Ermittlungen im Spannungsfeld von Freiheit und Sicherheit

Prof. Dr. Hannes Federrath
Lehrstuhl Management der Informationssicherheit
Universität Regensburg

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

Universität Regensburg

Internationales Seminar „Neue Medien und Kriminaltät – Kriminalität im Internet“, Deutsche Hochschule der Polizei, 13. Januar 2011

Gliederung des Vortrags

- Einführung
  - Schutzziele der IT-Sicherheit und Angreifermodell
  - Das Spannungsfeld von Freiheit und Sicherheit
- Technische Mechanismen zum Schutz (der Freiheit)
  - Unilateral-bilateral-trilateral-multilateral nutzbare Techniken
    - Verschlüsselung
    - Steganographie
    - Anonymisierung
- (Andere) Wege zu mehr Sicherheit?
  - Website-Fingerprinting
  - Anon-Perkeo
- Zusammenfassung

Schutzziele der IT-Sicherheit

»Unsere IuK-Welt«

Bedrohungen	Schutzziele
unbefugter Informationsgewinn	**Vertraulichkeit**
unbefugte Modifikation	**Integrität**
unbefugte Beeinträchtigung der Funktionalität	**Verfügbarkeit**

Gegensätzliche Schutzziele?

Voydock, Kent 1983

Schutzziele und Angreifermodell

Inhalte der Kommunikation	Kommunikationsumstände
Vertraulichkeit **Verdecktheit**	**Anonymität**
Inhalte	**Sender**, **Ort**, **Empfänger**

- Outsider
  - Abhören auf Kommunikationsleitungen
  - Verkehrsanalysen
- Insider
  - Netz- bzw. Dienstbetreiber oder bösartige Mitarbeiter
  - Staatl. Organisationen (des eigenen Staates / fremder Staaten)

Was ist zu schützen?

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

Angreifermodell

Schutz vor einem allmächtigen Angreifer ist unmöglich.

Das Angreifermodell definiert die maximal berücksichtigte Stärke eines Angreifers, gegen den ein Schutzmechanismus gerade noch wirkt.

- Es beschreibt
  - Rollen des Angreifers (Außenstehender, Benutzer, Betreiber, Wartungsdienst, Produzent, Entwerfer …), auch kombiniert
  - Verbreitung des Angreifers
  - Verhalten des Angreifers
    - passiv / aktiv
  - Rechenkapazität:
    - unbeschränkt: informationstheoretisch
    - beschränkt: komplexitätstheoretisch

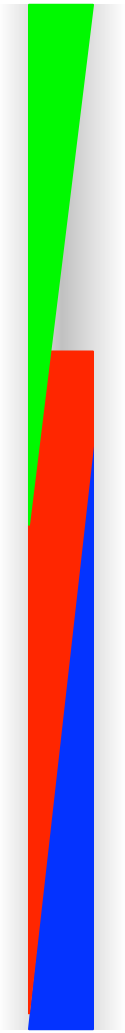
Geld

Zeit

Angriffsformen

- Passive Angriffe
  - Lauschangriff (eavesdropping)
  - Verkehrsflussanalyse (traffic analysis)

- Aktive Angriffe
  - Maskerade (masquerading)
    - Man-in-the-middle attack
  - Verändern von Daten (modification)
  - Einfügen von Daten (injection)
    - Wiederholen (replay)
    - Fluten (flooding, spamming)
  - Dienstverweigerung (denial of service)



Vertraulichkeit

Integrität

Verfügbarkeit

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

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

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.

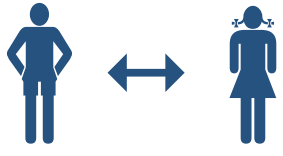
Nicht immer nur der Staat hat die Überwachungsmöglichkeiten

- Beispiele
  - Payback, Google, Facebook
- Situation von Geheimdiensten heute:
  - Aus der großen Menge (öffentlich) zugänglicher Daten die relevanten herausfinden
- 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)

Techniken zum Schutz

- Unilateral nutzbar
  - jede(r) kann allein entscheiden

- Bilateral nutzbar
  - nur wenn der Kommunikationspartner kooperiert



- Trilateral nutzbar
  - nur wenn zusätzlich ein vertrauenswürdiger Dritter kooperiert

- Multilateral nutzbar
  - nur wenn viele Partner kooperieren

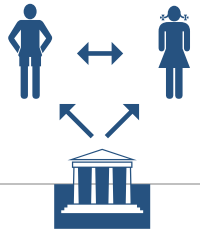
Techniken für Mehrseitige Sicherheit haben das Potential, Nutzer von IT-Systemen von Fremdbestimmung bzgl. ihrer (Un)-Sicherheit zu befreien.

Techniken zum Schutz

- Unilateral
  - Kryptographie zur Dateiverschlüsselung
  - Offenlegung Entwurf

- Selbstschutz-Beispiele
  - Verschlüsselung mit PGP, GnuPG
  - Filtersoftware, Personal Firewalls
  - Offene Betriebssysteme: Linux, BSD

- Bilateral
  - Kryptographie und Steganographie zur Kommunikation



  - Sichere Dienste anstelle ihrer unsicheren Vorläufer: telnet → ssh, ftp → scp, http → https

