Mehrseitige Sicherheit im Internet am Beispiel Privacy Enhancing Technologies (PET)

Hannes Federrath
Universität Regensburg

http://www-sec.uni-regensburg.de

Gliederung

- Einführung
  - Mehrseitige Sicherheit
  - Privacy Enhancing Technologies (PET)
- Bausteine
- Anpassung an realistische Kommunikationsbedingungen
  - Beispiel Mixe:
    - Skalierbarkeit bzgl. Performance und Sicherheit
    - Transparenz für den Benutzer bzgl. erreichter Sicherheit
- Schlussbemerkungen

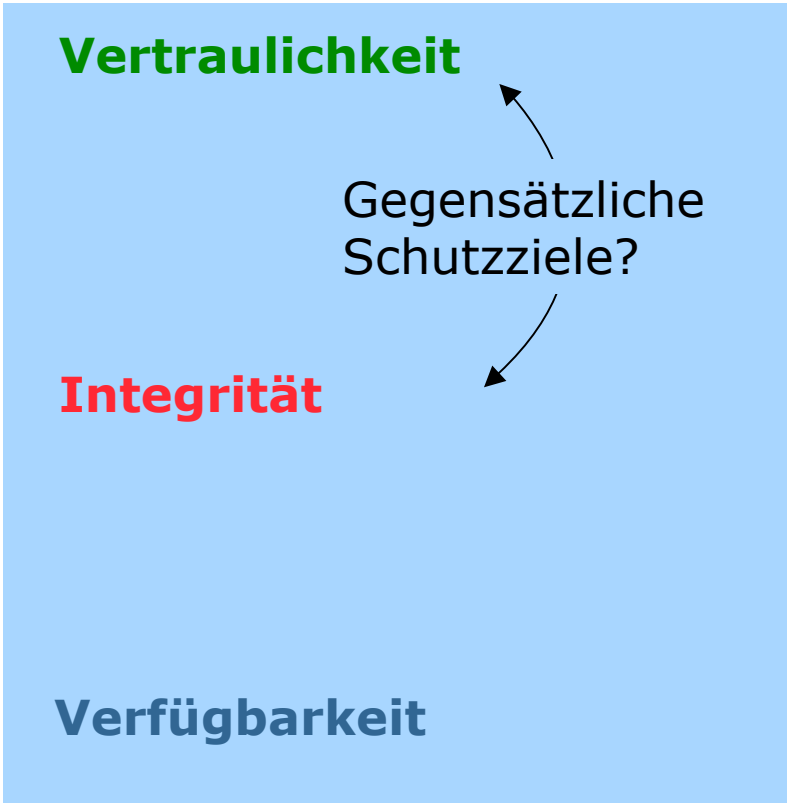
Schutzziele (Voydock, Kent 1983)

- Klassische IT-Sicherheit berücksichtigt im Wesentlichen Risiken, die durch *regelwidriges Verhalten* in IT-Systemen entstehen.

Vertraulichkeit	unbefugter Informationsgewinn
Integrität	unbefugte Modifikation
Verfügbarkeit	unbefugte Beeinträchtigung der Funktionalität

Mehrseitige Sicherheit (Müller et. al. 1997)

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



- Voraussetzung
  - regelwidriges Verhalten hält Systeme und Nutzer schadlos
- Ziel
  - gegensätzliche Sicherheitsinteressen werden erkannt, Lösungen ausgehandelt und durchgesetzt

Schutzziele (Federrath, Pfitzmann 1999)

Kommunikationsgegenstand WAS?		Kommunikationsumstände WANN?, WO?, WER?
Vertraulichkeit **Verdecktheit**	Inhalte	**Anonymität** **Unbeobachtbarkeit** Sender, Ort Empfänger
Integrität	Inhalte	**Zurechenbarkeit** **Rechtsverbindlichkeit** Absender, Bezahlung Empfänger
Verfügbarkeit	Inhalte	

Schutzziele: Datenschutzfördernde Technik

Kommunikationsgegenstand **WAS?**		**Kommunikationsumstände** **WANN?, WO?, WER?**
Vertraulichkeit **Verdecktheit**	**Inhalte**	**Anonymität** **Unbeobachtbarkeit** **Sender** **Ort** **Empfänger**

- 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

Angreifermodell: Datenschutzfördernde Technik

Kommunikationsgegenstand **WAS?**		**Kommunikationsumstände** **WANN?, WO?, WER?**
Vertraulichkeit **Verdecktheit**	**Inhalte**	**Anonymität** **Unbeobachtbarkeit** **Sender** **Ort** **Empfänger**

- Outsider
  - Abhören auf Kommunikationsleitungen
  - Verkehrsanalysen
- Insider
  - Netzbetreiber oder bösartige Mitarbeiter (Verkehrsprofile)
  - Staatliche Organisationen

Prinzipien: Datenschutzfördernde Technik

Kommunikationsgegenstand WAS?	**Kommunikationsumstände WANN?, WO?, WER?**
Vertraulichkeit Verdecktheit **Inhalte**	**Anonymität Unbeobachtbarkeit** **Sender** **Ort** **Empfänger**

- Datenvermeidung
  - Erfassungsmöglichkeit und Speicherung personenbezogener Daten vermeiden
- Datensparsamkeit
  - Jeder behält seine personenbezogenen Daten in seinem persönlichen Verfügungsbereich.

