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

Anonyme und unbeobachtbare Kommunikation im Internet

Hannes Federrath • Heinrich Langos
Freie Universität Berlin • Institut für Informatik

Stefan Köpsell
Technische Universität Dresden • Fakultät Informatik

> 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

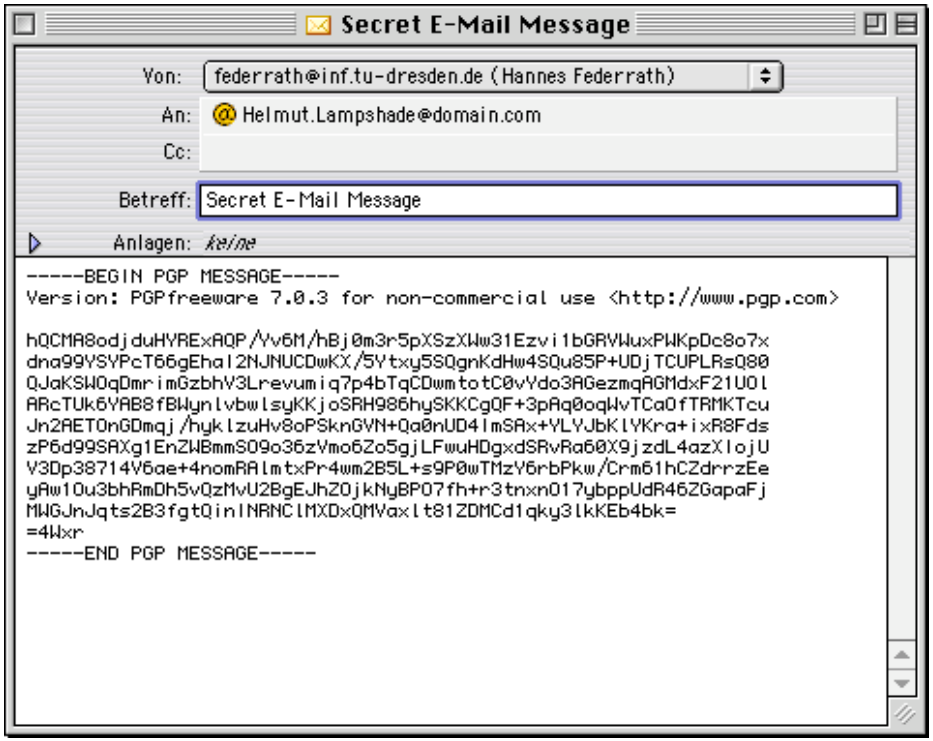
Source: http://ig.cs.tu-berlin.de/w2000/ir1/referate2/b-1a/

Vertraulichkeit; hier: Vertraulichkeit der Verkehrsdaten

- **Unbeobachtbarkeit**
  - Schutz von Sender und/oder Empfänger gegenüber allen Unbeteiligten (inkl. Netzbetreiber)
    - Niemand kann Kommunikationsbeziehungen verfolgen.
    - Unbeobachtbares Senden und/oder Empfangen von Nachrichten
- **Anonymität**
  - Schutz der Identität zusätzlich auch gegenüber dem Kommunikationspartner
    - Anonymität als *Sender* von Nachrichten
    - Anonymität als *Empfänger* von Nachrichten
- **Unverkettbarkeit**
  - Ereignisse werden vom Angreifer bzgl. des Senders und/oder Empfängers als unabhängig erkannt

Hilft Verschlüsselung?

⌘ Verschlüsseln hilft gegen Ausspähen der *Inhalte*



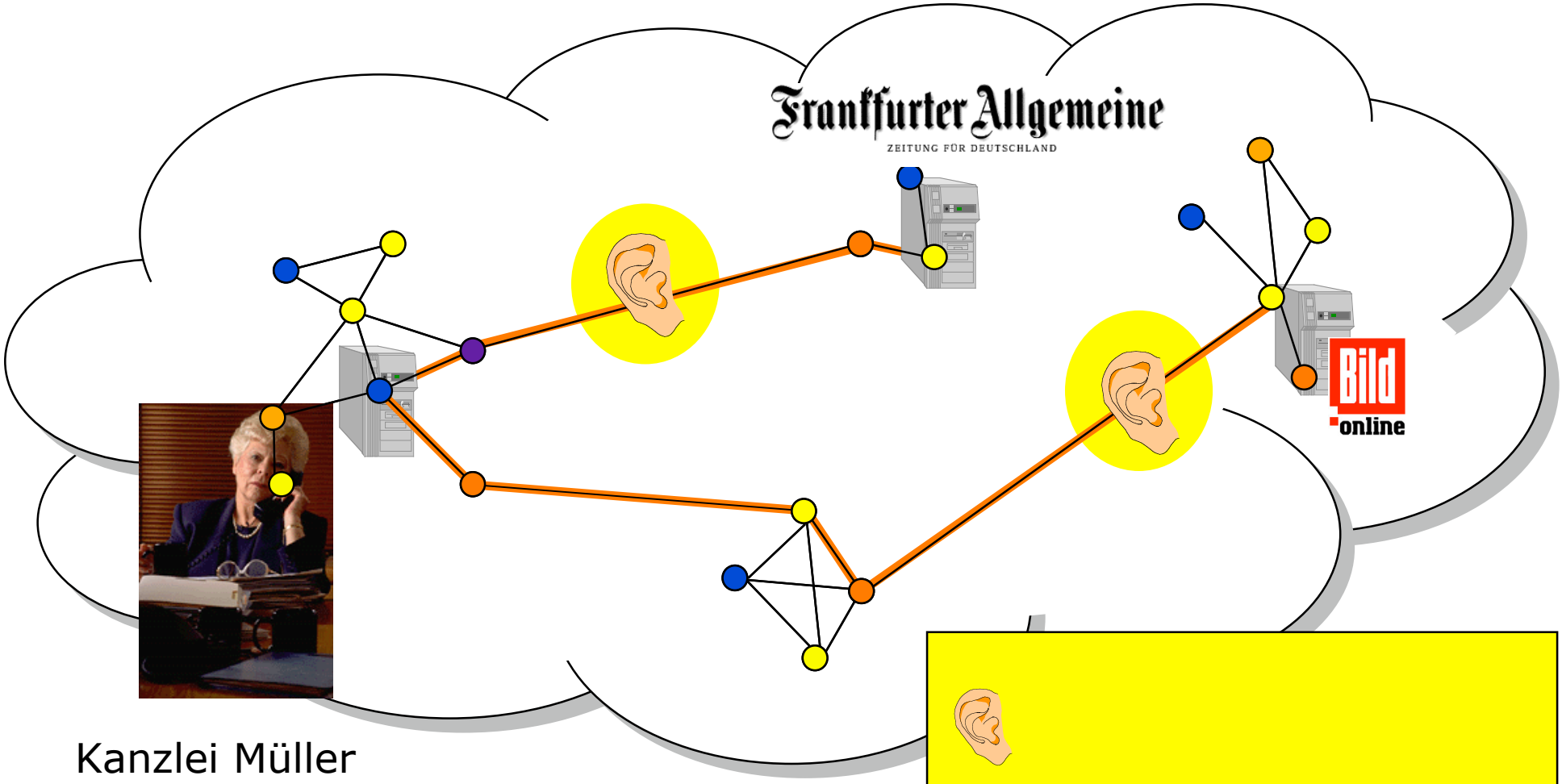
Trotzdem PGP verwenden!

Pretty Good Privacy

http://www.pgp.com

Verschlüsseln hilft überhaupt nichts gegen Beobachtung von Kommunikationsbeziehungen

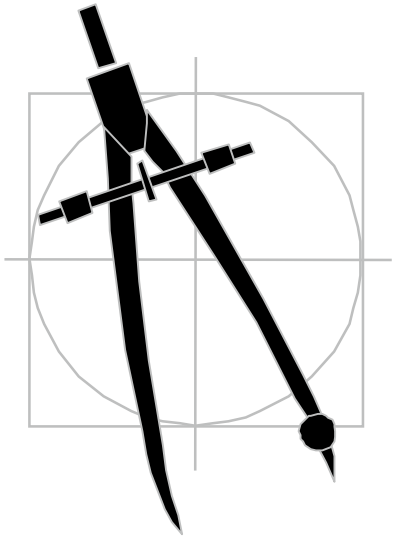
> Warum genügt Verschlüsselung nicht?



Kanzlei Müller
spezialisiert auf
Firmenfusionen

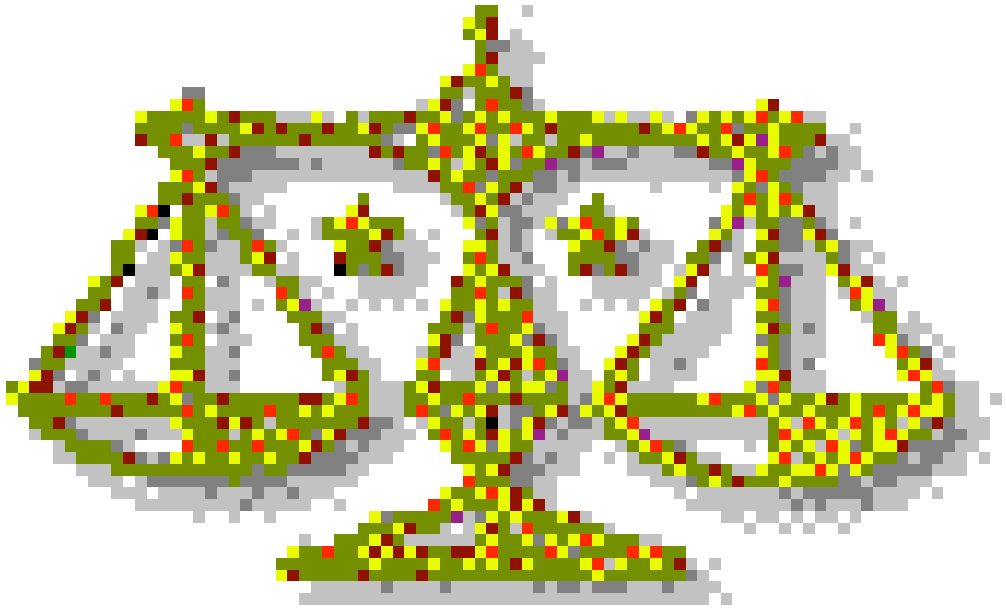
Beobachtung von
Kommunikationsereignissen
lässt auf Inhalte schließen

- 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



⌘ Teledienstedatenschutzgesetz (TDDSG)

- § 4 Absatz 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.

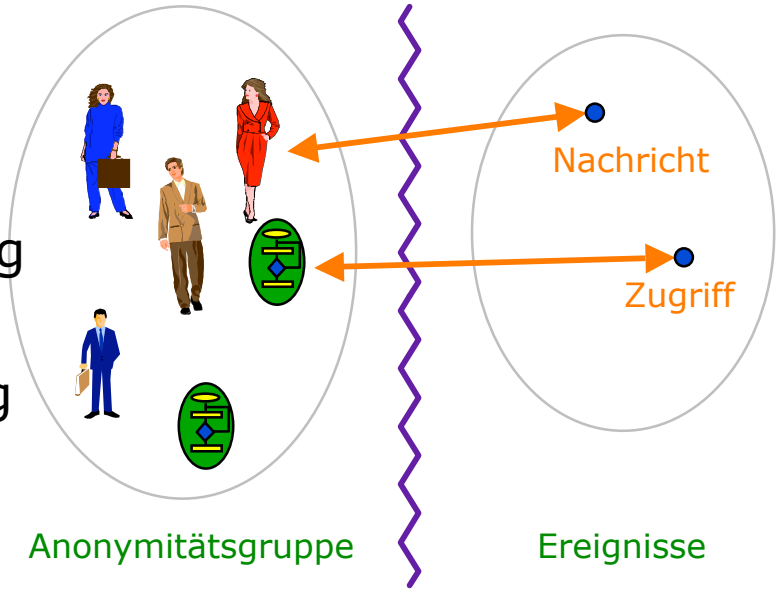


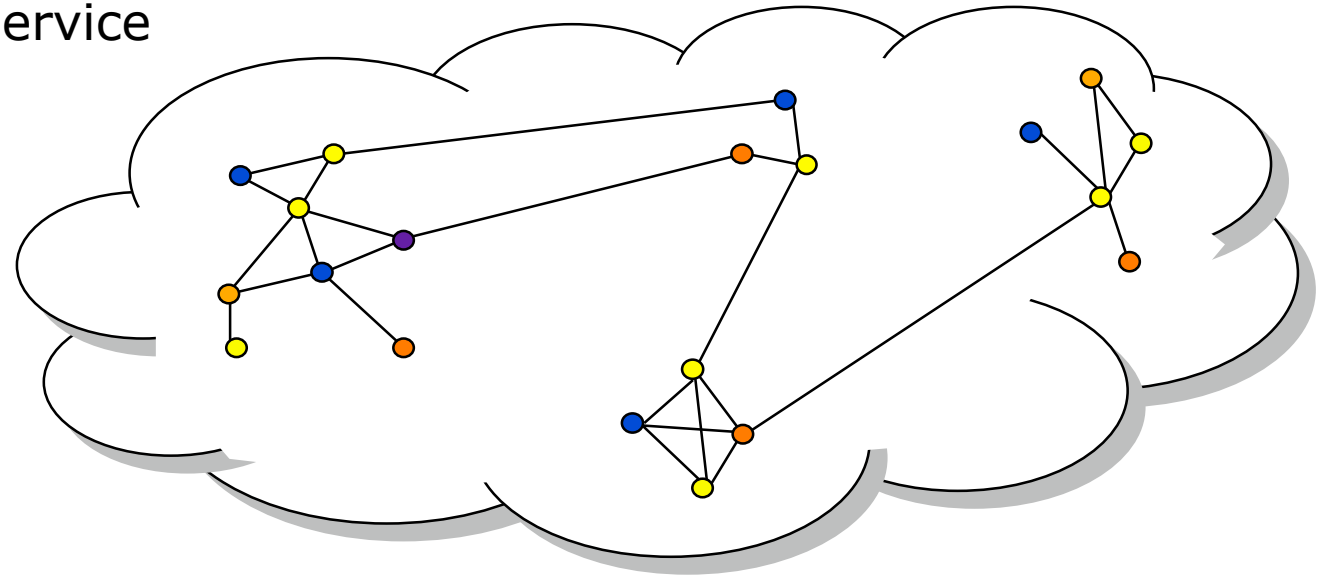
> Politisches und gesellschaftliches Umfeld

- 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

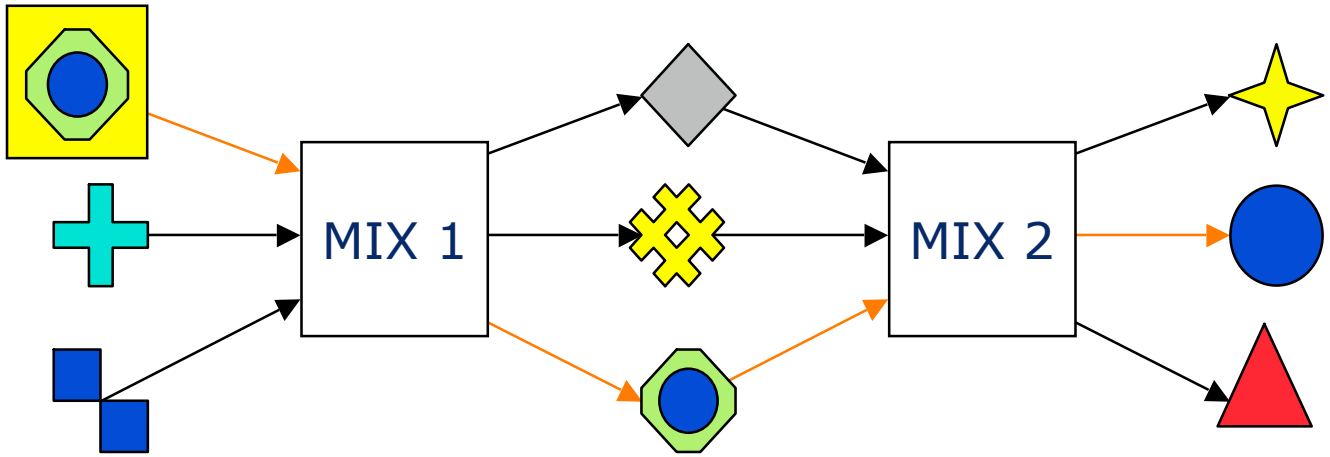




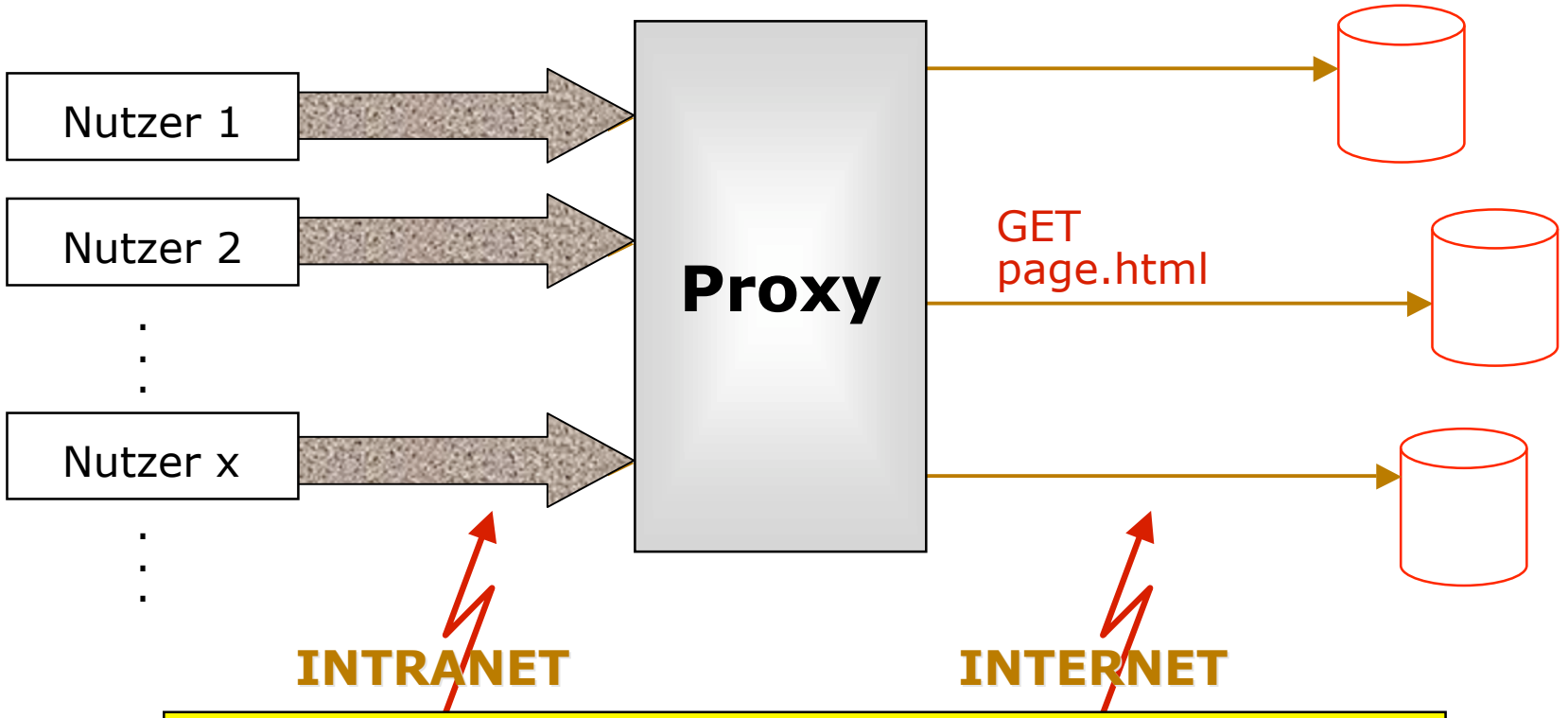
Mix-Netz

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



> Mixe: Warum überhaupt umkodieren?



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

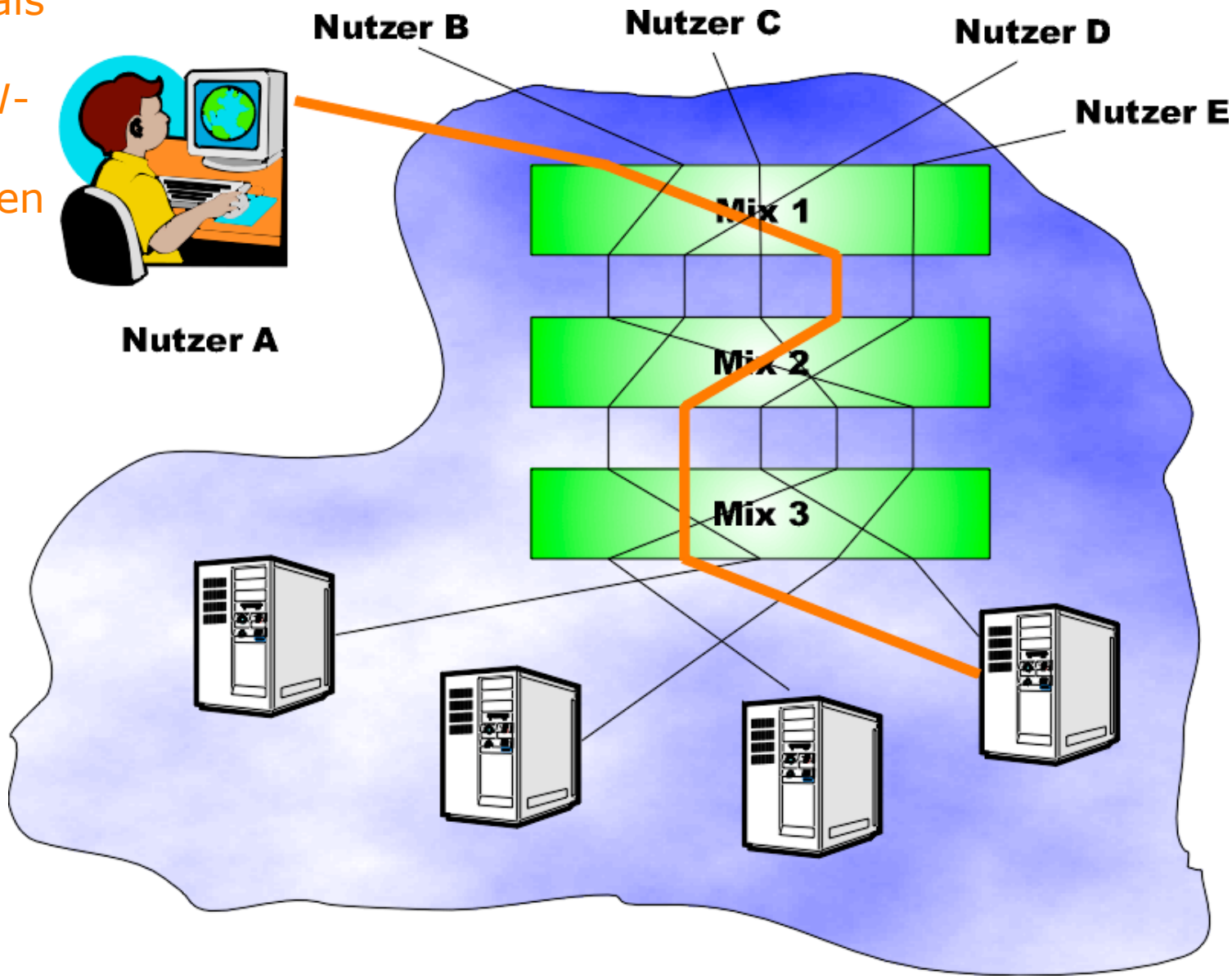
Verschlüsselung zwischen Browser und Proxy verhindert Korrelation über »Aussehen«, aber nicht über Nachrichtenlänge und Zeit und hilft nichts gegen den Proxy.

> Mixe: Warum mehr als ein Mix?

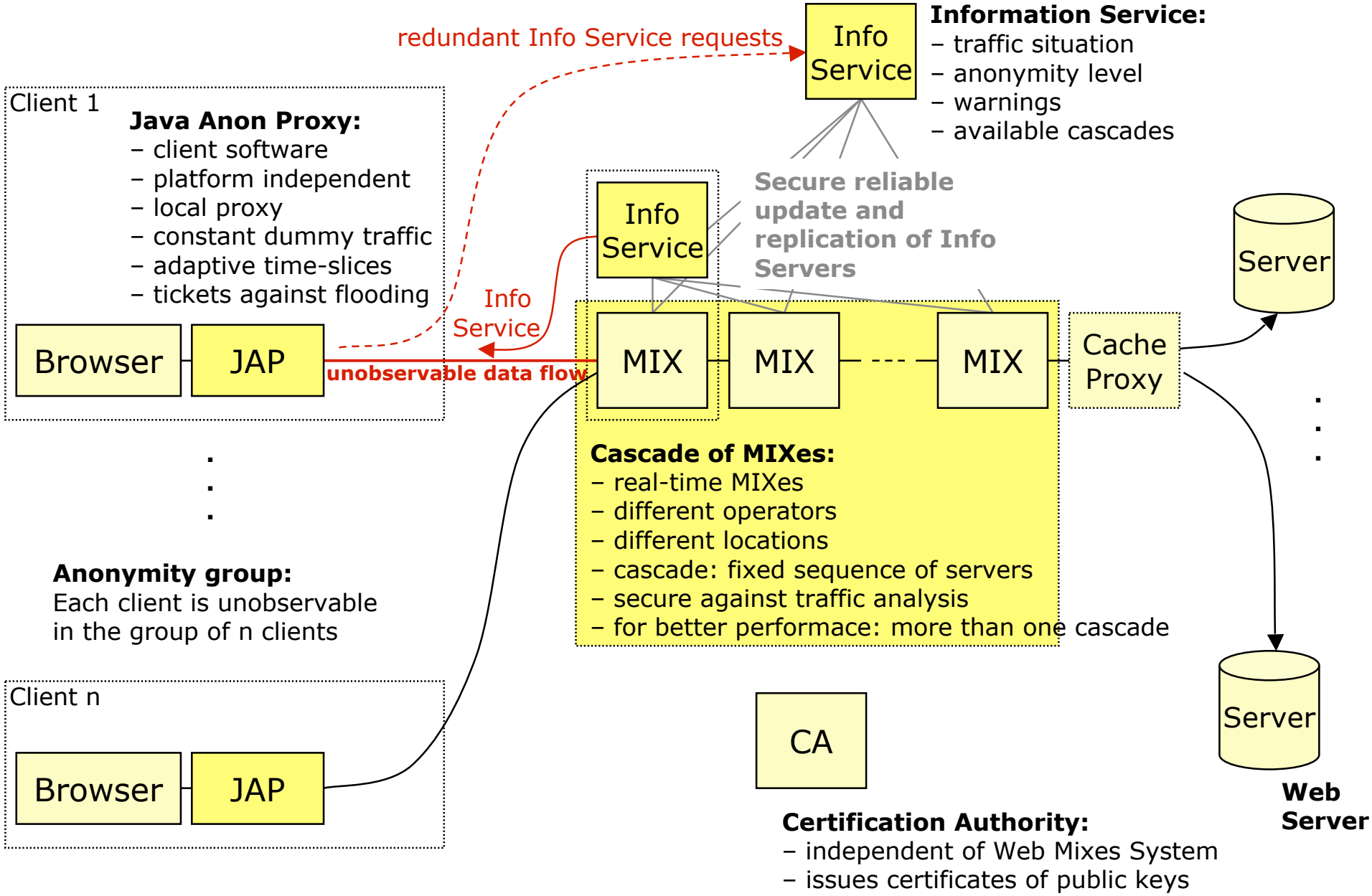
- Schutzziel: Auch Mix soll nicht beobachten können
  - Ein einzelner Mix kennt jedoch E-A-Zuordnung
- Verwende mindestens zwei Mixe
  - erster Mix kennt Sender
  - letzter Mix kennt Empfänger
- Allgemein:
  - Verwende so viele Mixe, dass sich in der Mix-Kette wenigstens ein Dir vertrauenswürdiger Mix befindet
- Praxis:
  - Je mehr Mixe verwendet werden, umso häufiger muss umkodiert werden und es steigt die Verzögerungszeit.
  - Es genügt, wenn ein einziger Mix tatsächlich vertrauenswürdig ist.
  - Lieber sorgfältig wenige Mixe auswählen.
  - Derzeit verwendet man wenigstens drei, besser fünf Mixe, aber das ist rein subjektiv.

> JAP/WebMixe

- JAP wird als Proxy für den WWW-Browser eingetragen



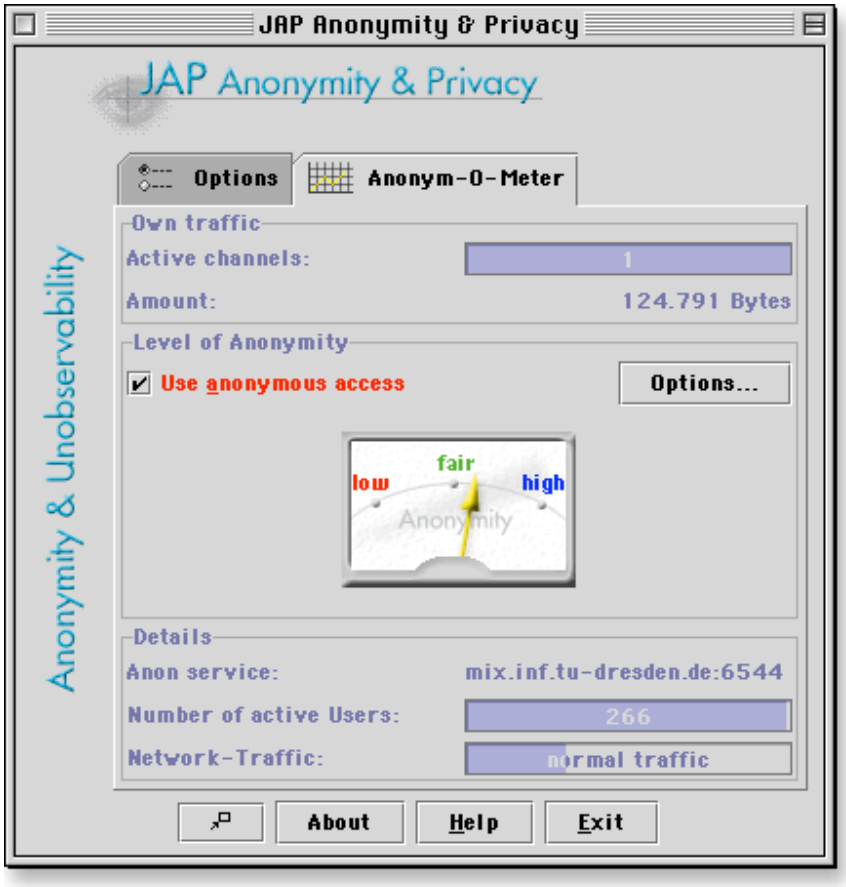
> WebMixe: Architektur



>> JAP: 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



Positive Erfahrungen

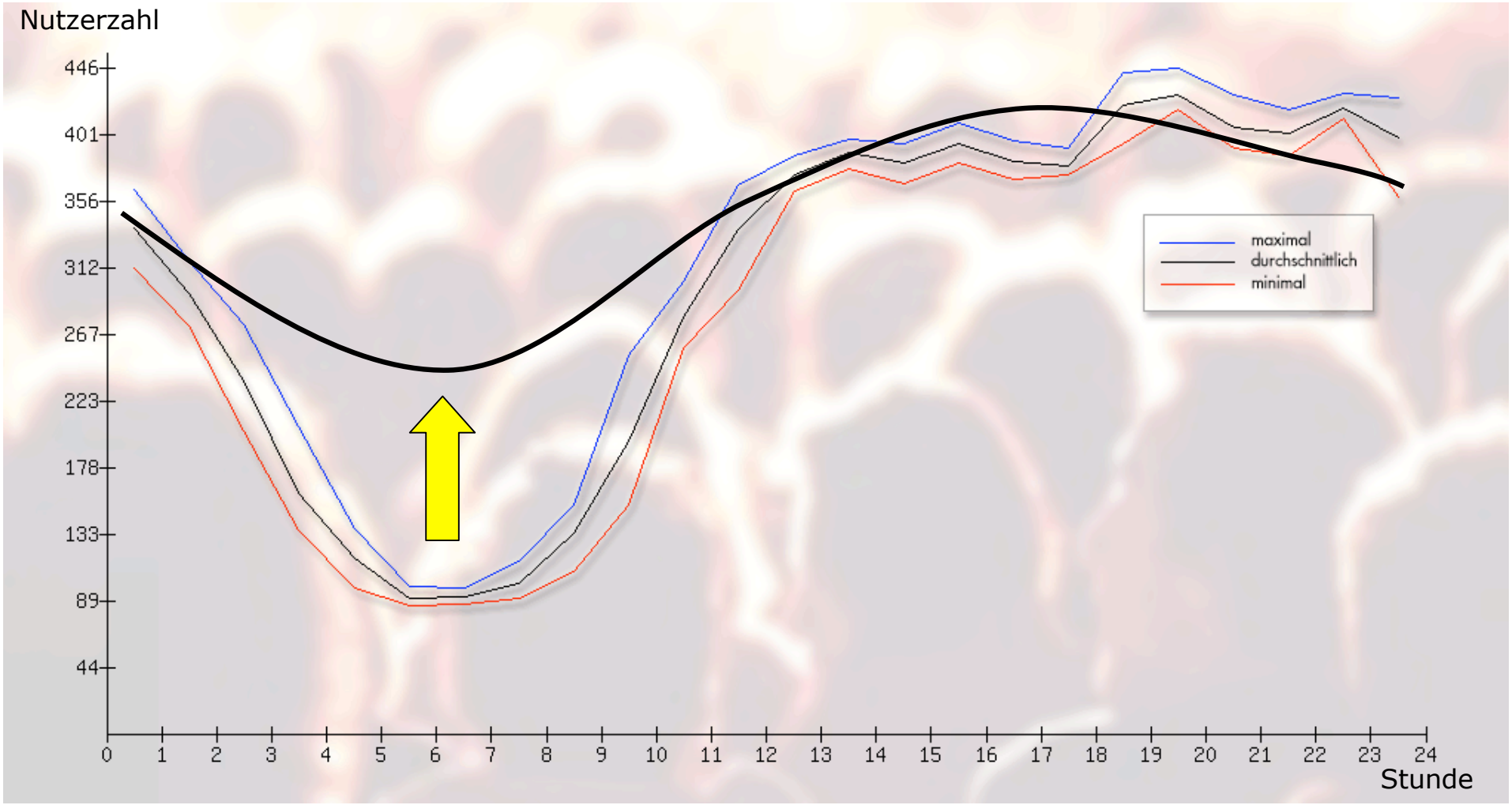
- Vorstellung auf der CeBit 2001 und 2002
  - Im Gegensatz zu 1997 wird heute nicht mehr gefragt, wogegen man sich eigentlich schützen soll.
- Größeres Interesse am Datenschutz und im Bewusstsein um Bedrohungen
  - Hohe Bereitschaft, praktikable Lösungen zum Selbstdatenschutz einzusetzen
- Kommerzielles 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 Enttarnung ohne Massenüberwachung durchgeführt werden?
- Länder (Saudi Arabien) haben Zugang zum Dienst gesperrt
  - Forschungsfrage: Anonymisieren des Anonymisierungsdienstes

Nutzung

⌘ Typischer Verlauf der Nutzerzahl eines Tages



Analyse der missbräuchlichen Benutzung von JAP

- Wie ist eine Anfrage aufgebaut?
  - Von einem Webserver mitprotokollierte IP-Adresse des JAP-Dienstes, Datum und genaue Uhrzeit der missbräuchlichen Nutzung
  - Meist kurze Angabe des Verdachts
    - Kreditkartenbetrug,
    - Computerbetrug,
    - Datenveränderung,
    - Computersabotage,
    - Beleidigung,
    - Verleumdung,
    - Morddrohung,
    - Abruf kinderpornographischer Inhalte
  - Entweder richterliche Anordnung, »Gefahr im Verzug« oder Voranfrage

Skizze der Antwort

Mit dem Schreiben vom dd.mm.jj fordern Sie die TU Dresden auf, Auskunft über die Verbindungsdaten für die IP-Adresse xx.yy.zz für den Zeitpunkt dd.mm.jj, hh:mm.ss Uhr zu geben. Dazu können wir Ihnen folgendes mitteilen:

Der von Ihnen erwähnte Server ist Teil eines Forschungsprojektes, das gemeinsam von der TU Dresden, Fakultät für Informatik, sowie dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein betrieben wird. Ziel des vom Bundeswirtschaftsministerium geförderten Projekts ist es, anonyme und unbeobachtbare Webzugriffe zu realisieren (http://anon.inf.tu-dresden.de/). Dabei geht es darum, die Vorschriften des Teledienstedatenschutzgesetzes (TDDSG) bzw. des Mediendienste-Staatsvertrages (MDStV) umzusetzen, die verlangen, dass Diensteanbieter den Nutzern die anonyme oder pseudonyme Nutzung ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 4 Abs. 6 TDDSG bzw. § 13 Abs. 1 MDStV).

Dabei wird schon auf technischer Ebene die Zuordnung von IP-Adressen zu einzelnen Nutzern oder zu sonstigen identifizierenden Merkmalen vermieden. Aus diesem Grund liegen hier keine Daten vor, über die aufgrund des richterlichen Beschlusses nach § 12 FAG Auskunft gegeben werden könnte.

Wir bedauern, Ihnen keine weiterführenden Hinweise bzgl. der Identität der Benutzer geben zu können.

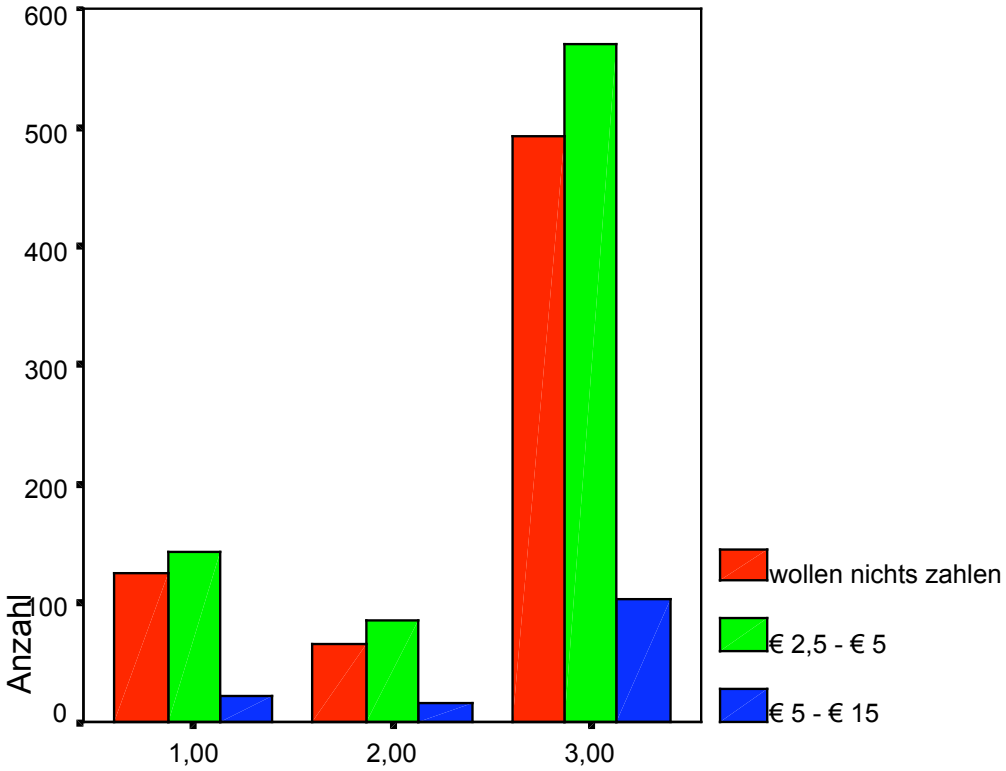
Analyse der missbräuchlichen Benutzung von JAP

- Umfang des bekannten Missbrauchs (Stand: September 2002)
  - 17 Anfragen deutscher Strafverfolgungsbehörden (Polizei, Staatsanwaltschaft)
  - 1 Anfrage einer engl. Polizeidienststelle (Verdacht auf Hackerangriff)
  - 15 Anfragen von Privater Seite (Störung von Chat-Foren, verdächtige Bestellungen, Hackerangriffe)
- Umfang der JAP-Nutzung (Stand: Ende Juli 2002)
  - Etwa 200.000 geschätzte Downloads
  - Etwa 1,2 Millionen JAP-Nutzungen in 13 Monaten (täglich etwa 3100 unterschiedliche Nutzer)
  - Monatliches Transfervolumen 3 Terabyte
  - Spitzenwert etwa 4000 Transaktionen pro Minute

Nutzerbefragung

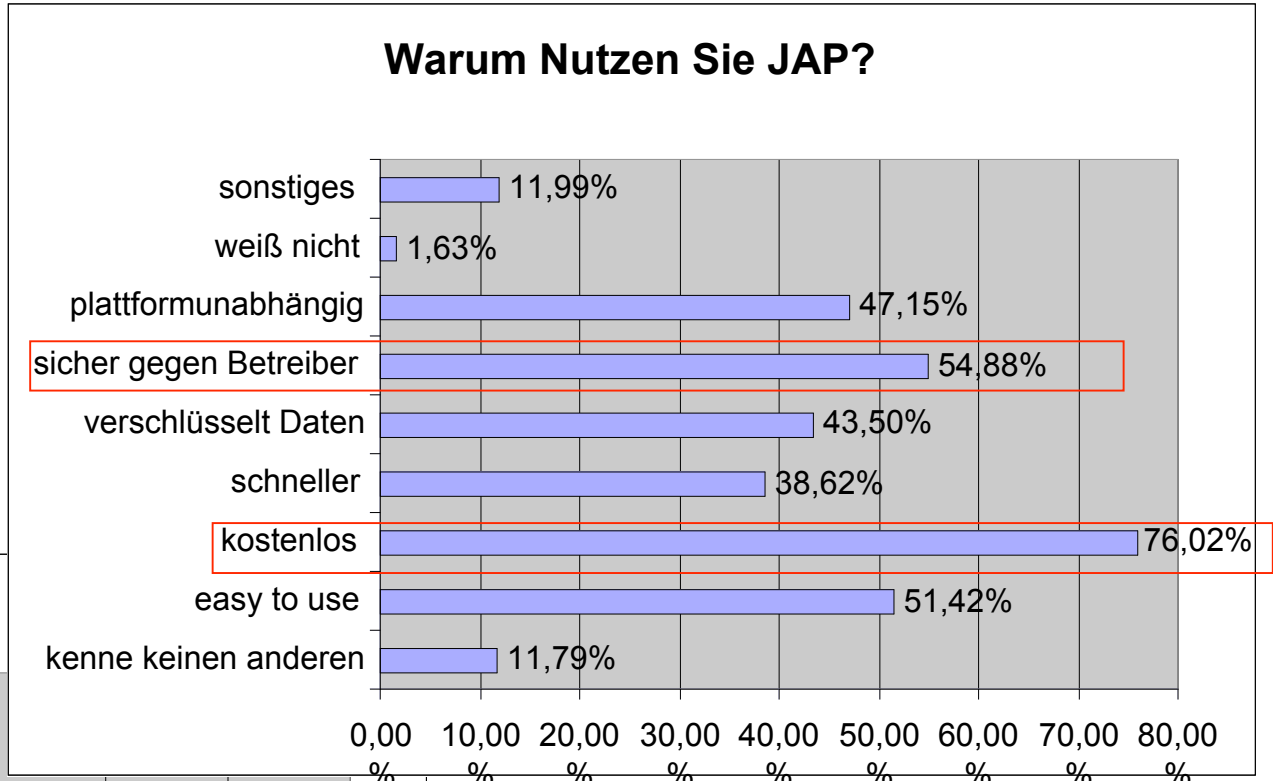
- Zahlungsbereitschaft
  - Rund 40% sind grundsätzlich nicht bereit, überhaupt etwas zu bezahlen.
  - Rund 50% sind bereit zw. € 2,5 und € 5 zu bezahlen
  - Rund 10% sind bereit auch mehr als € 5 zu bezahlen

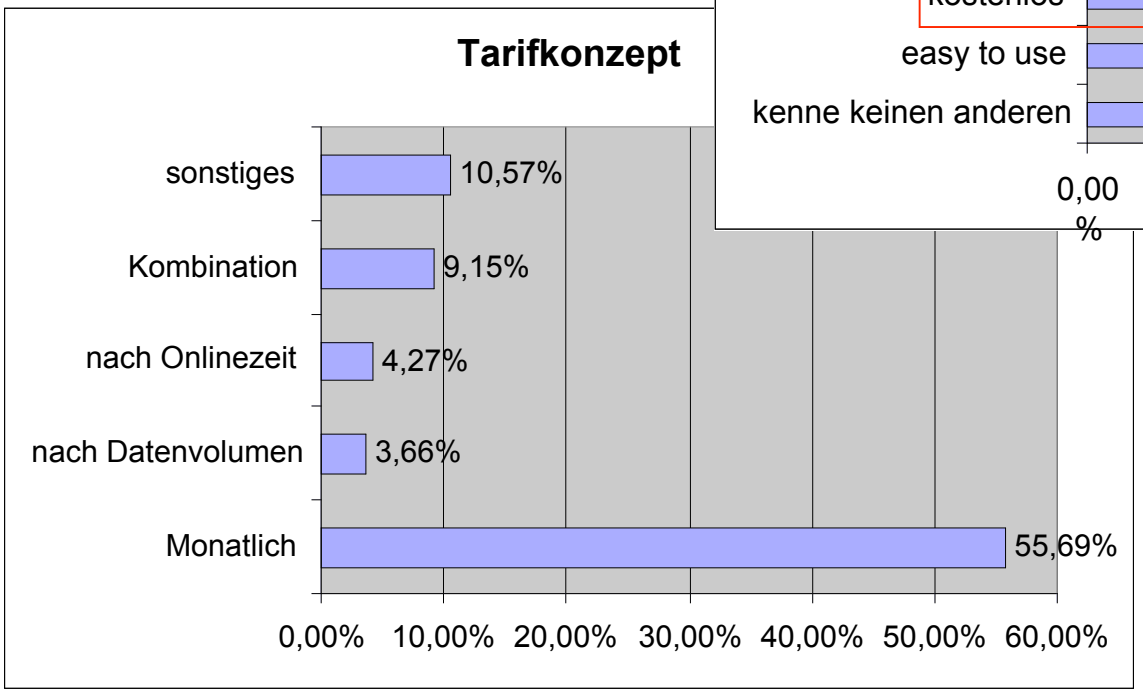
- 1800 Befragte haben freiwillig Internet-Fragebogen ausgefüllt



Nutzerbefragung

- Gründe für JAP-Nutzung
- Wunschtarif





CookieCooker

cookie.inf.tu-dresden.de

- Filter software für Cookies
  - ähnlich JunkBuster und WebWasher

- Aktiver Schutz durch Cookie-Austausch

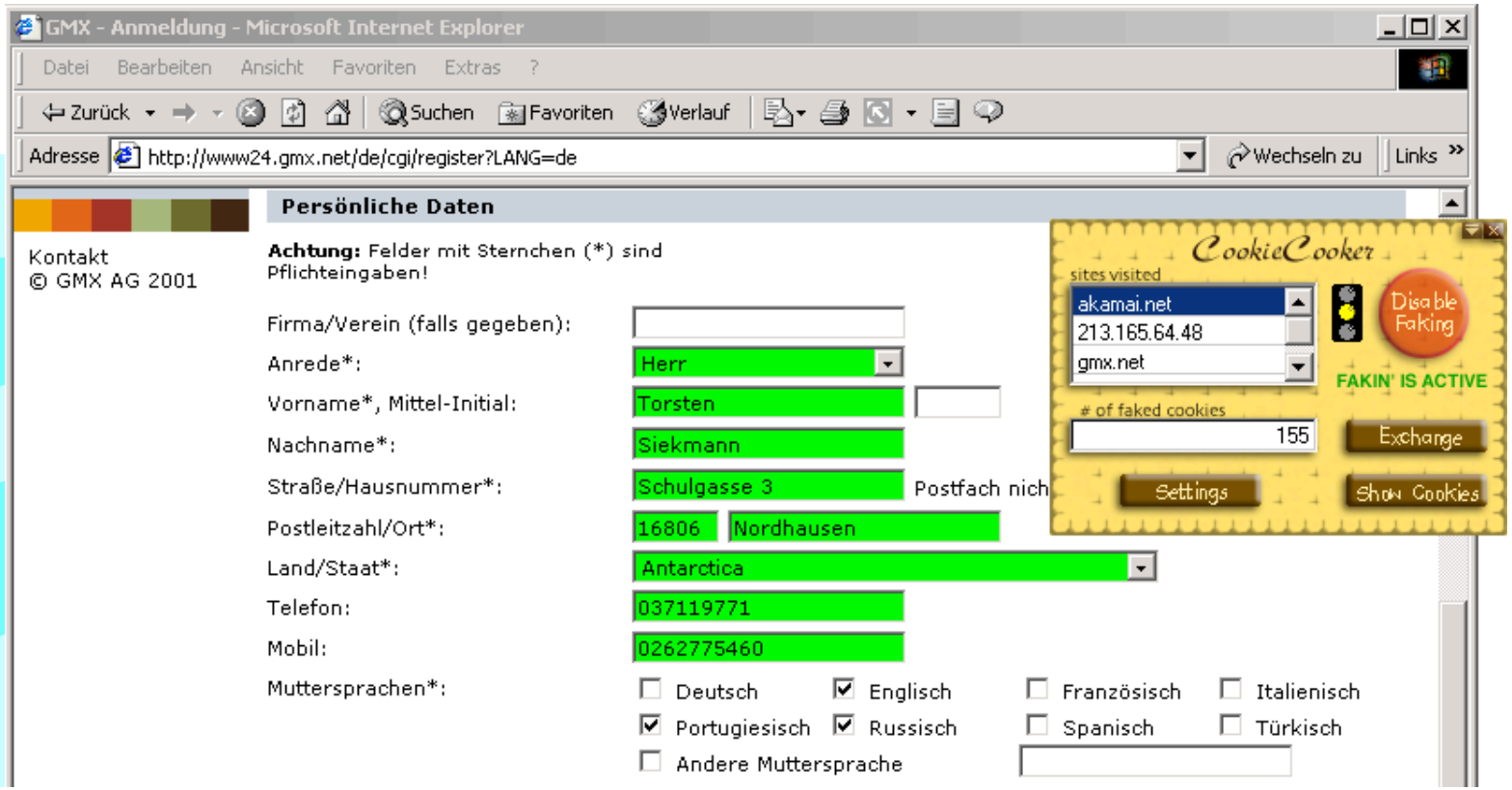
- Identitätsmanager

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.)



JAP Website

JAP Anonymity & Privacy

ANONYMITY IS NOT A CRIME

Kostenloser Download von JAP

http://jap.inf.tu-dresden.de

Weitere Informationen zur Anonymität im Internet

http://www.inf.tu-dresden.de/~hf2/anon/