> Anonymität im Internet — möglich und zumutbar!

http://www.anon-online.de/

Hannes Federrath

Freie Universität Berlin

Marit Hansen

Unabhängiges Landeszentrum für Datenschutz

> Anonymität im Internet ist eine Illusion

- Wer ist der Gegner?
  - Konkurrenz
  - Geheimdienste fremder Länder
  - Big Brother
  - Systemadministrator
  - Nachbar ...

Funküberwachungsantenne (AN/FLR9)

>> Anonymität im Internet ist eine Illusion

- Wer ist der Gegner?
  - Konkurrenz
  - Geheimdienste fremder Länder
  - Big Brother
  - Sys-admin
  - Nachbar ...

Bad Aibling Interception facility of the ECHELON system

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

>>> Anonymität im Internet ist eine Illusion

Electronic Mail: Log-Dateien zeigen Kommunikationsbeziehungen

```
>tail syslog
Oct 15 16:32:06 from=<feder@tcs.inf.tu-dresden.de>, size=1150
Oct 15 16:32:06 to=<hf2@irz.inf.tu-dresden.de>
```

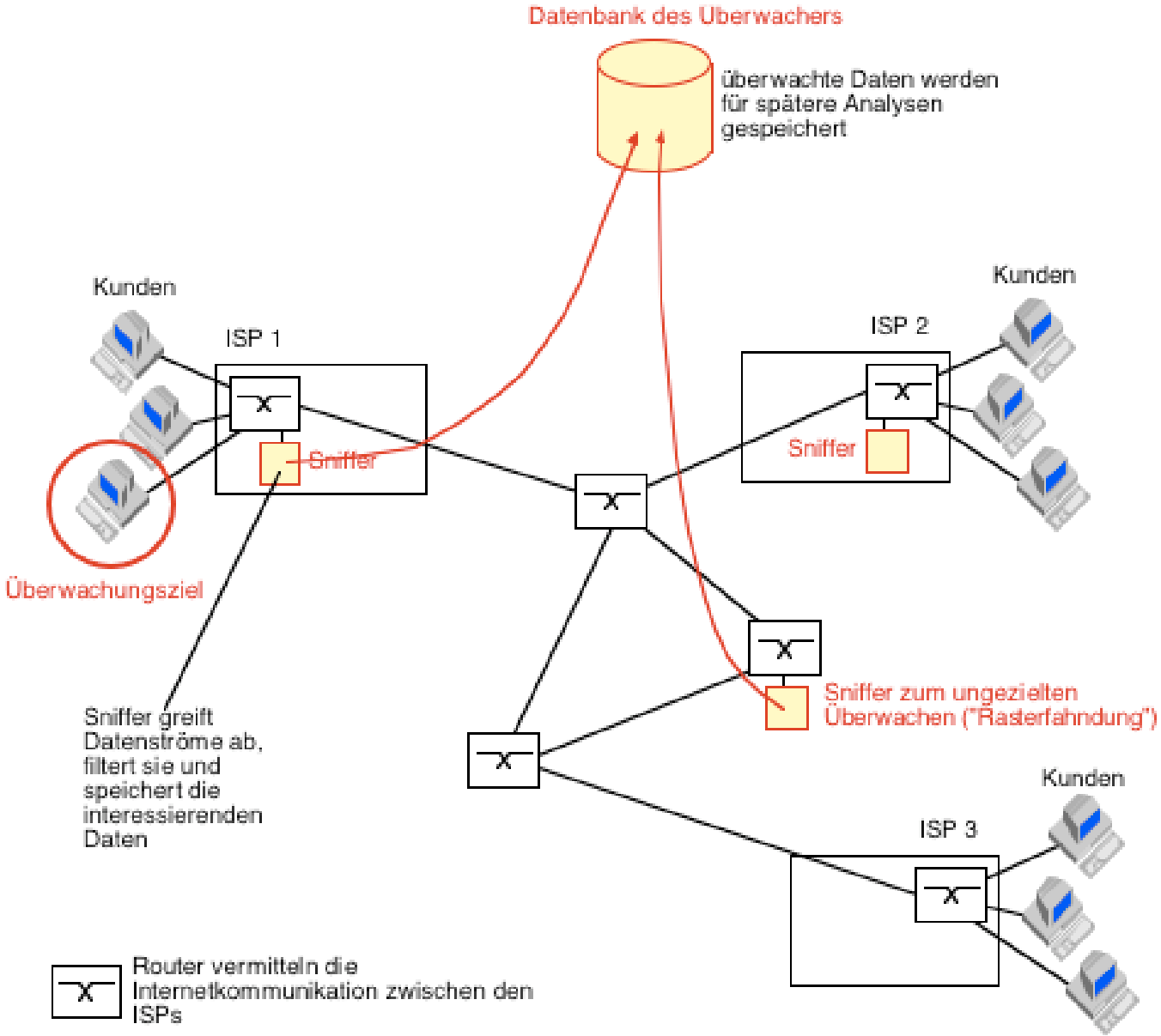
World Wide Web: Log-Dateien zeigen Interessensdaten

```
wwwtcs.inf.tu-dresden.de>tail access_log
amadeus.inf.tu-dresden.de - - [15/Oct/1997:11:50:01] "GET
/lvbeschr/winter/TechnDS.html HTTP/1.0" - "http://wwwtcs.inf.tu-
dresden.de/IKT/" "Mozilla/3.01 (X11; I; SunOS 5.5.1 sun4u)"
```

Finger: Die Ermittlung eines Rechnerbenutzers ist kein Problem

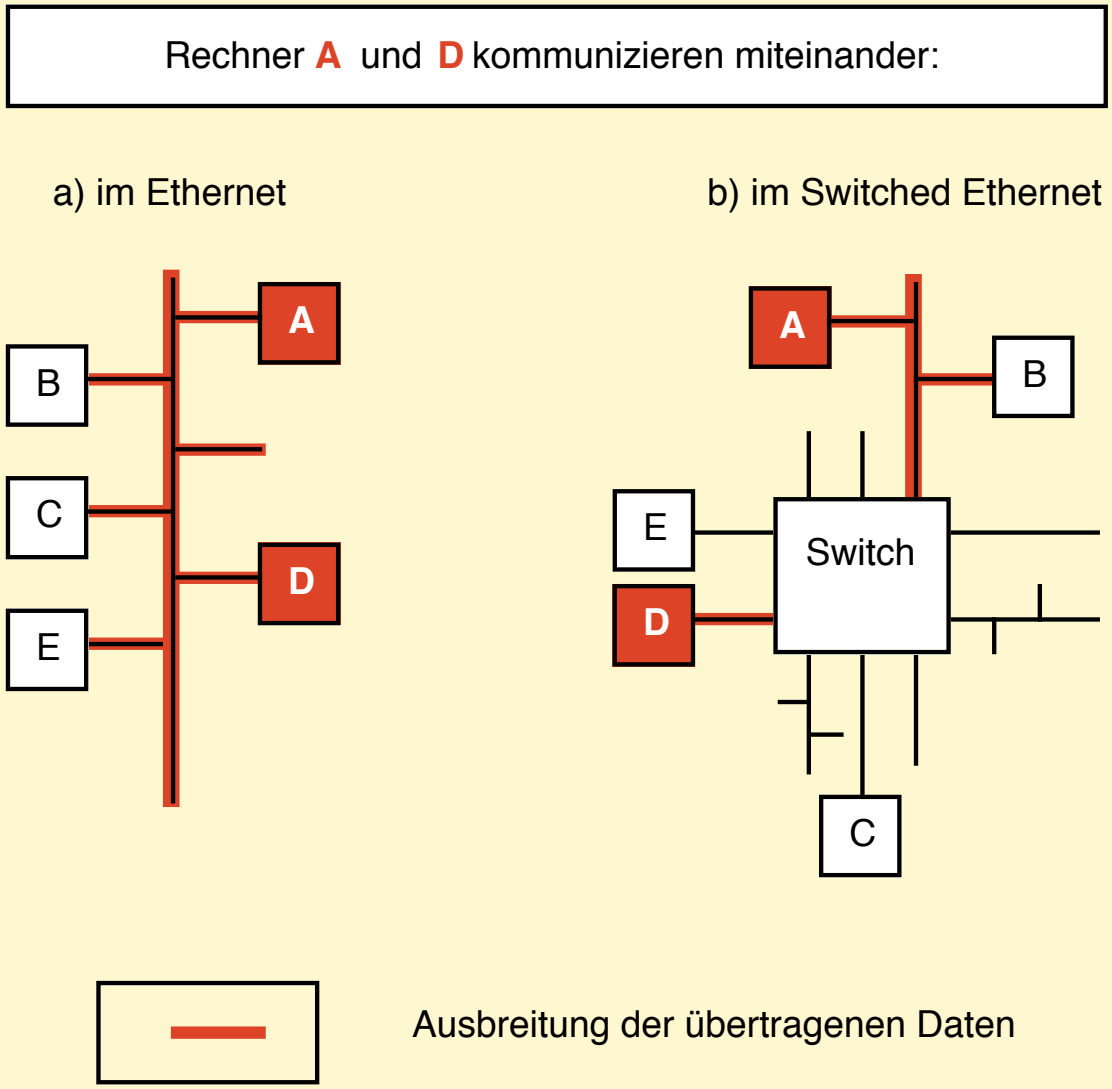
```
ithif19 logs 17 >finger @amadeus.inf.tu-dresden.de
[amadeus.inf.tu-dresden.de]
Login       Name                TTY         Idle    When
feder    Hannes Federrath       console             Wed 11:56
```

> Sniffing-Angriffe: Funktionsweise (ISP)



>> Sniffing-Angriffe: Funktionsweise (Ethernet)

- alle Stationen erhalten alle Datenpakete (im Ethernet)
- lokale Filterfunktion
- Abschalten des Filters möglich: **»promiscuous mode«**
- Sniffing im Switched Ethernet erschwert



>>> Sniffing-Angriffe: Vorgehen

- 1. Schritt – Beschaffung der Daten
  - Konfiguration der Netzwerkschnittstelle (promiscuous mode)
  - Auslesen sämtlicher Datenpakete
- 2. Schritt – Informationsgewinnung
  - Auswahl der »interessanten« Pakete anhand der Protokoll-Informationen (Sender- bzw. Empfängeradresse, TCP-Port etc.)
- 3. Schritt – Auswertung des Datenteils

/usr/bin/login (ttyp1)

```
11:47:15.106702 titanus.inf.fu-berlin.de.49615 > www.linux.org
11:47:15.171156 titanus.inf.fu-berlin.de.49619 > www.linux.org
11:47:15.220038 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.220170 titanus.inf.fu-berlin.de.49616 > www.linux.org
11:47:15.222498 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.222578 titanus.inf.fu-berlin.de.49617 > www.linux.org
11:47:15.233590 titanus.inf.fu-berlin.de.49608 > www.linux.org
11:47:15.237344 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.237472 titanus.inf.fu-berlin.de.49618 > www.linux.org
11:47:15.278850 titanus.inf.fu-berlin.de.49616 > www.linux.org
11:47:15.281037 titanus.inf.fu-berlin.de.49617 > www.linux.org
11:47:15.290554 titanus.inf.fu-berlin.de.49618 > www.linux.org
11:47:15.303033 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.303175 titanus.inf.fu-berlin.de.49619 > www.linux.org
11:47:15.417733 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.417745 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.426488 titanus.inf.fu-berlin.de.49619 > www.linux.org
11:47:15.430184 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.430194 www.linux.org.http > titanus.inf.fu-berlin.de.
11:47:15.431501 www.linux.org.http > titanus.inf.fu-berlin.de.
```

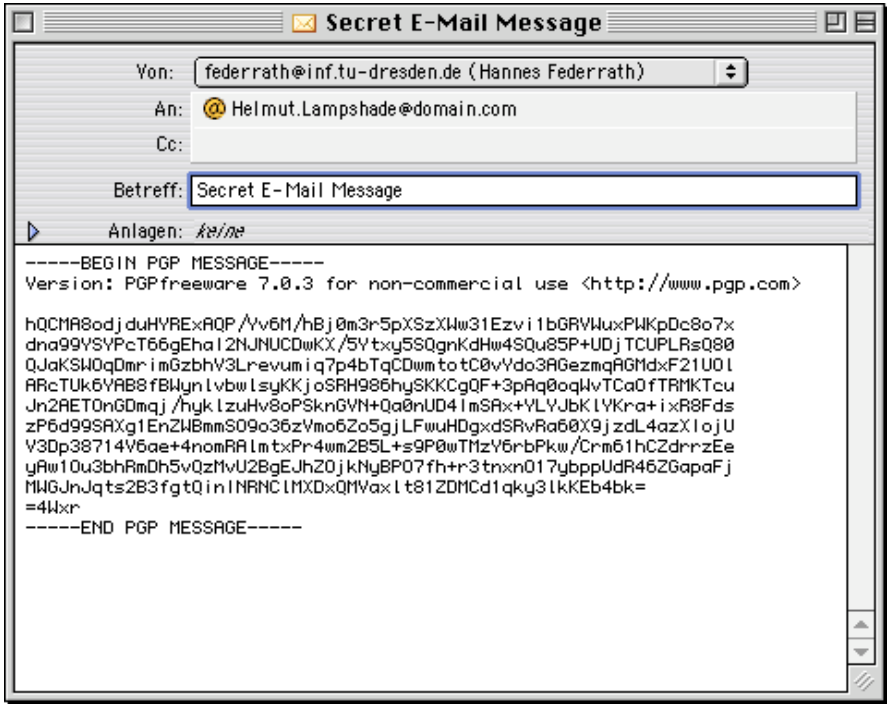
>>>> Sniffing-Angriffe: Vorgehen

- 3. Schritt – Auswertung des Datenteils
  - Im Beispiel ASCII-Textdarstellung eines Ethernet-Datenpaketes gewählt (Punkte stehen für Steuerzeichen)

```
....Ih..OyB..OyB...E...S'@......QP\.G<..C.H.M../(~.P....>..*... .....
..E.................w.R$.6..f%A....4.6.f%A.........................
............U..........MailSaveOptions...O.U..........SECUREMAIL..
U..............tmpReview...U..........Form MemoU............Type..
MemoU..............DeletionPeriod........>@U..........HoldPeriod..
............U..........ReturnReceiptS..OnU..........DeliveryReport
--B=U..............Sign..liU..........DefaultMailSaveOptions..lrU.
D............ReplyToa..U..........Body.............Hallo,........
.................,.....das ist ein Test f.r unsere Sneaker.........
.................-.....THE MAGIC WORDS ARE FEEBLE GIBBERISH........
.........................Gru.,.............................Matthias
 Mueller.................U..........ReminderDate..U..........Dele
tionDate..U..............Encrypts..OtU..........$Folders..U.......
....PreparedToSend..O U..............DeliveryPriority..NMU.........
..$KeepPrivate..U..............Subject ..Testmail fuer SniffingU.E.
..6.....SendTo..CN=Andreas Maier/OU=DuD/OU=Datenschutz/O=TUD@TU-Dresd
enU.E..........CopyTo..U.D............BlindCopyTo..U.E..../.....Fr
om..CN=Matthias Mueller/OU=DuD/OU=Datenschutz/O=TUD.EU............Po
stedDate..}.6..f%AU.....i..........$Signature.....X6..f%A........O...
...........6...H........j8..d%.....................&...@.........$.
.a%...$.t.%.....O=TUD......O=TUD..........BV...l.0.BC...BA..0BL..v.NN
P....w...%m...]i.u....;,..ys}.}...4]..yl.). ....c...|ohi<'.5L.r..B...
BZ%;m<.....L...Q])..EN..D..MA..l...So;|..PURSAFO..d.YK......<>3......
.#->k......|.Jj/..R.. |.U...ka..Ofz......@@
```

> Hilft Verschlüsselung?

⌘ Verschlüsseln hilft gegen Ausspähen der *Inhalte*



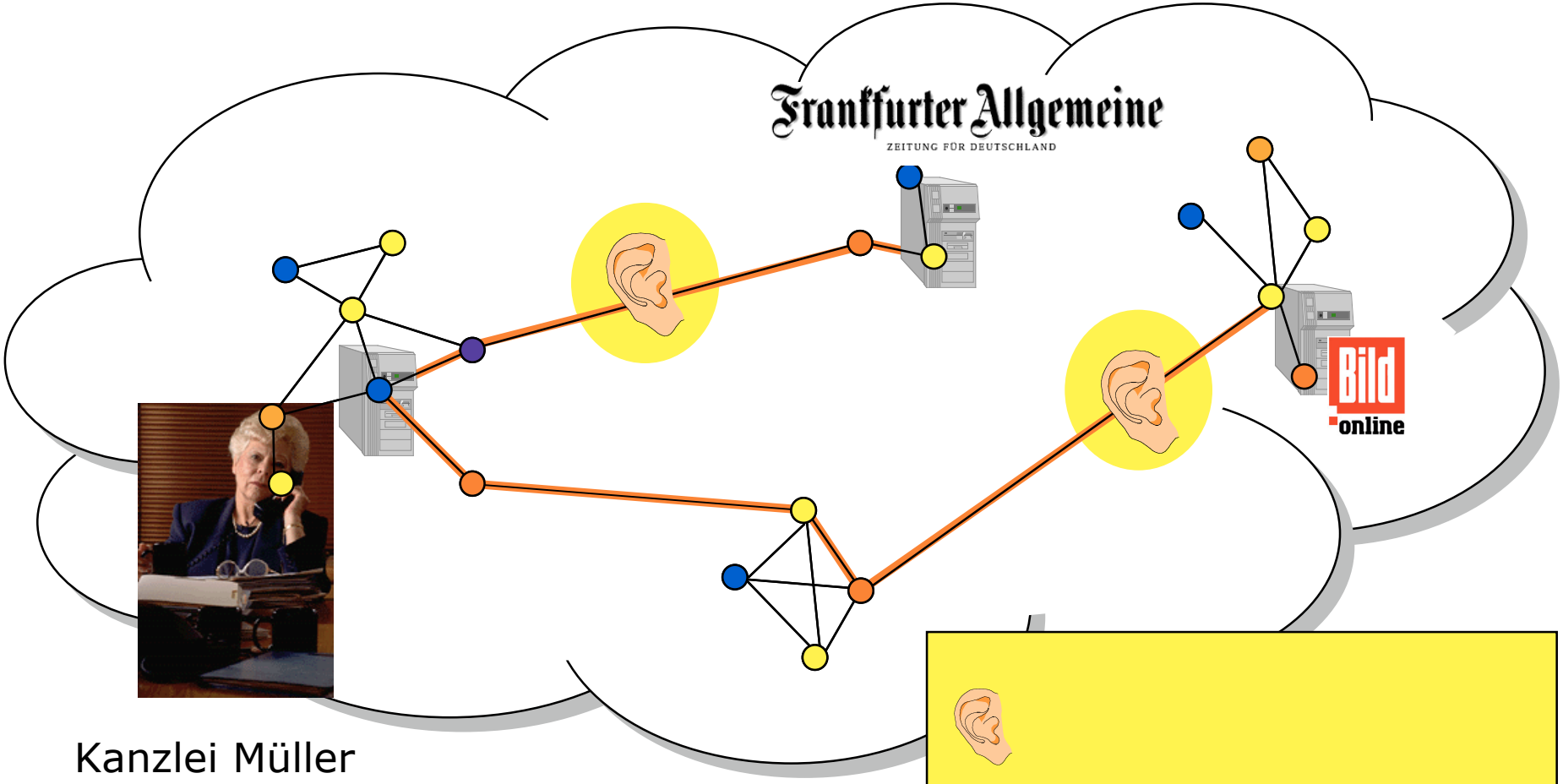
Trotzdem PGP verwenden!

Pretty Good Privacy

http://www.pgp.com

Verschlüsseln hilft überhaupt nichts gegen Beobachtung von Kommunikationsbeziehungen

> Warum genügt Verschlüsselung nicht?

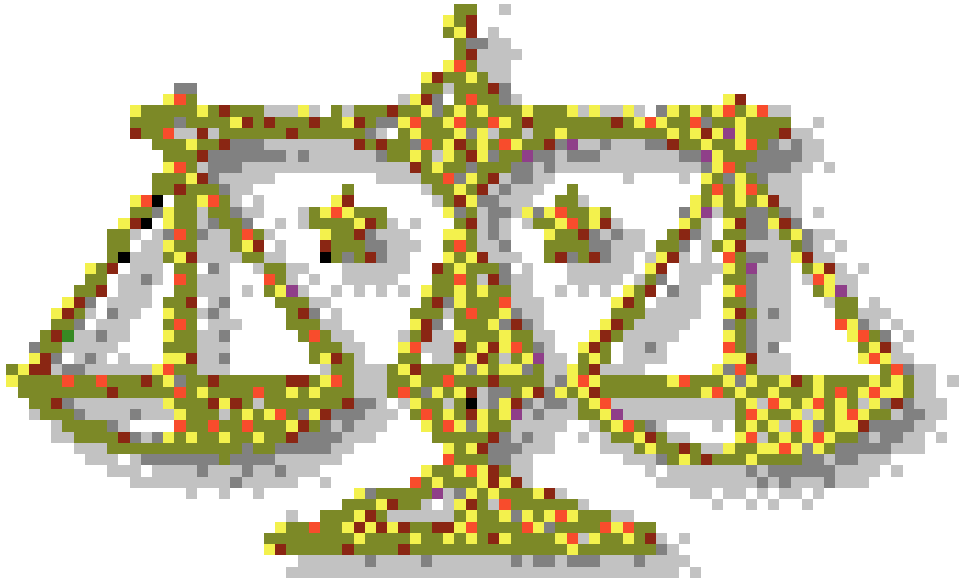


Kanzlei Müller
spezialisiert auf
Firmenfusionen

Beobachtung von
Kommunikationsereignissen
lässt auf Inhalte schließen

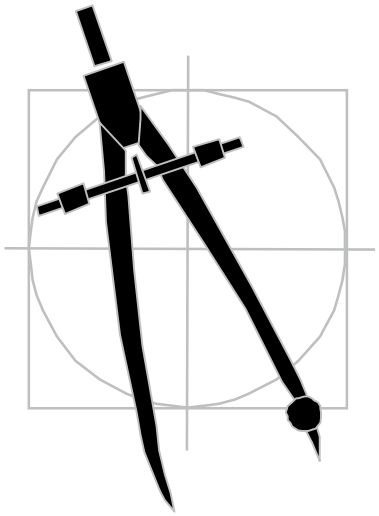
> Juristische Sicht

- Teledienstedatenschutzgesetz (TDDSG)
  - §4 (6): Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.



> Technischer Datenschutz

- Technischer Datenschutz
  - Systeme so konstruieren, dass unnötige Daten vermieden und nicht miteinander verkettet werden können.
- Zu verschleiern sind:
  - Adressen:
    - Sender, Empfänger, Kommunikationsbeziehung
  - Zeitliche Korrelationen:
    - Zeitpunkte, Dauer
  - Übertragenes Datenvolumen und inhaltliche Korrelationen
  - Orte:
    - Aufenthaltsorte, Bewegungsspuren

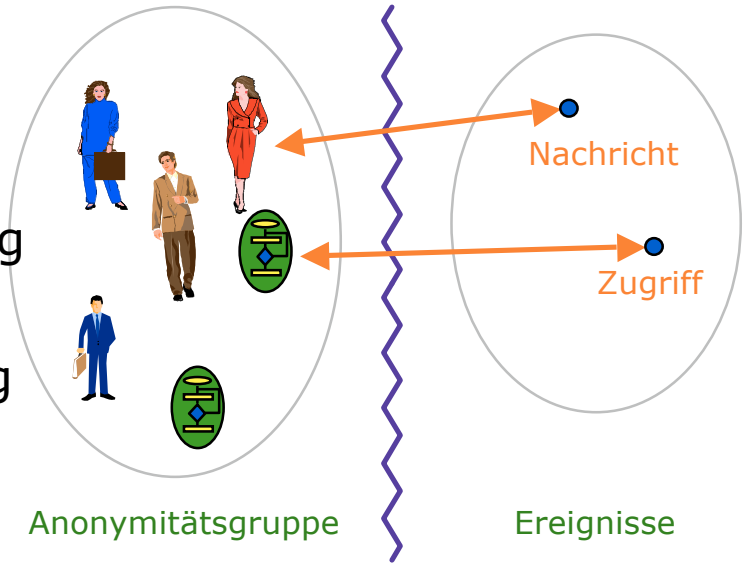


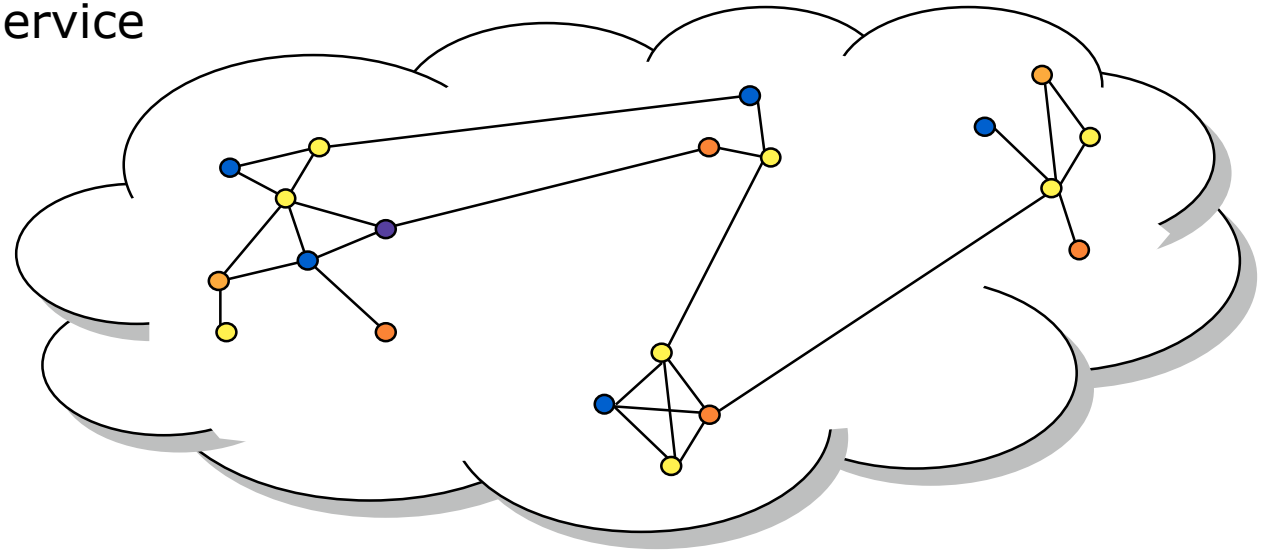
> Politisches und gesellschaftliches Umfeld

- Telekommunikationsüberwachung und Vorratsdatenspeicherung
  - Telekommunikationsüberwachungsverordnung (TKÜV)
    - http://www.bmwi.de/Homepage/download/telekommunikation_post/TKUEV-Entwurf.pdf
  - Cybercrime-Convention
    - http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm
  - Gesetzentwurf des Bundesrates zur Verbesserung der Ermittlungsmaßnahmen
    - http://www.dud.de/dud/documents/brdrs-0275-02-020531(beschluss).pdf
- Datenschutzgesetze
  - Neues Bundesdatenschutzgesetz (BDSG)
    - http://www.bfd.bund.de/information/bdsg_hinweis.html
  - EU-Datenschutzrichtlinie
    - http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html
- Ständiger Prozess
  - Balance zwischen den Interessen aller Parteien finden

> Verfahren zur unbeobachtbaren Kommunikation

- Wer ist zu schützen?
  - Schutz des Senders
  - Schutz des Empfängers
  - Schutz der Kommunikationsbeziehung
- Grundkonzepte:
  - Verteilung mit impliziter Adressierung
  - Dummy traffic
  - Proxies
  - DC-Netz
  - Blind-Message-Service
  - Mix-Netz
  - Steganographie

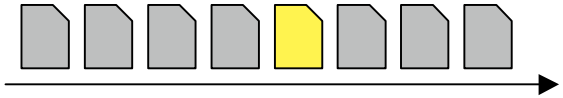




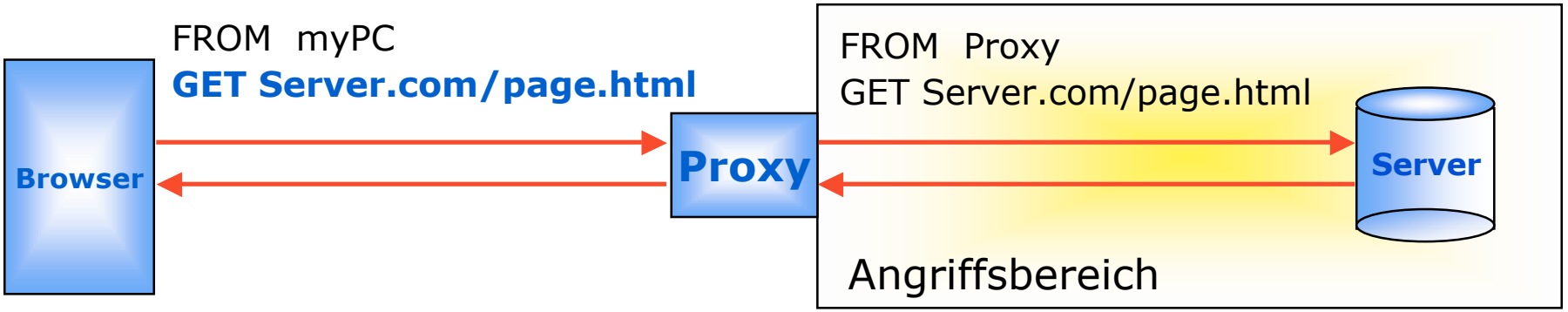
> Grundsätzliche Techniken (1)

- **Verteilung** (Broadcast) + implizite Adressierung
  - Schutz des Empfängers; alle erhalten alles
  - lokale Auswahl

- **Dummy Traffic:** Senden bedeutungsloser Nachrichten
  - Schutz des Senders



- **Proxies** zwischenschalten
  - Server erfährt nichts über Client, Proxy kann mitlesen



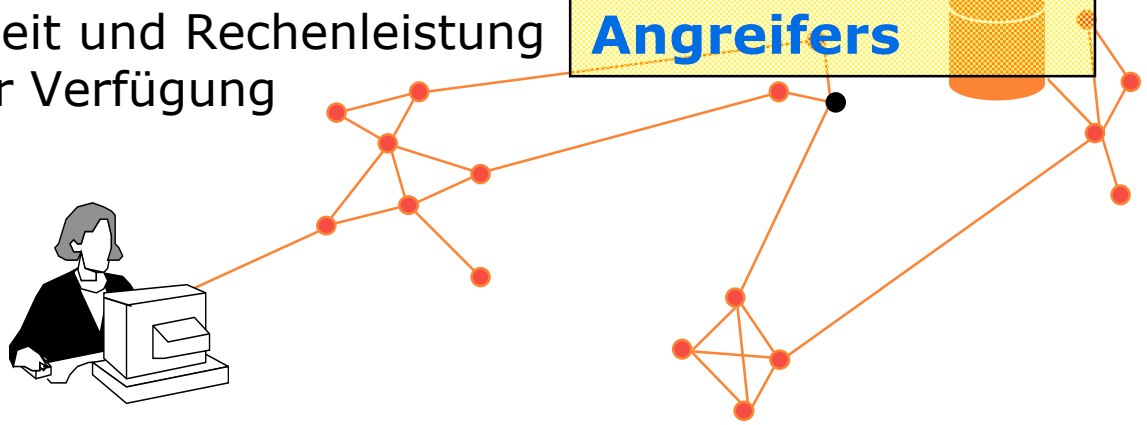
>> Grundsätzliche Techniken (2)

- **DC-Netz:** kombiniert u.a. Broadcast, Kryptographie und Dummy Traffic
  - Schutz des Senders
- **Blind-Message-Service:** Unbeobachtbare Abfrage aus von unabhängigen Betreibern replizierten Datenbanken
  - Schutz des Clients
- **MIX-Netz:** kombiniert u.a. hintereinander geschaltete Proxies von unabhängigen Betreibern, Kryptographie und Dummy Traffic
  - Schutz der Kommunikationsbeziehung
  - Effizient in Vermittlungsnetzen
- **Steganographie**
  - Verbergen einer Nachricht in einer anderen

> Angreifermodell

- Angreifer kann:
  - alle Kommunikationsleitungen passiv überwachen (Verkehrsanalysen durchführen),
  - ggf. aktiv eigene Nachrichten beisteuern,
  - ggf. fremde Nachrichten blockieren/verzögern,
  - ggf. selbst eine »Unbeobachtbarkeitsstation« sein
  - Empfänger oder Sender sein
- Angreifer kann nicht:
  - Kryptosysteme brechen,
  - in den persönlichen Rechner eindringen,
  - ist komplexitätstheoretisch beschränkt, d.h. hat begrenzte Zeit und Rechenleistung für seine Angriffe zur Verfügung

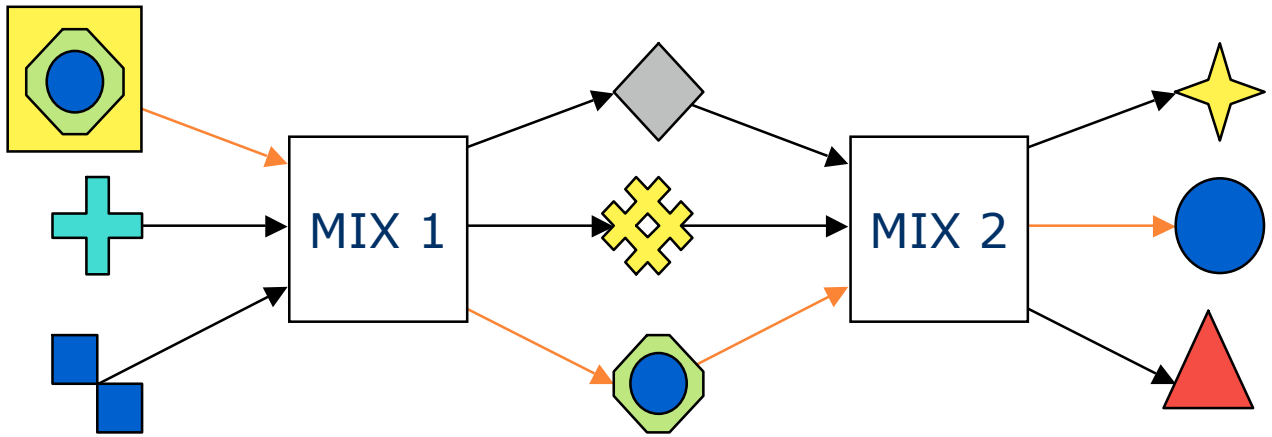
Ein sehr starkes Angreifermodell schützt vor dem Unterschätzen des realen Angreifers



> Das Mix-Netz

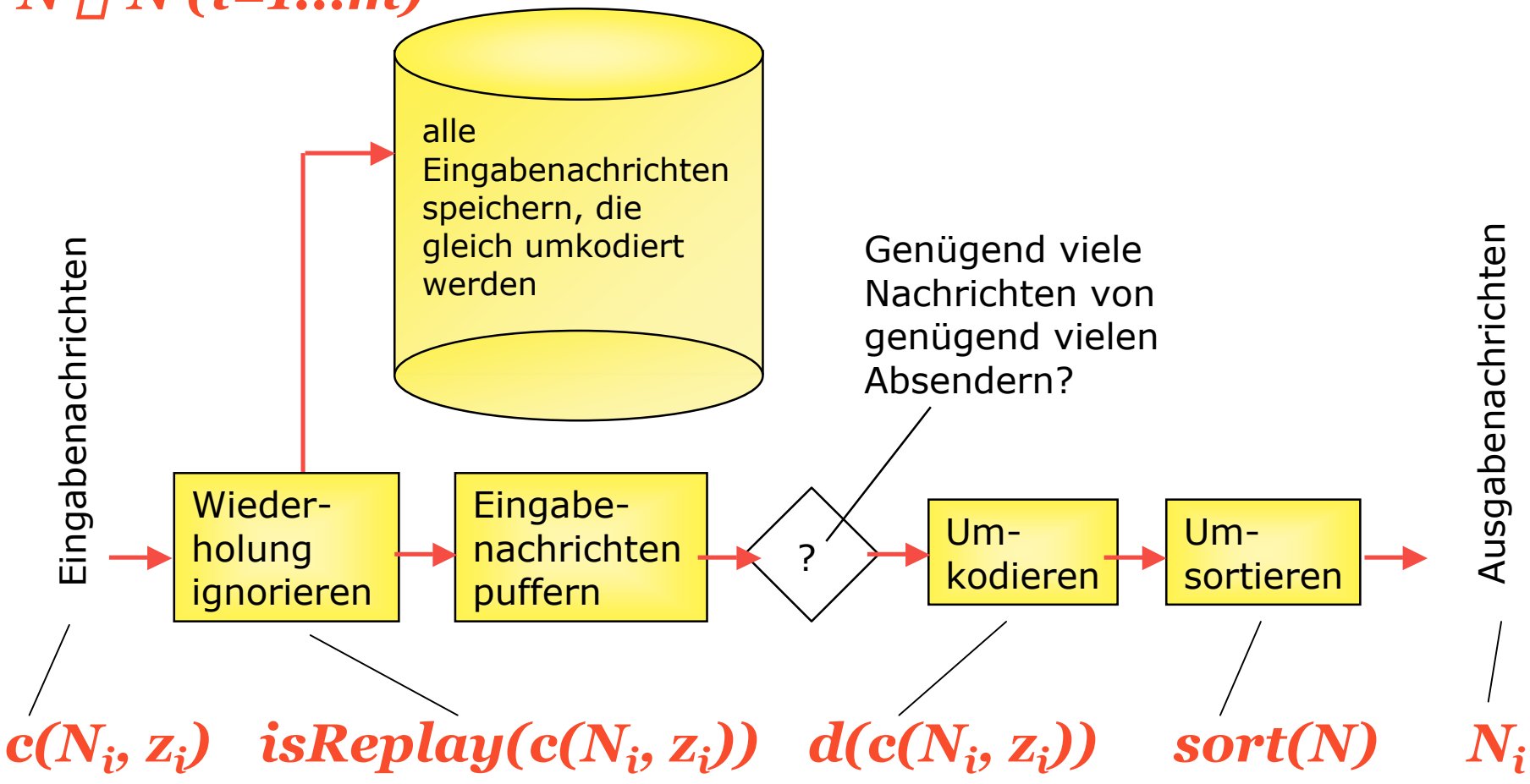
Chaum, 1981

- Grundidee:
  - Nachrichten in einem »Schub«
    - sammeln, Wiederholungen ignorieren, umkodieren, umsortieren, gemeinsam ausgeben.
  - Alle Nachrichten haben die gleiche Länge.
  - Mehr als einen Mix verwenden.
  - Wenigstens ein Mix darf nicht angreifen.
- Schutzziel:
  - Unverkettbarkeit von Sender und Empfänger
  - Schutz der Kommunikationsbeziehung
  - Zuordnung zwischen E- und A-Nachrichten wird verborgen



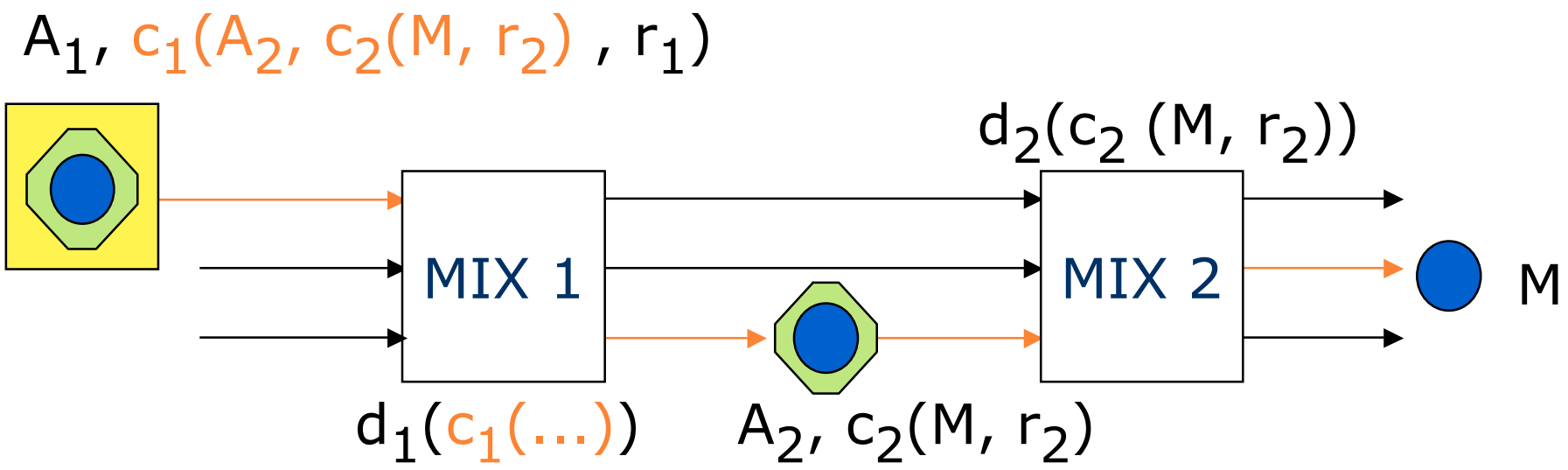
> Blockschaltbild eines Mix

$N = \{N_1, N_2, \ldots, N_m\}$
$N \not\subset N\ (i=1\ldots m)$



> Kryptographische Operationen eines Mix

- Verwendet **asymmetrisches Verschlüsselungssystem**
  - $c_i(...)$ Verschlüsselungsfunktion für Mix i
    - Jeder kann den öffentlichen Schlüssel c_i verwenden
  - $d_i(...)$ private Entschlüsselung von Mix i
    - Nur Mix i kann entschlüsseln
  - A_i Adresse von Mix i
  - r_i Zufallszahl (verbleibt im Mix, wird »weggeworfen«)
  - M (verschlüsselte) Nachricht für Empfänger (inkl. seiner Adresse)



> Praxis: Anonymisierung im Internet

- Anonymisierung von Electronic-Mail:
  - Typ-0-Remailer: anon.penet.fi
    - Header entfernen und anonym/pseudonym weiterleiten
    - Reply möglich, da der echte Absender gespeichert und durch ein Transaktionspseudonym ersetzt wurde
    - Verkettbarkeit über Länge und zeitliche Korrelation
  - Typ-1-Remailer: Cypherpunk-Remailer
    - wie Typ-0, zusätzlich Angabe über Verzögerungszeit bzw. Sendezeit, Kaskadierung
    - PGP-verschlüsselte Mails werden vom Remailer entschlüsselt
    - Verkettbarkeit über Länge, bei niedrigem Verkehrsaufkommen auch über zeitliche Korrelation
  - Typ-2-Remailer: Mixmaster (Cottrell, 1995)
    - Sammeln von Nachrichten
    - Mix-Modell im Pool-Mode
    - alle Nachrichten haben gleiche Länge

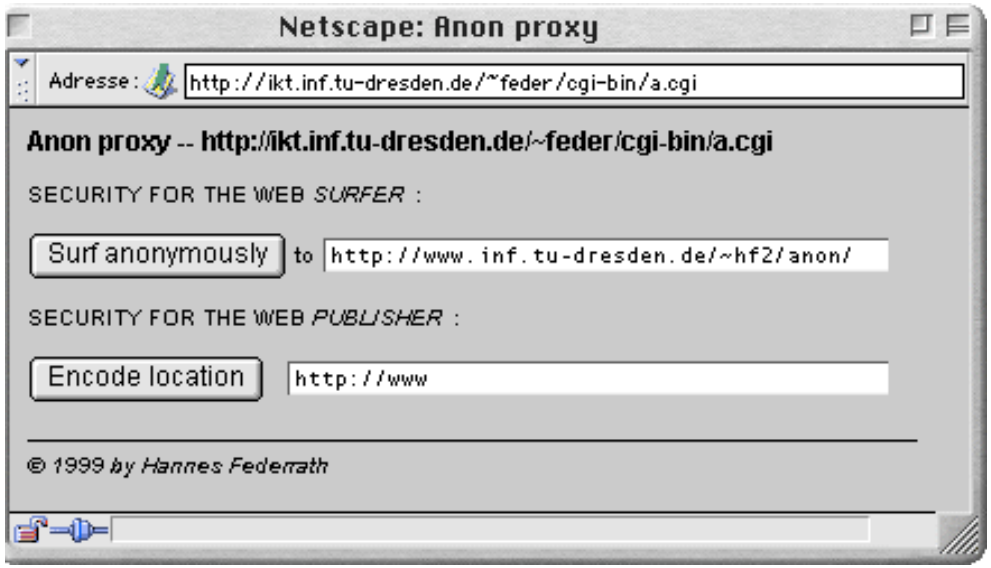
> Client-Anonymität

- Einfache Proxies (teilweise mit Filterfunktion: Cookies, JavaScript, active content)
  - Anonymizer.com (Lance Cottrell)
  - Aixs.net
  - ProxyMate.com (Lucent Personal Web Assistant, Bell Labs)
  - Rewebber.com (Andreas Rieke, Thomas Demuth, FernUni Hagen)
  - Jeder entsprechend konfigurierte Web-Proxy

- Verkehrsanalysen berücksichtigende Verfahren
  - Onion-Routing (Naval Research Center)
  - Crowds (Mike Reiter, Avi Rubin AT&T)
  - Freedom (Ian Goldberg, Zero-Knowledge Inc.)
  - WebIncognito (Privada)
  - Web-Mixe/JAP (TU Dresden)

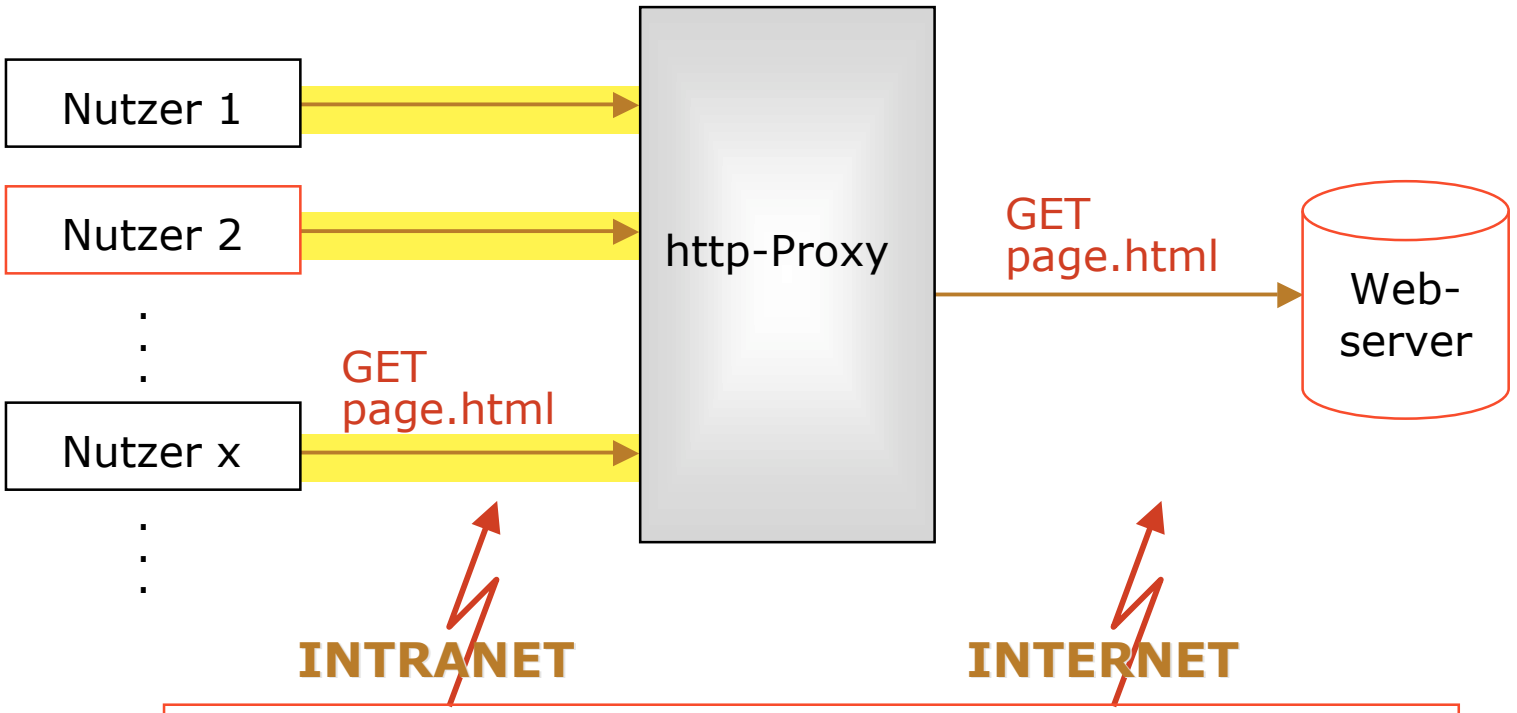
> Einfache Proxies

- Server besitzt keinerlei Information über den wirklichen Absender eines Requests
- **Kein Schutz gegen den Betreiber des Proxy**
- **Kein Schutz gegen Verkehrsanalysen**



- **Arbeitsprinzipien für Webzugriff:**
  1. **Formularbasiert**
     - URL eingeben
     - Proxy stellt Anfrage und versieht eingebettete URLs mit einem Präfix
  2. **Browserkonfiguration ändern**
     - »use proxy«

>> Einfache Proxies

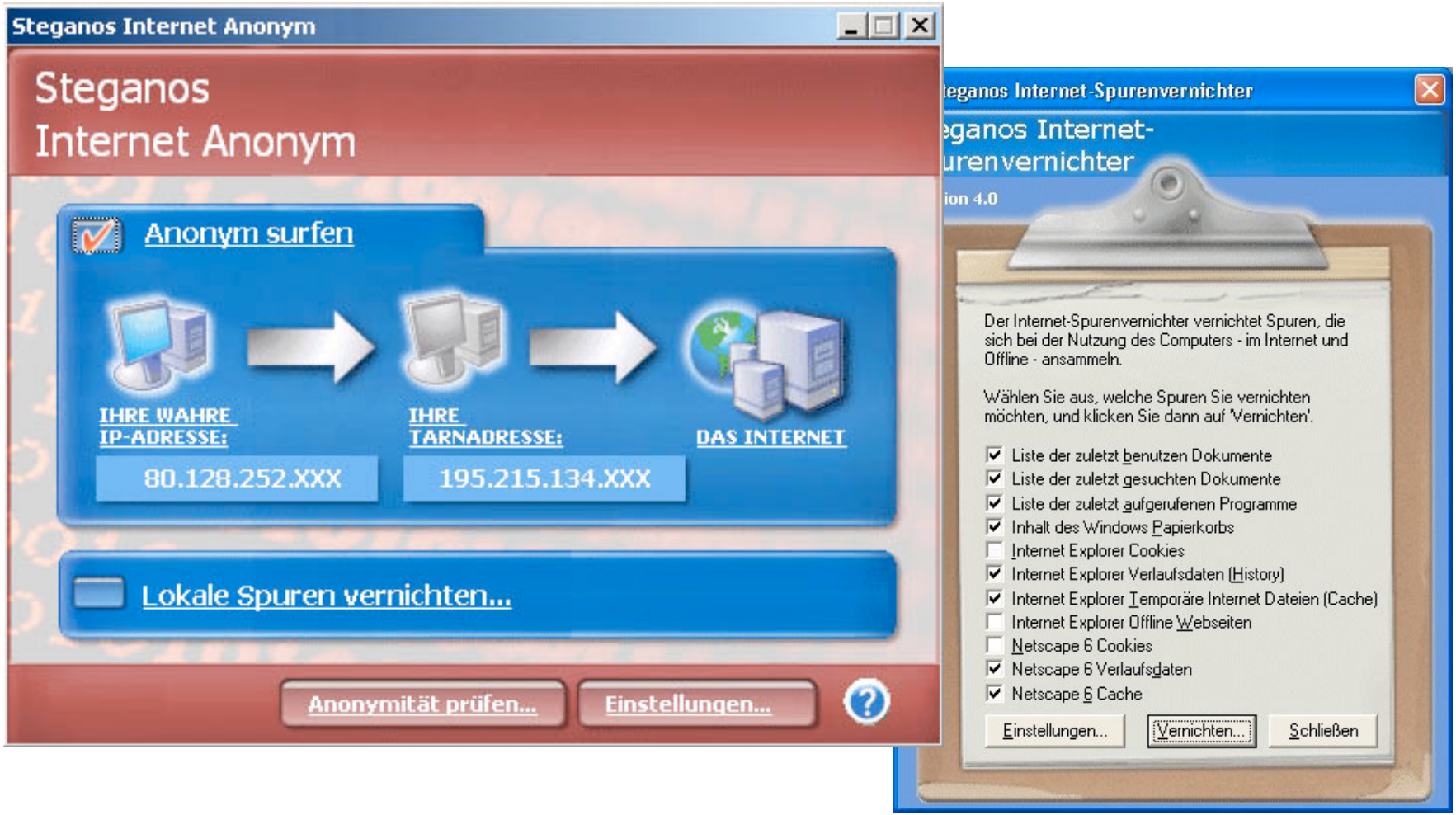


- Beobachtung und Verkettung ist möglich
  - zeitliche Verkettung
  - Verkettung über Inhalte (Aussehen, Länge)

Verschlüsselung zwischen Browser und Proxy verhindert Korrelation über »Aussehen«, aber nicht über Nachrichtenlänge und Zeit und hilft nichts gegen den Proxy.

>>> Einfache Proxies

- Steganos Internet Anonym: http://www.steganos.com/
  - Benutzt »offene« Proxies



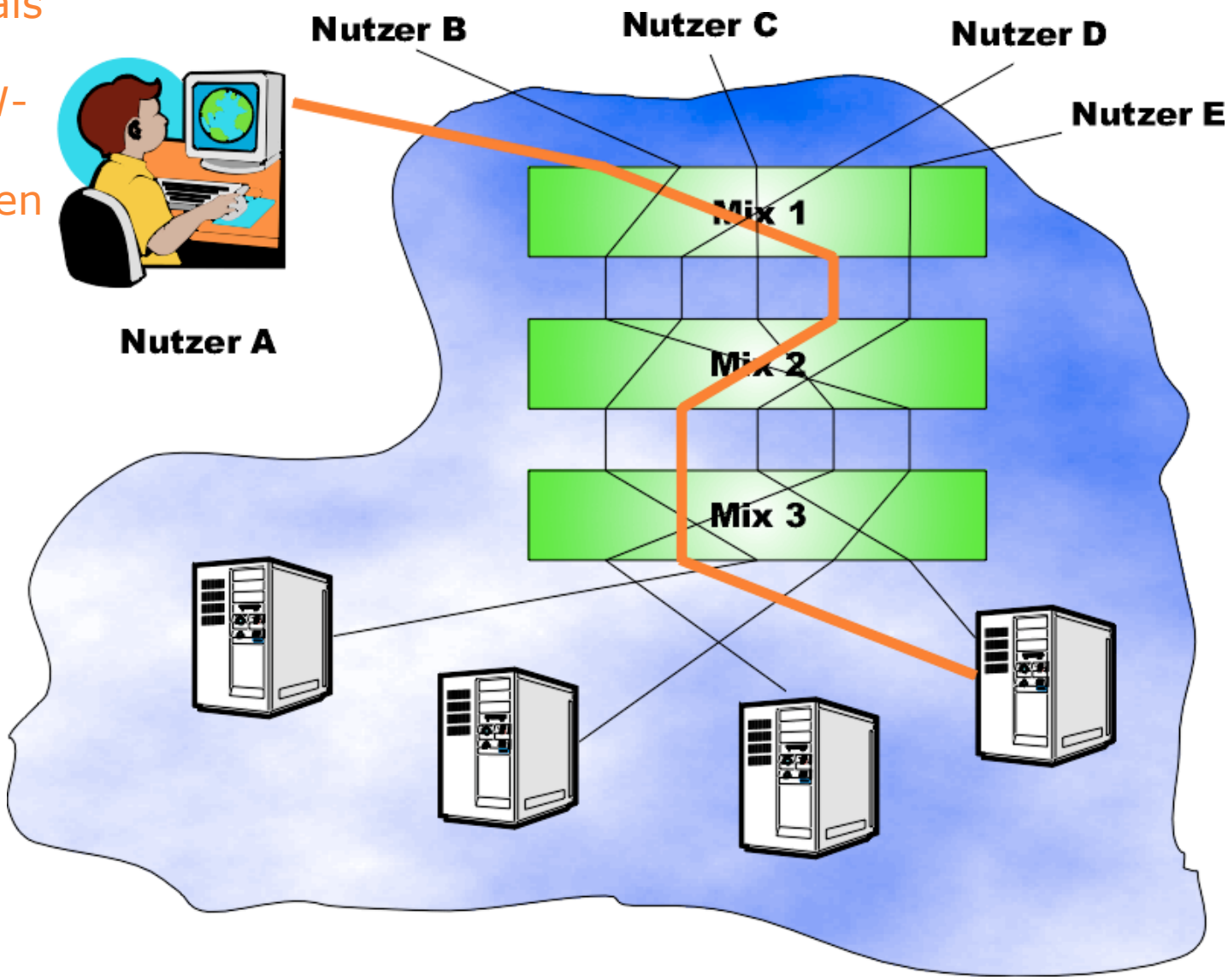
> Client-Anonymität

- Einfache Proxies (teilweise mit Filterfunktion: Cookies, JavaScript, active content)
  - Anonymizer.com (Lance Cottrell)
  - Aixs.net
  - ProxyMate.com (Lucent Personal Web Assistant, Bell Labs)
  - Rewebber.com (Andreas Rieke, Thomas Demuth, FernUni Hagen)
  - Jeder entsprechend konfigurierte Web-Proxy

- Verkehrsanalysen berücksichtigende Verfahren
  - Onion-Routing (Paul Syverson, Naval Research Center)
  - Crowds (Mike Reiter, Avi Rubin, AT&T)
  - Freedom (Ian Goldberg, Zero-Knowledge Inc.)
  - Web-Mixe/JAP (TU Dresden)

> Das Projekt AN.ON: JAP/WebMixe

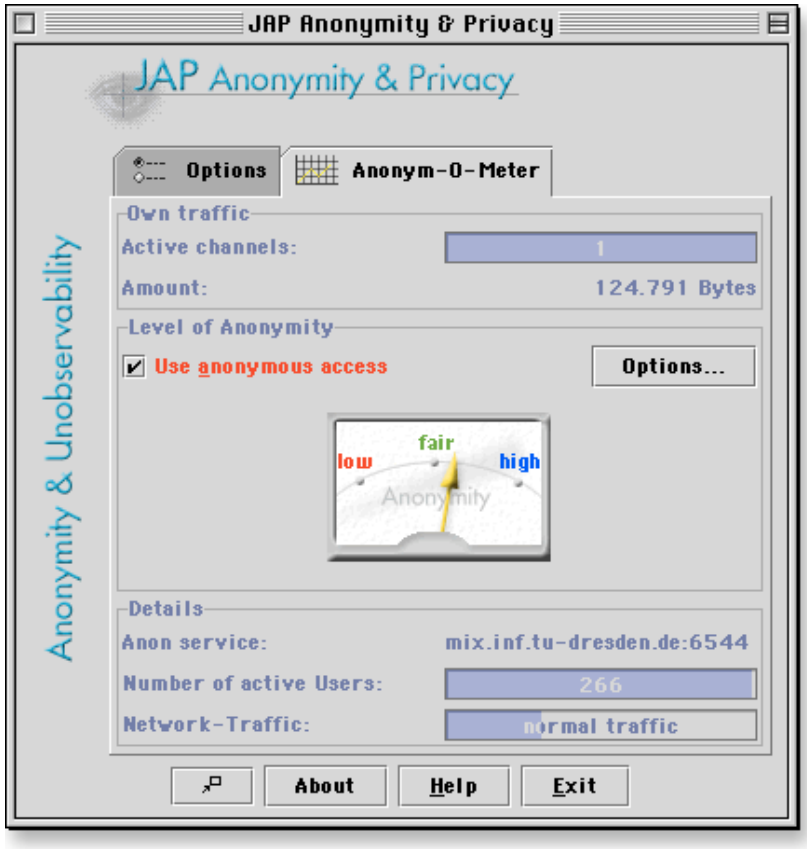
- JAP wird als Proxy für den WWW-Browser eingetragen



>> AN.ON: Technische Daten, Nutzerzahlen

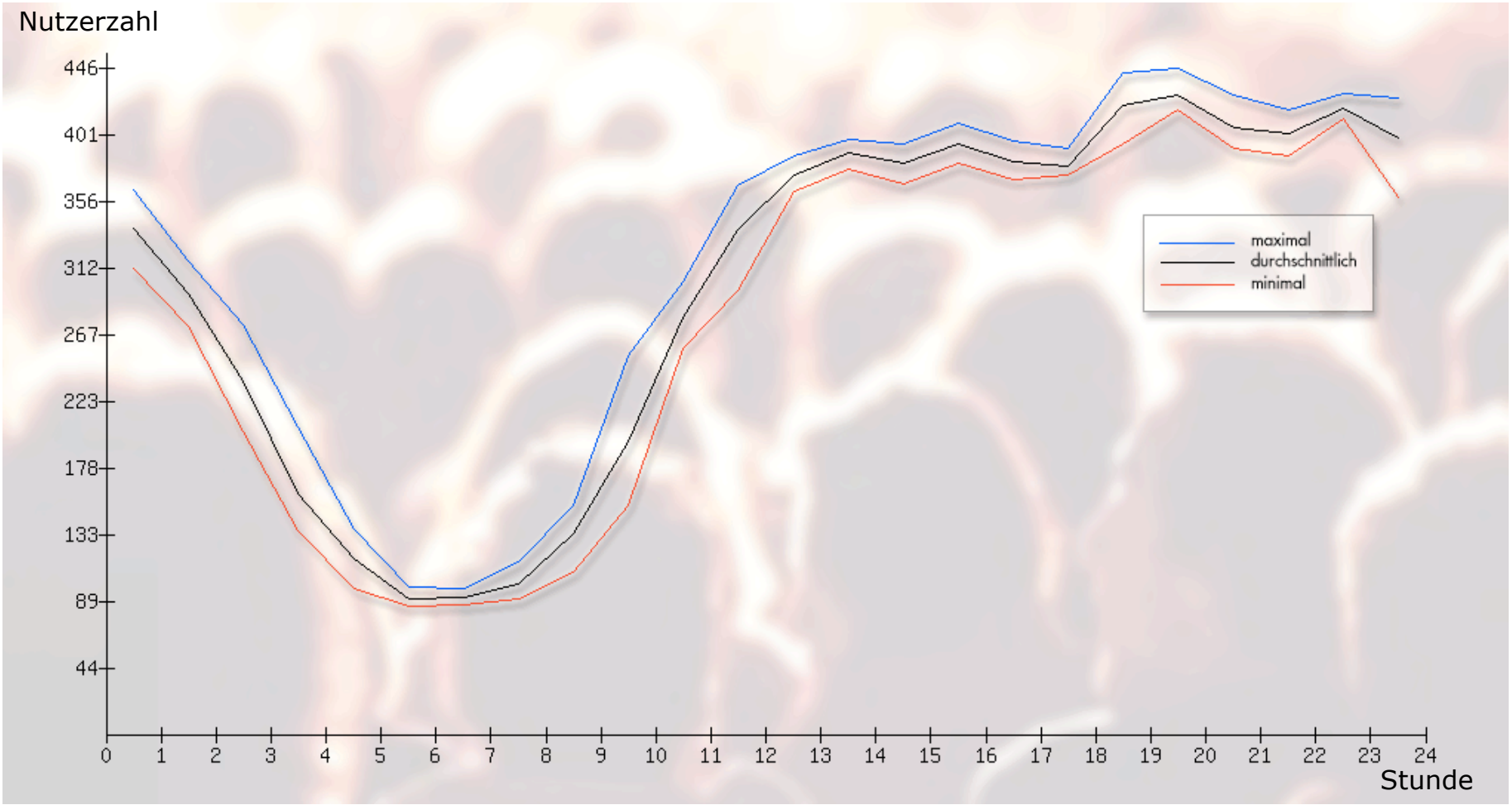
- Entwicklung eines praktisch nutzbaren Systems zum unbeobachtbaren Surfen im Internet
  - Schutz von personenbezogenen Daten bei der Benutzung des Internet
  - Verhinderung von »Profiling« und kommerzieller Nutzung
- Implementierung bestehend aus:
  - Java-Client-Programm »JAP«
  - Mix-Server (C++)
  - Info-Service (Java)
- Schätzung:
  - insgesamt ca. 20000 Nutzer
- Netzwerkverkehr ist zur Zeit der Hauptengpass:
  - ca. 3000 Gigabyte pro Monat
  - bei ca. 1000 Nutzern gleichzeitig online
  - zu Spitzenzeiten etwa 4000 Transaktionen (URLs) pro Minute
- 3 Mix-Kaskaden im Betrieb

JAP.inf.tu-dresden.de



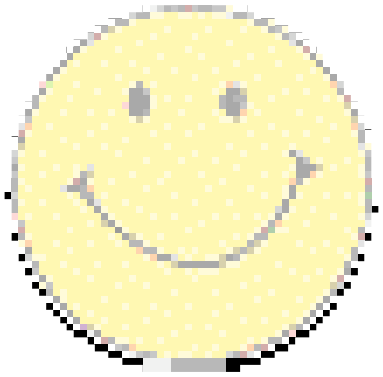
>>> AN.ON: Nutzung

⌘ Typischer Verlauf der Nutzerzahl eines Tages



> Positive Erfahrungen

- Vorstellung auf der CeBit 2001 und 2002
  - Im Gegensatz zu 1997 wird heute nicht mehr gefragt, wogegen man sich eigentlich schützen soll.
- Größeres Interesse am Datenschutz und im Bewusstsein um Bedrohungen
  - Hohe Bereitschaft, praktikable Lösungen zum Selbstdatenschutz einzusetzen
- Kommerzielles Interesse
  - Vermarktung als Dienstleistung möglich?



> Negative Erfahrungen

- Sehr schwer vermittelbar, warum ein System sicher bzw. unsicher ist
  - Verbreitete Vorstellung: ständig wechselnde IP-Adresse = hohe Anonymität
- Missbrauchsfälle aufgetreten
  - Dienst zur Zeit auf Web-Zugriffe beschränkt, obwohl allgemeiner anonymer TCP/IP möglich wäre
  - Nach juristischer Prüfung ist der Dienst legal, jedoch Überlegungen zur Deanonymisierung
  - Neue Forschungsfrage: Wie kann begründete Enttarnung ohne Massenüberwachung durchgeführt werden?
- Länder (Saudi Arabien) haben Zugang zum Dienst gesperrt
  - Forschungsfrage: Anonymisieren des Anonymisierungsdienstes

»AN.ON — Anonymität Online«

JAP Anonymity & Privacy

ANONYMITY IS NOT A CRIME

Kostenloser Download von JAP

http://www.anon-online.de/

Weitere Informationen in der Infobörse

- Kleiner Saal (hier!)