Bausteine datenschutzfördernder Technik

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

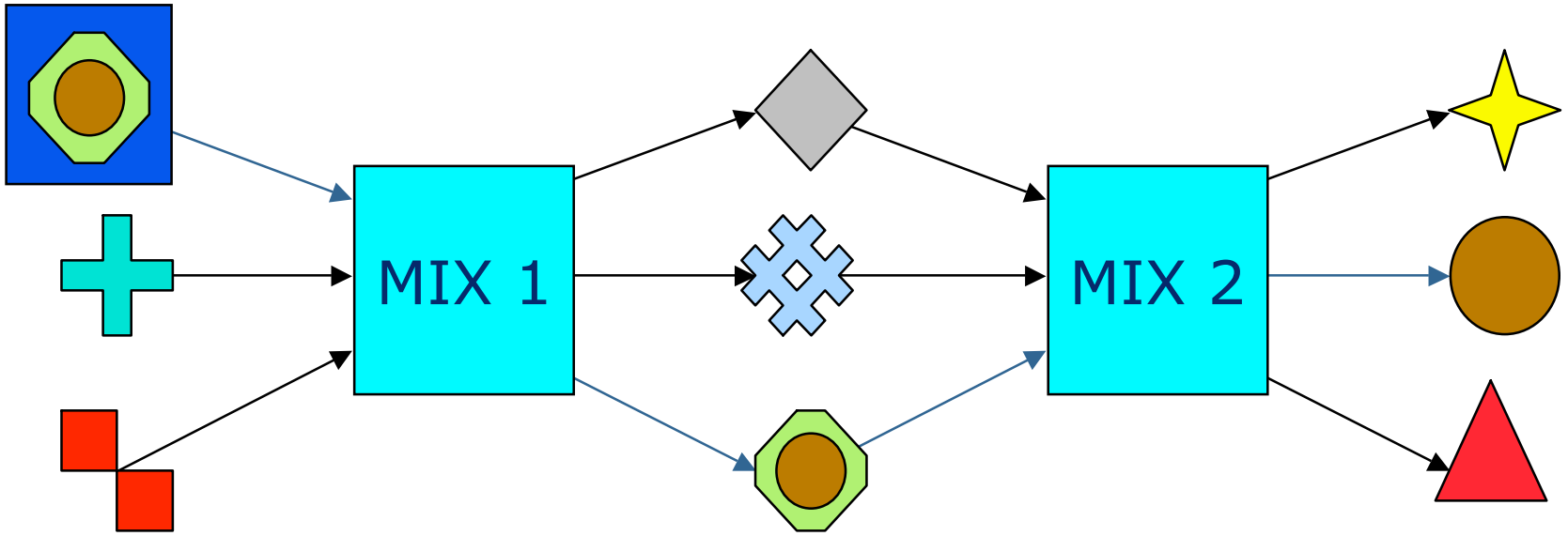
Historische Entwicklung

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 introduced
1999	Zeroknowledge Freedom Anonymizer
2000	*AN.ON/JAP Anonymizer* ←
2004	TOR

Grundverfahren
Anwendung

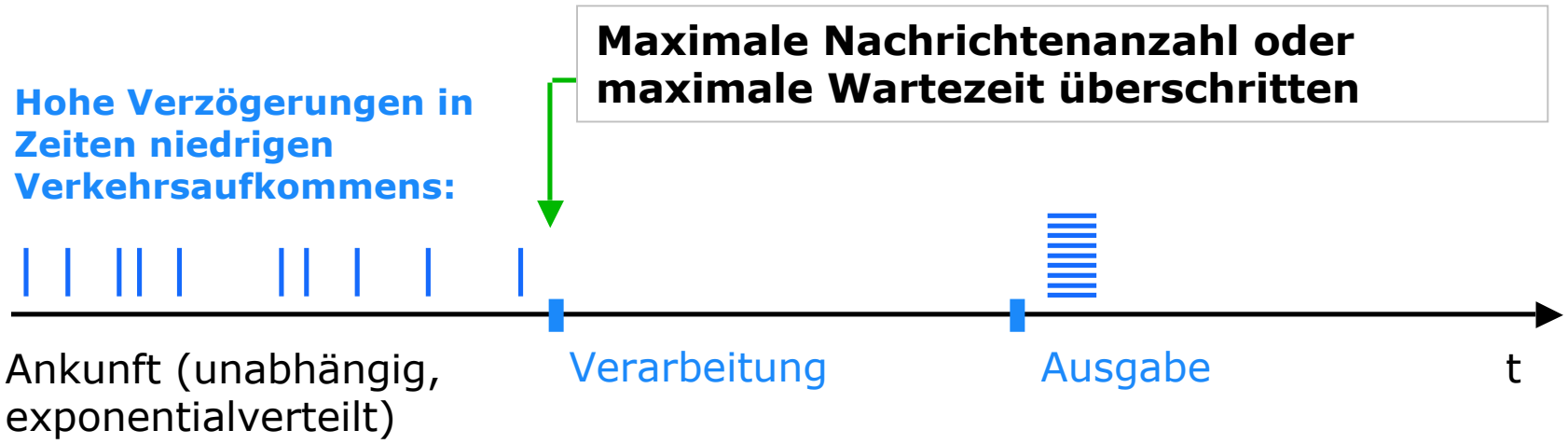
Mix-Netz (Chaum, 1981)

- Grundidee:
  - Nachrichten in einem »Schub« sammeln, Wiederholungen ignorieren, 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:
  - perfekte Unverkettbarkeit von Sender und Empfänger



