Sicherheit und Schutz im Internet

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de

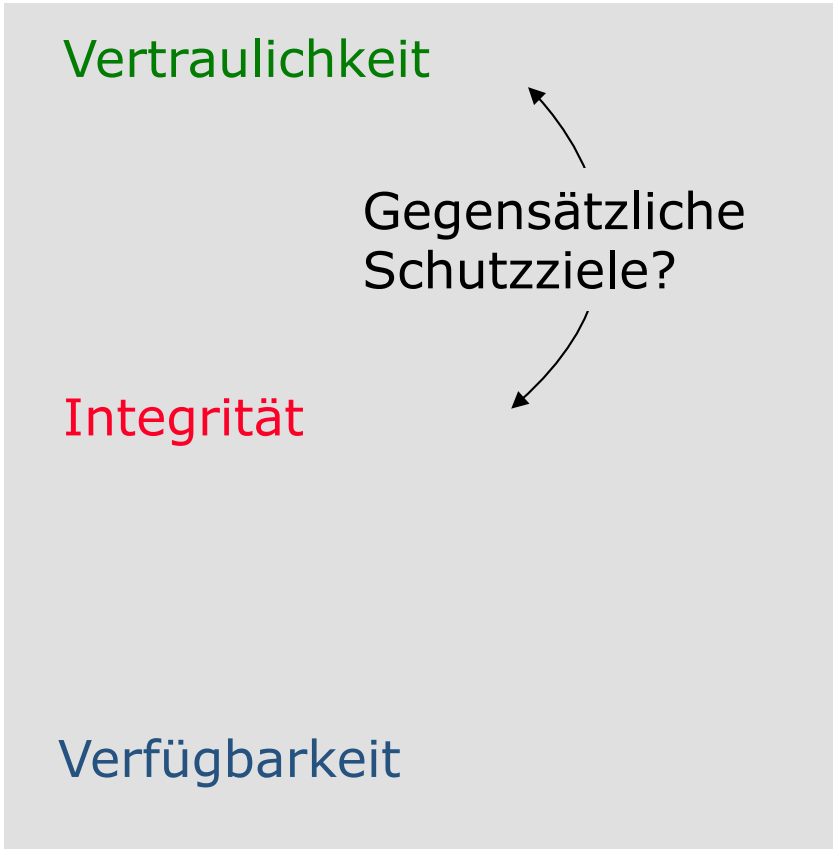
Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Unitag 2015, Hamburg, 25. Feburar 2015

Schutzziele

Voydock, Kent 1983

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



unbefugter Informationsgewinn

unbefugte Modifikation

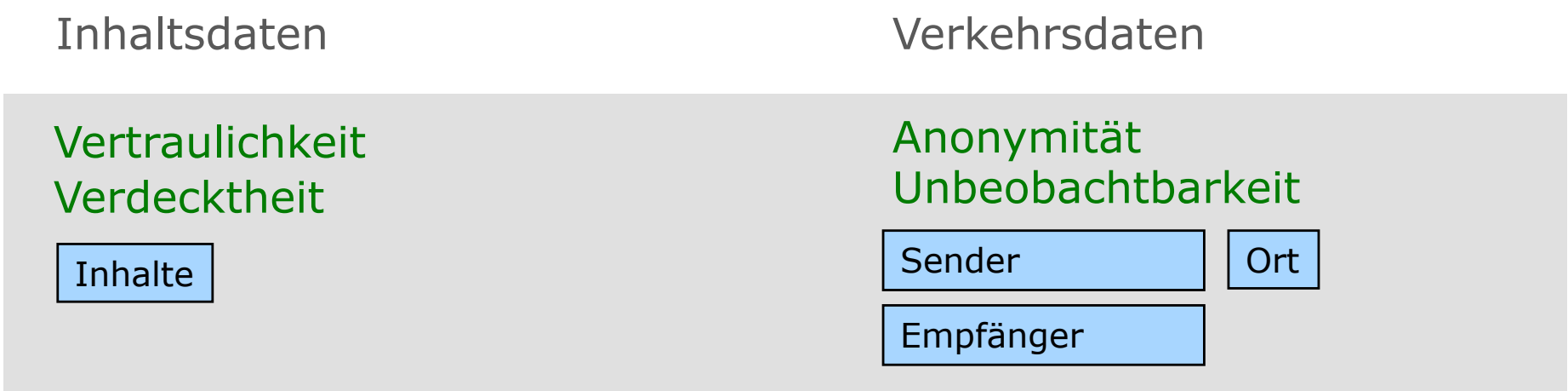
unbefugte Beeinträchtigung der Funktionalität

Vertraulichkeit: Schutzziele und Angreifermodell

Inhaltsdaten	Verkehrsdaten
Vertraulichkeit Verdecktheit	Anonymität Unbeobachtbarkeit
Inhalte	Sender, Ort, Empfänger

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

Vertraulichkeit: Schutzziele und Angreifermodell



- 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

Anonymität im Internet ist eine Illusion

- Wer ist der Gegner?
  - Konkurrenz
  - Geheimdienste fremder Länder
  - Big Brother
  - Systemadministrator
  - Nachbar ...
- Lesenswert: Interception Capabilities 2000
  - http://www.cyber-rights.org/interception/stoa/interception_capabilities_2000.htm

