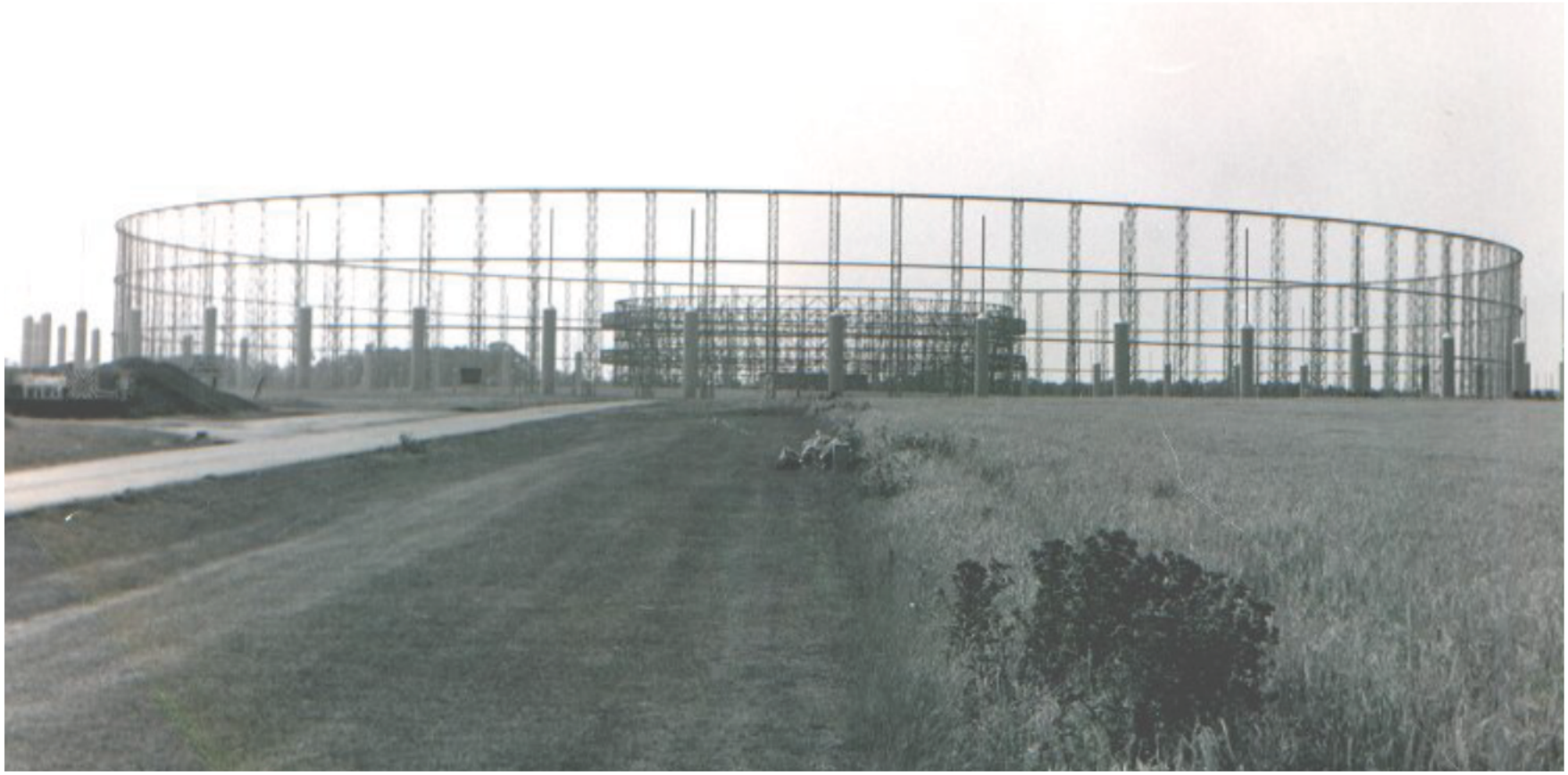
Das passiert beim anonymen Surfen unter der Haube

