

Symposium Privatheit und selbstbestimmtes Leben in der digitalen Welt

Rechtliche und technische Untersuchung von Privatheit unterstützenden Technologien

Alexander Roßnagel und
Michael Waidner

forum
<privatheit>
selbstbestimmtes_leben_
in_der_digitalen_welt

20. Oktober 2014, Berlin

GEFÖRDERT VOM



Bundesministerium
für Bildung
und Forschung

Recht und Technik

Notwendige Zusammenarbeit

- Rechtliche Ziele nur durch Technik zu erreichen
 - Technik eröffnet und begrenzt Handlungsmöglichkeiten
 - Technik ist selbstvollziehend
 - Technik wirkt weltweit
- Technik bedarf rechtlicher Rahmensetzung
 - Recht setzt Technik Ziele und Grenzen
 - Recht ermöglicht technische Umsetzung
 - Recht reguliert Konflikte in der Techniknutzung

Grundrechte

Normative Grundlage der digitalen Welt

- Schutz vor unerwünschter Datenverarbeitung
 - Art. 2 I i.V.m. Art. 1 I GG: Informationelle Selbstbestimmung
 - Art. 7 und 8 GrCh: Schutz des Privatlebens, Datenschutz
- Schutz von Eindringen und Manipulation
 - Art. 2 I i.V.m. Art. 1 I GG: Gewährleistung der Vertraulichkeit und Integrität selbstgenutzter informationstechnischer Systeme

Schutzpflicht des Staates

Verantwortung für Grundrechtsverwirklichung

- Pflicht des Staates (Gesetzgeber, Exekutive, Rechtsprechung)
 - „sich schützend und fördernd vor die Grundrechte zu stellen“
 - Verwirklichungsbedingungen für Grundrechtsausübung zu gewährleisten
- Ermessen des Staates
 - Auswahl der Mittel und Wege
 - Einklagbar ist nur Einhaltung eines Untermaßes
 - BVerfG und EuGH zur Vorratsdatenspeicherung: anlasslose, dauerhafte, allumfassende und flächendeckende Überwachung unzumutbar

Selbstdatenschutz

Schutzmöglichkeit des Staates

- Keine Bürgerpflicht - Möglichkeit, Selbstbestimmung durchzusetzen
- Pflicht des Staates, Bürger hierzu in die Lage zu versetzen
- Handlungsaufgaben
 - Werkzeuge zur Verfügung stellen oder fördern
 - Infrastruktur bereit stellen oder fördern
 - Informationen bereit stellen, Aufmerksamkeit wecken
 - Mögliche Konflikte lösen

Selbstdatenschutz

Technische Werkzeuge und Infrastrukturen für Privatheit in ...

Klassisches Internet

Industrie 4.0

Soziale Netze

Smart Home

Mobiles Internet

Speicher-Clouds

Rechen-Clouds

Big Data

Online Handel

Internet of Things

Smart Cars

e-Government



GEFÖRDERT VOM

Selbstdatenschutz

Technische Werkzeuge und Infrastrukturen für Privatheit in ...

Klassisches Internet

Industrie 4.0

Soziale Netze

Smart Home

Mobiles Internet

Speicher-Clouds

Rechen-Clouds

Big Data

Online Handel

Internet of Things

Smart Cars

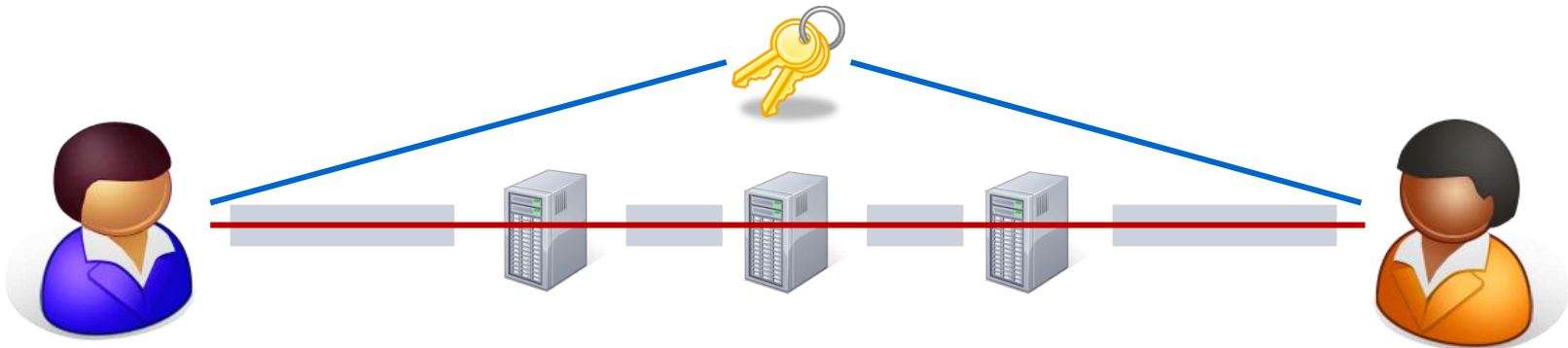
e-Government



GEFÖRDERT VOM

Klassisches Internet

Schutz von Inhaltsdaten



Ende-zu-Ende Verschlüsselung

- Sichere Kryptographie existiert
- Sichere Standards für Mail, Web, Chat, VoIP, ... existieren
 - S/MIME, TLS, SRTP, ...
- Diverse Verschlüsselungslösungen für Cloud-Speicherdienste

Was fehlt?