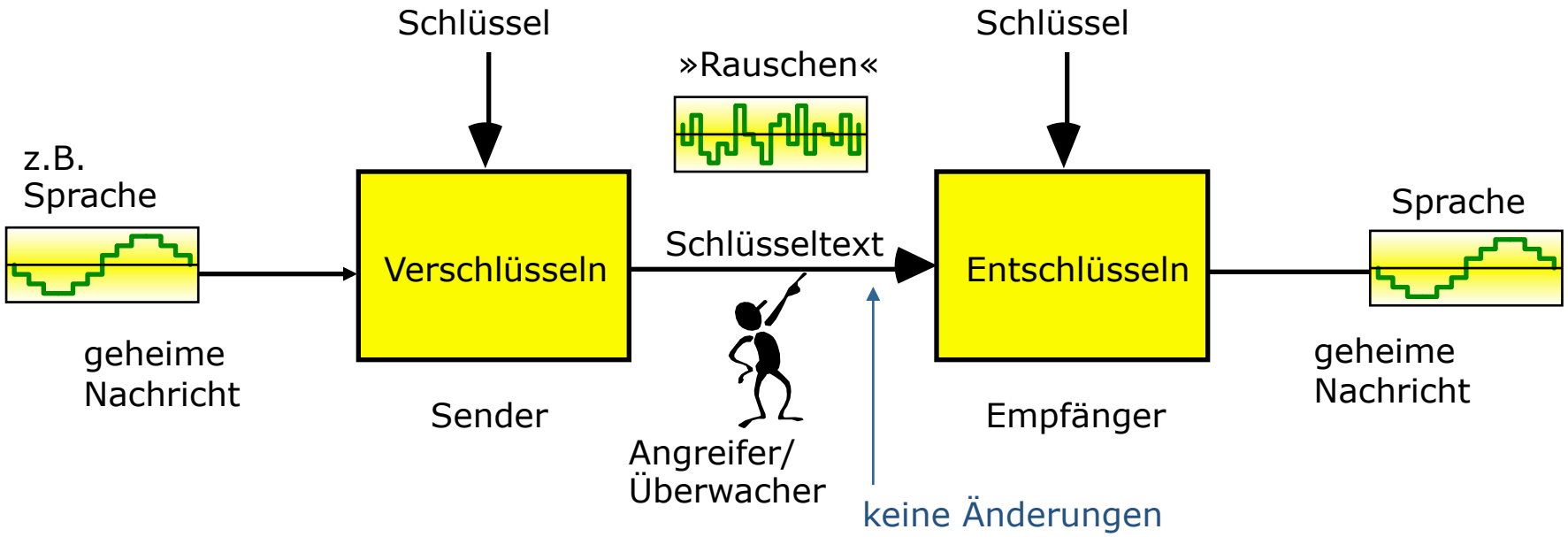
- Trilateral
  - Digitale Signatur und Public Key Infrastructures

  - HBCI
  - eGK

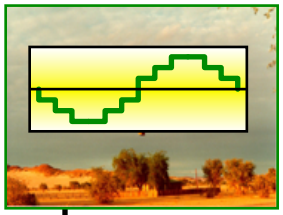
- Multilateral
  - Anonymität, Unbeobachtbarkeit und Pseudonymität in Kommunikationsnetzen

  - Anonymisierer: JAP, TOR

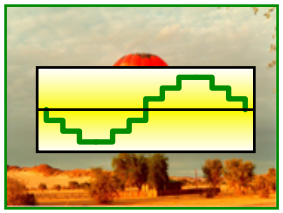
Verschlüsselung: Ziel: vertrauliche Kommunikation