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

Hamburg, 11. September 2013

Anonymität im Internet ist eine Illusion

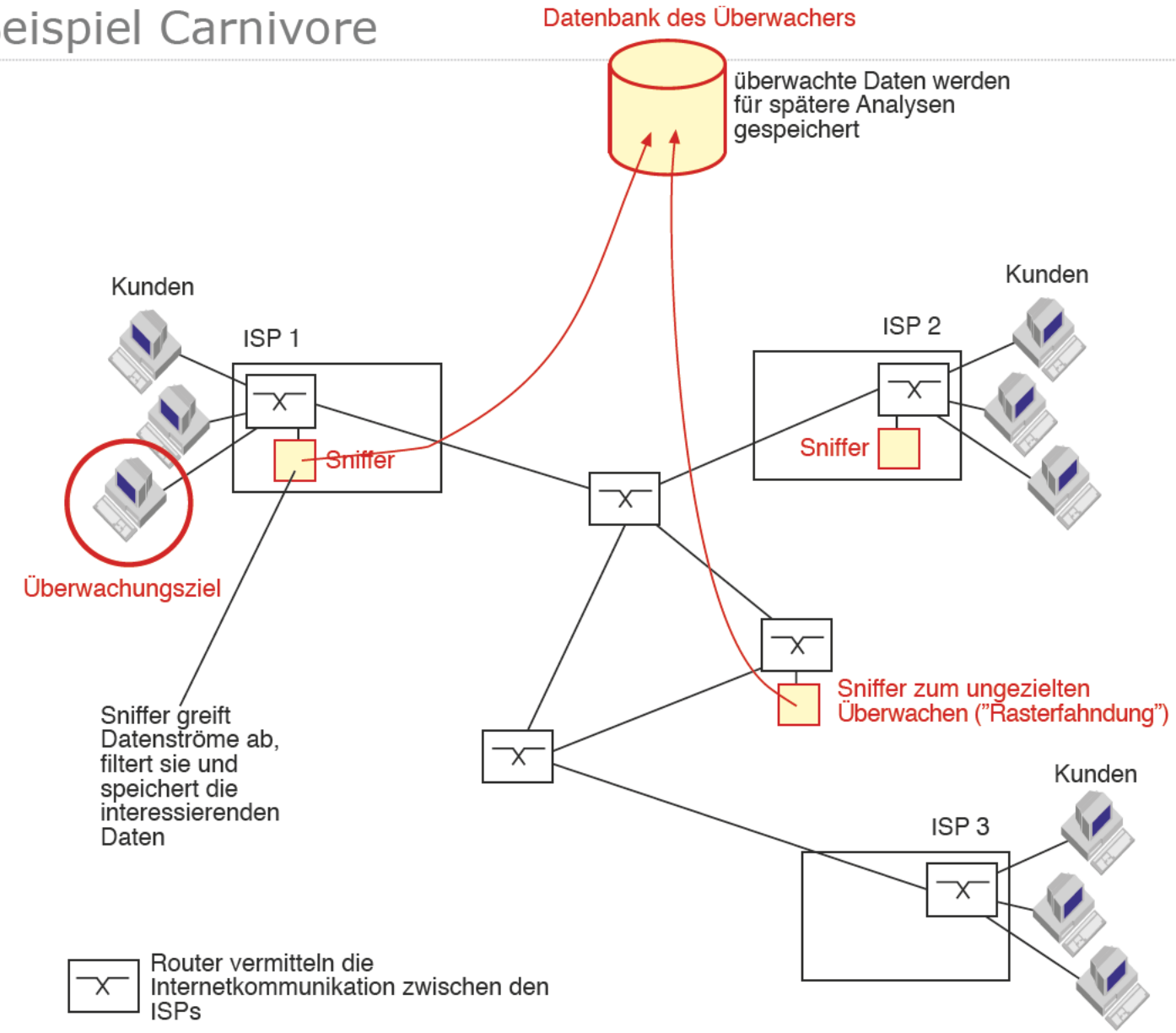
- Funküberwachungsantenne (AN/FLR9)
  - Quelle: Interception Capabilities 2000