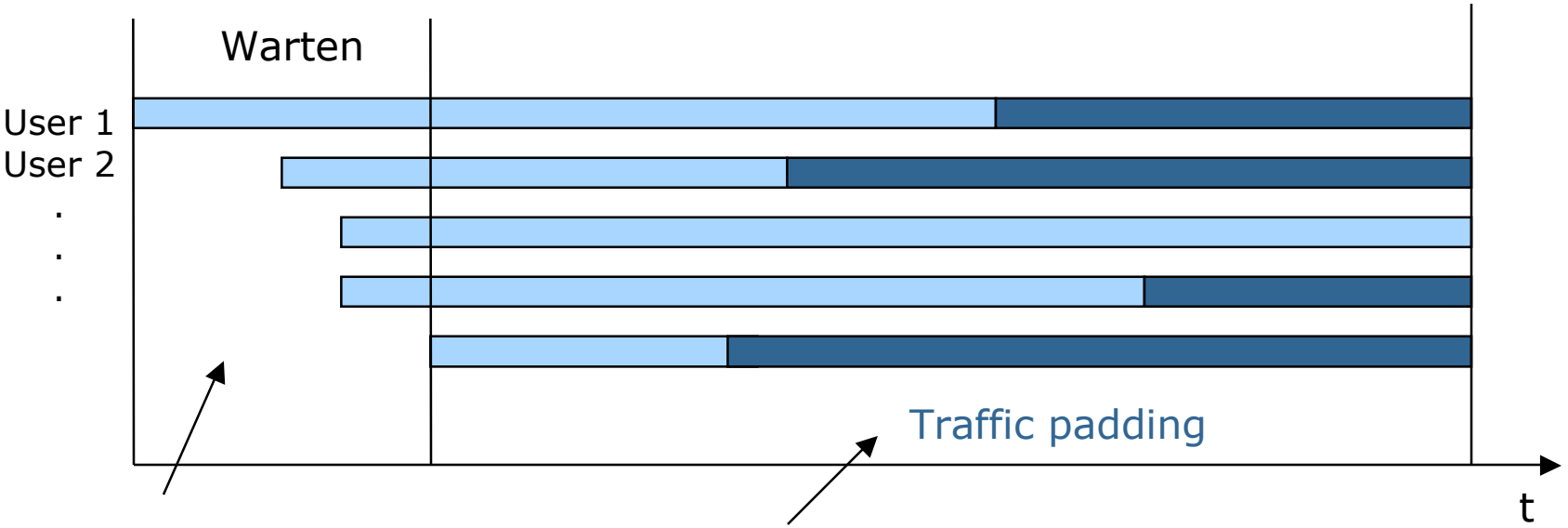
Echtzeitkommunikation und Mixe

- Mixe sind gut geeignet für wenig zeitkritische Dienste:
  - E-Mail
- Für Echtzeitkommunikation sind Modifikationen nötig:
  - Nachrichten sammeln führt zu starken Verzögerungen, da der Mix die meiste Zeit auf andere Nachrichten wartet
  - Nachrichtenlängen und Kommunikationsdauer variieren bei verbindungsorientierten Diensten stark
- Veränderungen nötig



Traffic padding

- Ziel: Verbergen, wann eine Kommunikation beginnt und endet
- Problem: Niemand weiß, wann der letzte Nutzer seine Kommunikation beenden möchte



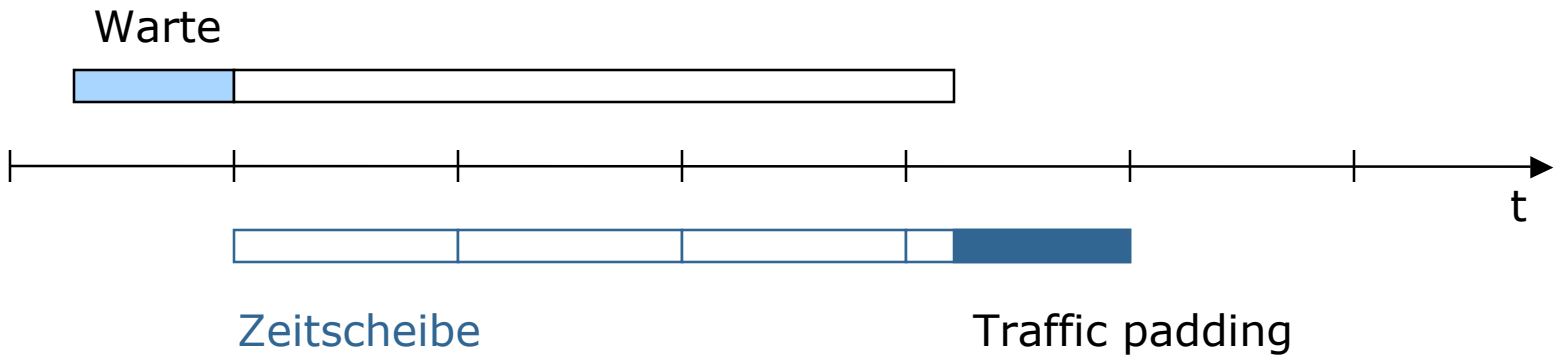
1. Warten, bis genügend Benutzer kommunizieren wollen (Bilden der Anonymitätsgruppe)
   Beispiel: 5 Nutzer

2. Nach Kommunikationsende senden die Nutzer solange Zufallszahlen, bis der letzte Nutzer seine Kommunikation beendet.

3. Problem: Niemand weiß, wann der letzte Nutzer seine Kommunikation beenden möchte, da niemand echte Nachrichten von Traffic padding unterscheiden kann.