Steganographie: Ziel: verdeckte Kommunikation



Schlüssel



Schlüssel

Hülldaten

einzubettende Daten

Einbetten

Stegodaten

Extrahieren

eingebettete Daten

Geheime Nachricht, ggf. vorverschlüsselt

Sender

Angreifer/ Überwacher sieht nur das Foto

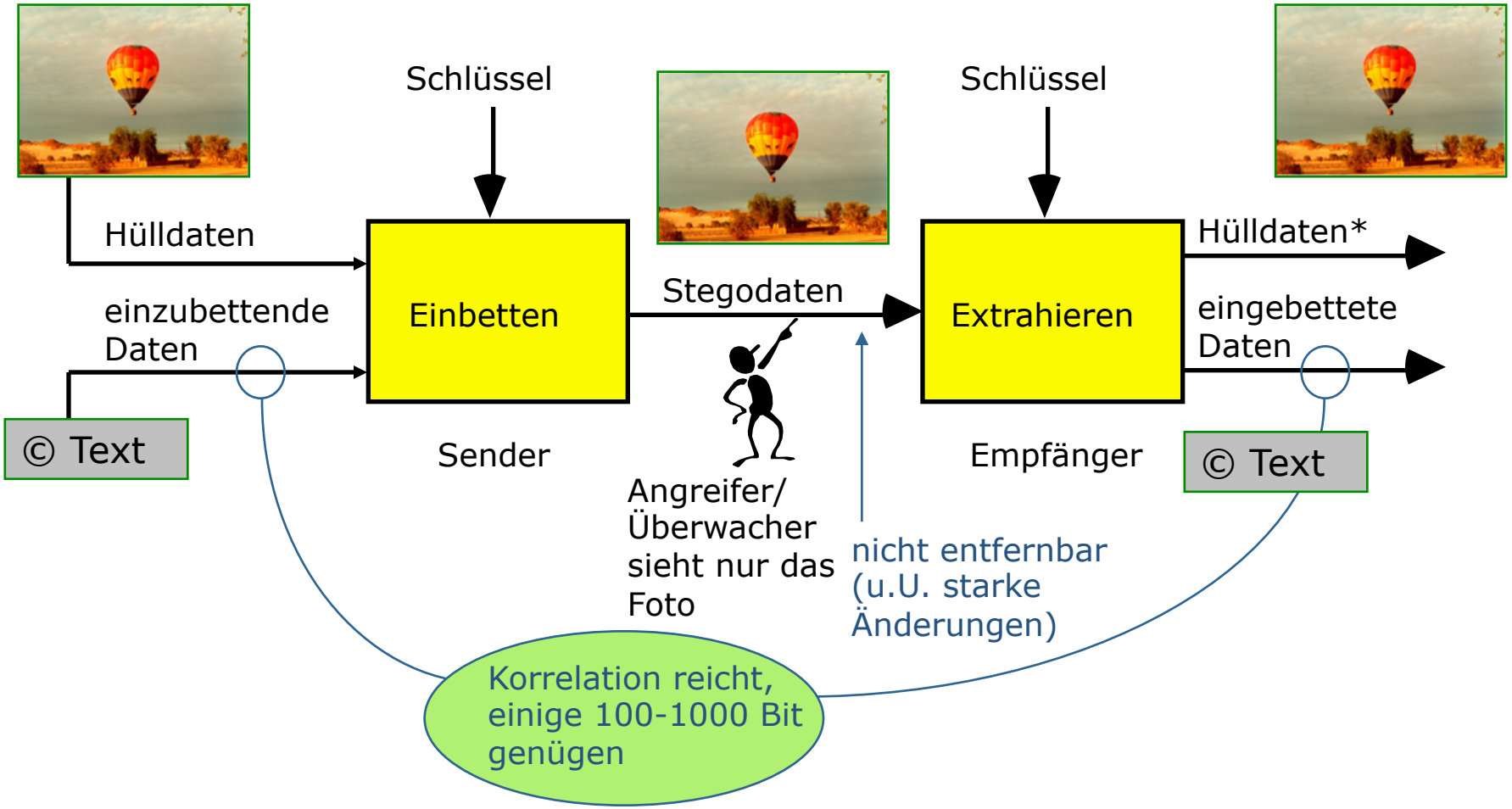
keine Änderungen

Empfänger

Geheime Nachricht

exakt gleich, nicht feststellbar, möglichst viel

Watermarking: Ziel: Urheberschaft digitaler Werke sichern

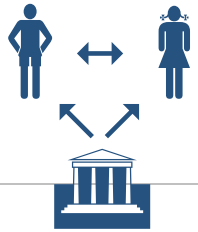


Techniken zum Schutz

- Unilateral
  - Kryptographie zur Dateiverschlüsselung
  - Offenlegung Entwurf

- Stand der Forschung?
  - Kryptographie: sehr gut
  - Betriebssysteme theoret.: sehr gut
  - Betriebssysteme praktisch: schlecht

- Bilateral
  - Kryptographie und Steganographie zur Kommunikation



  - Kryptographie: sehr gut
  - Steganographie: gut

- Trilateral
  - Digitale Signatur und Public Key Infrastructures

  - PKI: sehr gut

- Multilateral
  - Anonymität, Unbeobachtbarkeit und Pseudonymität in Kommunikationsnetzen

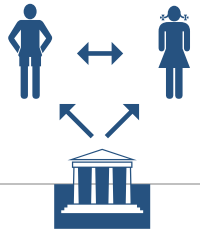
  - Anonymität theoretisch: sehr gut
  - Anonymität praktisch: befriedigend

Techniken zum Schutz

- Unilateral
  - Kryptographie zur Dateiverschlüsselung
  - Offenlegung Entwurf

- Regulierungsversuche?
  - Krypto-Verbot läuft leer, da «Kriminelle» auf Steganographie ausweichen können

- Bilateral
  - Kryptographie und Steganographie zur Kommunikation



  - Verbote laufen leer, da Steganographie nicht mehr erkennbar ist

- Trilateral
  - Digitale Signatur und Public Key Infrastructures

- Multilateral
  - Anonymität, Unbeobachtbarkeit und Pseudonymität in Kommunikationsnetzen

  - Vorratsdatenspeicherung ist weitestgehend sinnlos, da «Kriminelle» auf multilateral nutzbare Technik ausweichen, außerdem öffentliche Telefone, Prepaid Handies, offene WLANs, unsichere Bluetooth-Mobilfunkgeräte

Mix-Netz (Chaum, 1981)

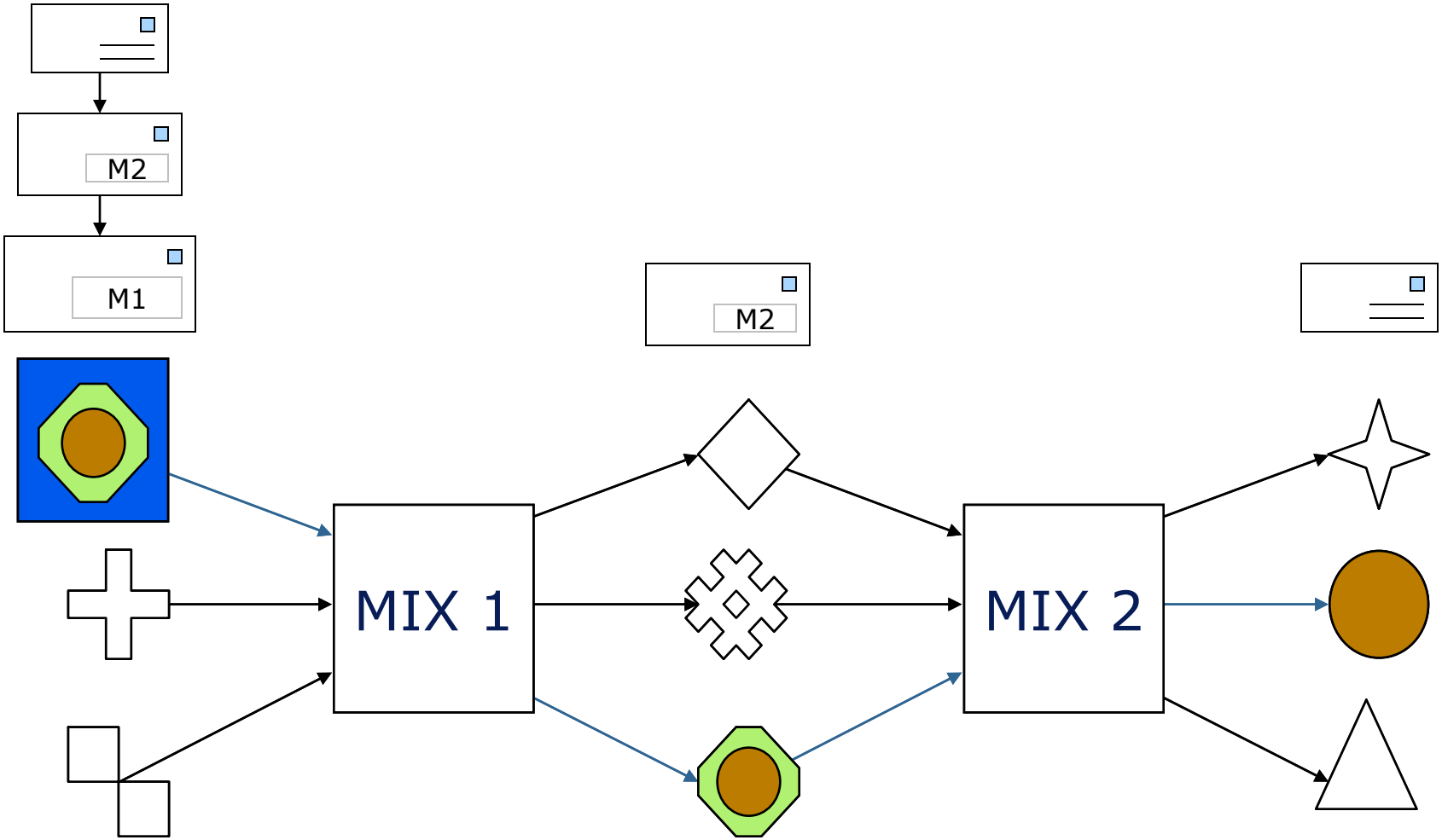
- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation

- 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

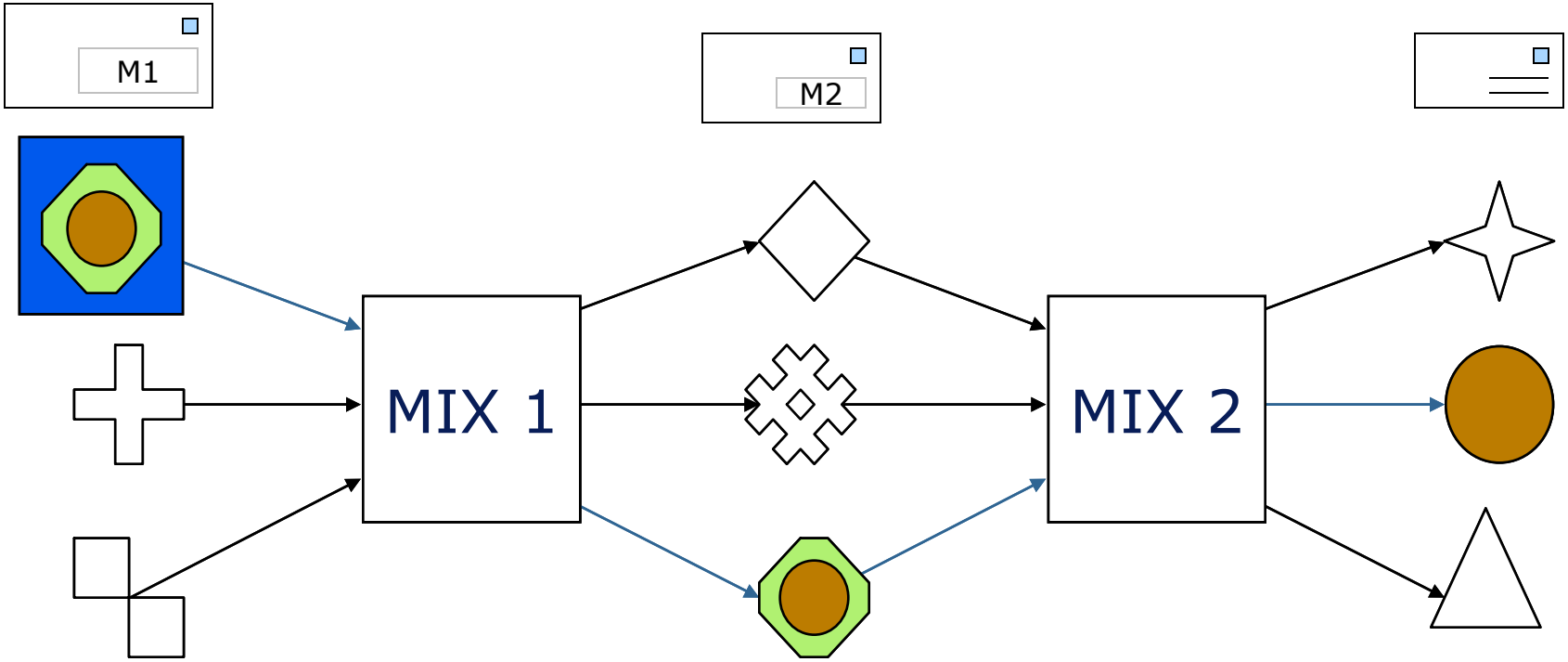
Mix-Netz (Chaum, 1981)

- 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.