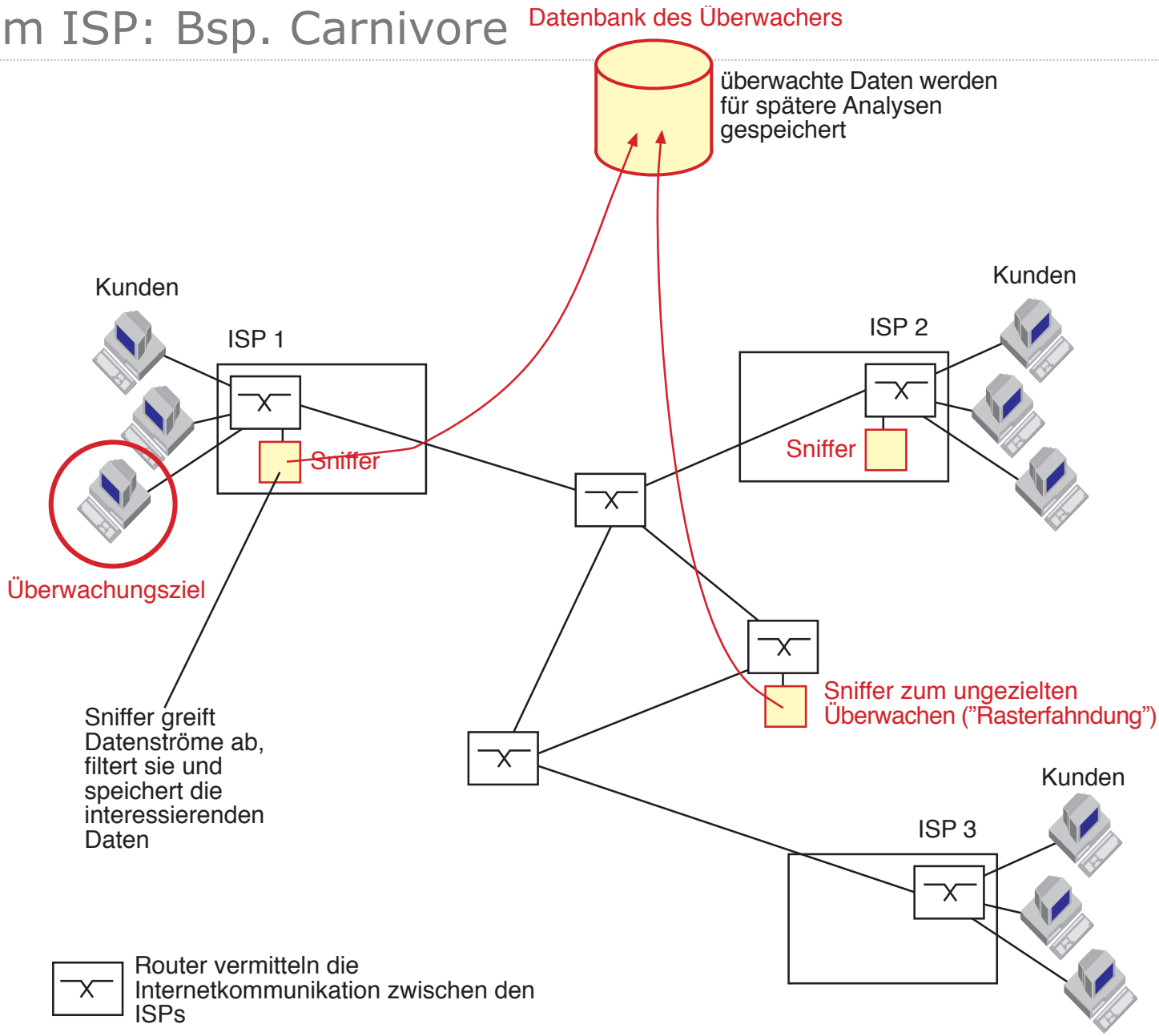
Funküberwachungsantenne (AN/FLR9) (aus Interception Capabilities 2000)