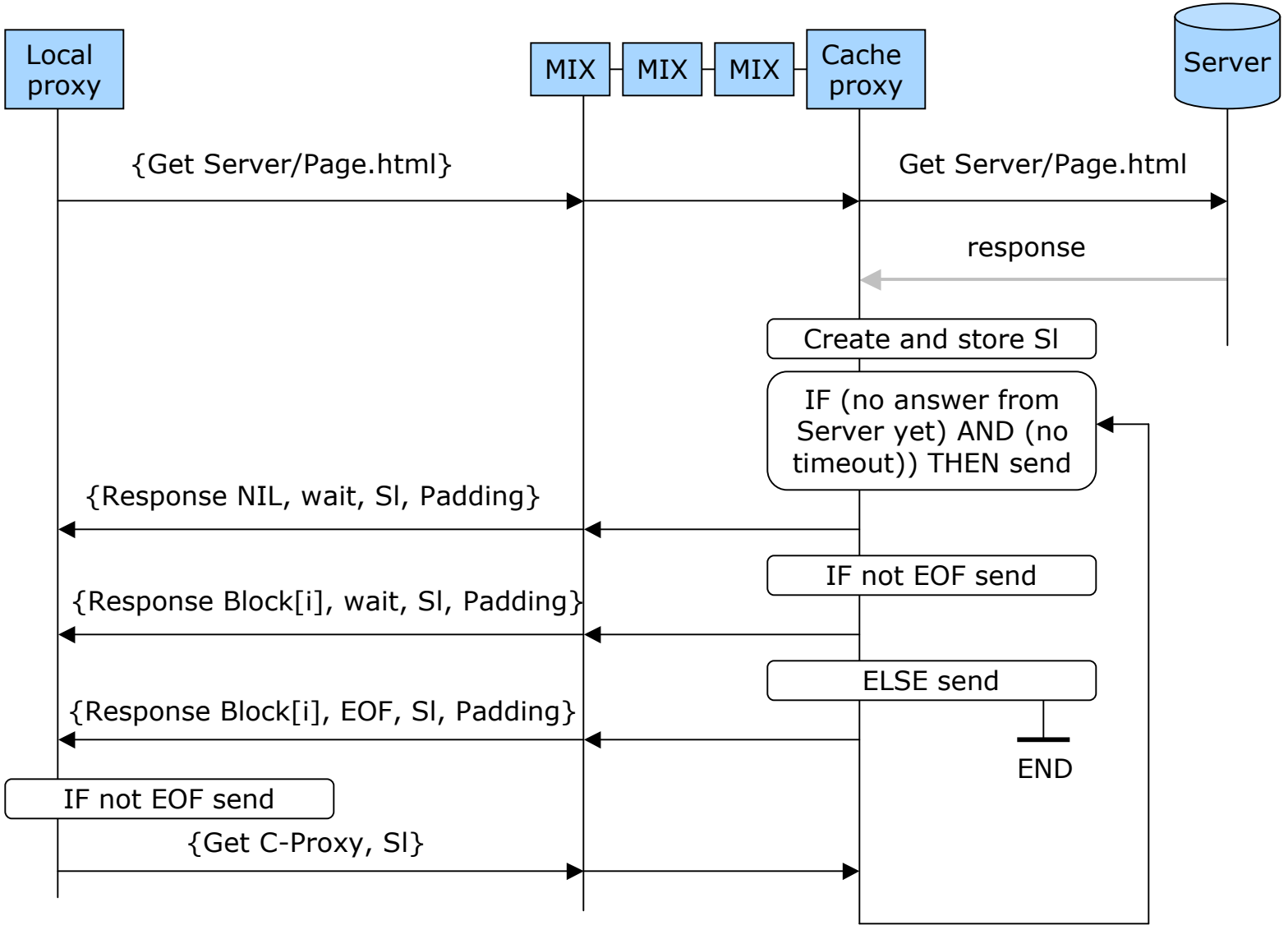
Zerlegen der Kommunikation in Zeit-/Volumenscheiben

- Zeitscheiben (Pfitzmann et. al. 1989)
  - Unbeobachtbarkeit innerhalb der Gruppe aller Nachrichten einer Zeitscheibe
  - Längere Kommunikationsverbindungen setzen sich aus mehreren Zeitscheiben zusammen
  - Zeitscheiben sind nicht verkettbar für Angreifer



- Volumenscheiben (Federrath et. al. 2000)
  - adaptive Anpassung der Scheibengröße in Abhängigkeit der aktuellen Verkehrssituation
  - Minimieren des Overheads

Volumenscheibenprotokoll



Problem bei Langzeitbeobachtung

- Schnittmengenangriff (Berthold, 1999)
  - Angreifer kann sehen, wann sich Benutzer an einer Volumenscheibe beteiligt und wann nicht
  - Angreifer beobachtet alle Kommunikationsleitungen, ohne in Mixe einzudringen
  - Schnittmenge der jeweiligen Anonymitätsgruppen enthält stets Benutzer
- Wie lange es dauert, die Aktionen eines Benutzers zu verketten, hängt von der Gruppengröße und dem Benutzerverhalten ab.
  - Beachte: Nur relevant bei wiederkehrender anonymer Nutzung eines Kommunikationsendpunkts
- Derzeit ist kein Schutz vor Schnittmengenangriffen in Sicht.
- Ausweg: Warnung des Benutzers