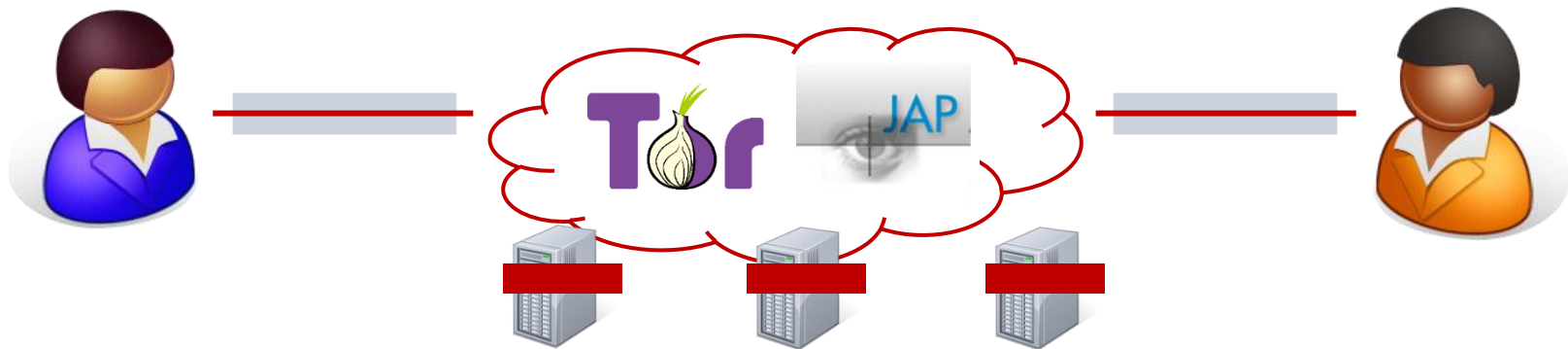
- Internet-weit verfügbare, vertrauenswürdige Schlüsselinfrastruktur (PKI)
- Lientaugliche Integration in Mail, Web, Chat, VoIP, ...

GEFÖRDERT VOM

Klassisches Internet

Schutz von Metadaten

Wer, wann, mit wem, mit welchem Dienst?



Anonyme Kommunikation

- Tor de-facto Standardsystem
- Gut für technik-affine Nutzer und schmalbandige Dienste

Was fehlt?

- Lientauglichkeit
- Massentauglichkeit
- Schutz gegen PRISM-artige Globalüberwachung

GEFÖRDERT VOM

Technische Forschungsaufgaben: Was fehlt?

Zahlreiche offene technische und fundamentale Forschungsfragen, zum Beispiel ...

Klassisches Internet

- Schlüssel für alle,
- Benutzbare Verschlüsselung,
- Massentaugliche anon. Kommunikation

Soziale Netze

Smart Home

Mobiles Internet

- Schutz von Positionsdaten

-Clouds

Rechen-Clouds

Big Data

- Umgang mit abgeleiteten Daten

- Rechnen mit verschlüsselten Daten
- Überprüfbarkeit der Betreiber-IT

Internet of Things

- Management persönlicher Daten

- Privacy by Design
- Bewertung
- Klassische IT-Sicherheit

GEFÖRDERT VOM

Technische Forschungsaufgaben

Mit Blick auf Massenüberwachung im Internet:

12 Forschungs- und Entwicklungsaufgaben



Quelle: www.sit.fraunhofer.de/reports

1. Verteilung vertrauenswürdiger Schlüssel
2. Sichere Verschlüsselung
3. Beobachtbarkeit im Netz
4. Bewegungsprofile in Mobilfunknetzen
5. Tracking
6. Speichern und Teilen in der Cloud
7. Berechnen in der Cloud
8. Aggregierende Dienste
9. System-und Softwaresicherheit
10. Benutzbarkeit
11. Transparenz und Intervenierbarkeit
12. Finanzierbarkeit

GEFÖRDERT VOM

Rechtliche Forschungsaufgaben

Aufgaben der Zukunftsgestaltung

- Gesetzgeberischer Gestaltungsspielraum
 - Pflicht zur Beobachtung und Nachbesserung
 - Pflicht zur Forschungsförderung von Selbstschutztechniken
- Interessenausgleich
 - Verschlüsselung und Strafverfolgung
 - Anonymität und Identifizierung
- Gesellschaftliche Einpassung von Selbstschutztechniken
 - Organisation der Infrastrukturen und des Marktangebots
 - Anforderungen an das Angebot von Selbstschutztechniken
 - Anspruch und Grenzen von Selbstschutz
 - Konfliktmöglichkeiten und Konfliktausgleich