ECHELON

- Bad Aibling Interception facility of the ECHELON system

Source: http://ig.cs.tu-berlin.de/w2000/ir1/referate2/b-1a/

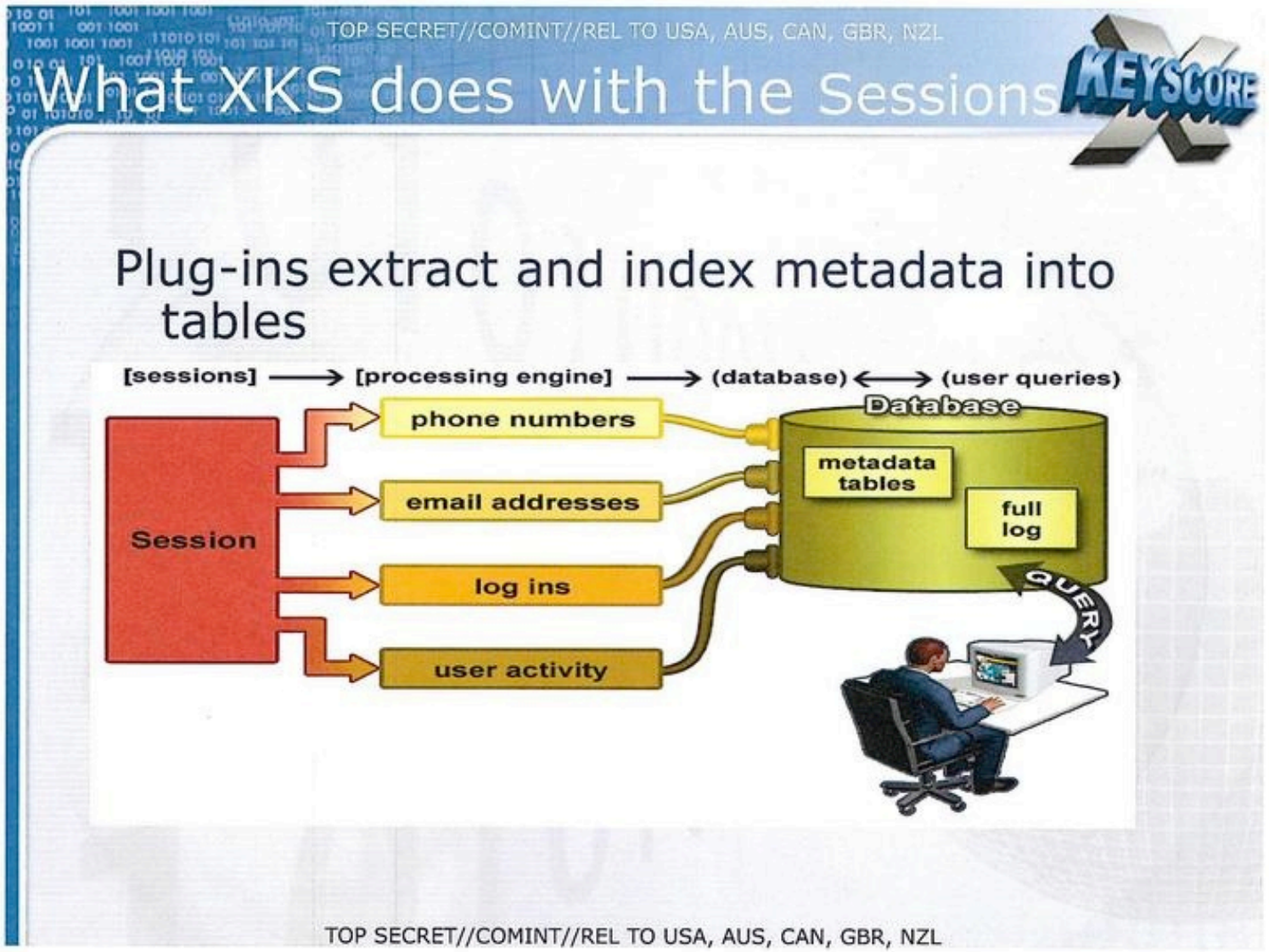
Sniffing beim ISP: Bsp. Carnivore



Sniffing beim ISP: Bsp. Carnivore

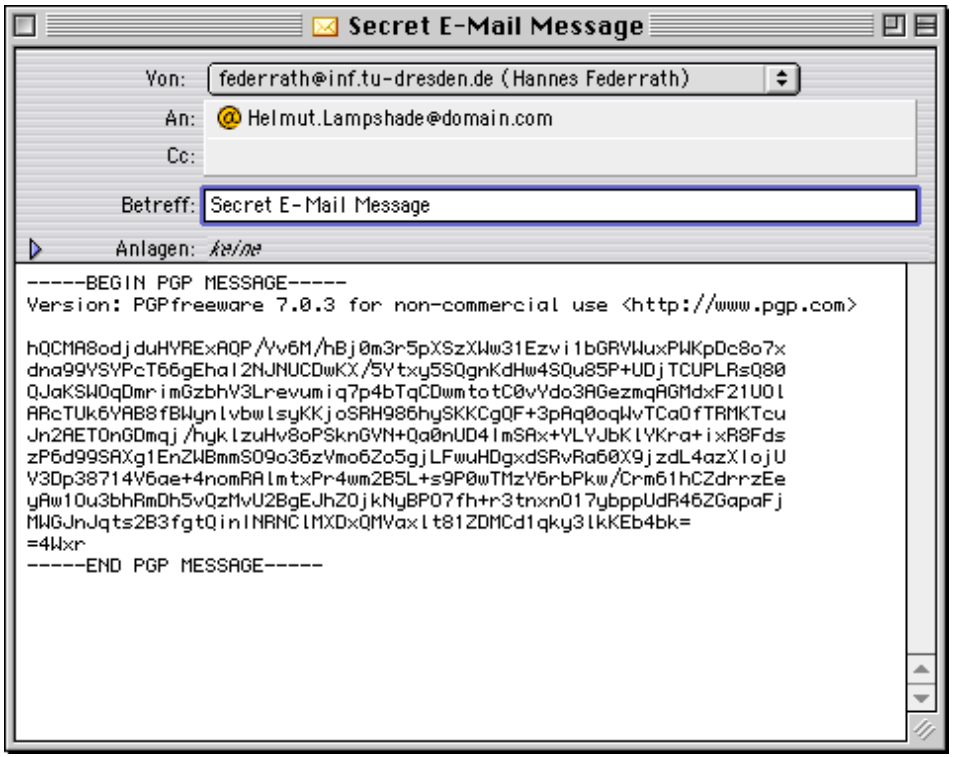
Datenbank des Überwachers

Quelle: Wikimedia



Hilft Verschlüsselung?

- Verschlüsseln hilft gegen Ausspähen der *Inhalte*



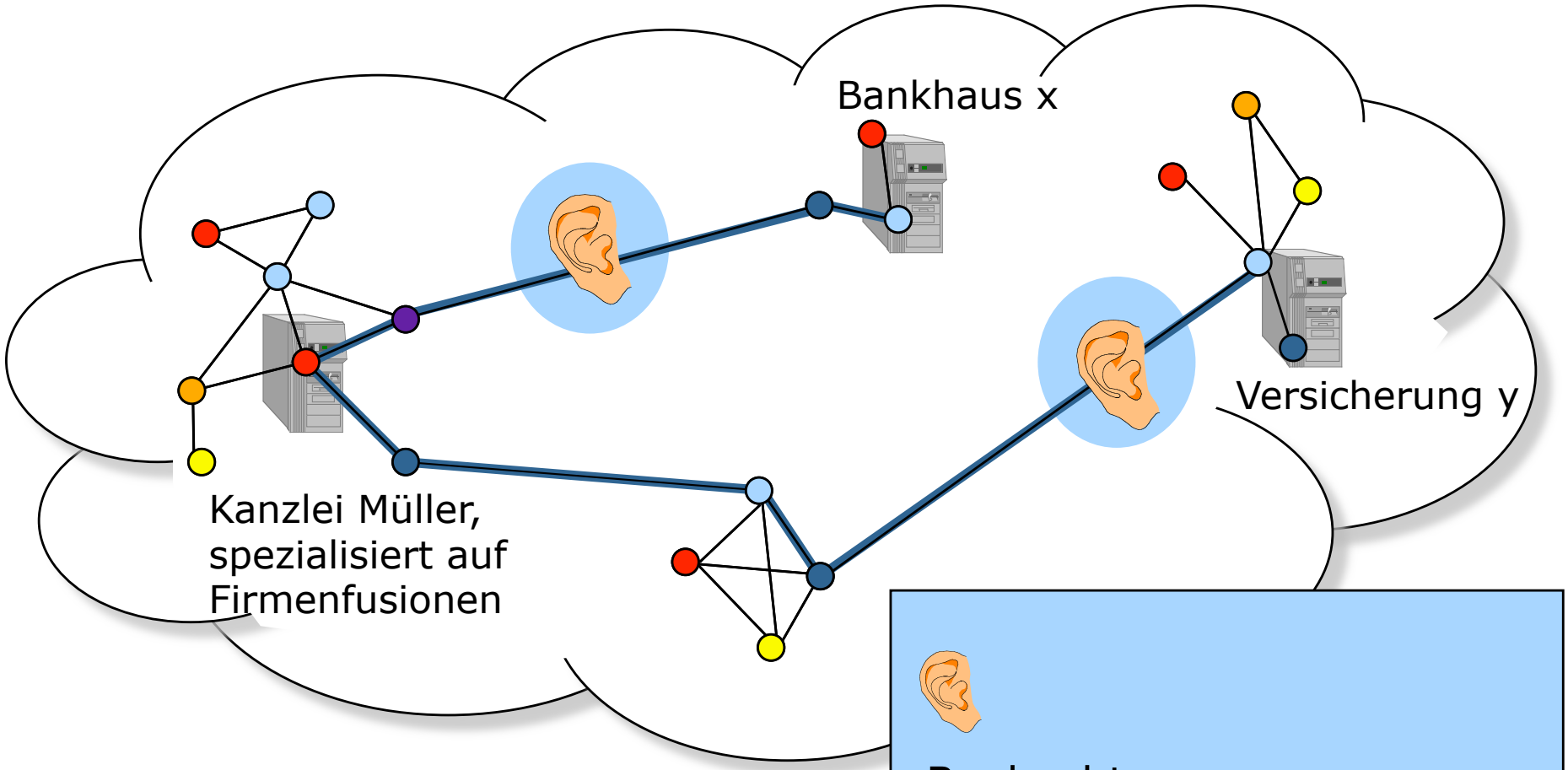
Trotzdem PGP verwenden!

Pretty Good Privacy

http://www.pgp.com

Verschlüsseln hilft überhaupt nichts gegen Beobachtung von Kommunikationsbeziehungen

Warum genügt Verschlüsselung nicht?