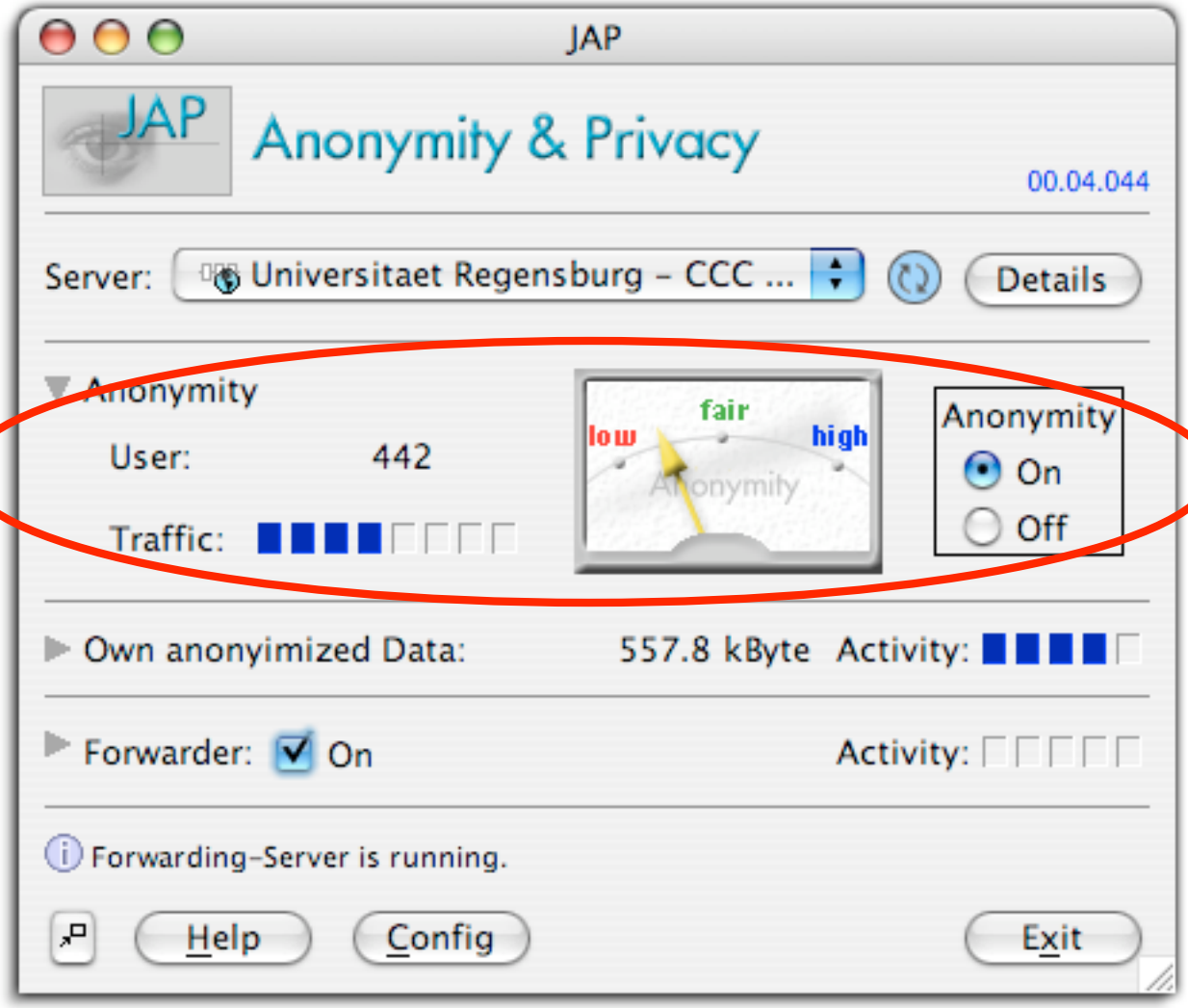
Problem bei Langzeitbeobachtung

- Schnittmengenangriff (Berthold, 1999)
  - Angreifer kann sehen, wann sich Benutzer an einer Volumenscheibe beteiligt und wann nicht
  - Angreifer beobachtet alle Kommunikationsleitungen, ohne in Mixe einzudringen
  - Schnittmenge der jeweiligen Anonymitätsgruppen enthält stets Benutzer

  - Schnittmengenangriff bildet obere Schranke bzgl. des erreichbaren Schutzes, die nicht noch überschritten werden muss durch zugrunde liegendes Anonymitätsverfahren
  - Schnittmengenangriff begrenzt die Stärke des maximalen Schutzes