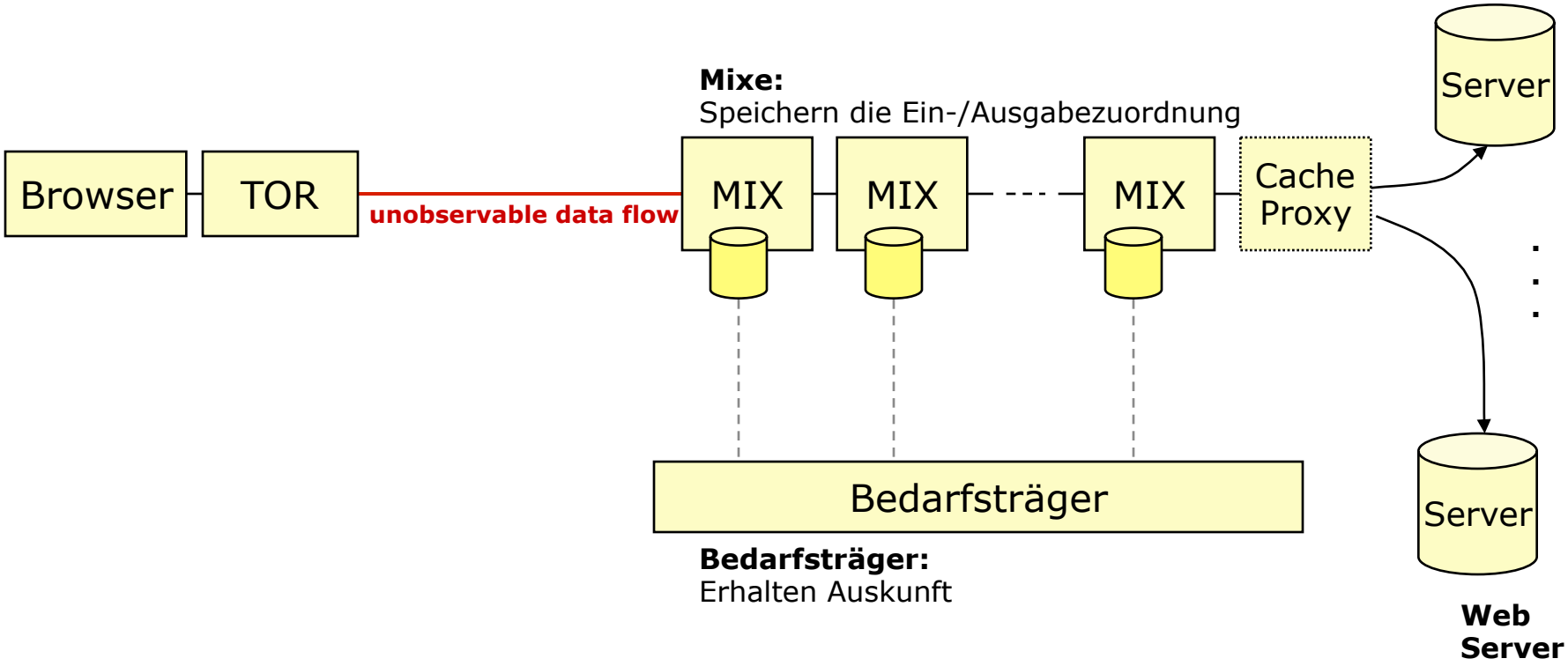


Gliederung des Vortrags

- Einführung
  - Schutzziele der IT-Sicherheit und Angreifermodell
  - Das Spannungsfeld von Freiheit und Sicherheit
- Technische Mechanismen zum Schutz (der Freiheit)
  - Unilateral, bilateral und multilateral nutzbare Techniken
    - Verschlüsselung
    - Steganographie
    - Anonymisierung
- (Andere) Wege zu mehr Sicherheit?
  - Website-Fingerprinting
  - Anon-Perkeo
- Zusammenfassung

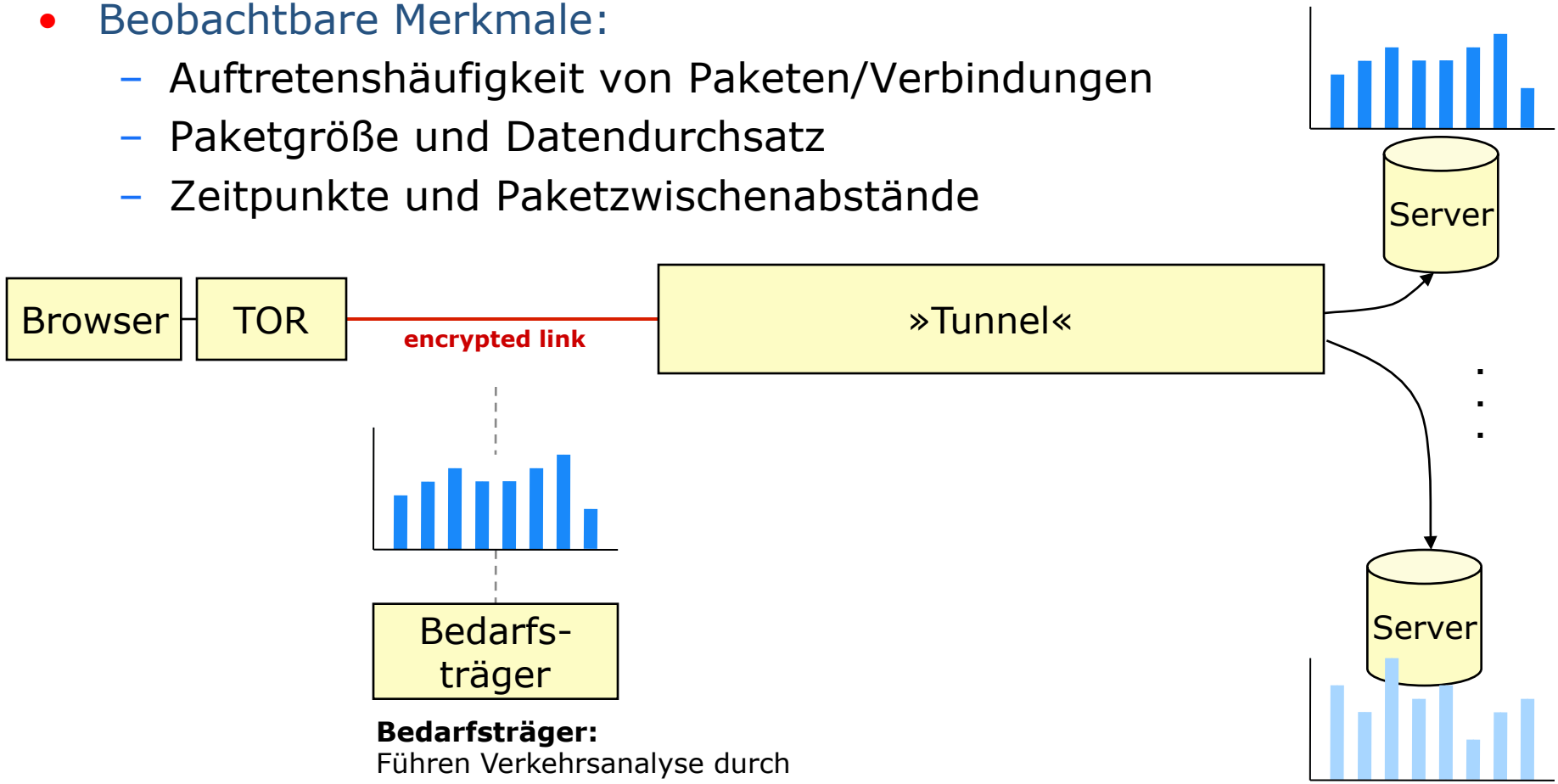
Anstelle von Vorratsdatenspeicherung…

- 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

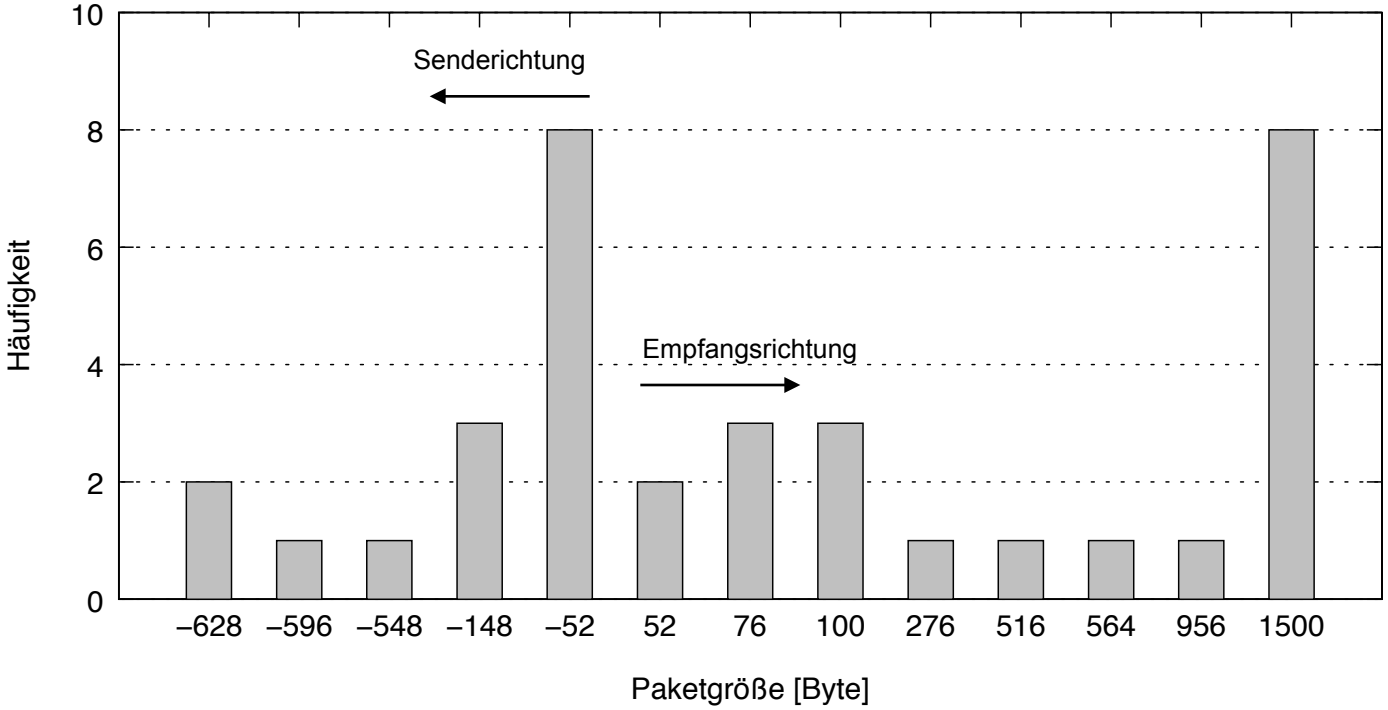
- Traffic-Analyse: Durch Analyse charakteristischen Eigenschaften des Datenverkehrs kann ein passiver Beobachter auf Inhalts und/oder Adressdaten schließen.
- Beobachtbare Merkmale:
  - Auftretenshäufigkeit von Paketen/Verbindungen
  - Paketgröße und Datendurchsatz
  - Zeitpunkte und Paketzwischenabstände



Bedarfsträger:
Führen Verkehrsanalyse durch

Verbessertes Website-Fingerprinting-Verfahren

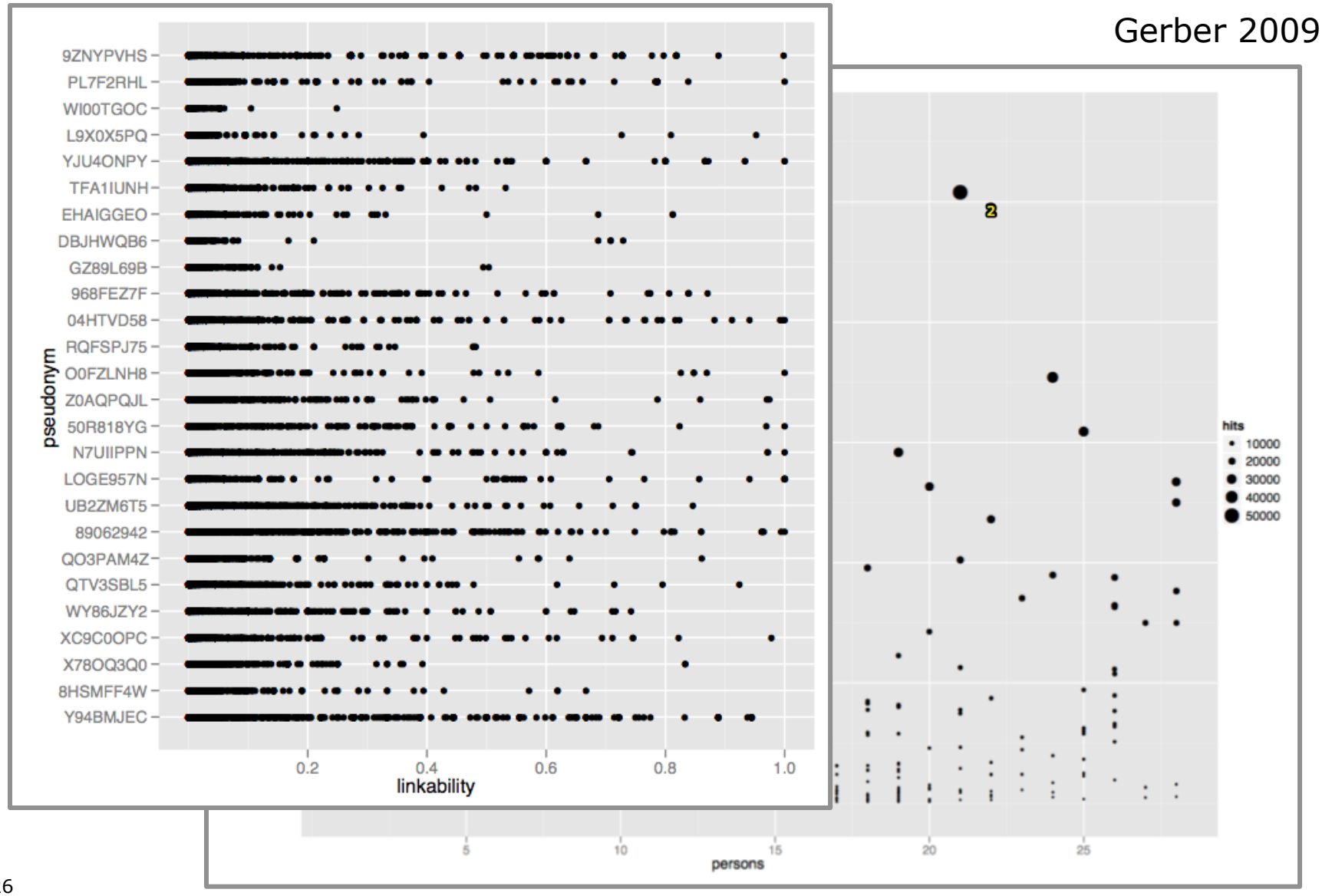
- Analyse der charakteristischen Häufigkeitsverteilung der IP-Paketgrößen



- Schutz durch datenschutzfreundliche Systeme?
  - gering: SSH-Tunnel und VPNs; Erkennungsrate: 90-97%
  - moderat: Anonymisierer wie Tor und JAP/JonDonym; Erkennungsrate: < 20%

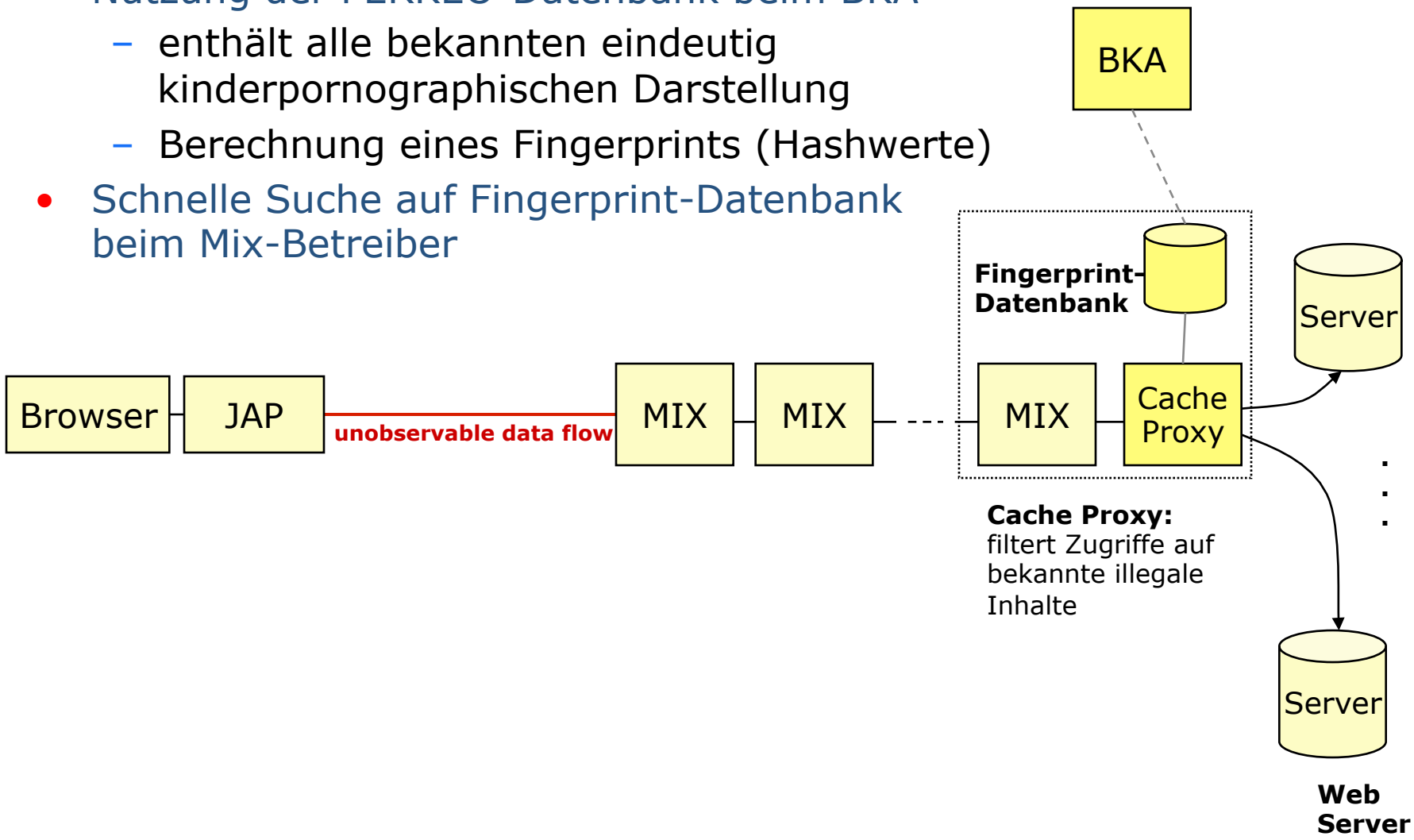
Website- und DNS-Fingerprinting

Gerber 2009

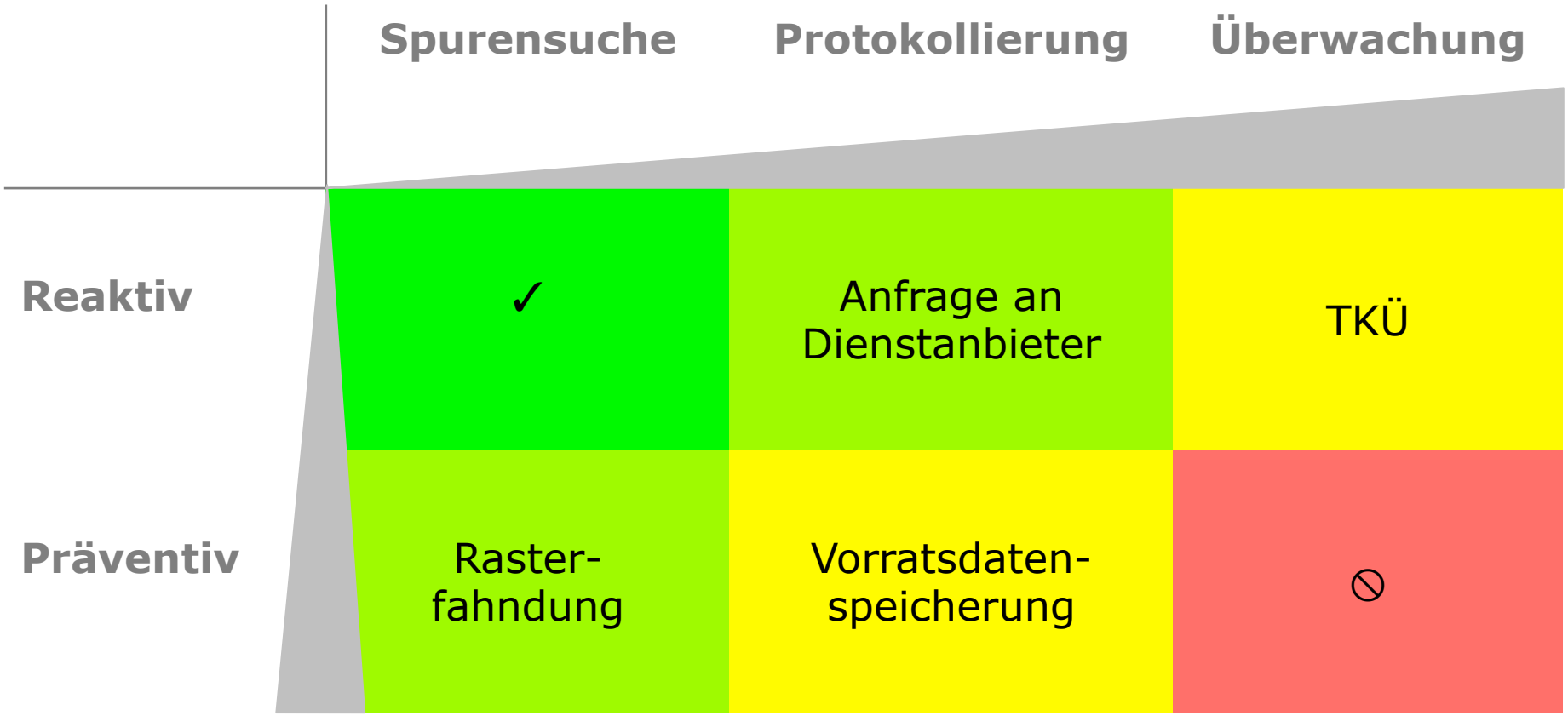


Prävention ist besser als Strafverfolgung

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



Eingriffstiefe von Ermittlungsmethoden in die Freiheit



Zusammenfassung

- Existierende Daten zunächst effektiv für Ermittlungszwecke nutzen
  - Social Networks, Google Services
- Nur wirkungsvolle erweiterte Befugnisse und Technologien fordern
  - Negativbeispiele
    - Biometrischer Reisepass
    - Zugangserschwerungsgesetz
- Mehr auf Prävention setzen
  - Stärkung des Nutzers
    - Einsatz von Firewalls
    - Updates (Erschwerung Botnet-Angriffe)
- Stärker den Kontakt zur Forschung suchen

Prof. Dr. Hannes Federrath
Lehrstuhl Management der Informationssicherheit
Universität Regensburg
D-93040 Regensburg

E-Mail: hannes.federrath@wiwi.uni-regensburg.de
WWW: http://www-sec.uni-regensburg.de

Phone +49-941-943-2870
Telefax +49-941-943-2888