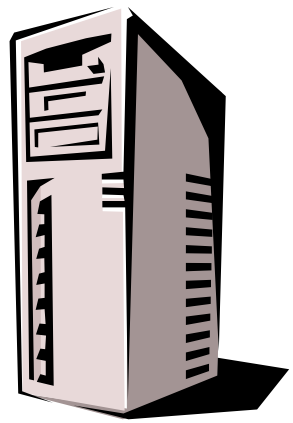
IP-Adressen zur Überwachung

- Statische IP-Adressen
  - stellen ein Personenpseudonym dar
  - sehr leichte Verkettbarkeit der Benutzeraktionen

Adresse:
123.45.6.7
(federrath-pc.uni-hamburg.de)

GET www.buchshop.example.com
To: 98.76.5.4
From: 123.45.6.7

HTTP ...
To: 123.45.6.7
From: 98.76.5.4

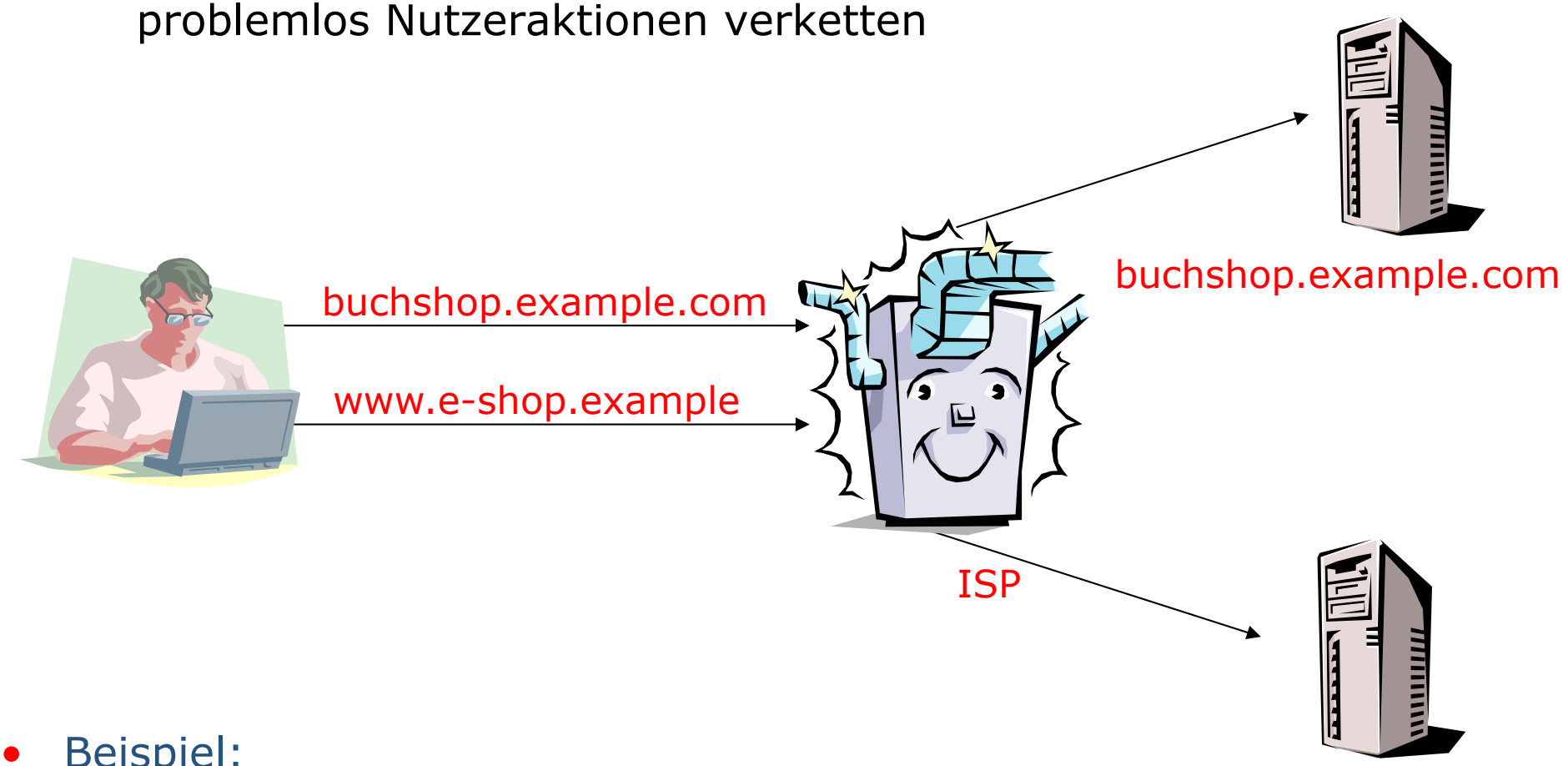


Adresse:
98.76.5.4

  - fahrlässig:
    - DNS-Name mit Personenbezug
- Einschränkung:
  - Zuweisung dynamischer IP-Nummern bei Einwahlzugang

IP-Adressen zur Überwachung

- Überwachung durch Internet Service Provider (ISP)
  - selbst bei dynamischer Adressenvergabe kann eigener ISP problemlos Nutzeraktionen verketten



- Beispiel:
  - http://www.predictivenetworks.com/

Cookies

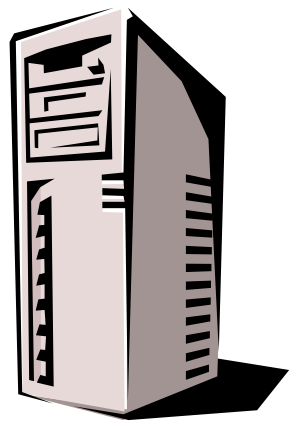
Cookies können zur Überwachung eingesetzt werden

- Funktionsweise von Cookies

Erster Besuch:

1. GET www.buchshop.example.com →

← 2. Set Cookie: id=12241235564



3. ggf. Warnung

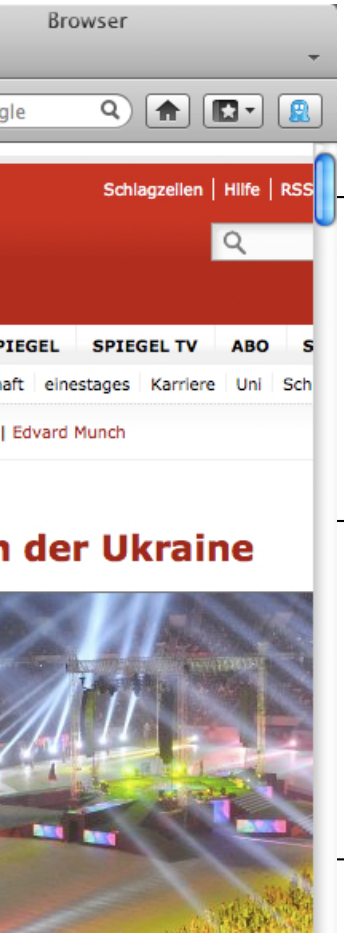
4. Speichern auf Festplatte

Folgende Besuche:

GET www.buchshop.example.com
Cookie: id=12241235564 →

  - wird nur an zugehörigen Server zurückgesendet
  - hat ein vom Server definiertes Verfallsdatum
  - wird auch bei Abruf eingebetteter Objekte gesendet (z.B. Bilder)

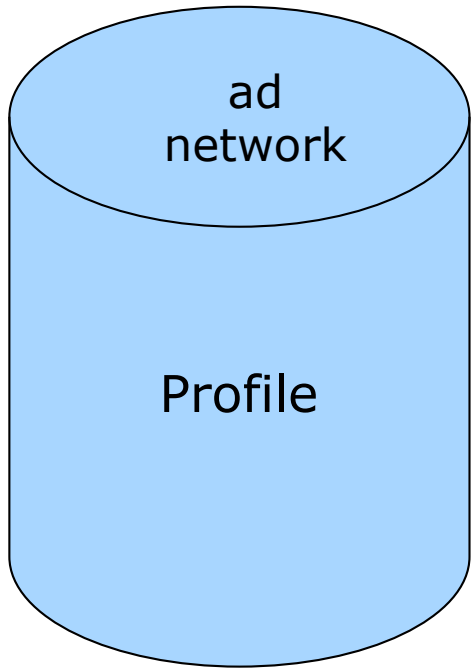
Third-Party Cookies



GET http://adnet.example.net/banner1.gif
Cookie: guid=8867563
Referer: http://www.bookshop.example

GET http://adnet.example.net/banner2.gif
Cookie: guid=8867563
Referer: http://www.healthinfo.example

GET http://adnet.example.net/banner3.gif
Cookie: guid=8867563
Referer: http://www.lifeinsurance.example



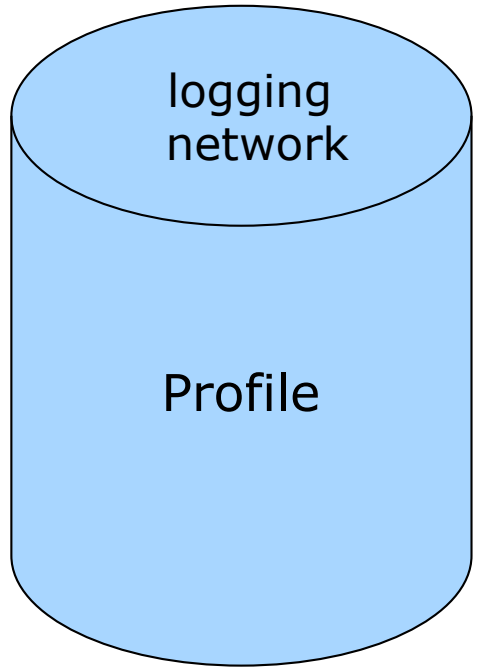
Schutz: Cookies beim Schließen des Browsers löschen

Mobile logging networks

App 1: SN-Device, start, stop, …
82031M6UV2F, 2012-12-19T16:39:57,
2012-12-19T16:45:33

App 2: SN-Device, start, stop, address book, …
82031M6UV2F, 2012-12-20T12:19:11,
2012-12-20T12:25:01, data

App 3: SN-Device, start, stop, location info, …
82031M6UV2F, 2012-12-20T12:21:23,
2012-12-20T12:21:55, data



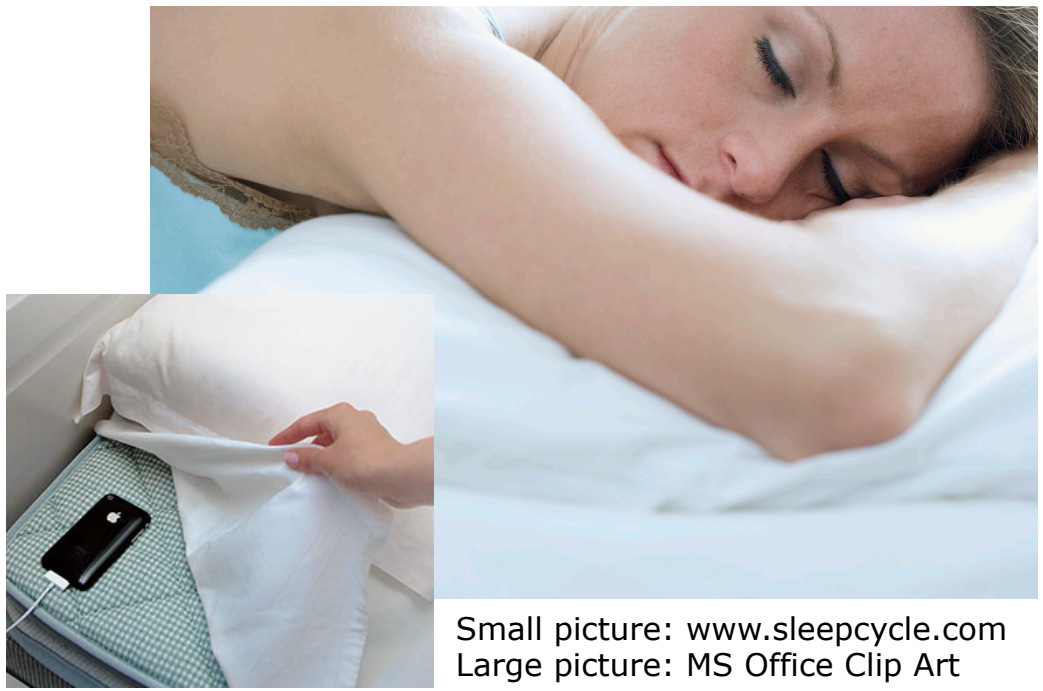
Schutzmöglichkeiten?

Appification

- Für jeden Zweck eine eigene App
  - Taxi
  - Weather
  - Wikipedia
  - Shopping list
  - Writing app
  - Notebook
  - Doc scanning
  - Sleep rhythm
  - Running app