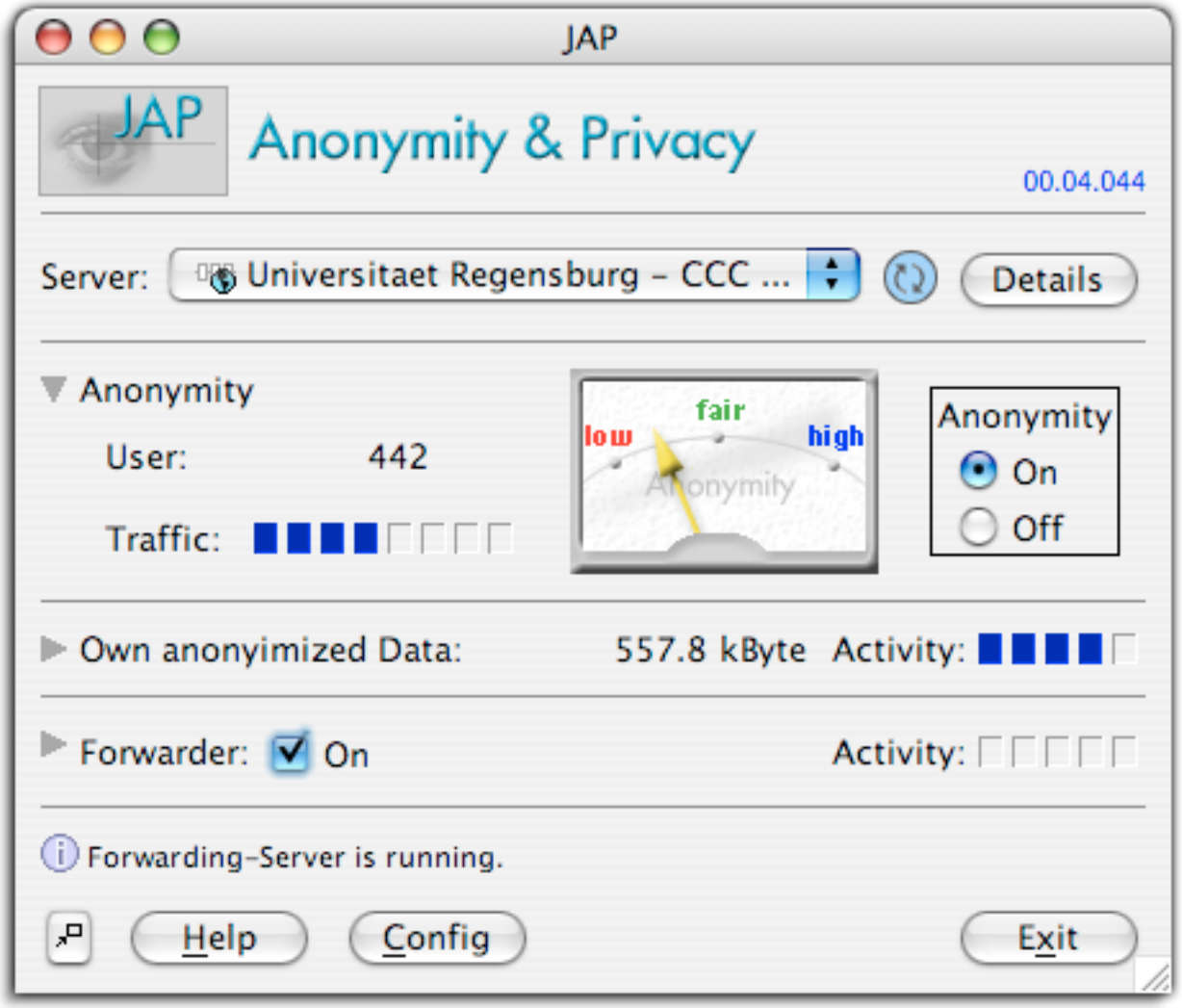
- Ausweg: Warnung des Benutzers

AN.ON/JAP



Rückmeldung über Verkehrssituation und Beobach-tungsrisiko (Lang-zeitbeobachtung)

AN.ON/JAP



Ziele:

Schaffen einer praktikablen Lösung für anonyme und unbeobachtbare Basiskommunikation

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

OpenSource

>10.000 Nutzer

>6 TB/Monat

www.anon-online.de

AN.ON/JAP

Förderer: BMWA, 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)

OpenSource

>10.000 Nutzer

>6 TB/Monat

www.anon-online.de

AN.ON/JAP

Förderer: BMWA, 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

Aktuelle Arbeiten:

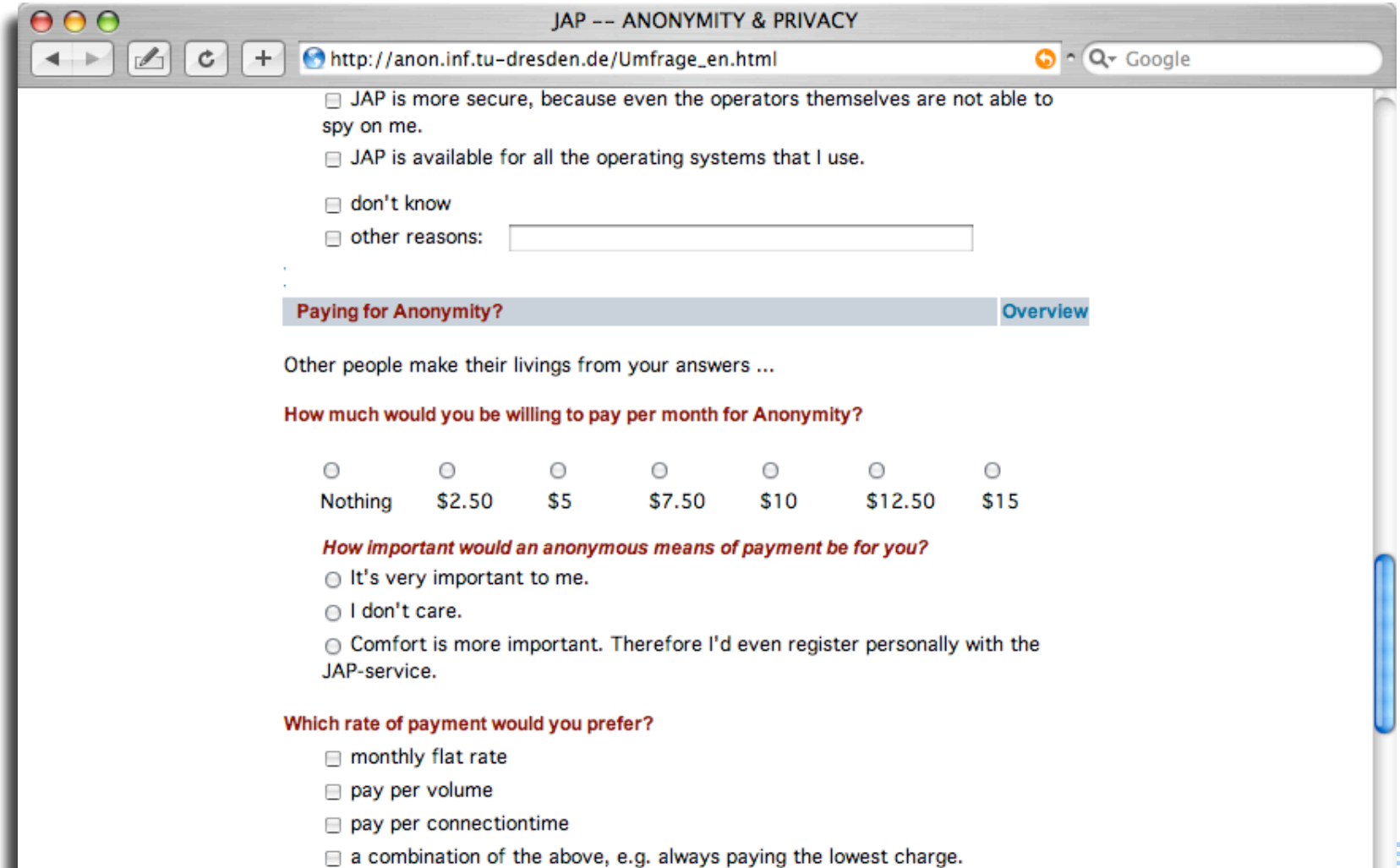
Bezahlfunktion

Strafverfolgungs-funktion

www.anon-online.de

Umfrage unter JAP-Benutzern (Spiekermann, 2003)

- Stichprobe:
  - 1800 JAP-Nutzer

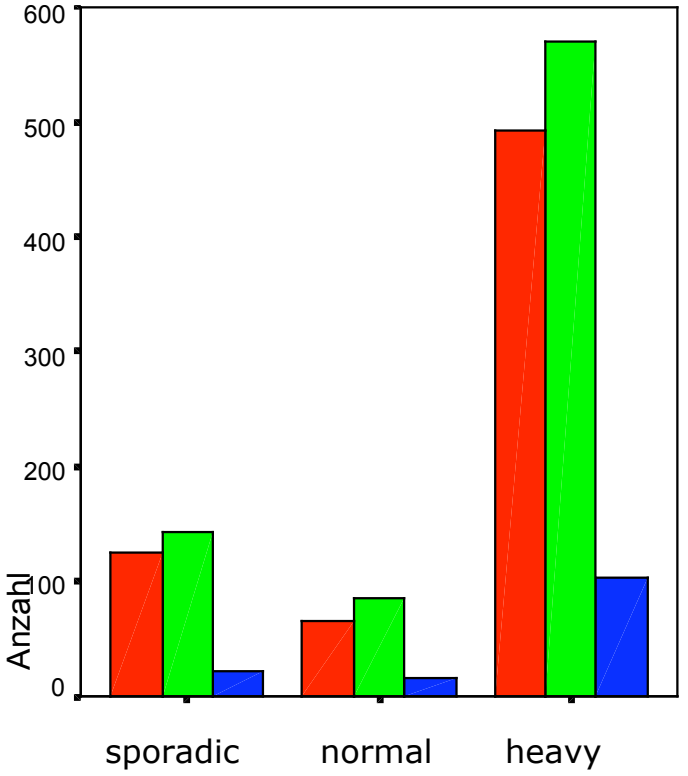


Umfrage unter JAP-Benutzern

- Zahlungsbereitschaft für Anonymität
  - ≈ 40% keine
  - ≈ 50% monatlich zwischen € 2,5 … € 5
  - ≈ 10% mehr als € 5 pro Monat

- Zahlungsbereitschaft korreliert nicht mit der Intensität der Nutzung

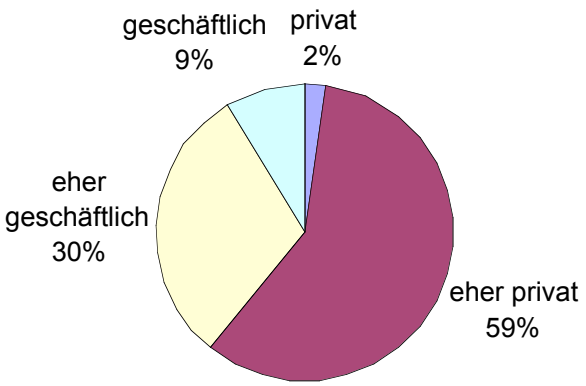
- Intensität der Nutzung
  - ≈ 73% heavy: tägliche Nutzung
  - ≈ 10% «normal»: ≥ 2x pro Woche
  - ≈ 17% sporadic: < 2x pro Woche



Umfrage unter JAP-Benutzern

- Gründe für die Nutzung
  - ≈ 31% Free speech
  - ≈ 54% Schutz vor Geheimdiensten
  - ≈ 85% Schutz vor Profiling (Webnutzung)
  - ≈ 64% Schutz vor eigenem ISP

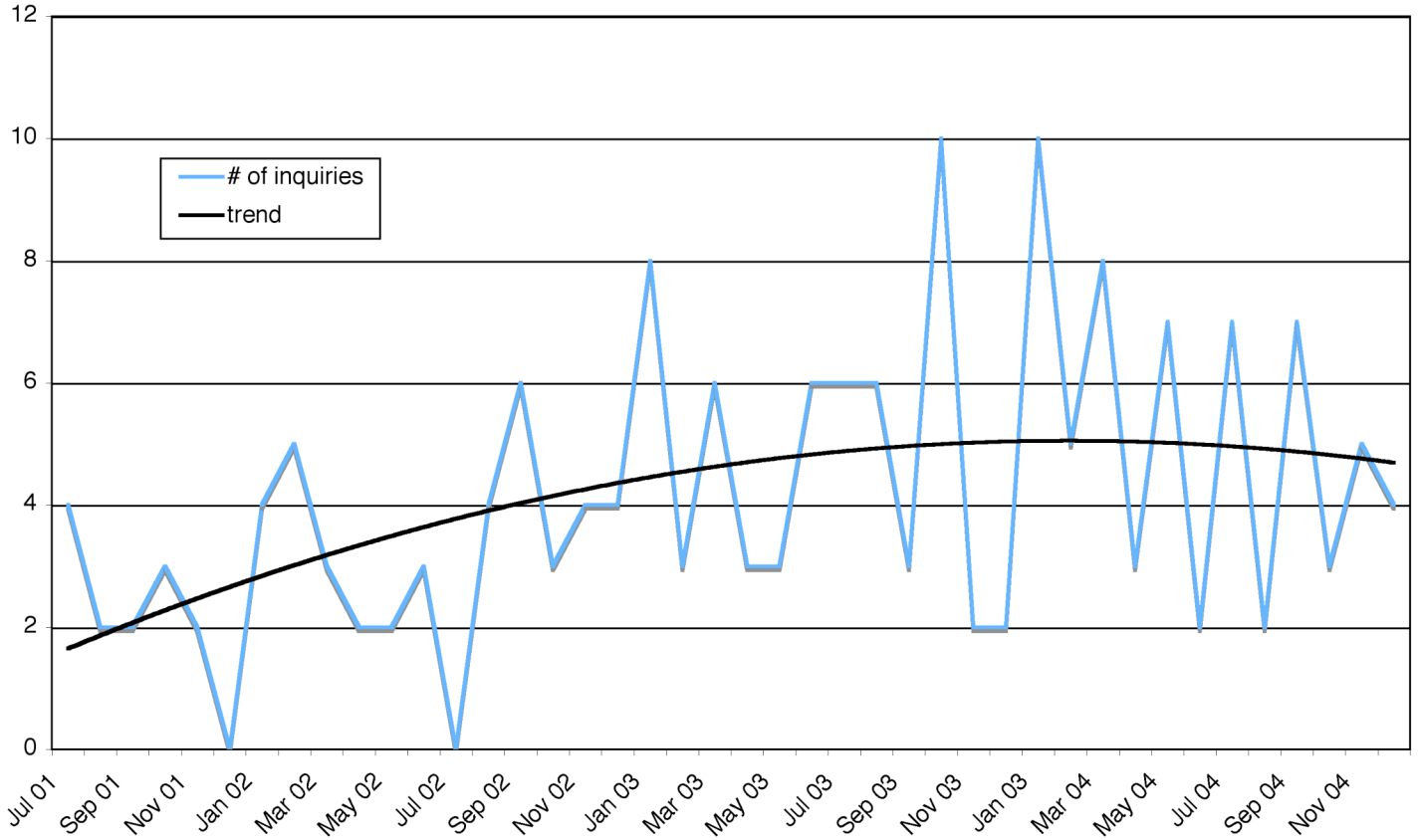
- Private oder geschäftliche Nutzung?
  - ≈ 2% ausschließlich privat
  - ≈ 59% überwiegend privat
  - ≈ 30% überwiegend geschäftlich
  - ≈ 9% ausschließlich geschäftlich



- Warum JAP?
  - ≈ 76% kostenlos
  - ≈ 56% schützt vor Betreibern
  - ≈ 51% einfach benutzbar

Missbrauch und Strafverfolgung AN.ON/JAP

- durchschnittlich 4-5 Anfragen von Strafverfolgern und Privatpersonen pro Monat



Schlussbemerkungen

- Privacy Enhancing Technologies (PET)
  - realisieren insbesondere Vertraulichkeitseigenschaften
    - Anonymität, Unbeobachtbarkeit
  - stärken Nutzer und Betreiber gleichermaßen

- Gesellschaftliches Umfeld beachten
  - Telekommunikationsüberwachung und Vorratsdatenspeicherung
    - Telekommunikationsüberwachungsverordnung
    - Cybercrime-Convention
  - Datenschutzgesetze
    - Bundesdatenschutzgesetz
    - EU-Datenschutzrichtlinien
  - Balance zwischen den Interessen aller Parteien finden