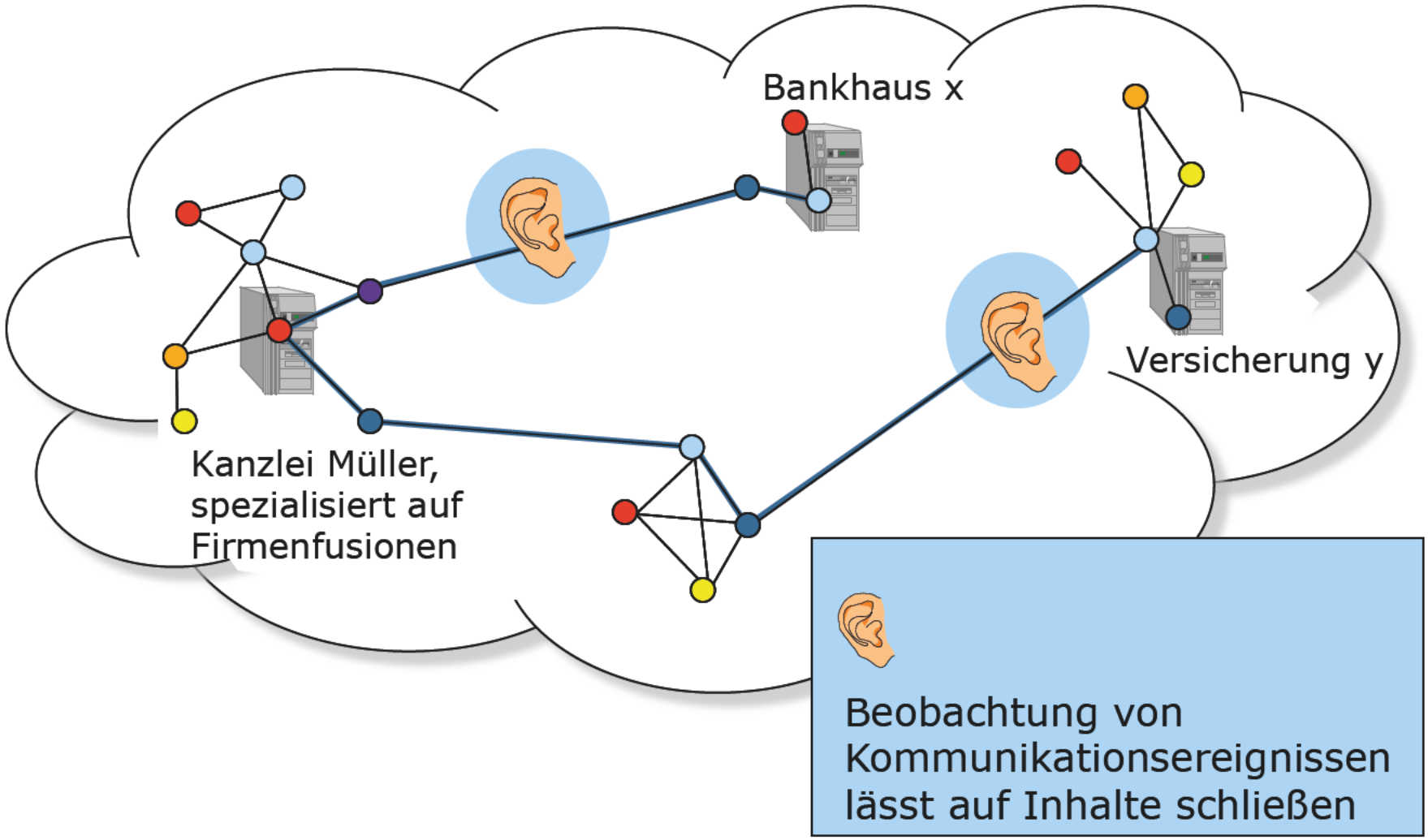
Anonymität im Internet ist eine Illusion