    …

  - Video apps (product advertisement)
  - Torch apps



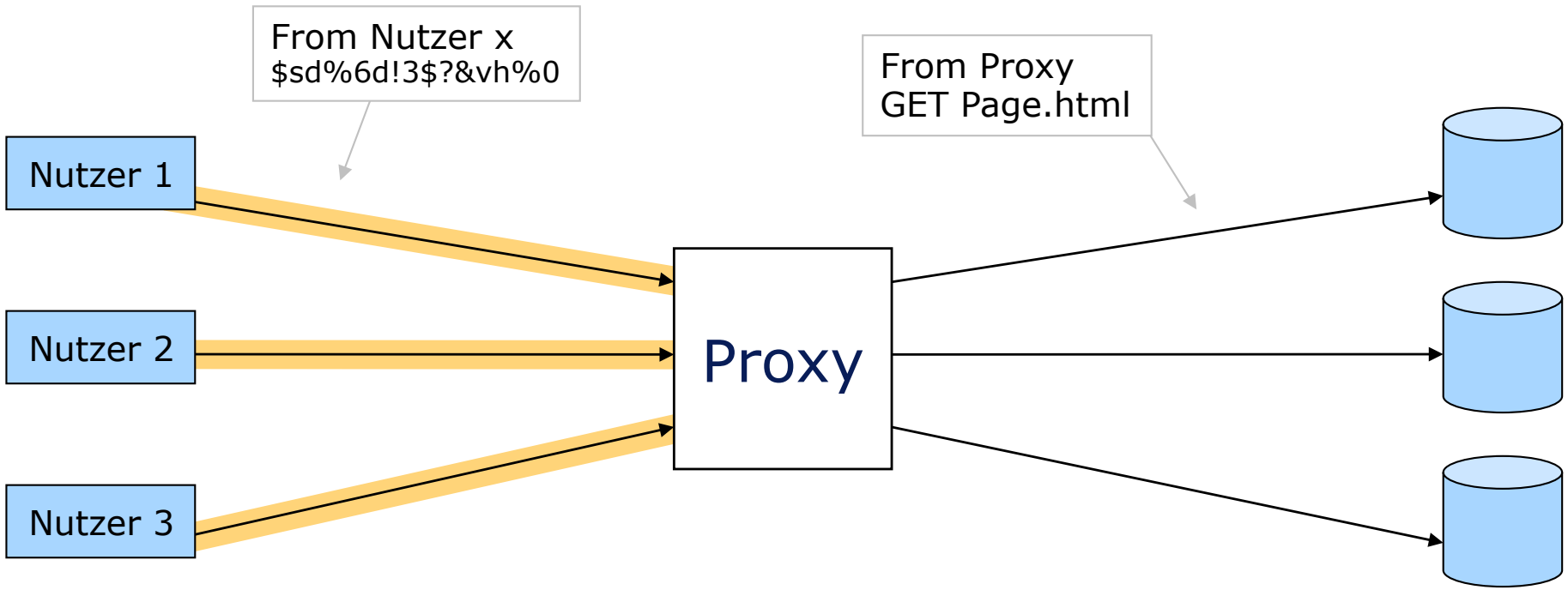
Small picture: www.sleepcycle.com
Large picture: MS Office Clip Art

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)

