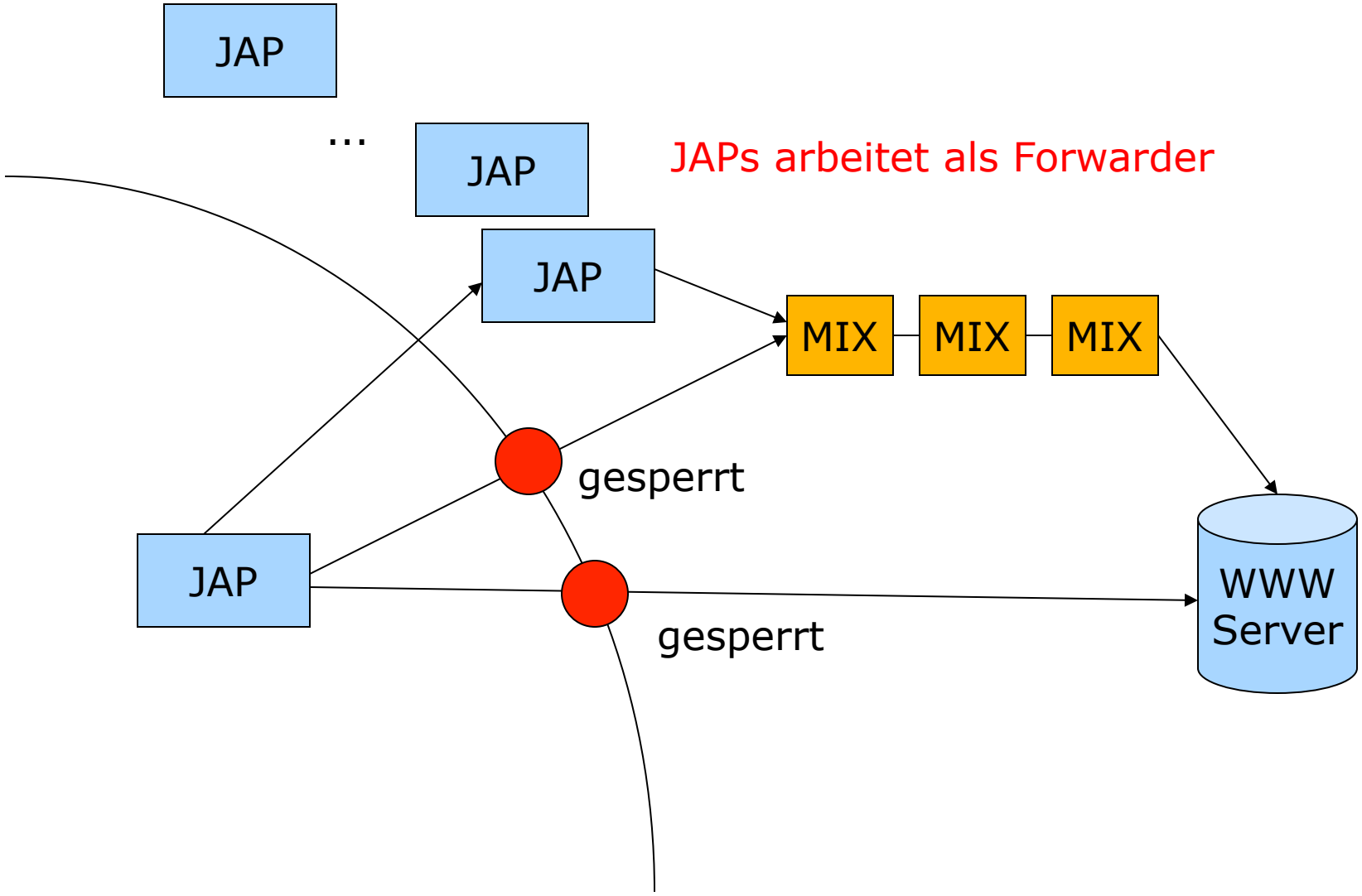
Wo kommen die JAP-Nutzer her?

- Dayline of Aug 1, 2005

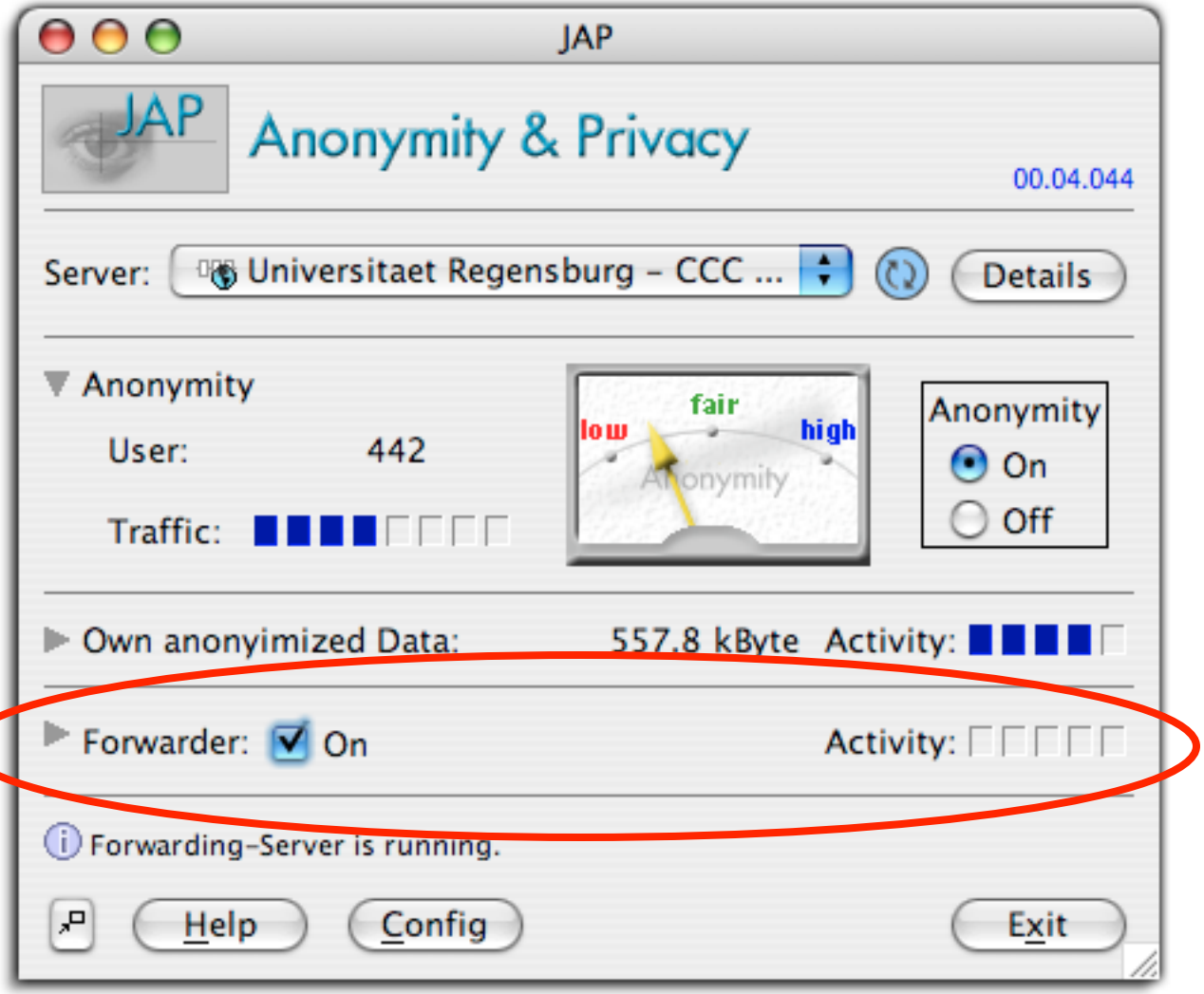


Iran?

Blockingresistenz



Blockingresistenz

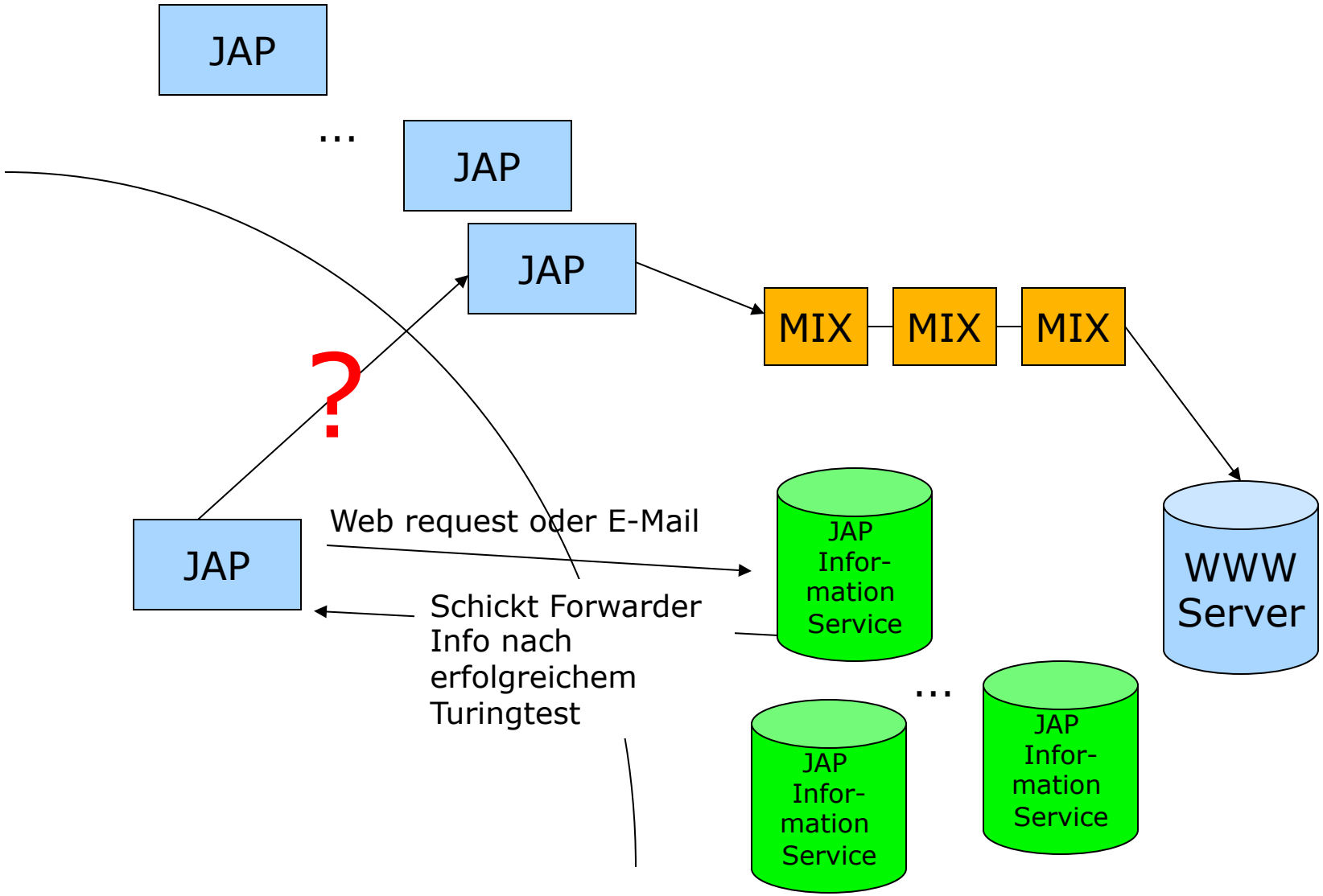


JAP-Nutzer stellen Teil ihrer Bandbreite zur Verfügung

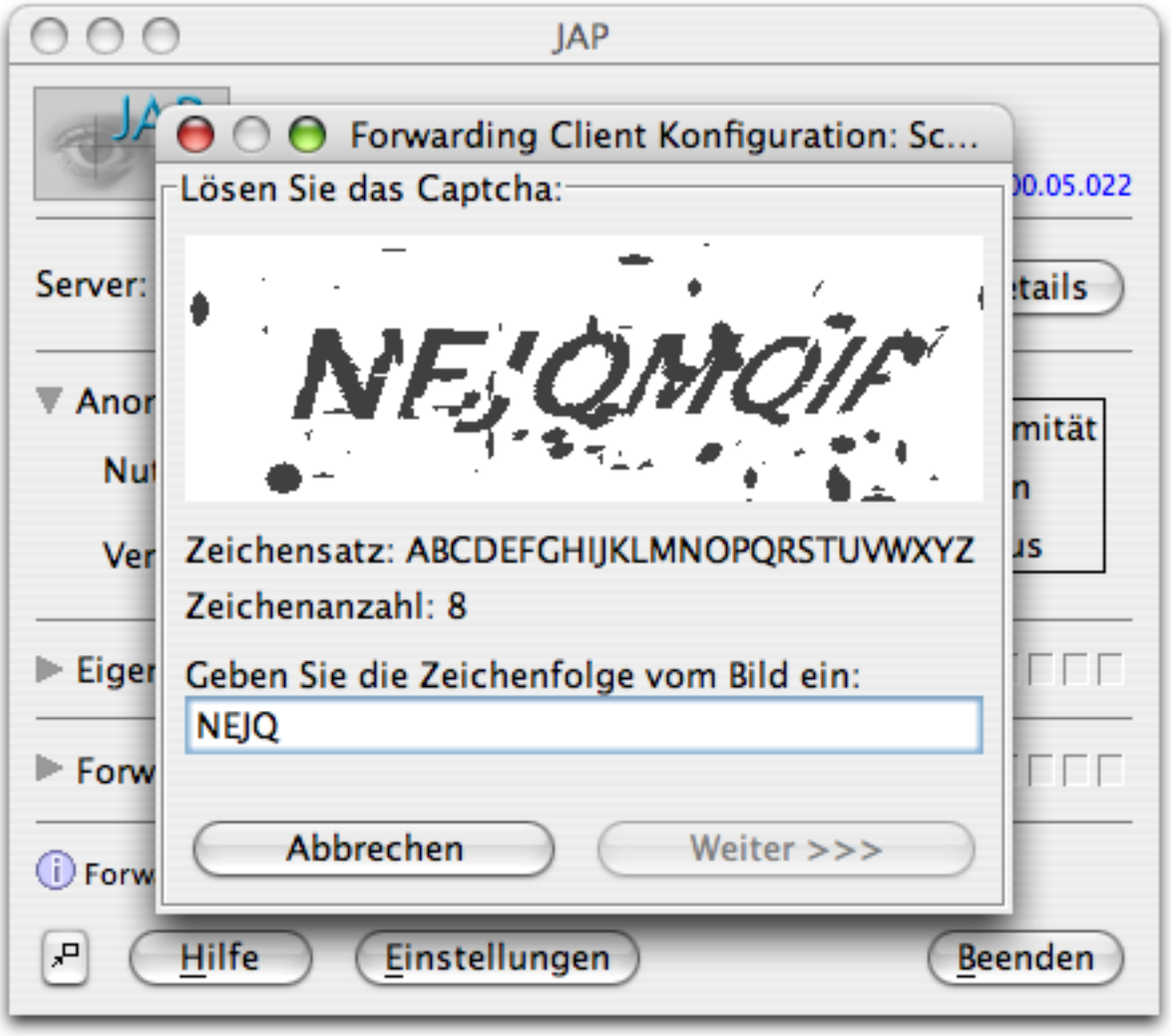
Zugriffe werden durch die Mixe anonymisiert

Forwarder erfahren nichts über die zugegriffenen Inhalte

Blockingresistenz



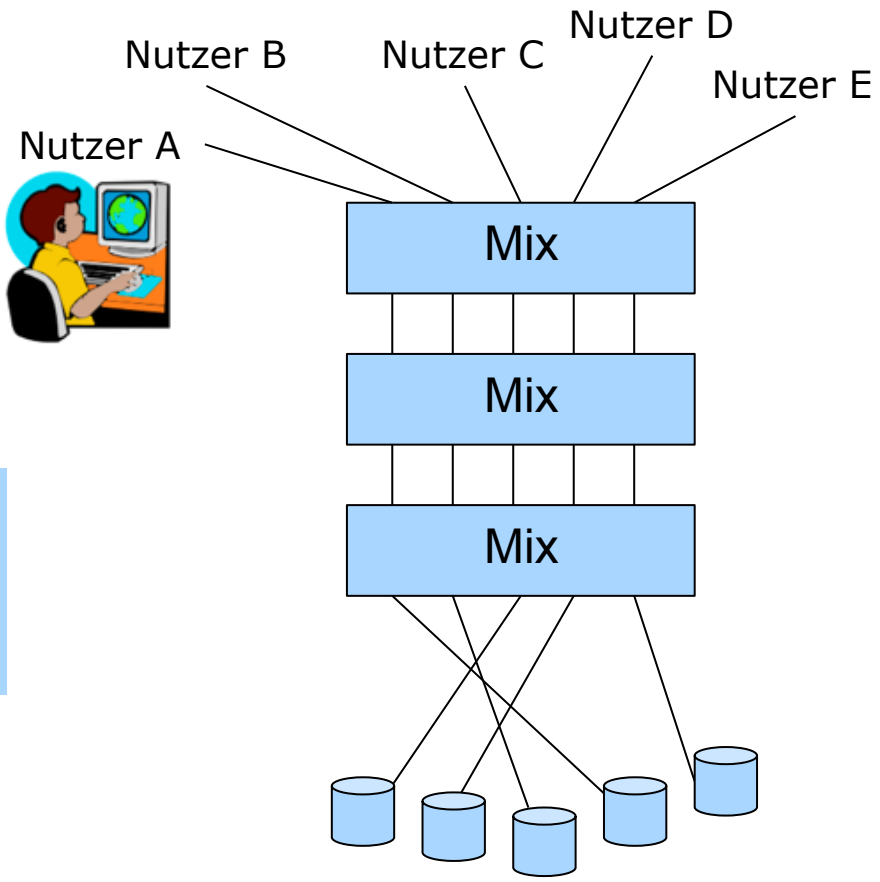
Blockingresistenz



InfoService schickt Forwarder Info nach erfolgreichem Turingtest

Fallbeispiele

- Informationsfreiheit durch Anonymität
- Unterstützung der Meinungsfreiheit in Diktaturen
- Vorratsdatenspeicherung vs. gezielte Verbrechensbekämpfung



Spannungsfeld von Freiheit und Sicherheit

- Ziel der Informationssicherheit: möglichst wenig Vertrauen in andere setzen müssen
  - Wo keine Sicherheit erreichbar ist, bleibt nur Vertrauen [müssen]

- Freiheit: insbesondere Grundrechte
  - Recht auf informationelle Selbstbestimmung
  - Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme (Computer-Grundrecht)

- Sicherheit
  - Vorratsdatenspeicherung
  - Bundestrojaner

»Nur in schweren Fällen…«

…aber die Menschen leiden unter dem Vertrauensverlust gegenüber dem Staat

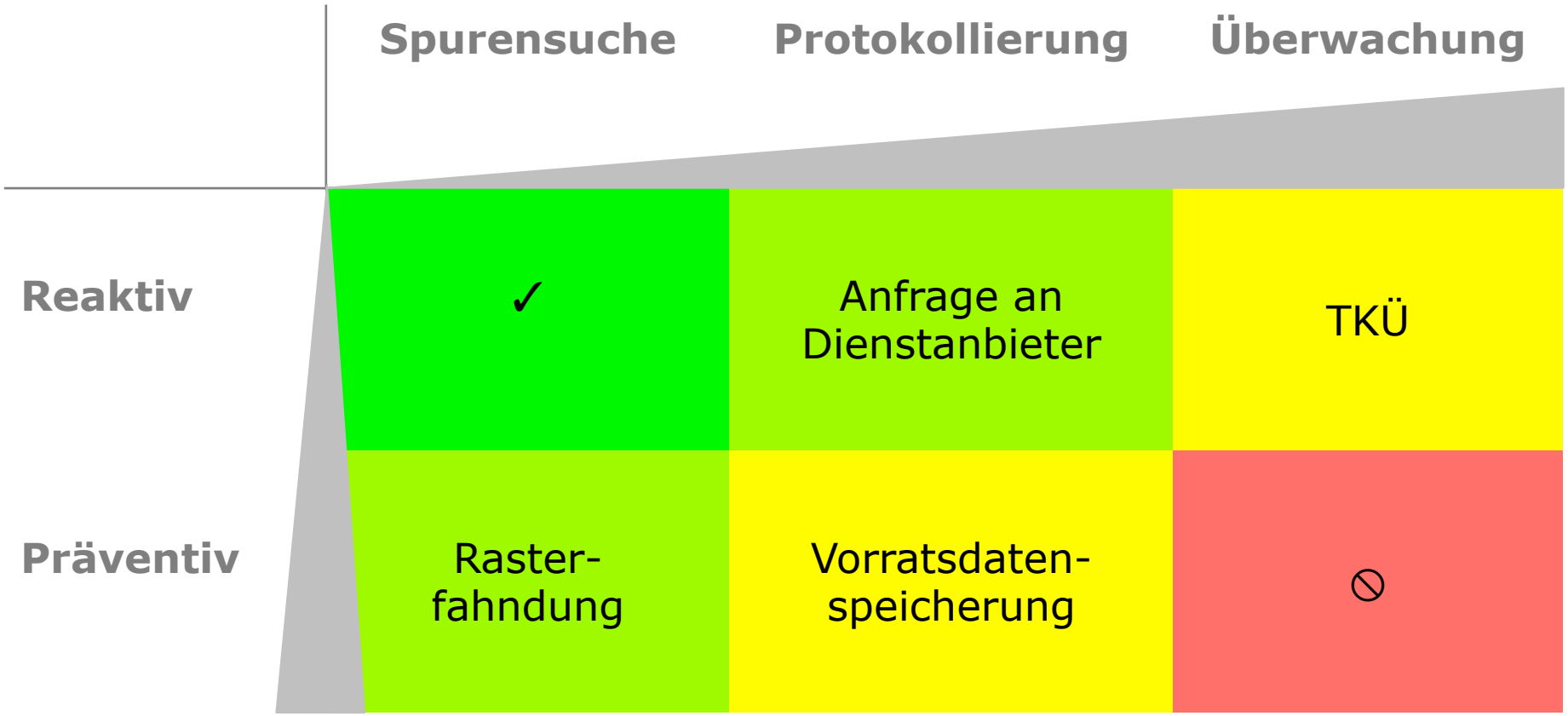
Aufgabe des Staates: Schutz seiner Bürger

- Thomas Hobbes (1588-1679): Staat als Beschützer der Bürger
  - Der Staat hat das Leben seiner Bürger zu schützen, ebenso dessen Besitz und Freiheit.
  - Staat gibt Regeln für das Zusammenleben der Menschen vor.
  - Je stärker der Staat, umso besser kann er Eigentum und Freiheit schützen.
  - Die Bürger haben dem Staat das Monopol der legitimen Machtausübung gegeben.

nach: Hobbes: Leviathan (1651)

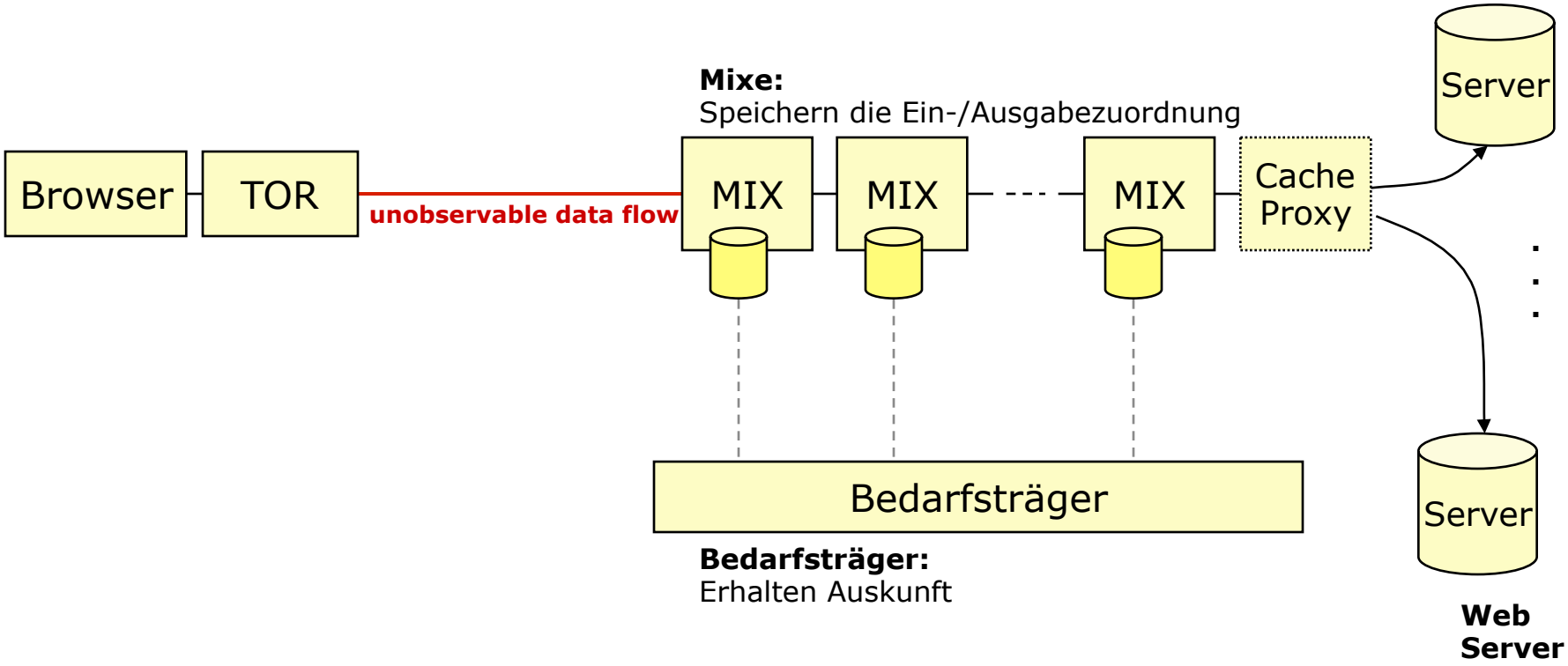
- Problem:
  - Hobbes‘ Staatsmodell ist auch „kompatibel“ mit dem Konzept eines Überwachungsstaates.
    - Recht auf informationelle Selbstbestimmung aufgegeben
  - Auch vom Staat gehen Gefahren aus:
    - Am Ende dient der Staat nur noch seiner Selbsterhaltung.

Eingriffstiefe von Ermittlungsmethoden in die Freiheit



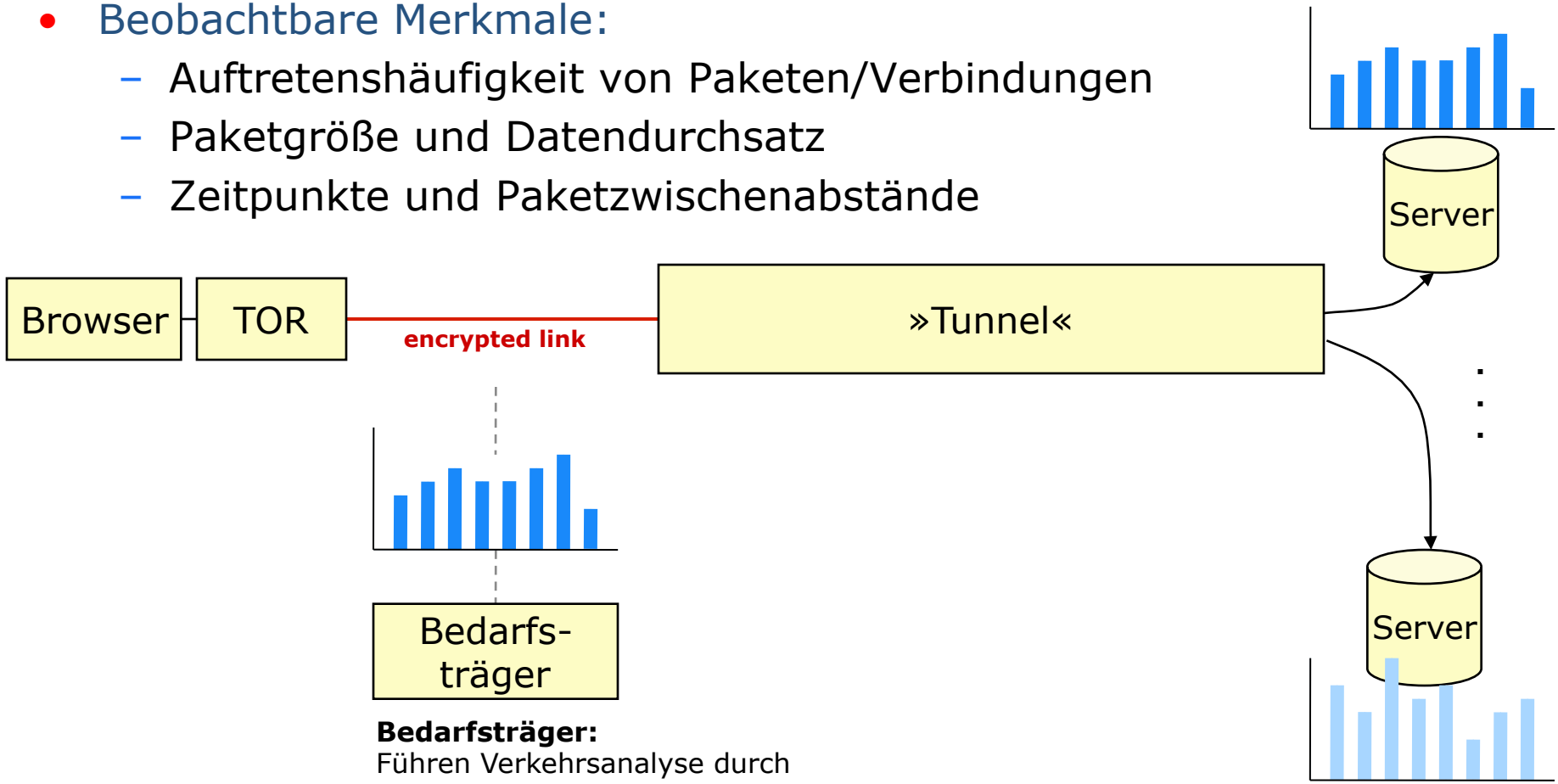
Anstelle von Vorratsdatenspeicherung…

- Mixe speichern Ein-/Ausgabezuordnung für 6 Monate
  - Problem: Ziel-URLs dürfen nicht gespeichert werden
  - Auskunftsersuchen bezieht sich auf ausgehende IP (Cache-Proxy) und Uhrzeit



…Website-Fingerprinting

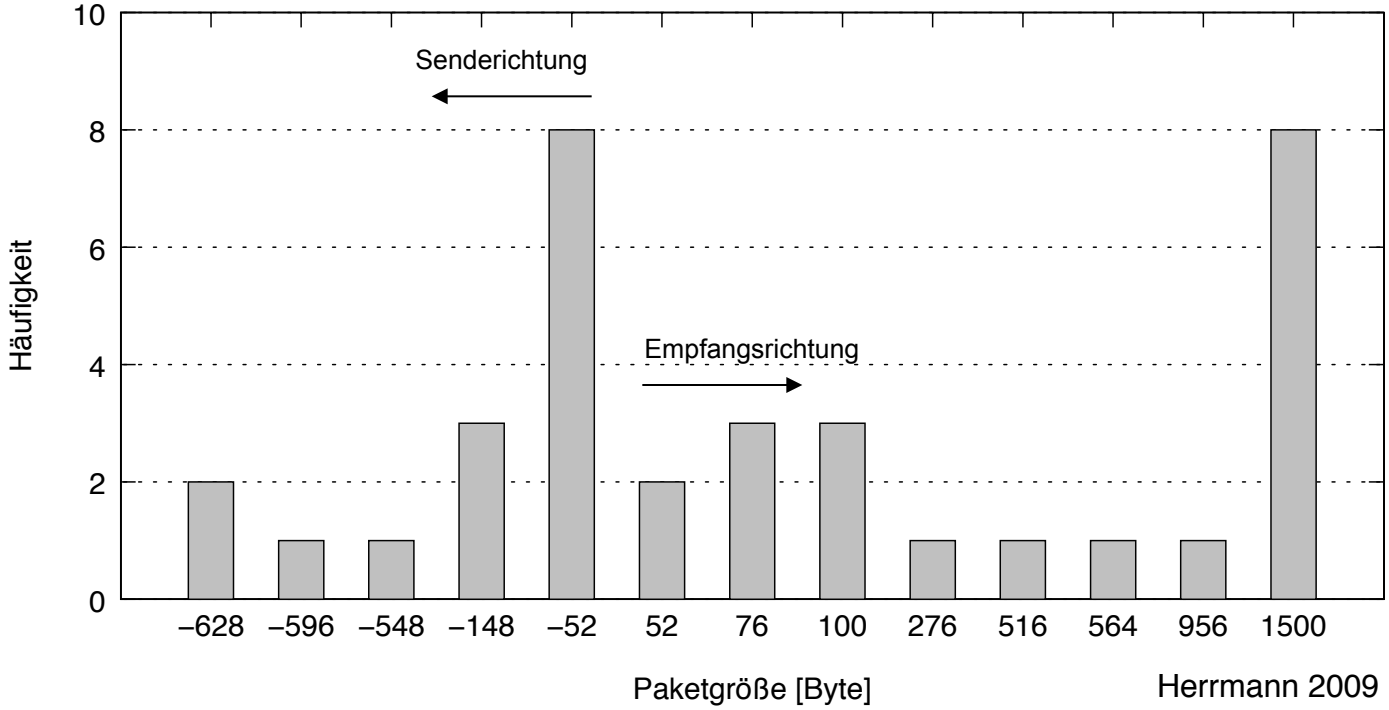
- Traffic-Analyse: Durch Analyse charakteristischen Eigenschaften des Datenverkehrs kann ein passiver Beobachter auf Inhalts und/oder Adressdaten schließen.
- Beobachtbare Merkmale:
  - Auftretenshäufigkeit von Paketen/Verbindungen
  - Paketgröße und Datendurchsatz
  - Zeitpunkte und Paketzwischenabstände



Bedarfsträger:
Führen Verkehrsanalyse durch

Verbessertes Website-Fingerprinting-Verfahren

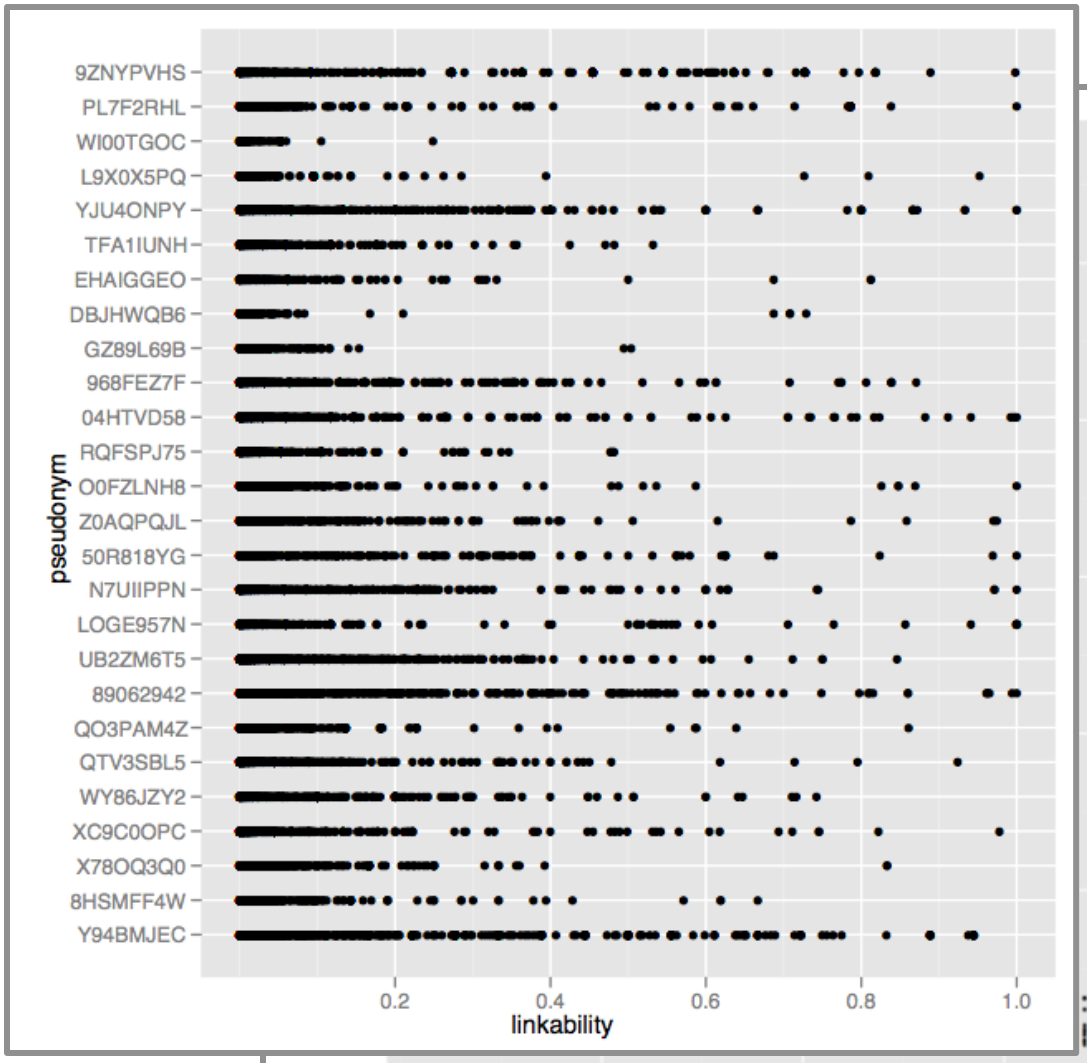
- Analyse der charakteristischen Häufigkeitsverteilung der IP-Paketgrößen



- Schutz durch datenschutzfreundliche Systeme?
  - gering: SSH-Tunnel und VPNs; Erkennungsrate: 90-97%
  - moderat: Anonymisierer wie Tor und JAP/JonDonym; Erkennungsrate: < 20%; neuere Arbeiten: <70% (Panchenko 2010)

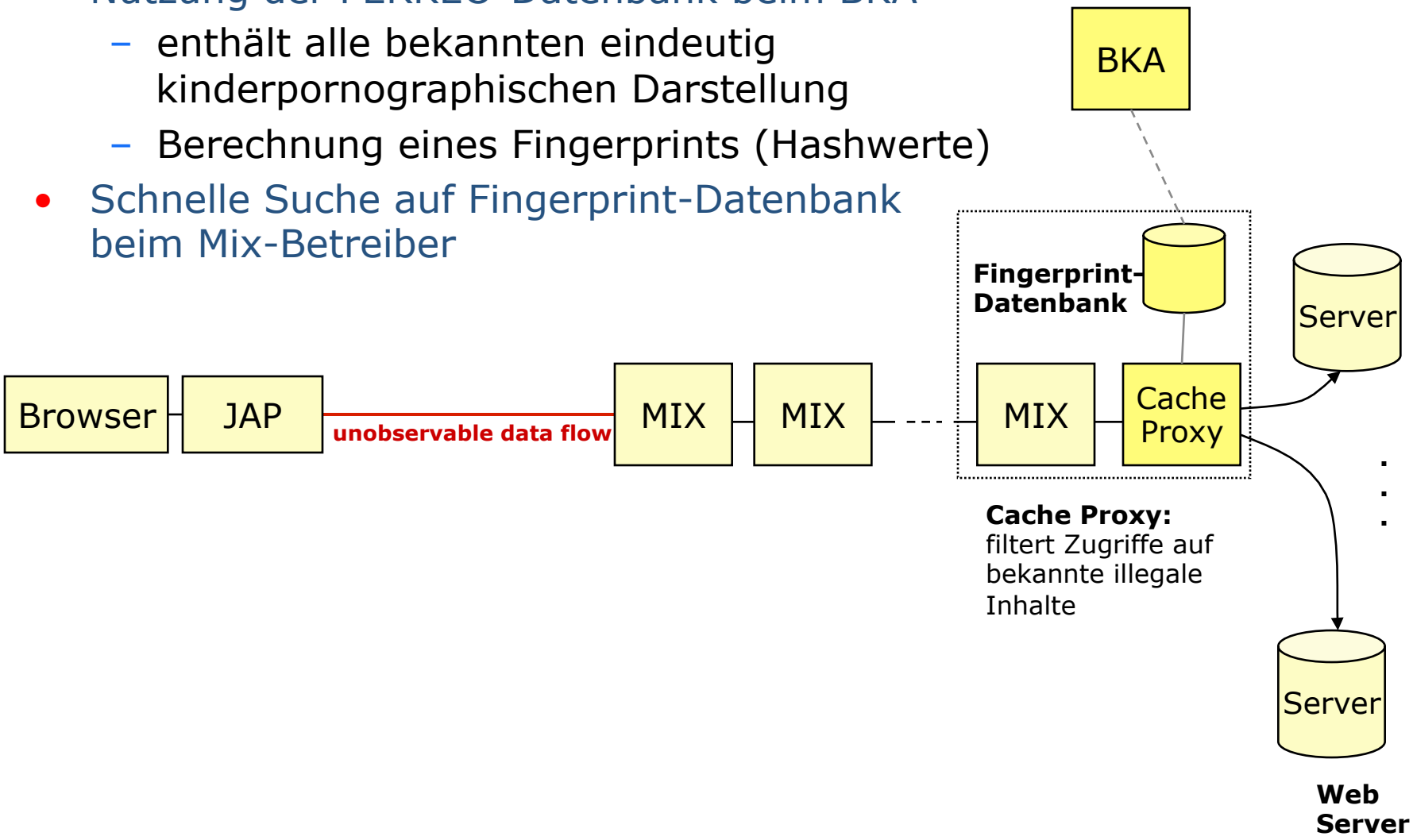
Website- und DNS-Fingerprinting

Gerber 2009



Prävention ist besser als Strafverfolgung

- Nutzung der PERKEO-Datenbank beim BKA
  - enthält alle bekannten eindeutig kinderpornographischen Darstellung
  - Berechnung eines Fingerprints (Hashwerte)
- Schnelle Suche auf Fingerprint-Datenbank beim Mix-Betreiber



Einsichten

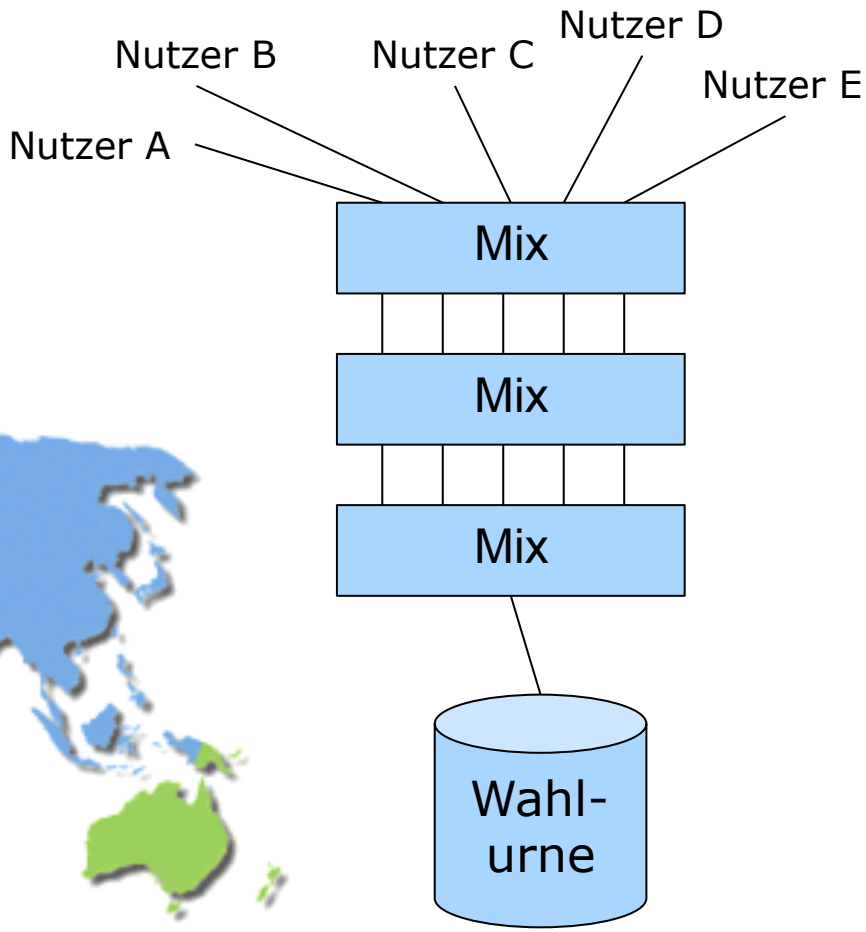
- Grenzenlose Freiheit ist ebenso schädlich wie grenzenloser Schutz.

- Demokratien haben eine besondere Verantwortung bei der Verbreitung von Informationstechnologien:
  - Rüstungskontrolle -> Exporte
  - Sicherheitstechnologie -> Exporte
    - Trend: Videoüberwachung, Sperrtechnologien, Biometrie werden gewinnbringend ins Ausland verkauft
    - Staat sollte die Regulierung nicht nur dem Markt überlassen

- Grenzenlose Kommunikation als Voraussetzung ist häufig selbst in Ländern der dritten Welt bereits gegeben.
  - Twitter, Facebook
  - Fördern der Nutzung für demokratische Prozesse -> z.B. Elektronische Wahlen

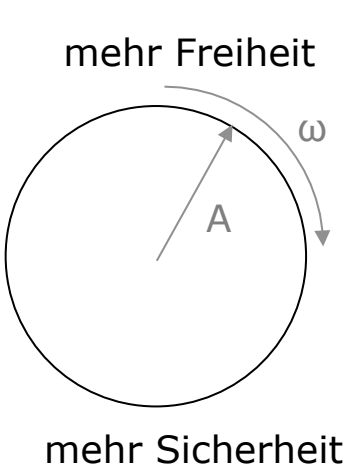
AN.ON – http://www.anon-online.de

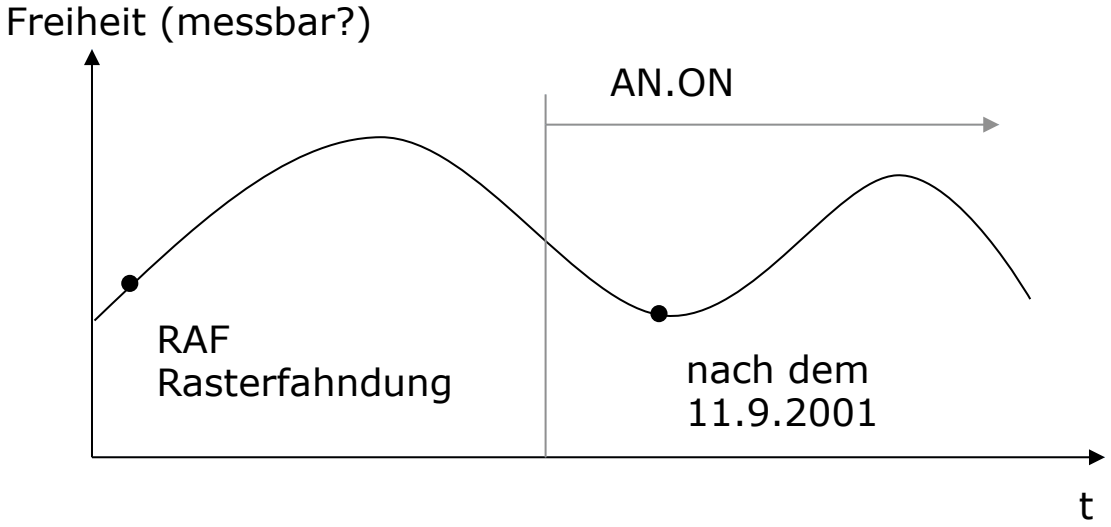
- Fördern der Nutzung von Techniken zum Schutz der Vertraulichkeit und Anonymität für demokratische Prozesse
  - z.B. Elektronische Wahlen



Zyklus von Freiheit und Sicherheit

- Variablen:
  - ω
  - A





Prof. Dr. Hannes Federrath
FB Informatik, AB SVS
Universität Hamburg
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

http://svs.informatik.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG