GET http://anon.nowhere.com/
>please type in your name
>set cookie

Die Tarnkappe im Internet

Hannes Federrath • Freie Universität Berlin • Institut für Informatik

Von der anonymen Benutzung des World Wide Web

> 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

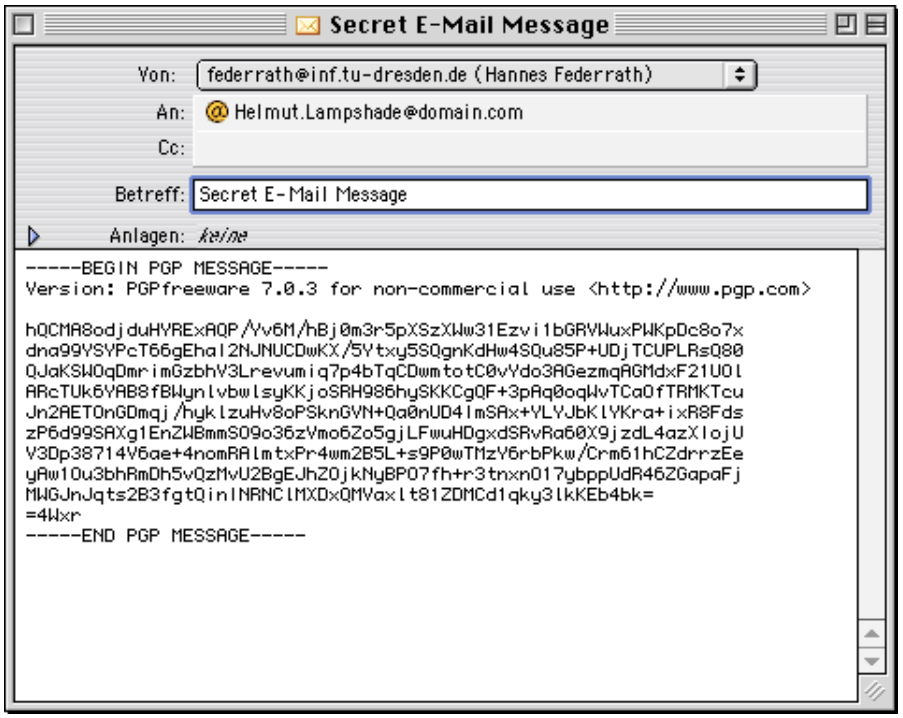
```
wwwtcs.inf.tu-dresden.de>tail access_log
amadeus.inf.tu-dresden.de - - [15/Oct/1997:11:50:01] "GET
/lvbeschr/winter/TechnDS.html HTTP/1.0" - "http://wwwtcs.inf.tu-
dresden.de/IKT/" "Mozilla/3.01 (X11; I; SunOS 5.5.1 sun4u)"
```

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
```

Hilft Verschlüsselung?

⌘ Verschlüsseln hilft gegen Ausspähen der *Inhalte*



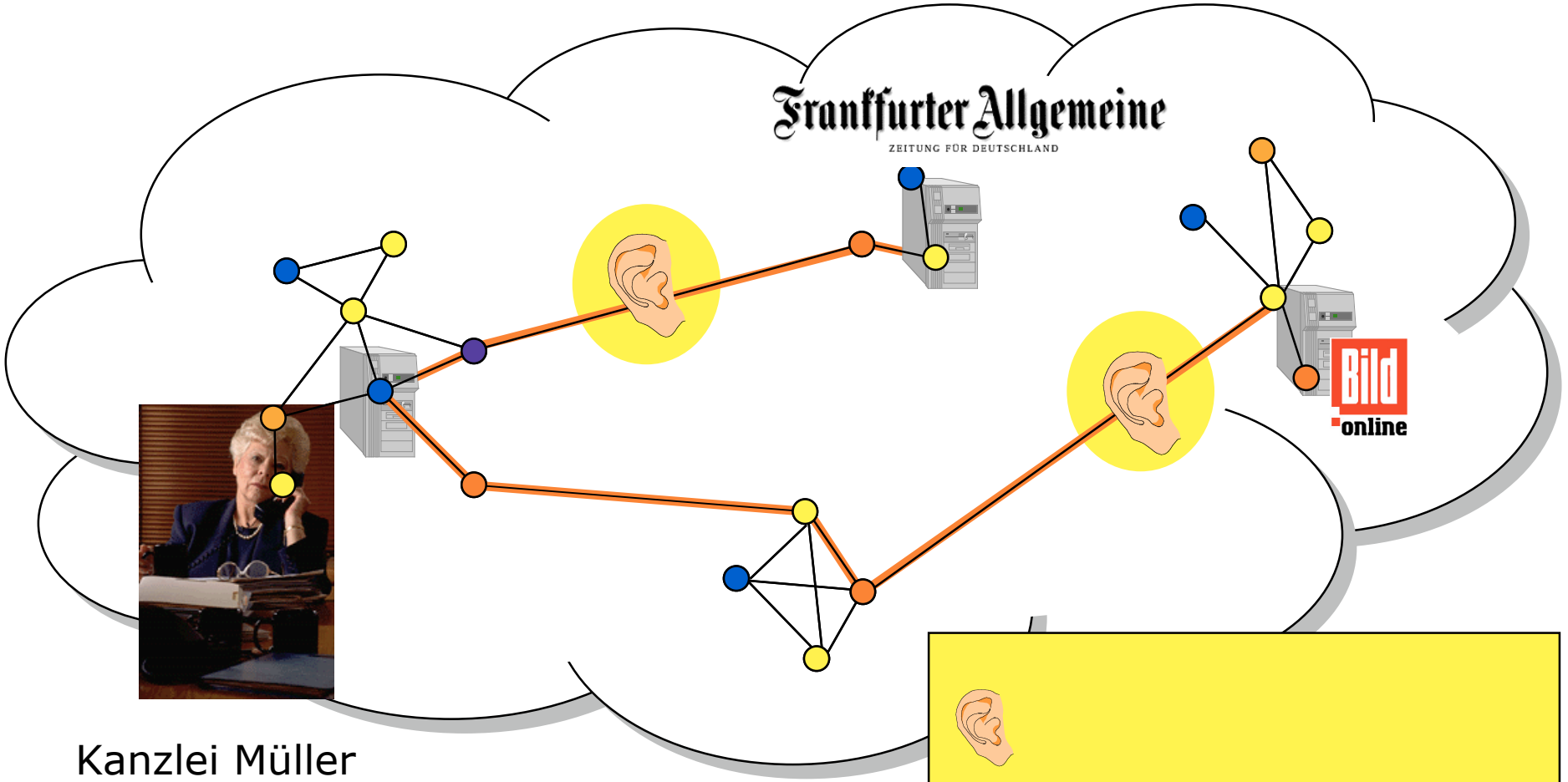
Trotzdem PGP verwenden!

Pretty Good Privacy

http://www.pgp.com

Verschlüsseln hilft überhaupt nichts gegen Beobachtung von Kommunikationsbeziehungen

> Warum genügt Verschlüsselung nicht?



Kanzlei Müller
spezialisiert auf
Firmenfusionen

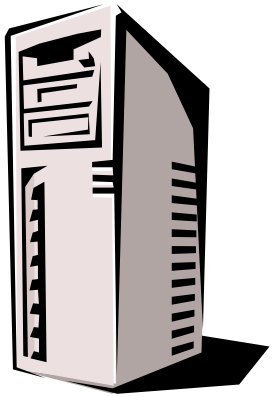
Beobachtung von
Kommunikationsereignissen
lässt auf Inhalte Schließen

Funktionsweise von Cookies

Erster Besuch:

1. GET www.amazon.de

2. Set Cookie: id=12241235564



3. ggf. Warnung

4. Speichern auf Festplatte

Folgende Besuche:

GET www.amazon.de
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)

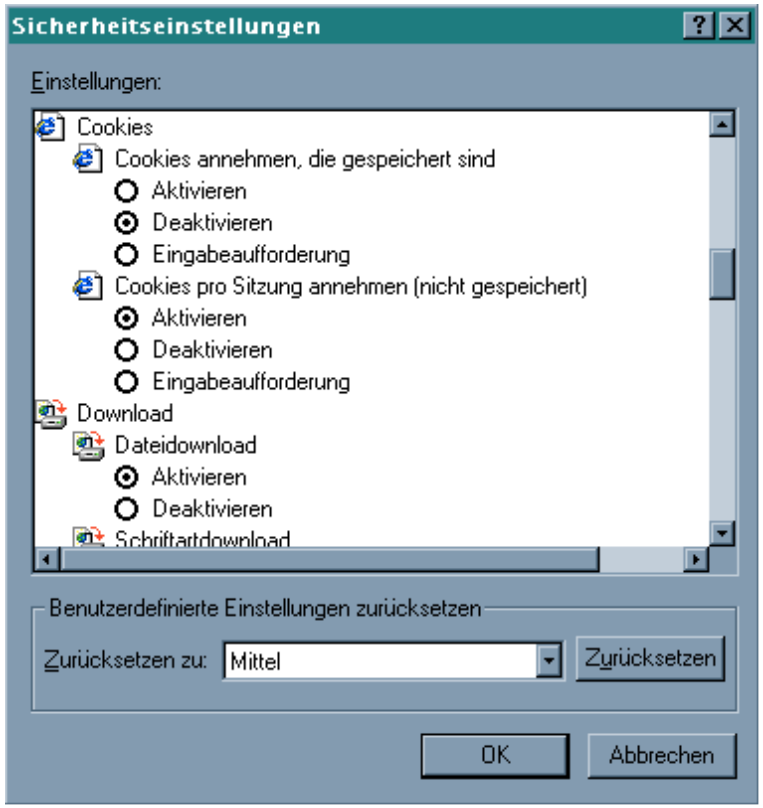
Ungefährliche Kekse ?

- Löschen nicht die Festplatte
- Übertragen keinen Viren
- Verraten keine lokal gespeicherten Daten
  - Passwörter, geheime Schlüssel usw.
- Webserver erkennt Nutzer bei jedem Besuchen seiner Seite wieder
  - Positiv:
    - personalisierte Webseiten
  - Negativ:
    - Erstellung von Nutzerprofilen

Gefährliche Kekse !

- Werberinge (z.B. Doubleclick.com):
  - Plazieren Banner auf Seiten vieler Anbieter
  - Alle Banner werden von zentralem Server geladen, Cookie wird gesendet
  - Werbeserver erhält globales Nutzungsprofil
  - Alle Server könnten Informationen erfahren, die man an einen gesendet hat.

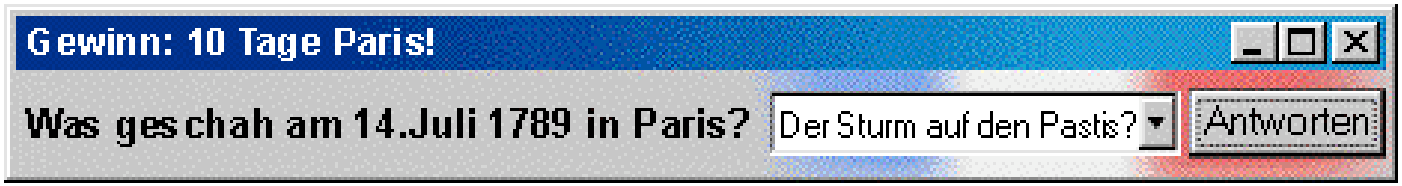
- Gegenmaßnahmen
  - Cookies deaktivieren
  - Problem:
    - Viele Angebote nur mit Cookies verfügbar
    - nützliche Anwendungen für Cookies



Third-Party Cookies

- Laden eines eingebetteten Bildes (z.B. Werbebanner) von einem fremden Server (z.B. Werbering)
  - Werbering setzt Cookie
  - Referer verrät Herkunft des Requests

- Verschiedene Shops arbeiten mit demselben Werbering zusammen:
  - Website A (z.B. Bookshop)
  - Website B (z.B. Lebensversicherung)
  - Website C (z.B. Gesundheitsberatung)



Third-Party Cookies

GET http://werbering.de/werbebanner1.gif
Cookie id=12241235564
Referer: http://www.bookshop.de

GET http://werbering.de/werbebanner2.gif
Cookie id=12241235564
Referer: http://www.lebensversicherung.de

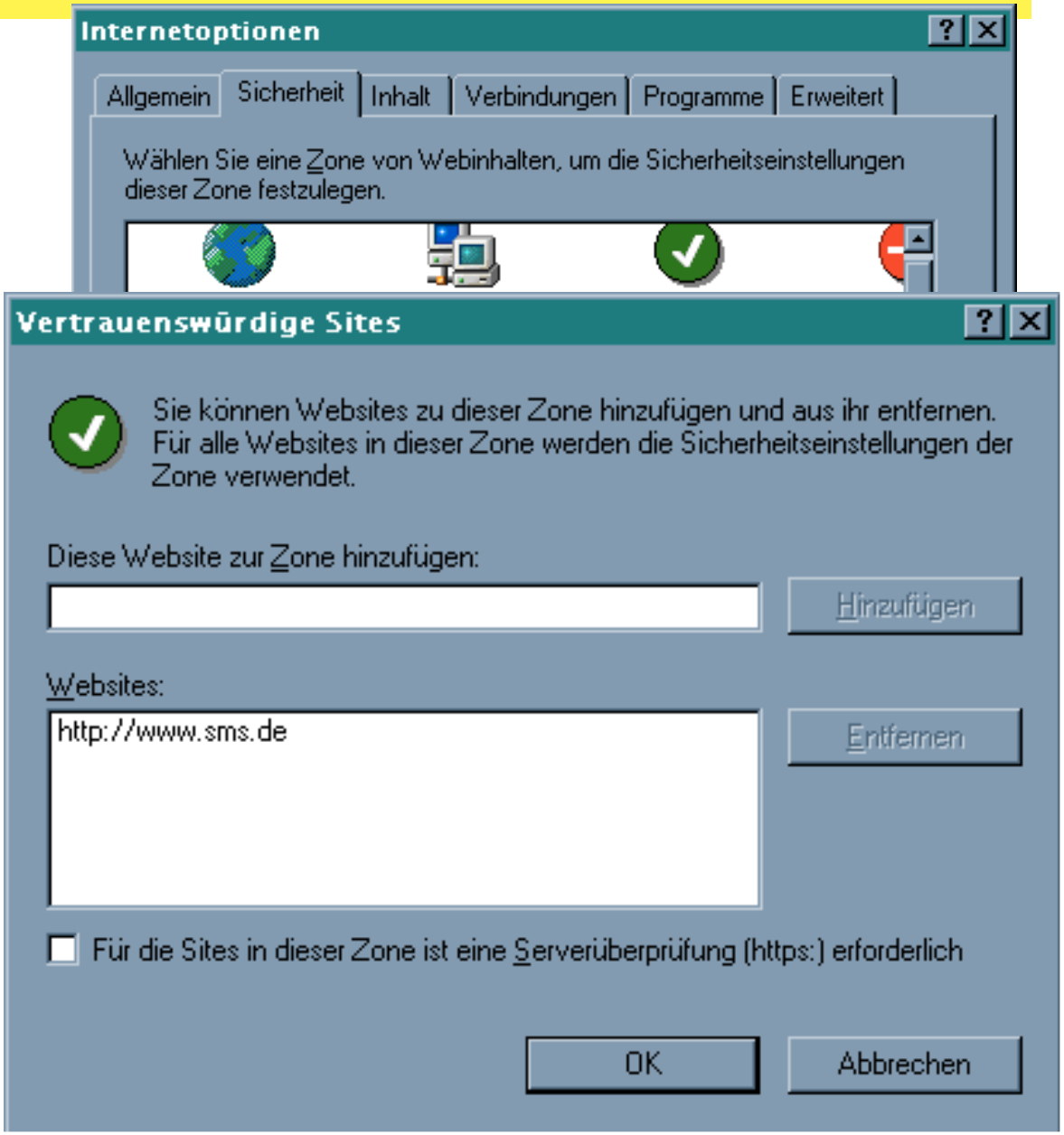
GET http://werbering.de/werbebanner3.gif
Cookie id=12241235564
Referer: http://www.gesundheitsberatung.de

Gläserner Bürger? Legal?

Gegenmaßnahmen

Cookies

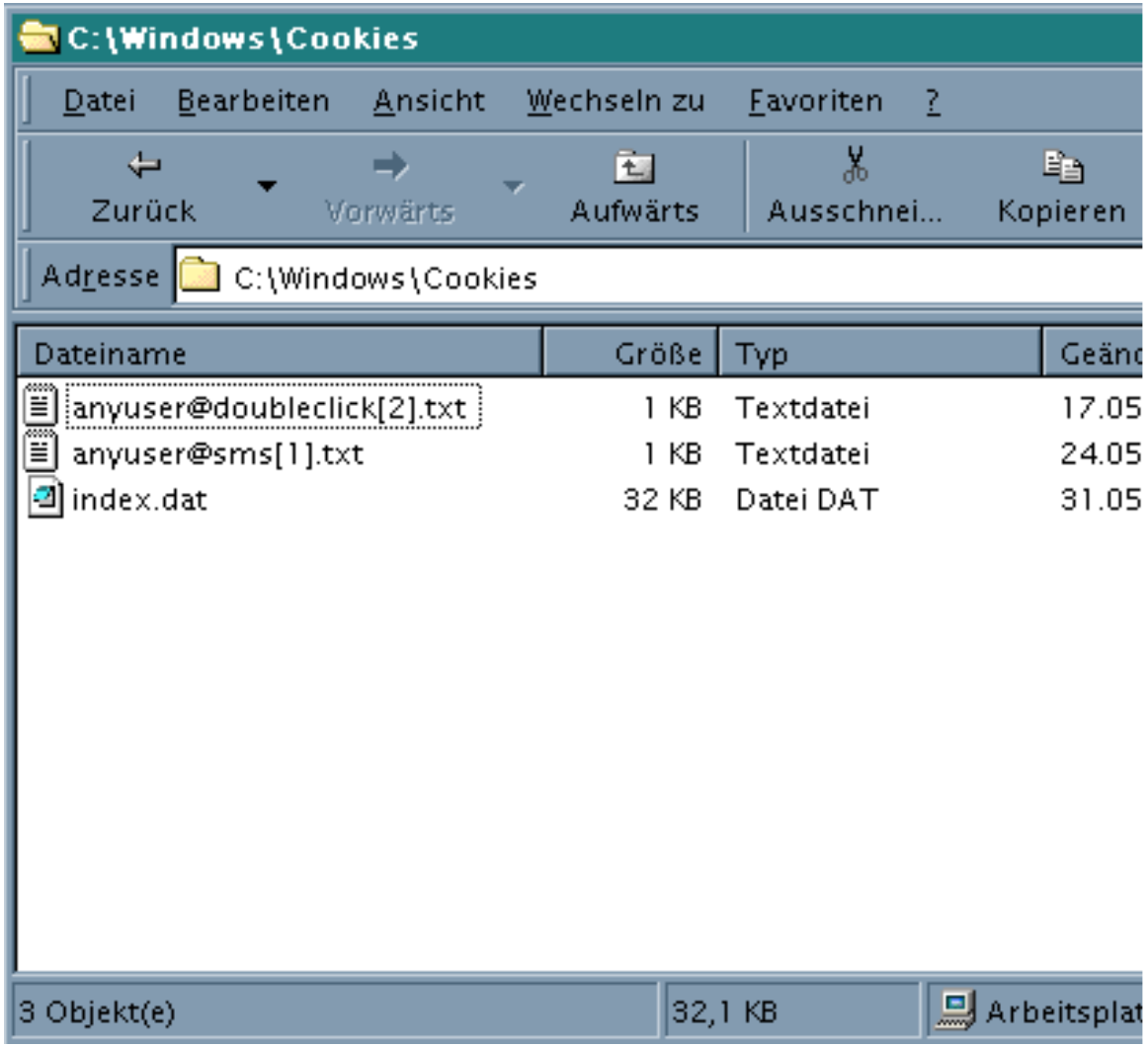
- nur bei ausgewählten Seiten speichern
- regelmäßig löschen
- filtern
- regelmäßig weltweit austauschen



Gegenmaßnahmen

Cookies

- nur bei ausgewählten Seiten speichern
- regelmäßig löschen
- filtern
- regelmäßig weltweit austauschen



Gegenmaßnahmen

Cookies

- nur bei ausgewählten Seiten speichern
- regelmäßig löschen
- filtern
- regelmäßig weltweit austauschen

http://www.junkbusters.com/

http://www.guidescope.com/

http://www.webwasher.com

Gegenmaßnahmen

Cookies

- ⌘ nur bei ausgewählten Seiten speichern
- ⌘ regelmäßig löschen
- ⌘ filtern
- ⌘ regelmäßig weltweit austauschen

CookieCooker
cookie.inf.tu-dresden.de

CookieCooker

cookie.inf.tu-dresden.de

- Filter software für Cookies
  - ähnlich JunkBuster und WebWasher

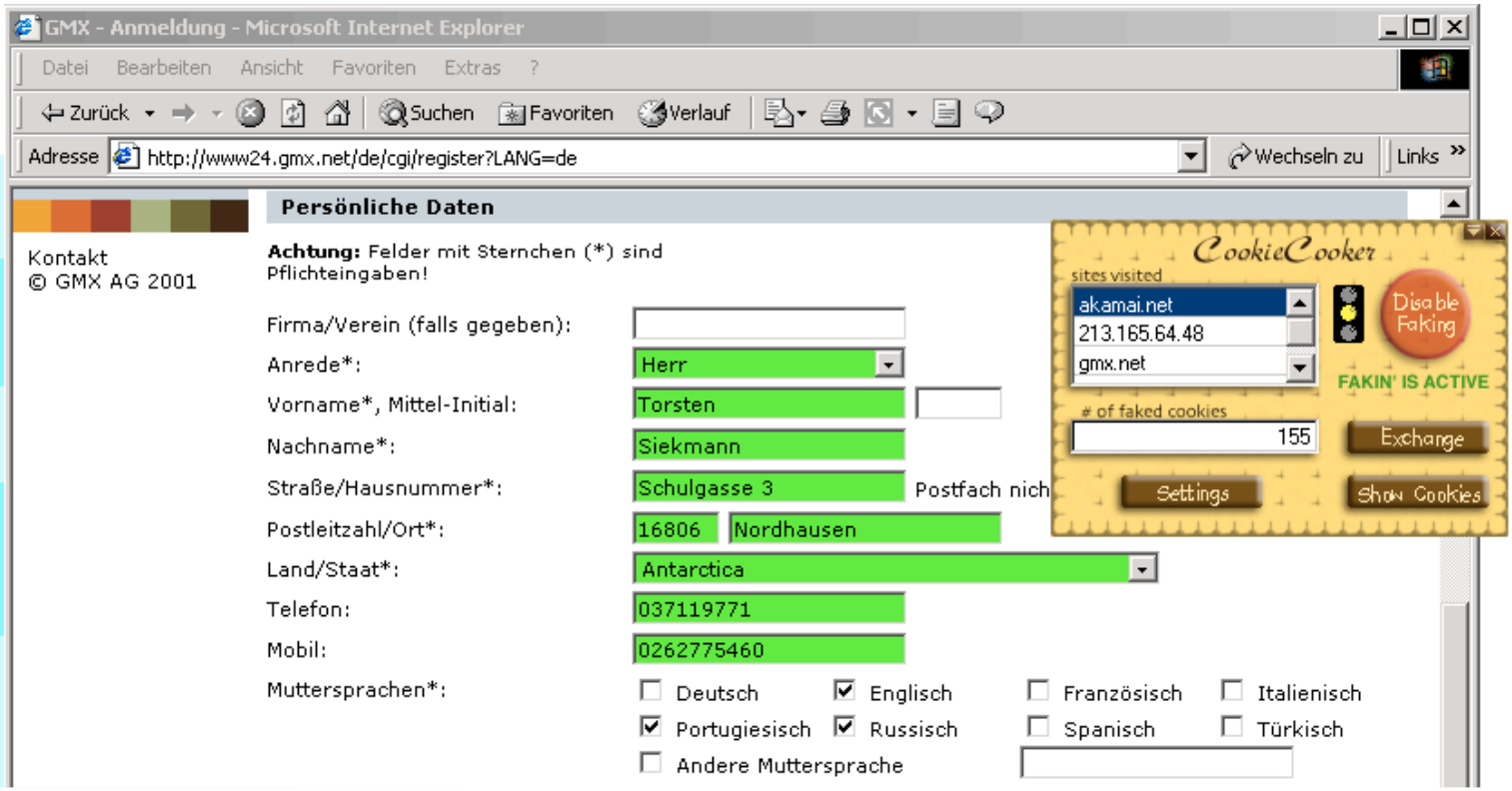
- Aktiver Schutz durch Cookie-Austausch

CookieCooker

cookie.inf.tu-dresden.de

- Idee:
  - Aktiver Schutz durch Cookie-Austausch zwischen Nutzern
  - Andere Personen surfen unter dem fremden Cookie
  - Verfälschung der Nutzerprofile
- Unterscheidung nötig zwischen nützlichen und ungewollten Cookies
- Cookie-Austausch über Peer-to-Peer-Service

- Zusätzliche Funktionen:
  - Automatisiertes Ausfüllen von Web-Formularen
    - sehr schnelles Anlegen von Free-Mail-Accounts
  - Identitätsmanagement
    - Cookie Cooker merkt sich (pseudonyme) Zugangsdaten (Name/Passwort etc.)



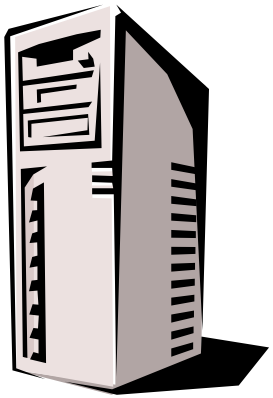
Überwachung auch ohne Cookies

- IP-Nummern

Adresse:
123.86.9.5

GET www.amazon.de
To: 195.66.15.4
From: 123.86.9.5

HTTP ...
To: 123.86.9.5
From: 195.66.15.4



Adresse:
195.66.15.4

Einschränkung:

Zuweisung dynamischer IP-Nummern bei Einwahlzugang

Überwachung auch ohne Cookies

- Überwachung durch Internet Service Provider

Beispiel:

http://www.predictivenetworks.com/

> Empfehlungen für sicheres Surfen

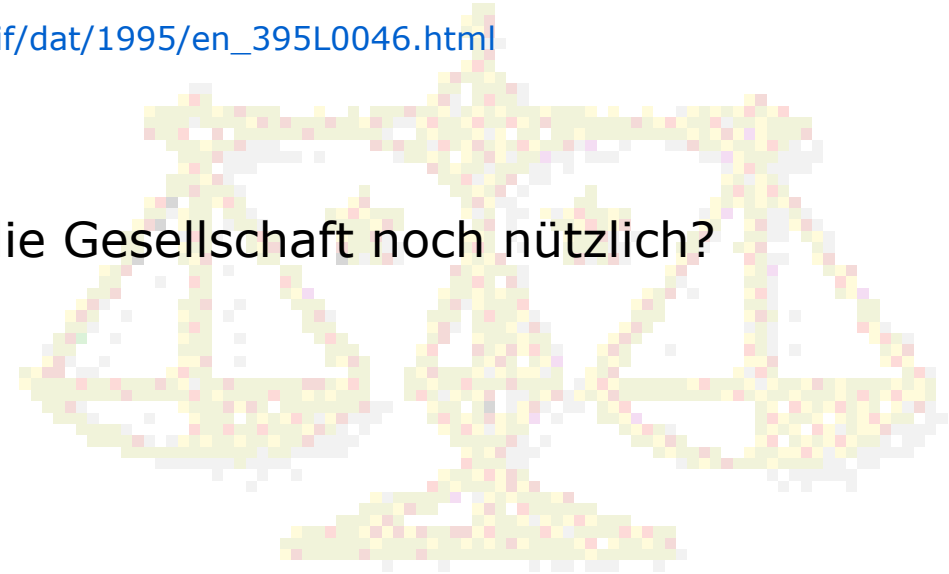
- Cookies und andere Verkettungsmerkmale deaktivieren
  - Web Server kann alle Benutzeraktivitäten verketten
  - Zusätzlicher Filter nützlich (WebWasher, JunkBuster, CookieCooker)
  - Ebenfalls filtern: »Web Bugs« (transparente 1x1-Grafiken)
- Java und JavaScript im Browser deaktivieren
  - IP-Adresse kann abgefragt und übermittelt werden
    - Teilnehmer u.U. identifizierbar durch Server
- ActiveX und andere aktive Inhalte deaktivieren
  - Unberechtigter Zugriff auf Systemressourcen (Festplatte etc.) möglich
- Profil der Dienstnutzung kann zur Beobachtung führen
  - Online-/Offline-Phasen
  - Gleicher Nutzer besucht gleiche Webseite häufiger
    - Aktionen verkettbar

> Politisches und gesellschaftliches Umfeld

- Telekommunikationsüberwachung
  - Telekommunikationsüberwachungsverordnung (TKÜV)
    - http://www.bmwi.de/Homepage/download/telekommunikation_post/TKUEV-Entwurf.pdf
  - Cybercrime Convention
    - http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm

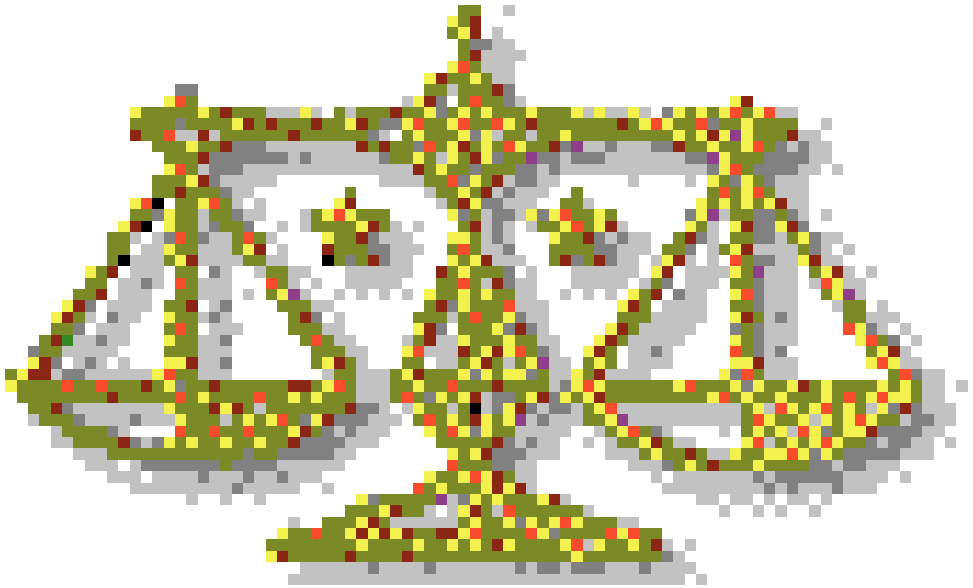
- Datenschutzgesetze
  - Neues Bundesdatenschutzgesetz (BDSG)
    - http://www.bfd.bund.de/information/bdsg_hinweis.html
  - EU-Datenschutzrichtlinie
    - http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

- Offene Frage
  - Wieviel Privatheit ist für die Gesellschaft noch nützlich?

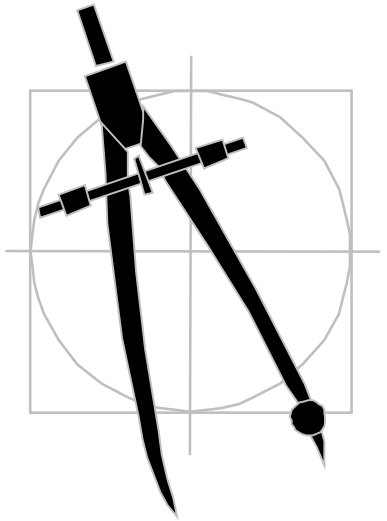


> Juristische Sicht

- Teledienstedatenschutzgesetz (TDDSG)
  - §3(4): Die Gestaltung und Auswahl technischer Einrichtungen für Teledienste hat sich an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen.
  - §4(1): 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 Möglichkeiten zu informieren.

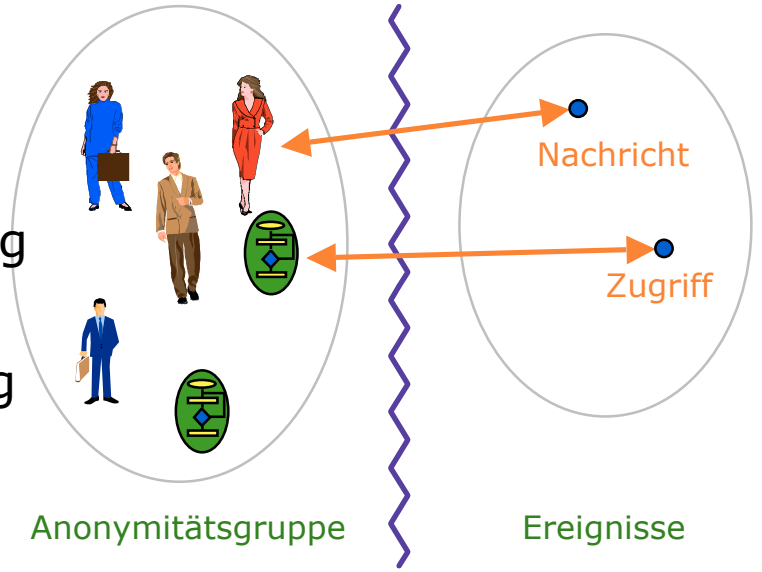


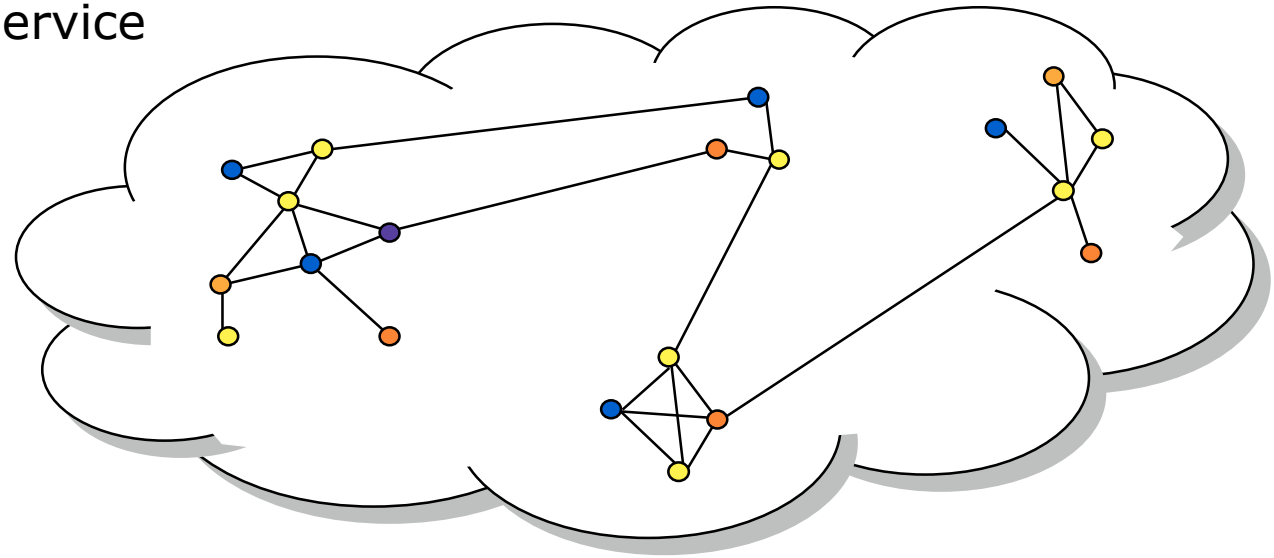
- Technischer Datenschutz
  - Systeme so konstruieren, dass unnötige Daten vermieden und nicht miteinander verkettet werden können.
- Zu verschleiern sind:
  - Adressen:
    - Sender, Empfänger, Kommunikationsbeziehung
  - Zeitliche Korrelationen:
    - Zeitpunkte, Dauer
  - Übertragenes Datenvolumen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



> 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

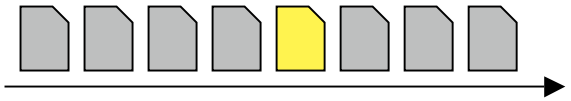




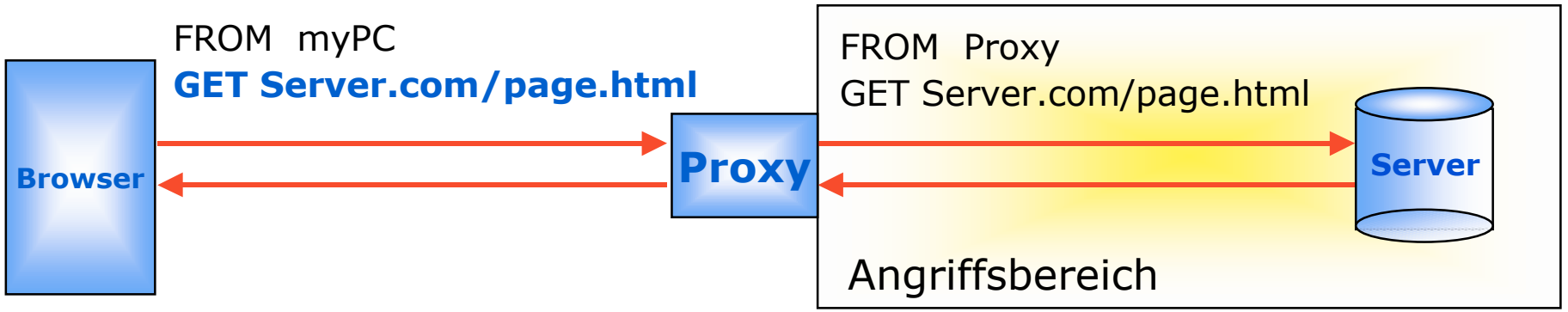
> Schwacher Schutz

- **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



> Anonymisierung von Verbindungen (HTTP, FTP)

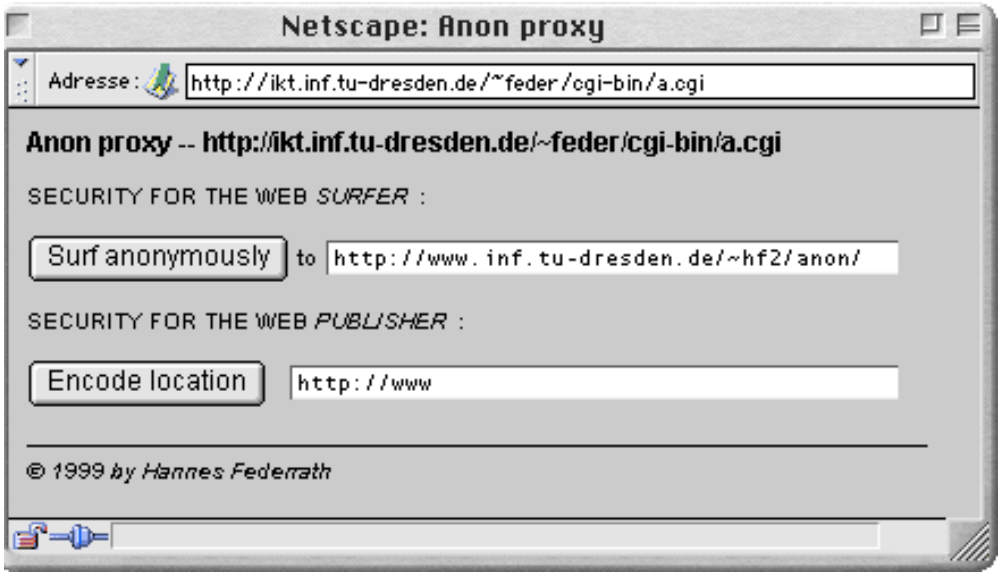
⌘ Client-Anonymität

- Einfache Proxies (teilweise mit Filterfunktion: Cookies, JavaScript, active content)
  - Anonymizer.com (Lance Cottrel)
  - 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)
  - Web-Mixe/JAP (TU Dresden/FU Berlin)

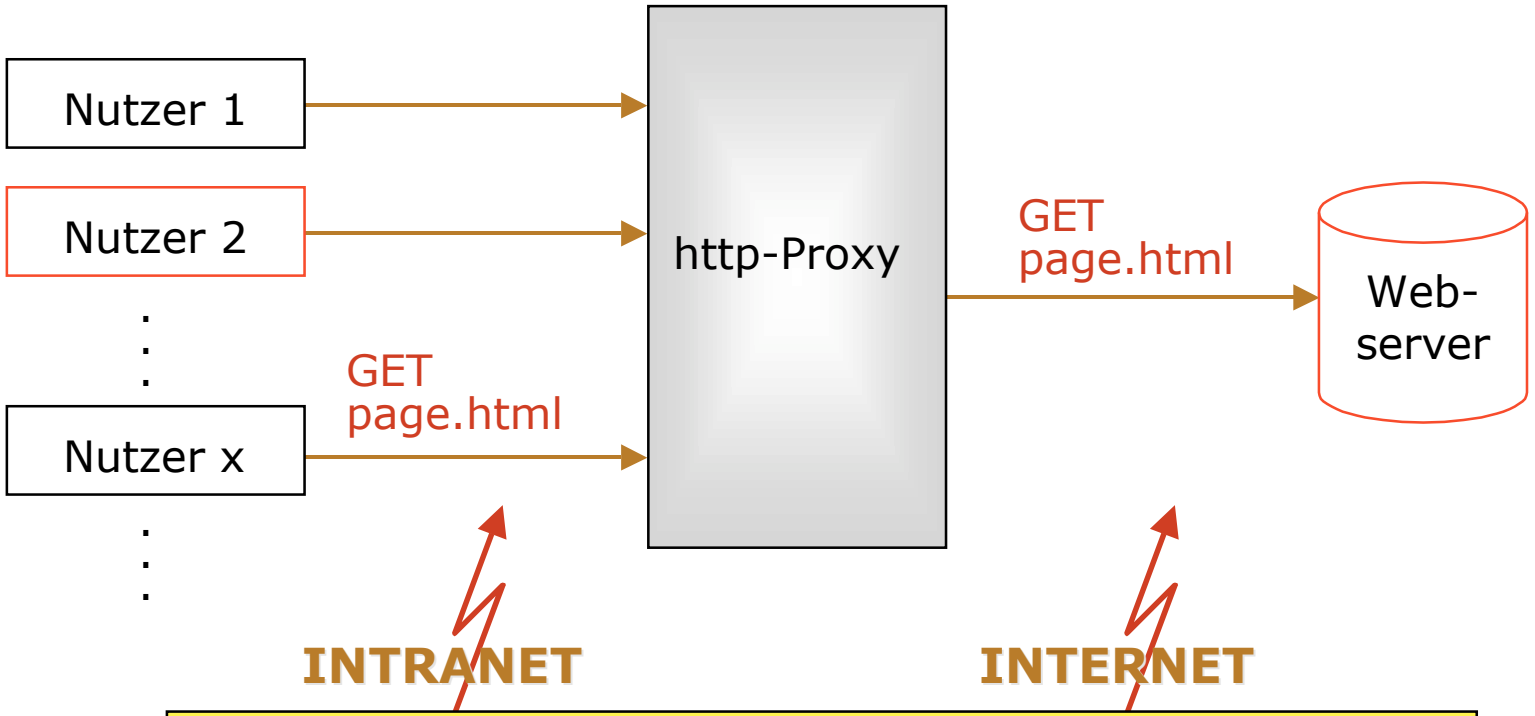
> Einfache Proxies

- 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.

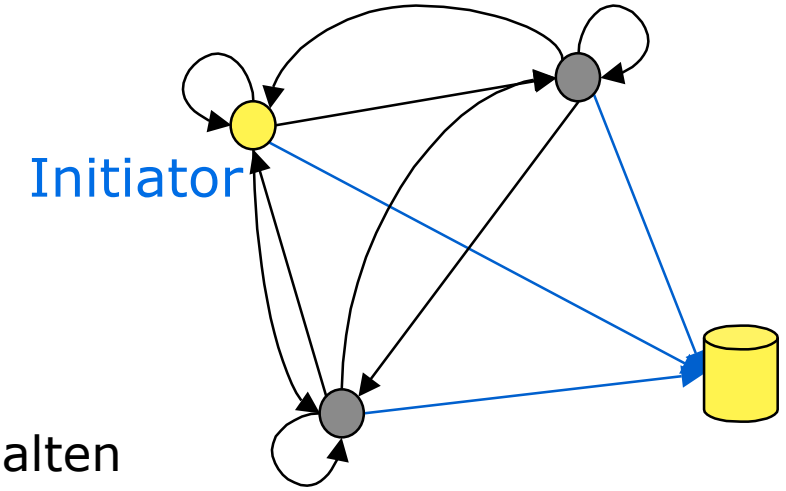
> Anonymisierung von Verbindungen (HTTP, FTP)

⌘ Client-Anonymität

- Einfache Proxies (teilweise mit Filterfunktion: Cookies, JavaScript, active content)
  - Anonymizer.com (Lance Cottrel)
  - 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
  - Crowds (Mike Reiter, Avi Rubin AT&T)
  - Onion-Routing (Naval Research Center)
  - Web-Mixe/JAP (TU Dresden/FU Berlin)

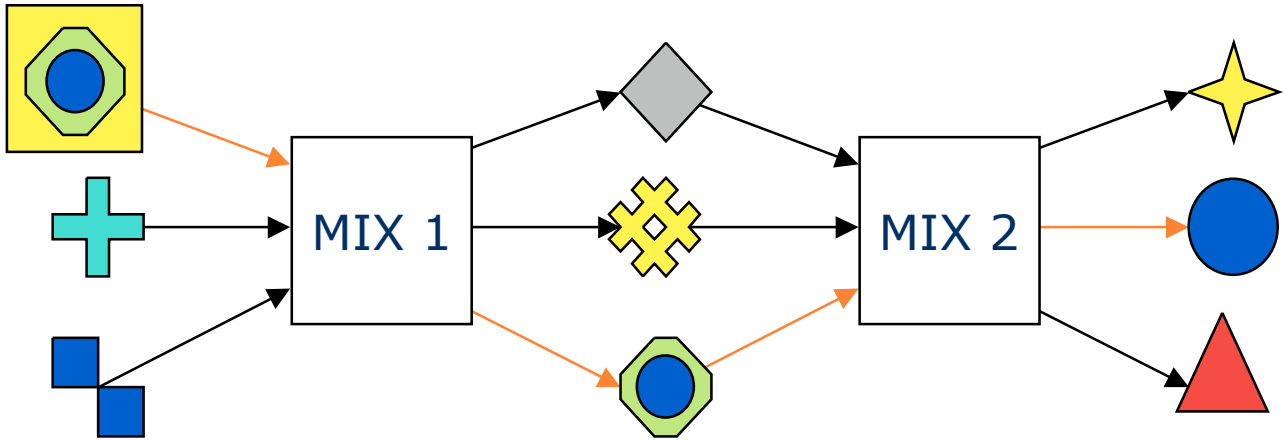
- **Webanfrage wird mit einer Wahrscheinlichkeit P direkt an Server geschickt oder alternativ (mit 1-P) an anderen Teilnehmer (Jondo)**
- **Symmetrische Verbindungsverschlüsselung** zwischen den Nutzern
  - Verkettung über Kodierung verhindern
  - Jedoch zeitliche Verkettung möglich
- Eingebettete Objekte (**Images** etc.) werden vom letzen Jondo angefordert.
  - Anfrage-Bursts unterbinden
- **Sicherheitseigenschaft:**
  Nutzer kann stets behaupten, sein Jondo habe die Anfrage zur Weiterleitung erhalten
- **Schwächen:**
  - zeitliche Korrelationen bleiben erhalten
  - Jondos können mitlesen (problematisch bei personalisierten Sites)



Mix-Netz

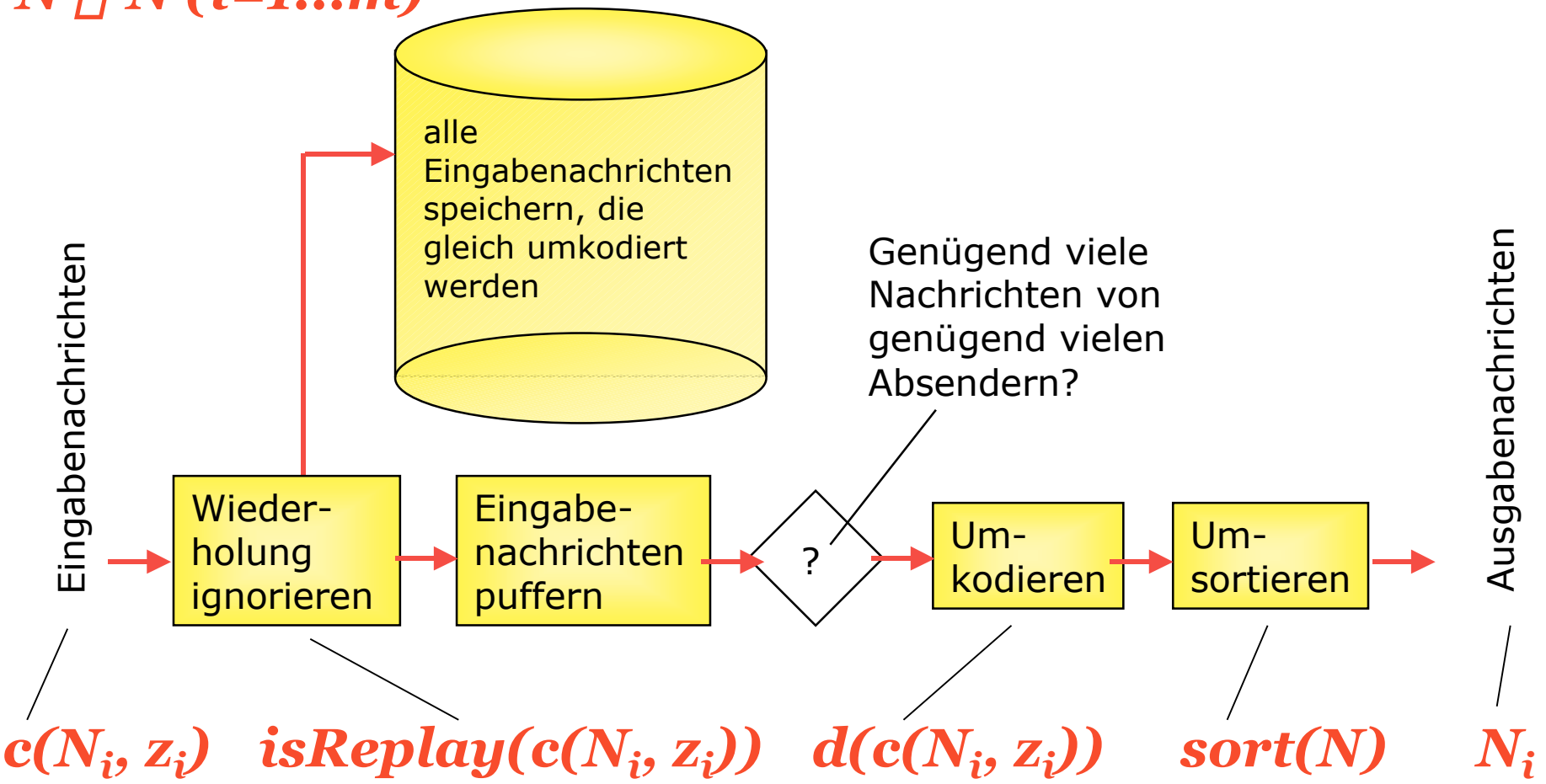
Chaum, 1981

- 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



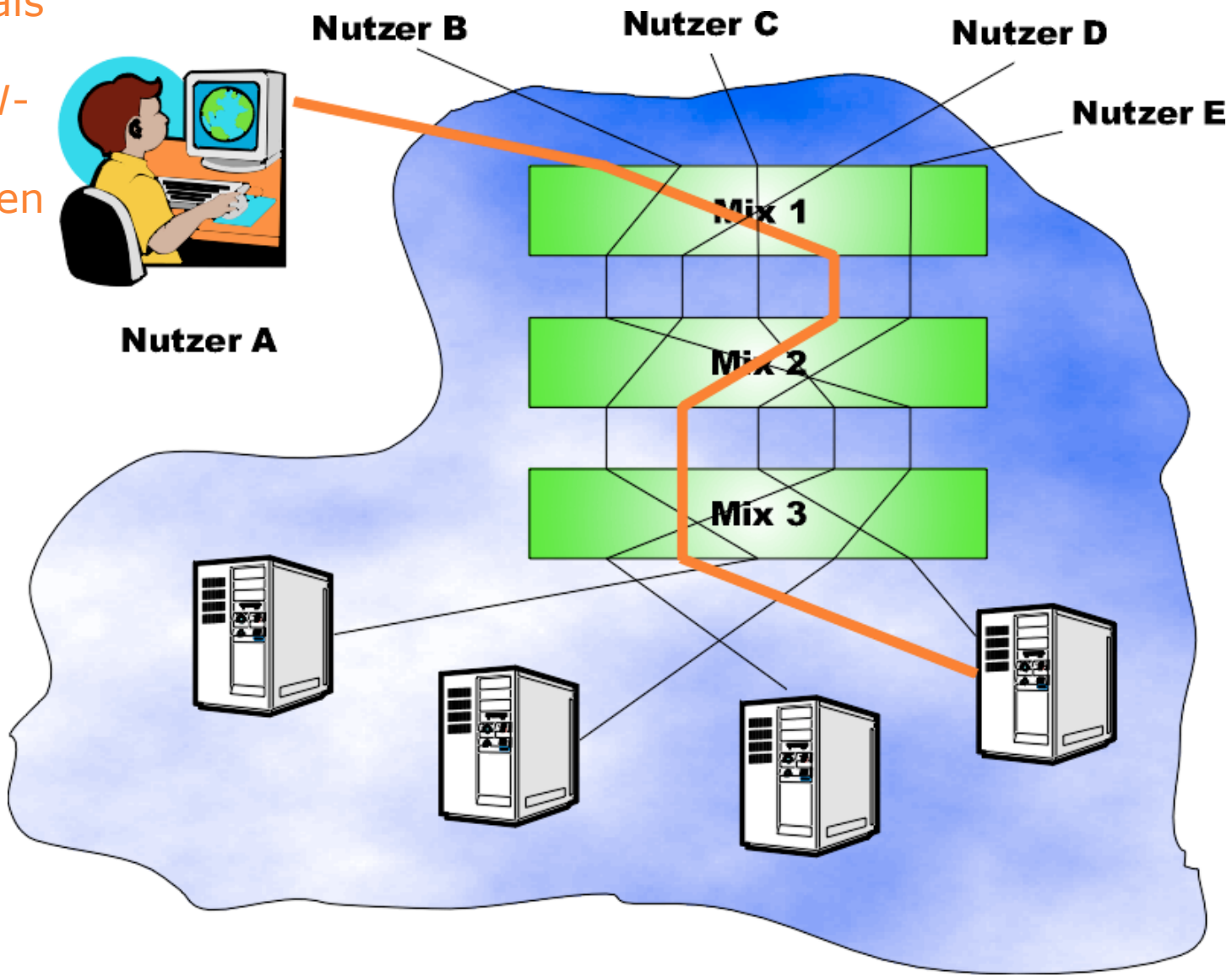
> Blockschaltbild eines Mix

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



JAP/WebMixe

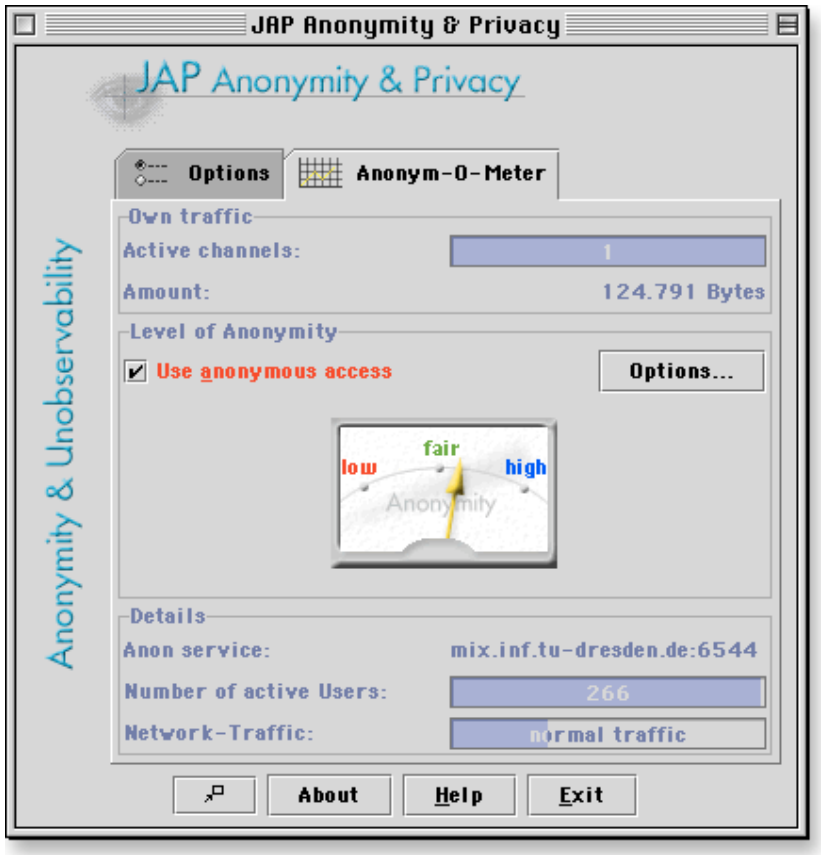
- JAP wird als Proxy für den WWW-Browser eingetragen



Technische Daten, Nutzerzahlen

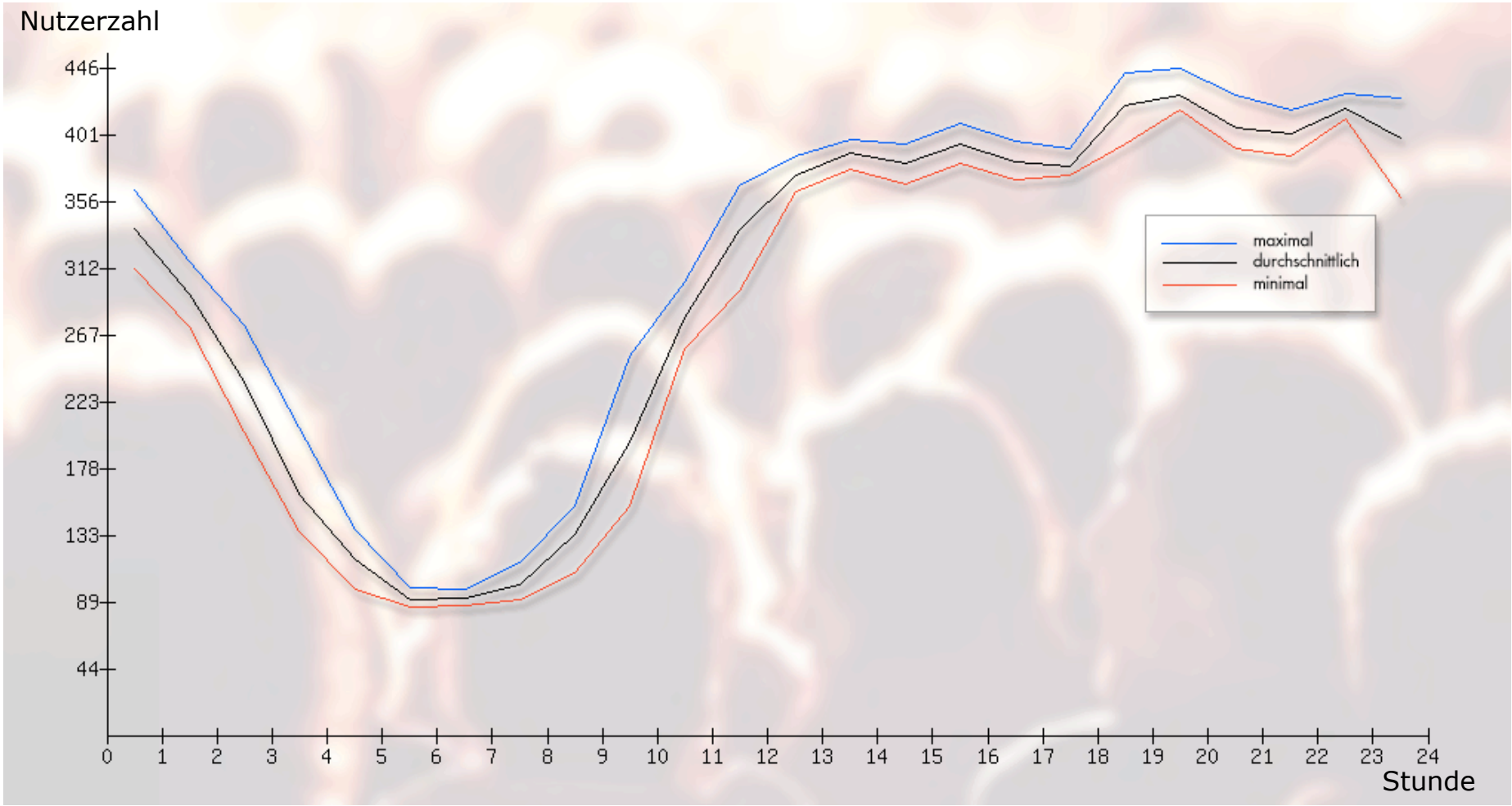
JAP.inf.tu-dresden.de

- 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. 18000 Nutzer
- Netzwerkverkehr ist zur Zeit der Hauptengpass:
  - ca. 1000 Gigabyte pro Monat
  - bei bis zu 650 Nutzern gleichzeitig online
  - zu Spitzenzeiten etwa 2000 Transaktionen (URLs) pro Minute
- 3 Mix-Kaskaden im Betrieb



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 geplant

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 Deanonymisierung ohne Massenüberwachung durchgeführt werden?
- Länder (Saudi Arabien) haben Zugang zum Dienst gesperrt
  - Forschungsfrage: Anonymisieren des Anonymisierungsdienstes


JAP
Stop Big Brother!
JAVA ANON PROXY
http://www.anon-online.de