- Bad Aibling Interception facility of the ECHELON system
  - Quelle: http://ig.cs.tu-berlin.de/w2000/ir1/referate2/b-1a/

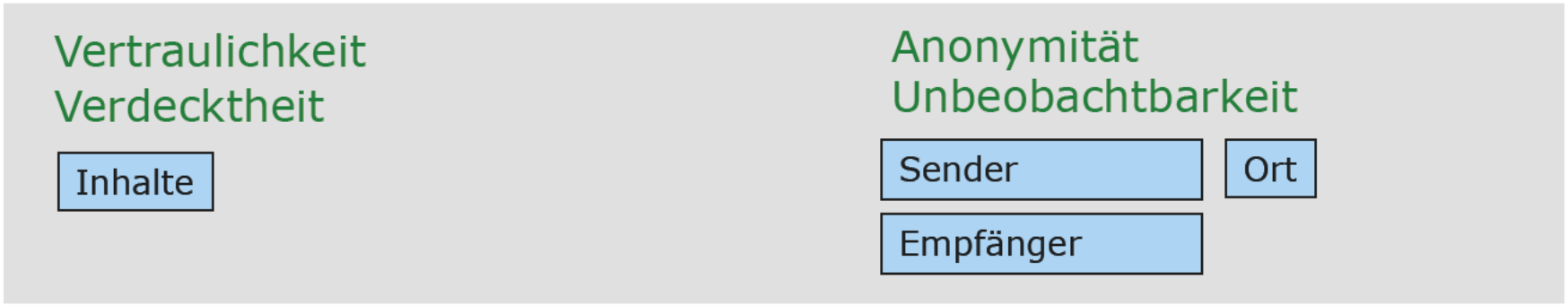
Sniffing: Beispiel Carnivore



Warum genügt Verschlüsselung nicht?



Vertraulichkeit: Schutzziele und Angreifermodell



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

Vertraulichkeit: Verfahren und Algorithmen

Verfahren

Algorithmen

Inhaltsdaten

Vertraulichkeit

Verschlüsselung

Inhalte

DES, 3-DES, OTP, IDEA, AES, RSA, ElGamal, …

Verdecktheit

Steganographie

Inhalte + Existenz

F5, …

Verkehrsdaten

Anonymität Unbeobachtbarkeit

Sender

Ort

Empfänger

Web-Anonymisierer, Remailer, anonyme Zahlungssysteme

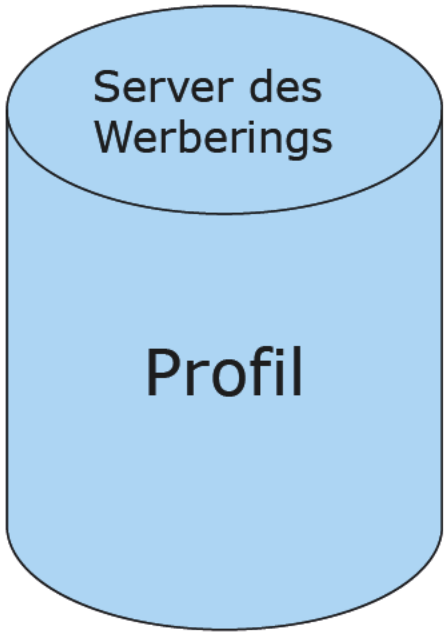
Pseudonyme, Proxies, umkodierende Mixe, DC Netz, Private Information Retrieval, …

Third-Party Cookies

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

GET http://werbering.example.net/banner2.gif
Cookie: guid=8867563
Referer: http://www.gesundheitsberatung.example

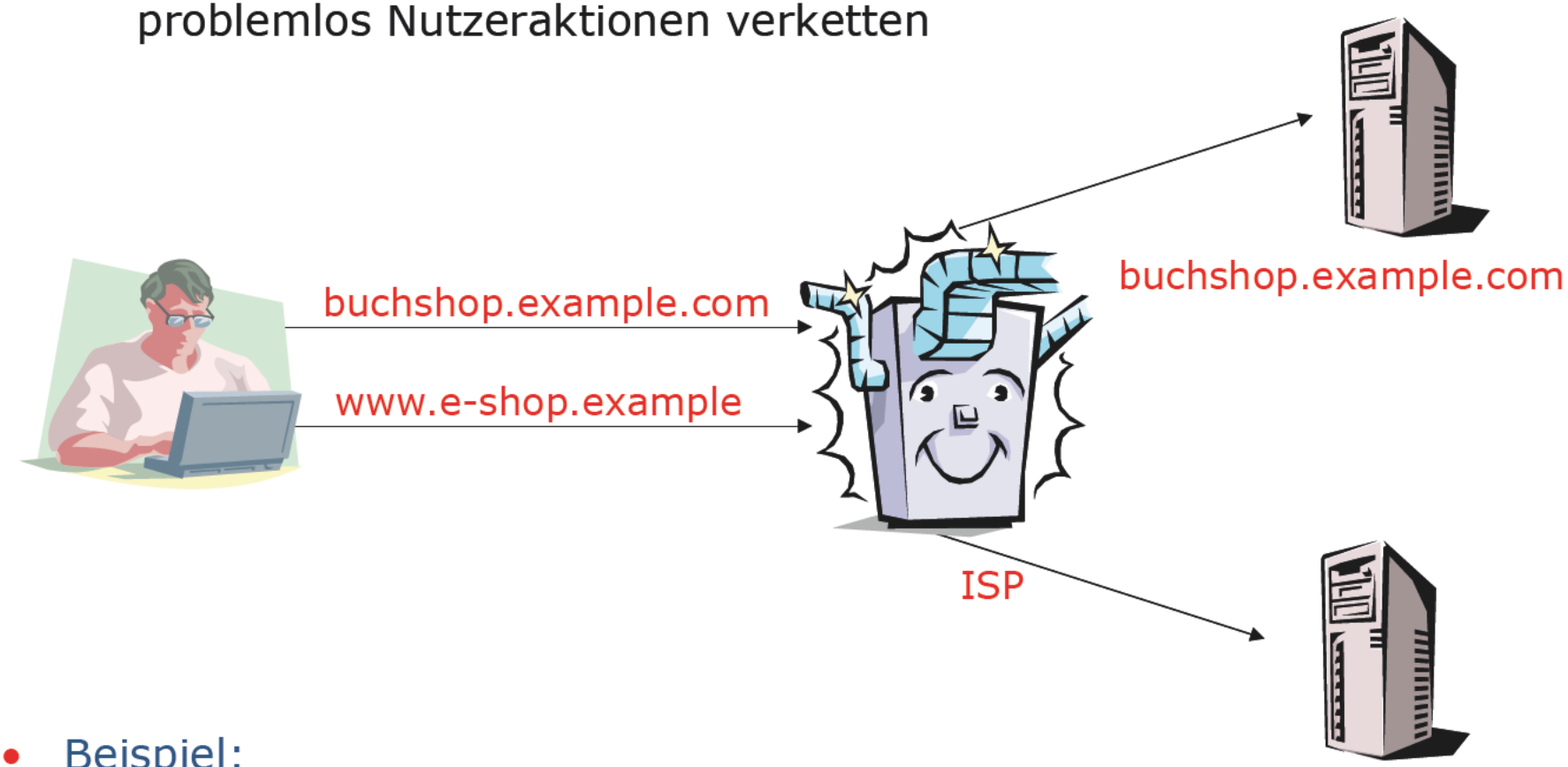
GET http://werbering.example.net/banner3.gif
Cookie: guid=8867563
Referer: http://www.lebensversicherung.example



Gläserner Bürger? Legal?

IP-Adressen zur Überwachung

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

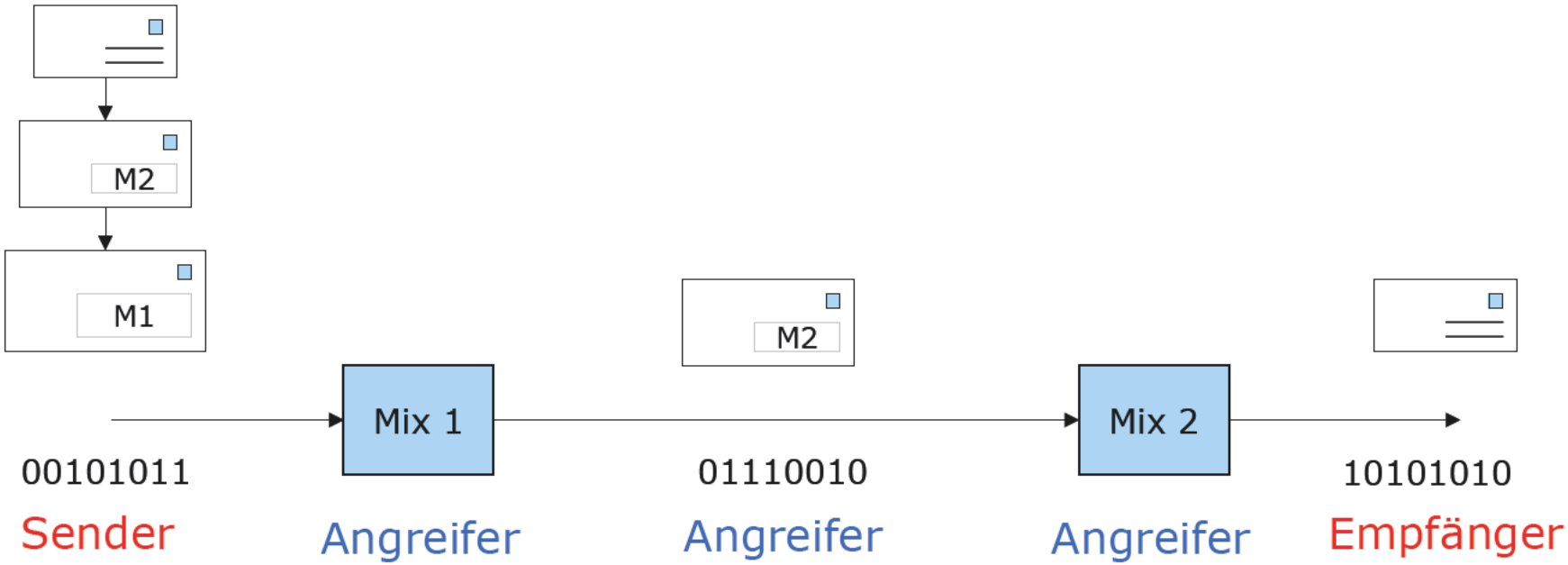


- Beispiel:
  - http://www.predictivenetworks.com/

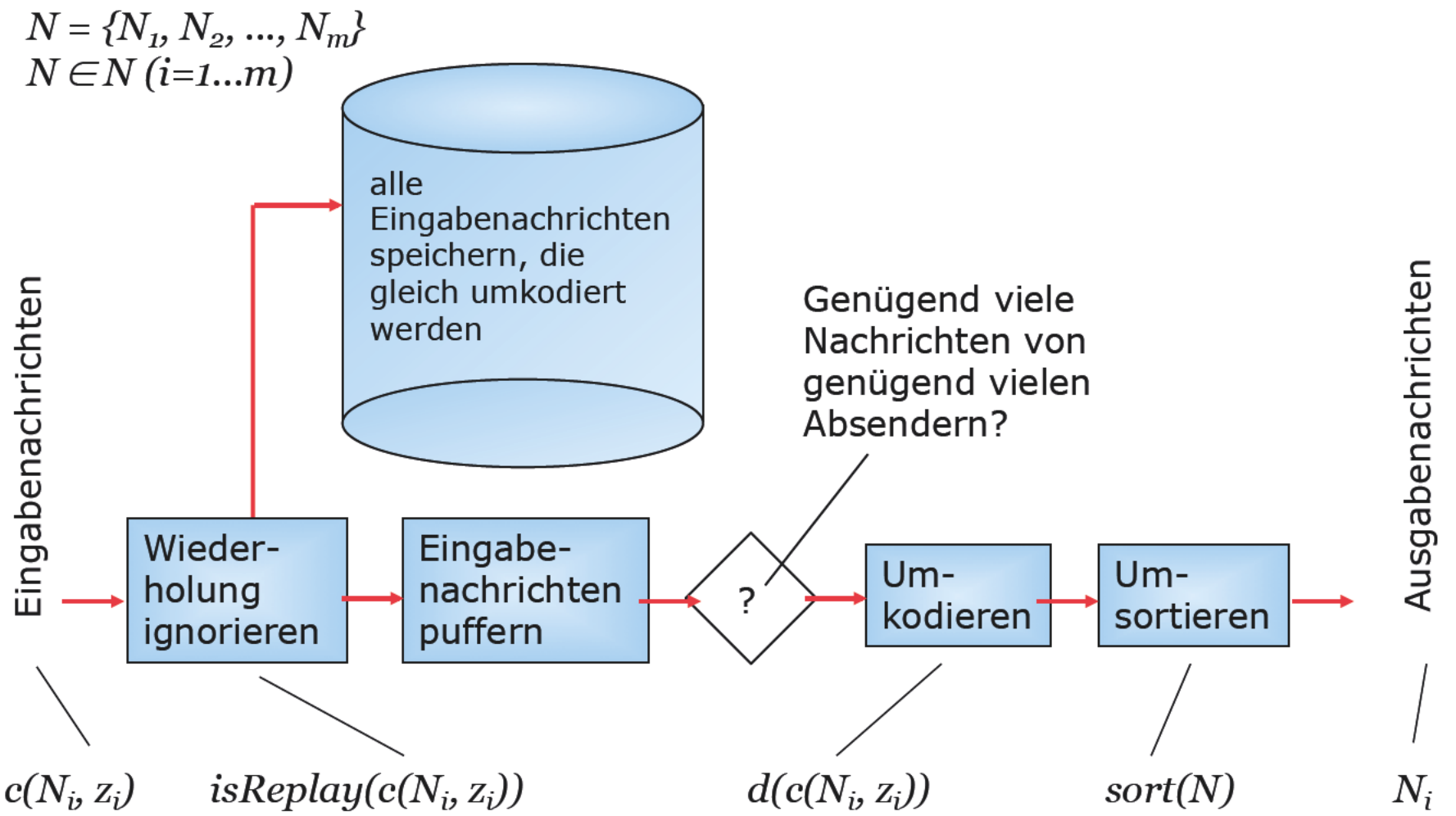
Umkodierende Mixe

Chaum, 1981

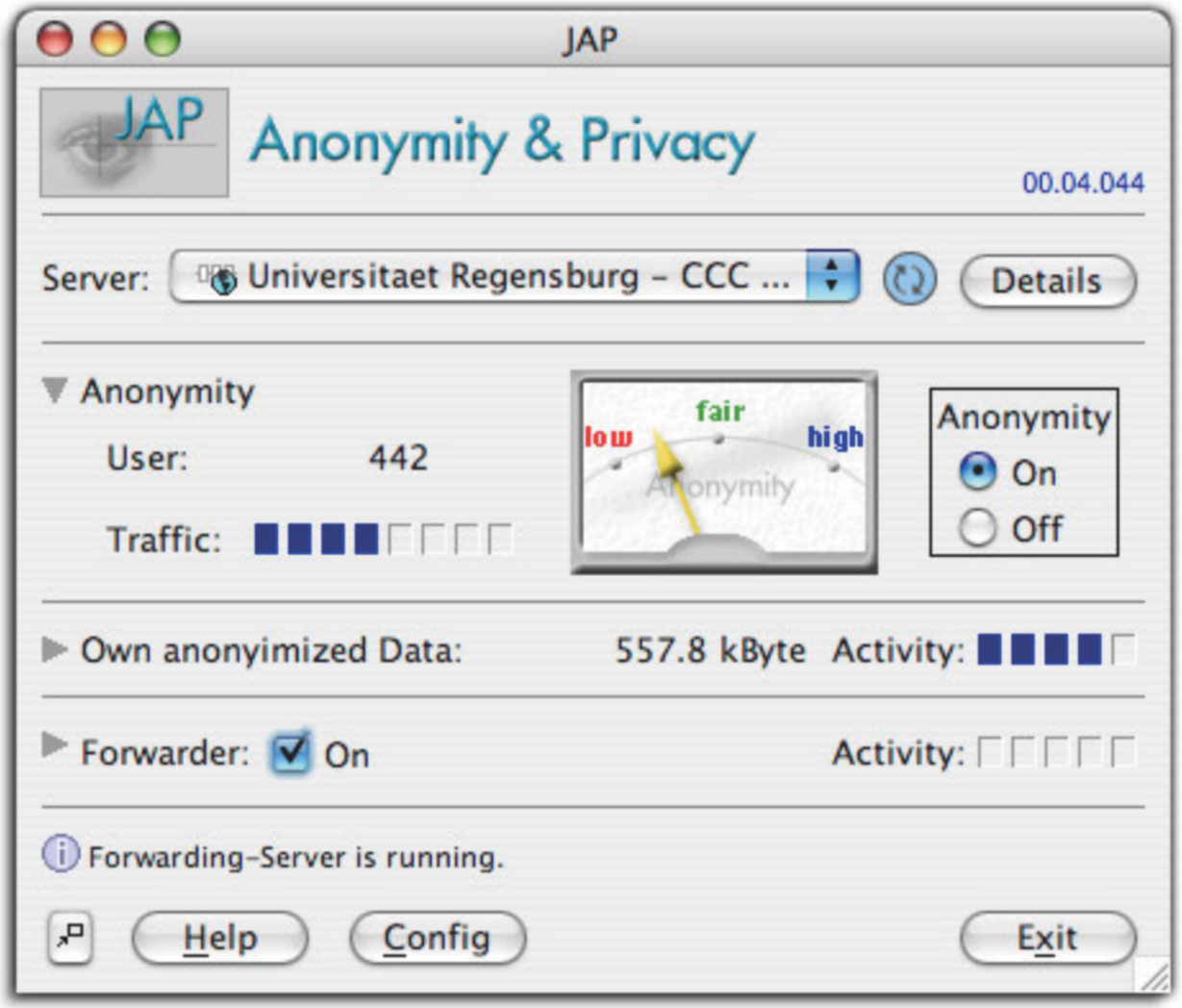
- Grundidee:
  - Nachrichten in einem »Schub« sammeln, Wiederholungen ignorieren, umkodieren, umsortieren, gemeinsam ausgeben.
- Randbedingungen
  - Alle Nachrichten haben die gleiche Länge.
  - Mehr als einen Mix verwenden.
  - Wenigstens ein Mix darf nicht angreifen.



Blockschaltbild eines Mix



AN.ON/JAP/Jondos



Ziele:

Schaffen einer praktikablen Lösung für anonyme und unbeobachtbare Basiskommunikation

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

OpenSource

www.anon-online.de

TOR

Ziele:

Freier Informationszugang, voll dezentrale Strukturen

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

OpenSource

www.torproject.org

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