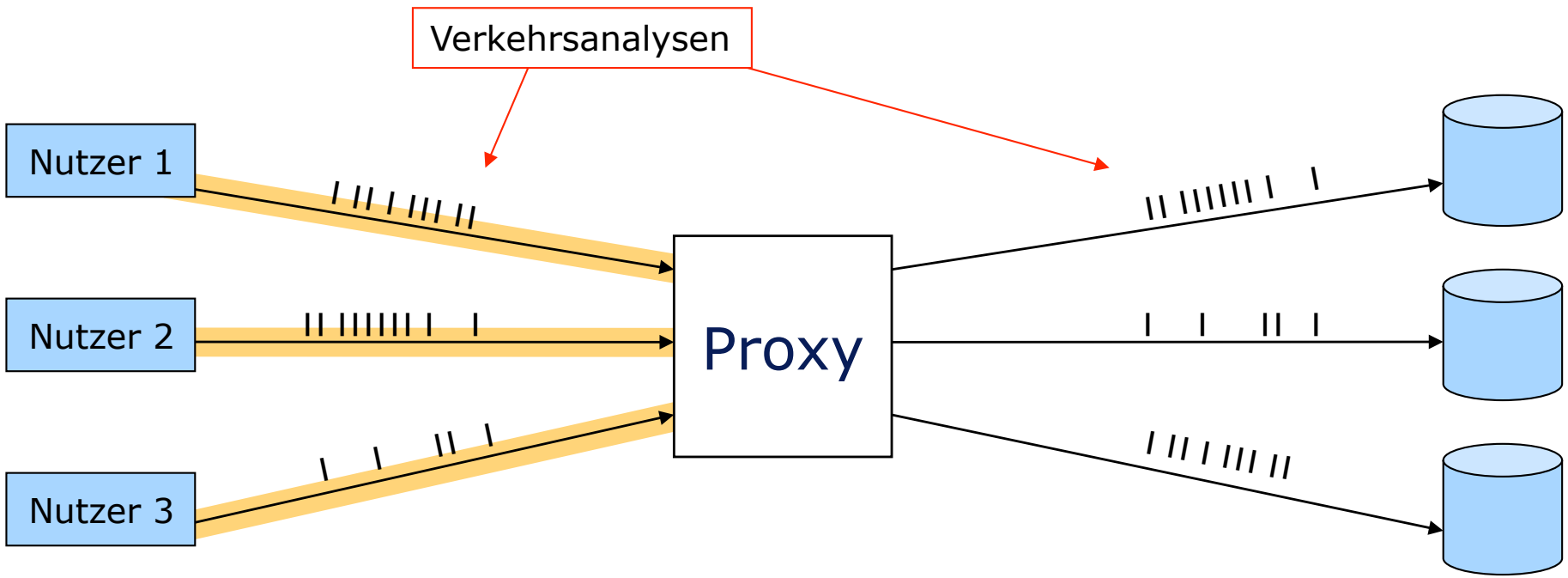
Proxies: Outsider

- 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

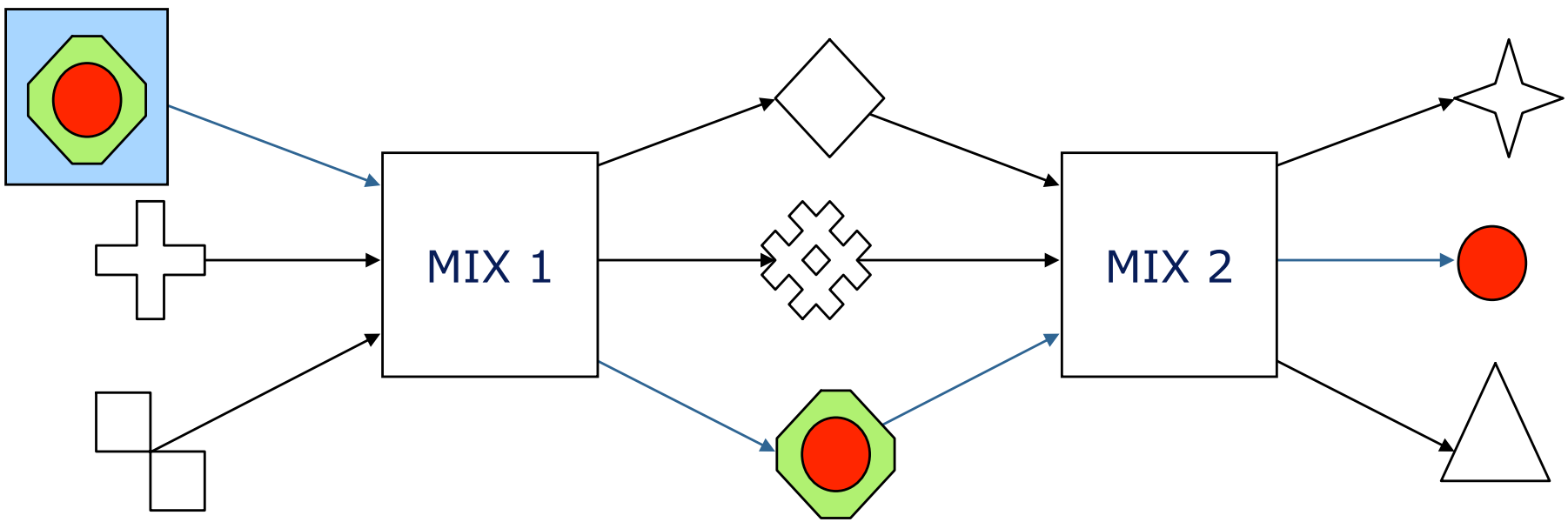


Beispiele für Bausteine datenschutzfördernder Technik

- 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)

- Auch die Betreiber der Mixe erfahren nichts mehr über die Kommunikationsbeziehung zwischen Sender und Empfänger.

- Randbedingungen
  - Alle Nachrichten haben die gleiche Länge.
  - Mehr als einen Mix verwenden.
  - Wenigstens ein Mix darf nicht angreifen.

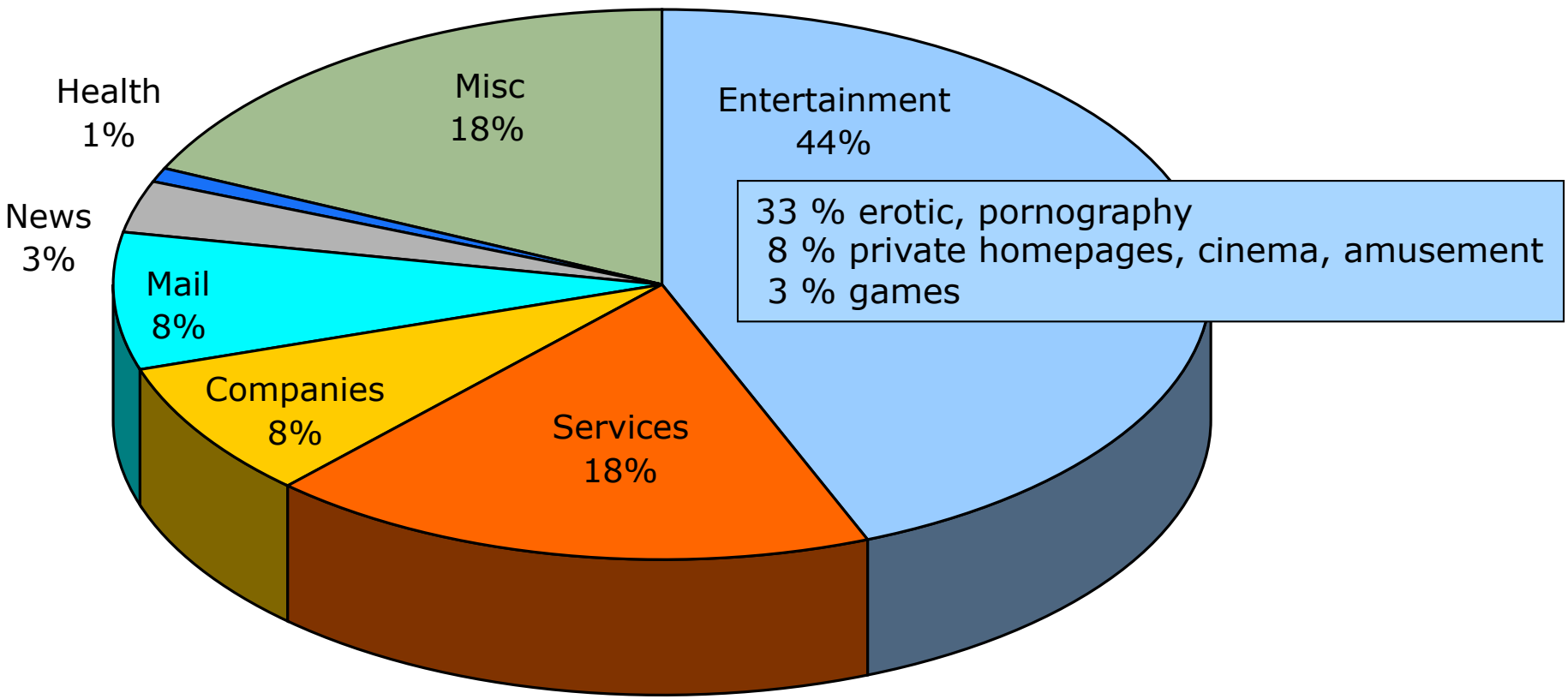


Tor und JonDonym: Anonymes Sufen

- Schutz auch vor dem Betreiber des Anonymisierungsdienstes
  - https://www.torproject.org
  - http://www.anon-online.de
- Besonders einfache Verwendung beim anonymen Websurfen mit den integrierten Browsern
  - Tor Browser Bundle
  - JondoFox

Anonymisierte Inhalte

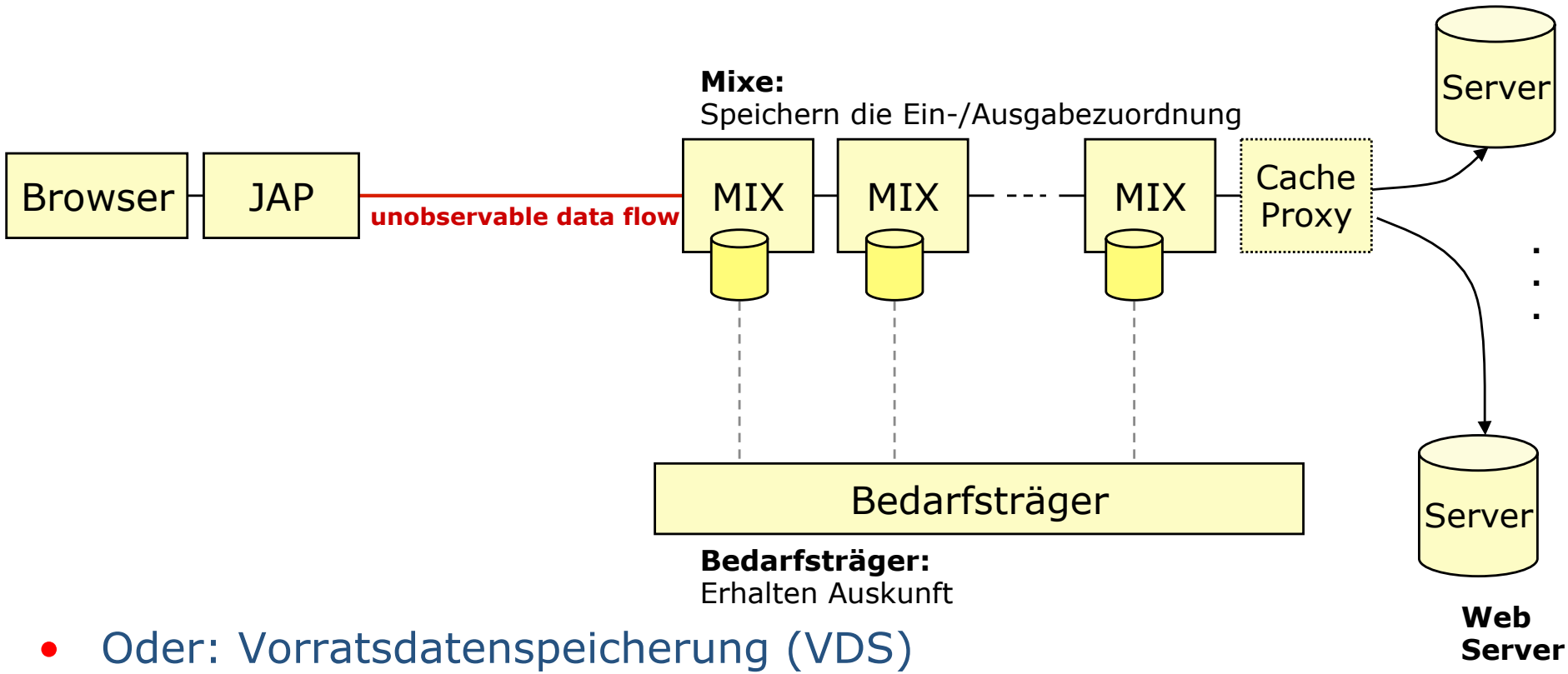
- Zuordnung von 150 zufällig ausgewählten Requests aus mehreren Millionen Zugriffen im Juni 2005



Strafverfolgung bei schweren Straftaten

- Entweder: Anordnung nach § 100a,b StPO

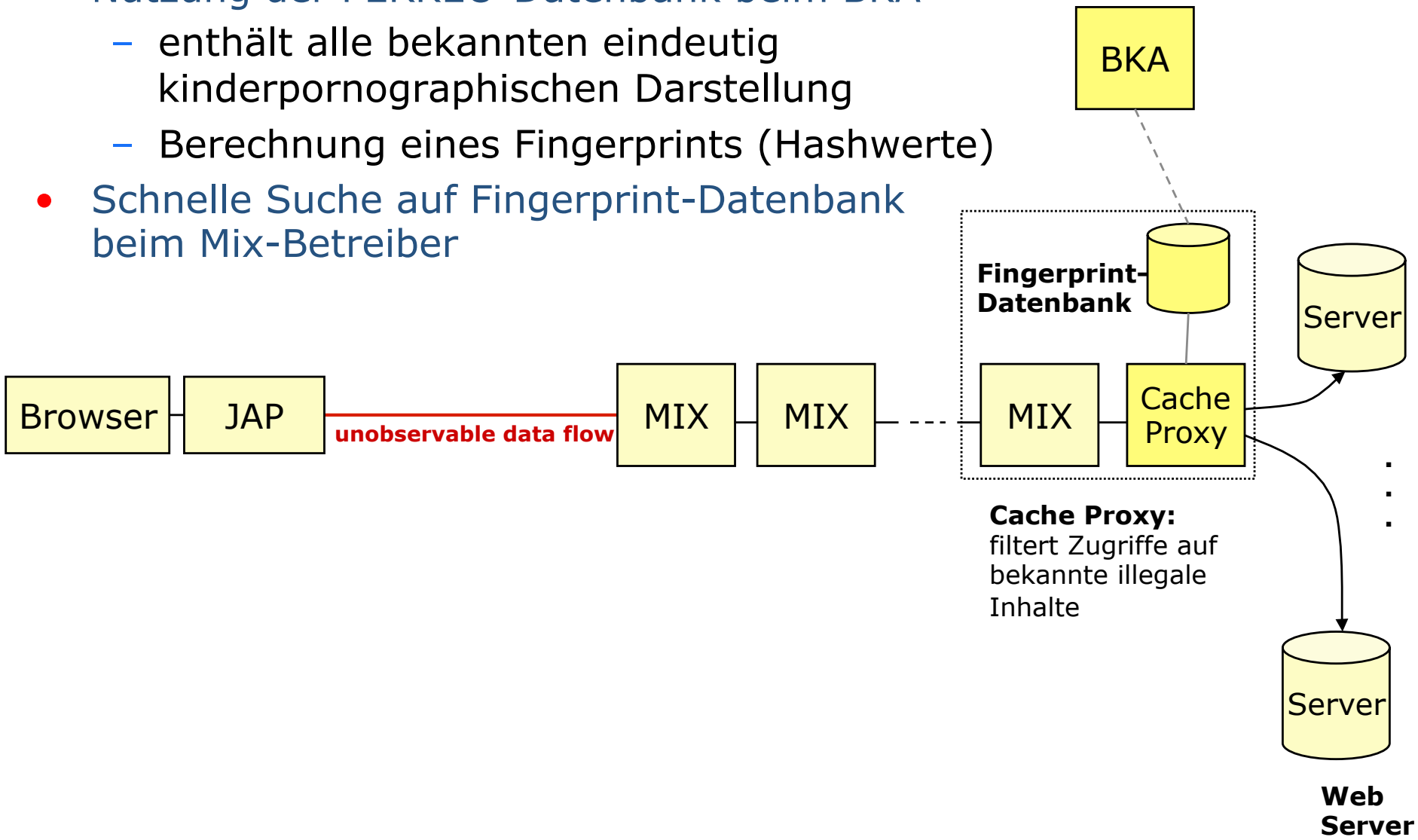
```
CAMsg::printMsg(LOG_INFO,"Loading Crime Detection Data....\n");
CAMsg::printMsg(LOG_CRIT,"Crime detected - ID: %u – Content: \n%s
    \n",id,crimeBuff,payLen);
```



- Oder: Vorratsdatenspeicherung (VDS)

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



Universität Hamburg
Fachbereich Informatik
Arbeitsbereich SVS
Prof. Dr. Hannes Federrath
Vogt-Kölln-Straße 30
D-22527 Hamburg

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

Telefon +49 40 42883 2358

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

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG