Privacy Enhanced Technologies

Methods -- Markets -- Misuse

Hannes Federrath

University of Regensburg · Information Systems · Management of Information security

Protection Goals

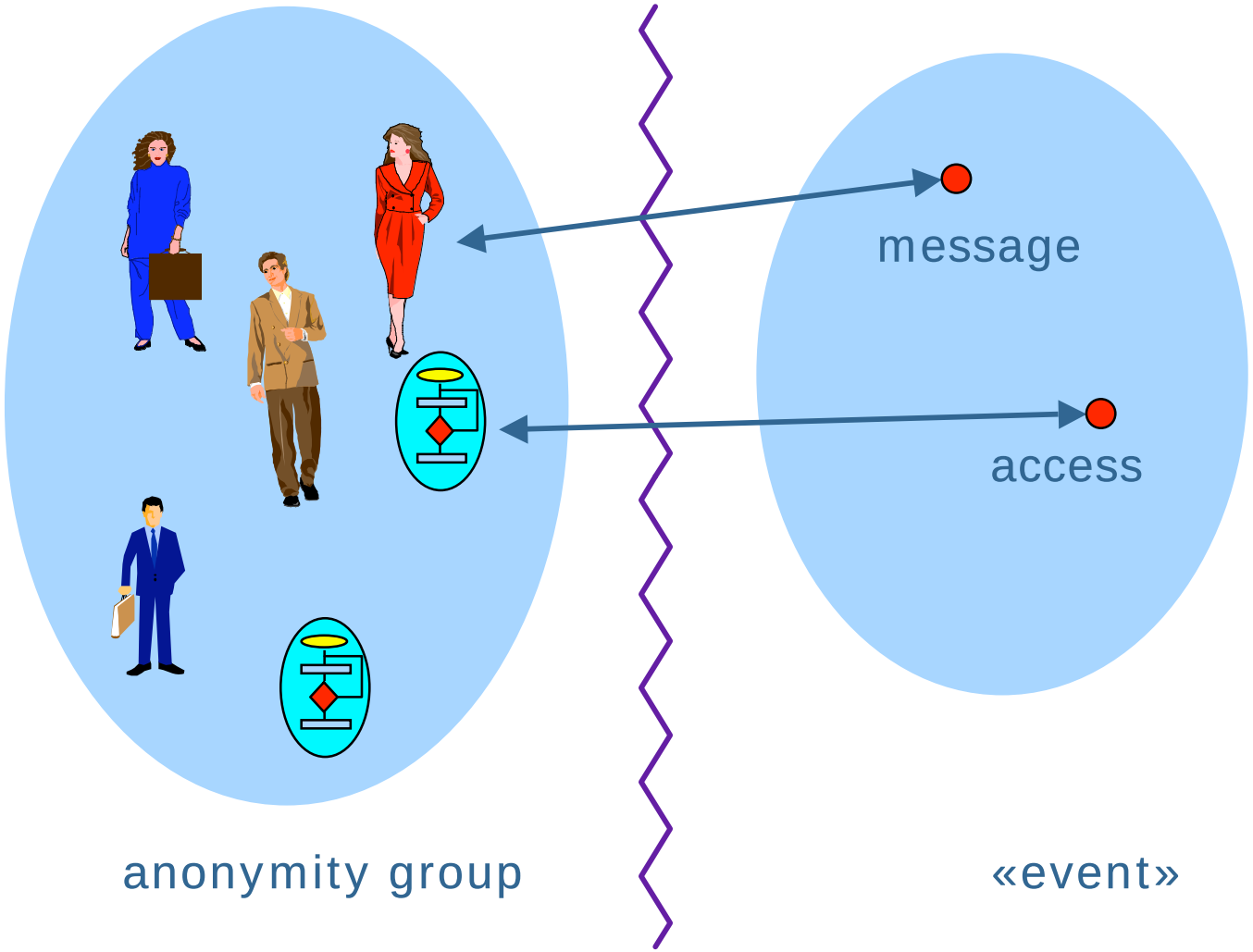
Subject of communication WHAT?	Circumstances of comm. WHEN?, WHERE?, WHO?
Confidentiality Contents	**Anonymity** **Unobservablity** Sender, Location, Recipient
Integrity Contents	**Accountability** **Legal Enforcement** Sender, Billing, Recipient
Availability	

Protection Goals

Subject of communication WHAT?	**Circumstances of comm. WHEN?, WHERE?, WHO?**
Confidentiality	**Anonymity Unobservablity**
Contents	**Sender** **Location** **Recipient**

- Protection goals — confidentiality
  - Protection of the identity of a user while using a service
    - Anonymity in counseling services
  - Protection of the communication relations of users
    - Users may know identity of each other

Anonymity and unobservability



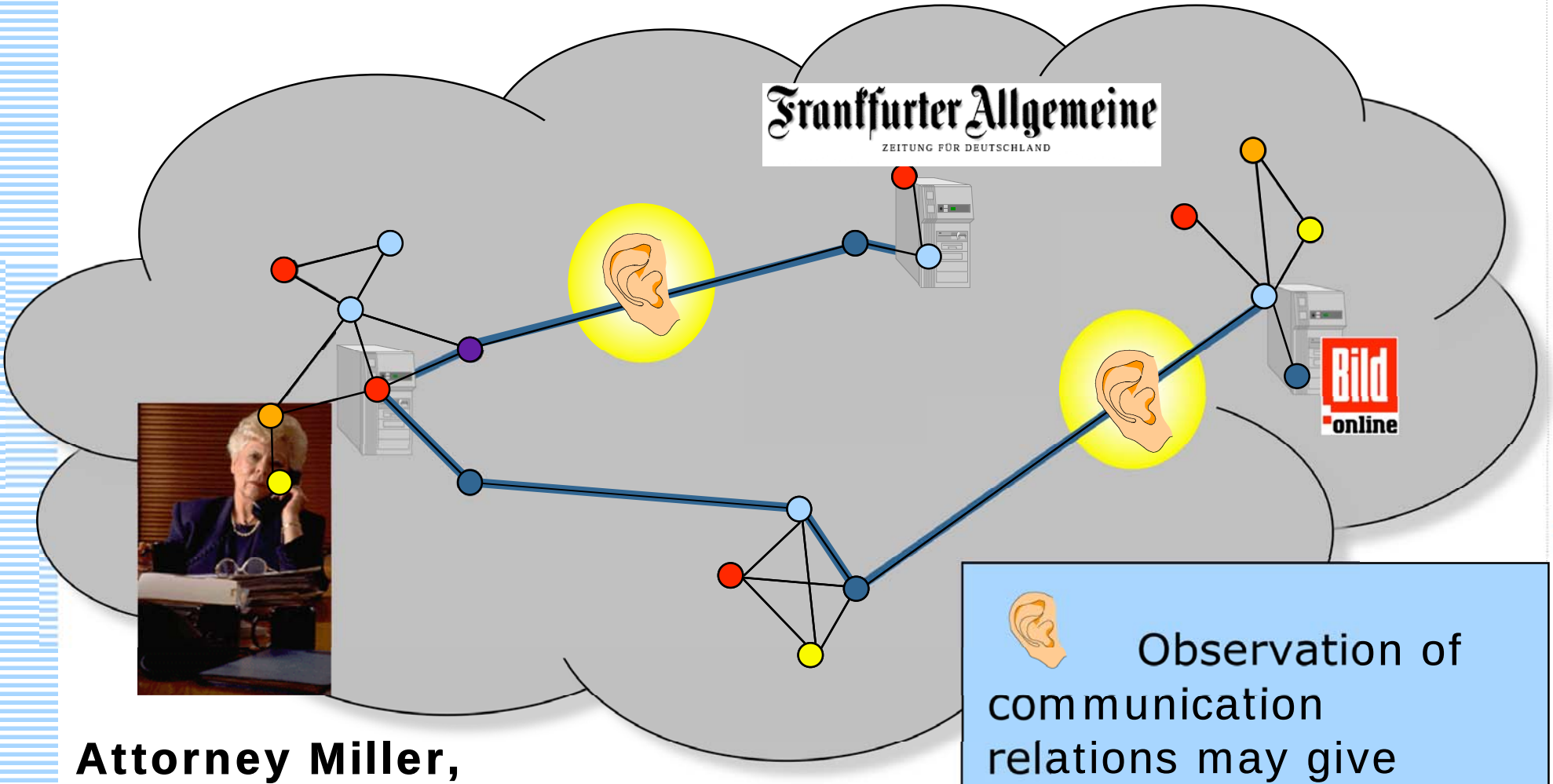
Everybody can be the originator of an «event» with an equal likelyhood

Protection Goals

Subject of communication WHAT?	**Circumstances of comm. WHEN?, WHERE?, WHO?**
Confidentiality	**Anonymity Unobservablity**
Contents	**Sender** **Location** **Recipient**

- Protection goals — confidentiality
  - Protection of the identity of a user while using a service
    - Anonymity in counseling services
  - Protection of the communication relations of users
    - Users may know identity of each other

Why encryption is not enough



Attorney Miller, specialized in mergers

Observation of communication relations may give information about contents

Protection Goals

Subject of communication WHAT?	Circumstances of comm. WHEN?, WHERE?, WHO?
Confidentiality	**Anonymity** **Unobservablity**
Contents	**Sender** **Location**
	Recipient

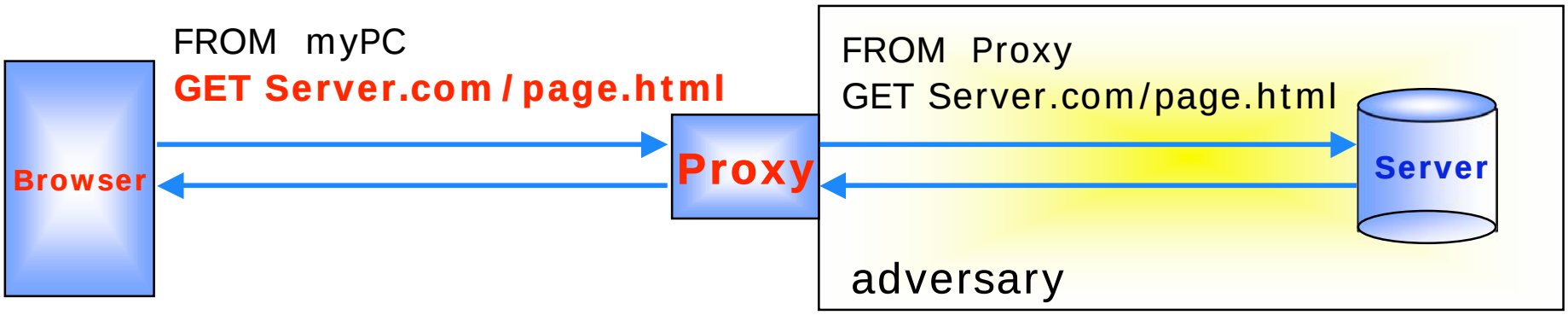
- Outsiders
  - … tapping the «line»
  - … doing traffic analysis
- Insiders
  - Network operator (or corrupt staff) reading e.g. billing data
  - Governmental organizations asking for log files

Building blocks of Privacy Enhancing Technologies

- Encryption
- Hiding communication relations
  - Against weak outsiders
    - Proxies
  - Against insiders
    - Broadcast
    - Blind message service
    - DC network
    - MIX network
- Hiding transactions
  - Pseudonyms
  - Credentials (link properties to pseudonyms)

Protection ideas (selection)

- Against weak outsider attacks
  - Encryption — does not protect from traffic analysis
  - Use a mediator:
    - PROXY



- Users need to trust the proxy
- proxy knows all communication relations

Protection ideas (selection)

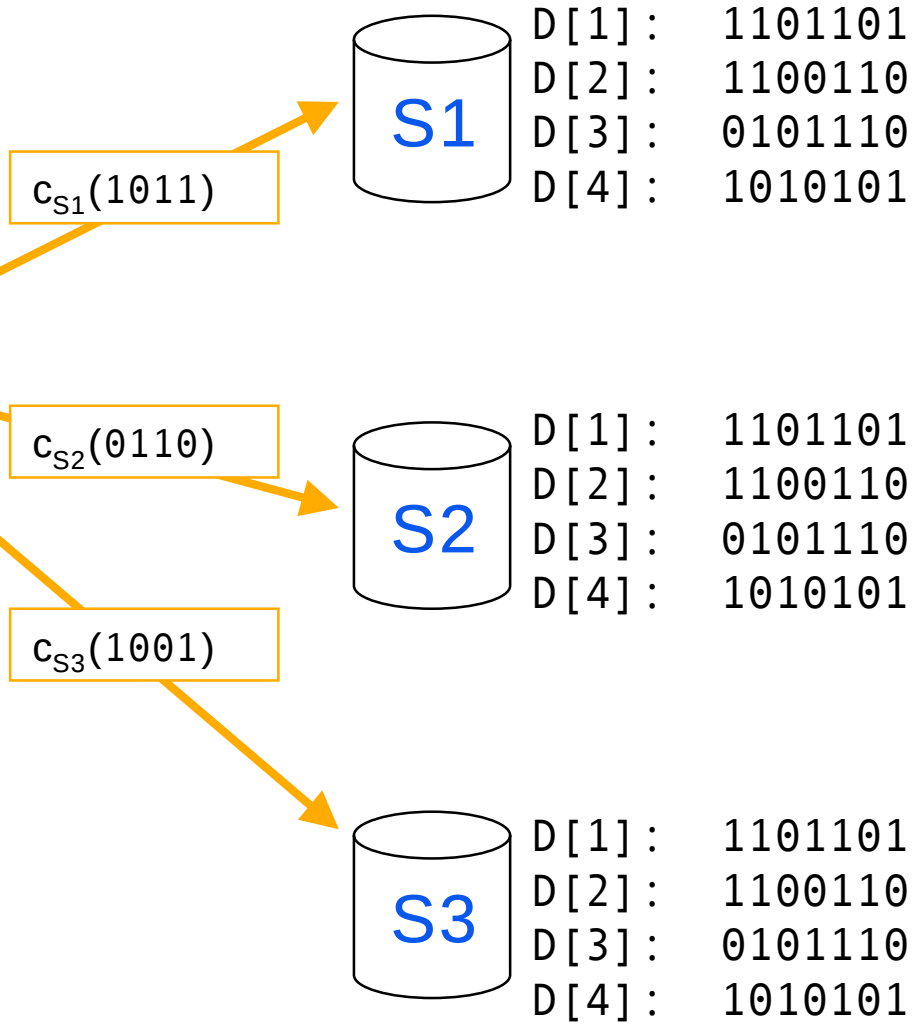
- Against insider attacks
  - Goal:
    - Users need not trust the operator of anonymizing service
  - Idea:
    - Use more than one «mediator» from different operators
    - At least one operator must be trustworthy
  - Examples:
    - Broadcast
    - Blind message service
    - DC network
    - MIX network

Blind-Message-Service (Cooper, Birman, 1995): Query

Client queries for D[2]:

Index = 1234

Set vektor = 0100
Choose randomly request(S1) = 1011
Choose randomly request(S2) = 0110
Calculate request(S3) = 1001



- Protection goal:
  - Databases gain no information which entry the client is interested in
- Replicated databases of different operators

Blind-Message-Service (Cooper, Birman, 1995): Answer

Client queries for D[2]:

Index = 1234

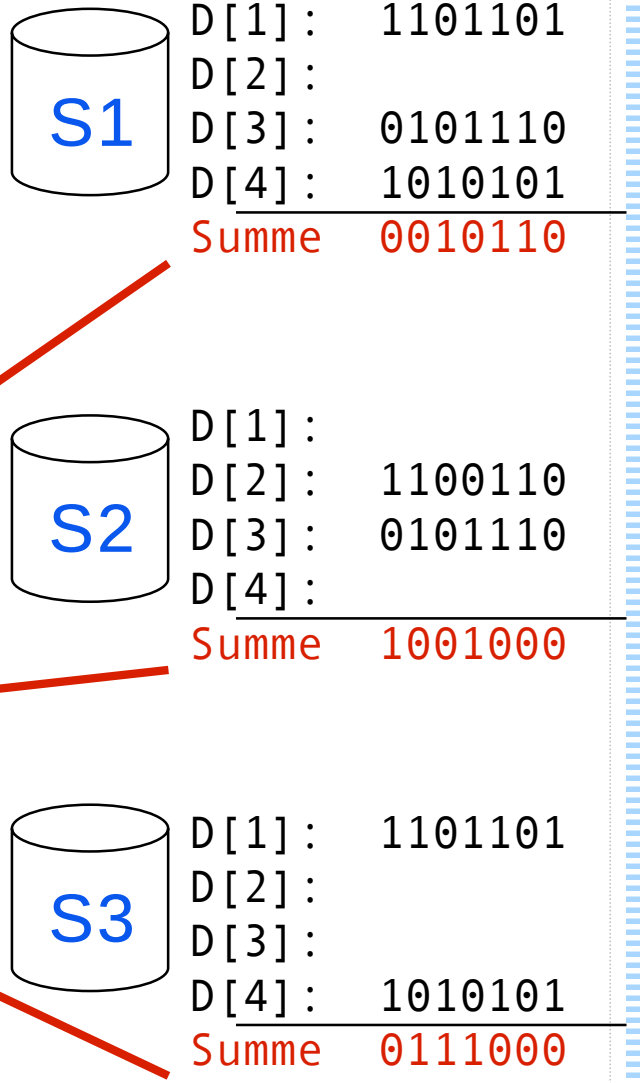
Set vektor = 0100
Choose randomly request(S1) = 1011
Choose randomly request(S2) = 0110
Calculate (xor) request(S3) = 1001

Answers from

S1: 0010110
S2: 1001000
S3: 0111000

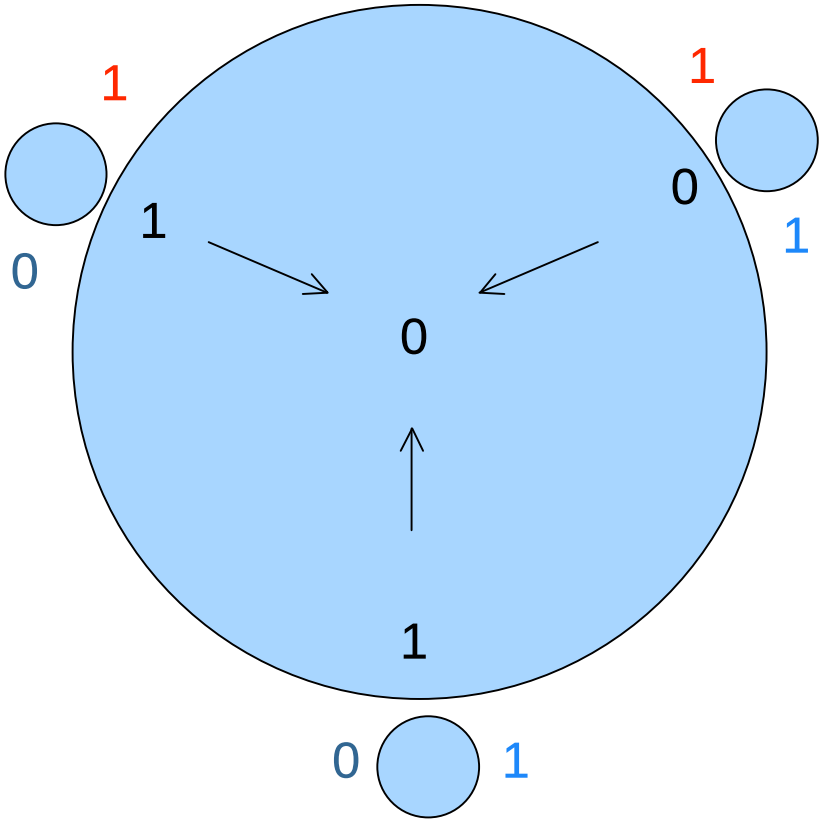
Xor equals D[2]: 1100110

Link encryption between client and databases



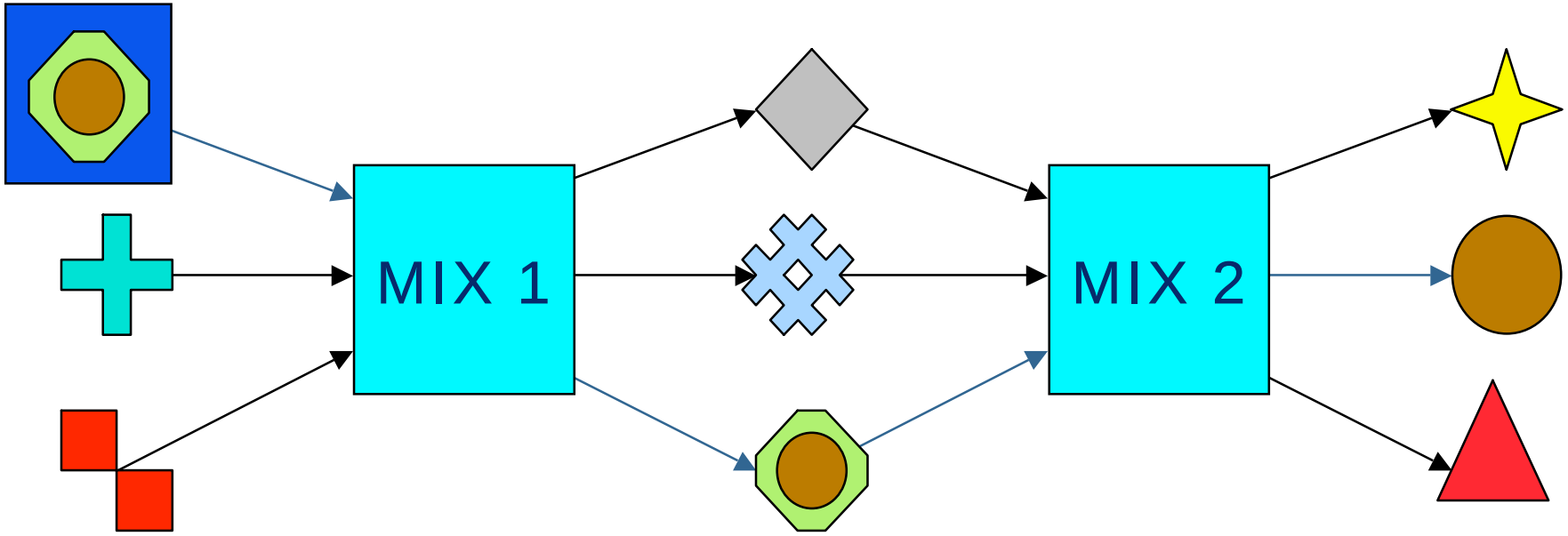
DC network (Chaum, 1988)

- Everybody
  1. Flip a coin with each other
  2. Calculate xor of the two bits
  3. If paid xor a 1 (negate the result of step 2)
  4. Tell your result
- Together
  1. Calculate xor of the three (local) results
  2. If global result is Zero an external person has paid



Mixes (Chaum, 1981)

- Basic idea:
  - Sample messages in a batch, change their coding and forward them all at the same point of time but in a different order. All messages have the same length.
  - Use more than one Mix, operated by different operators.
  - At least one Mix should not be corrupt.
- Then:
  - Perfect unlinkability of sender and recipient.



Timeline of development

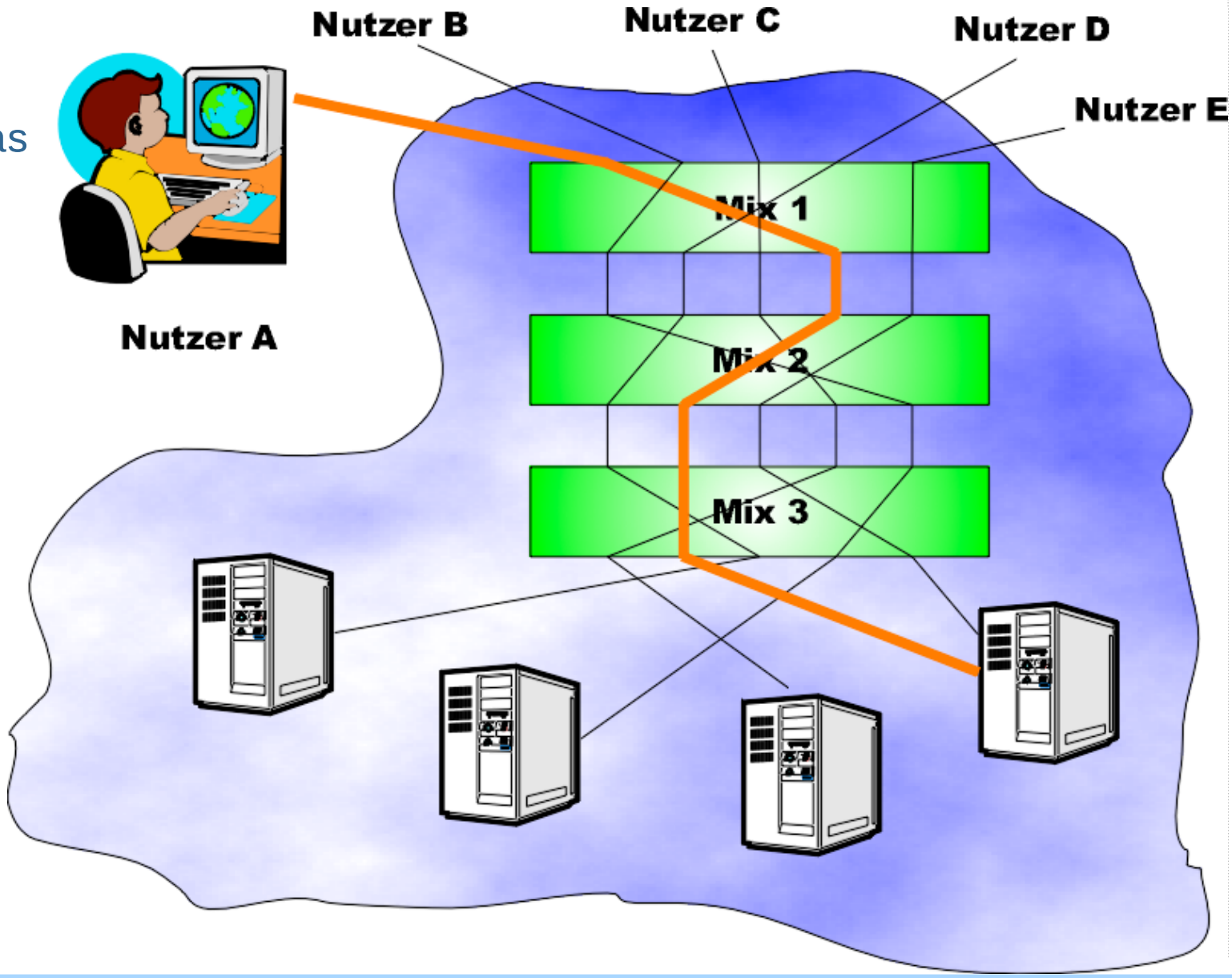
Year	Idea / PET system
1978	Public-key encryption
1981	MIX, Pseudonyms
1983	Blind signature schemes
1985	Credentials
1988	DC network
1990	Privacy preserving value exchange
1991	ISDN-Mixes
1995	Blind message service
1995	Mixmaster
1996	MIXes in mobile communications
1996	Onion Routing
1997	Crowds Anonymizer
1998	Stop-and-Go (SG) Mixes introduced
1999	Zeroknowledge Freedom Anonymizer (service meanwhile closed)
2000	AN.ON/JAP Anonymizer ←
2004	TOR

Internet/Web

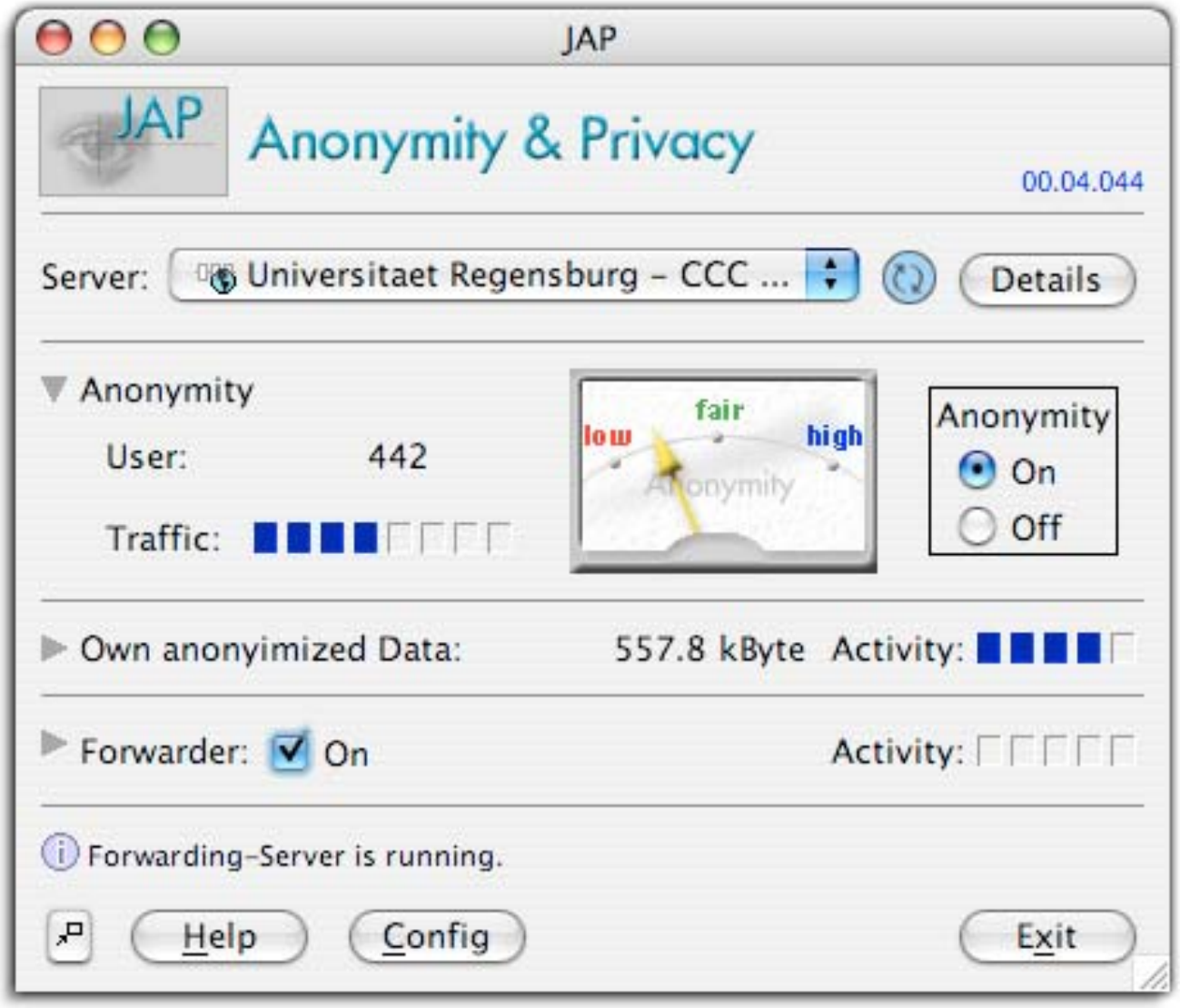
- Technical background
  - MIX based unobservable transport system
  - Should withstand strong (big brother) attacks
- Information service (impossible to operate a perfect Anon system)
  - Current level of protection (Anonymity level)
  - Trade-off between performance and protection should be decided by the user
- Open source project
  - Client software: Java (platform independent)
  - Server software: C/C++ (Win/NT, Linux/Unix)
- Technical and jurisdictional knowledge to serve legal issues

Internet/Web

- JAP acts as a local proxy on the local machine



Internet/Web



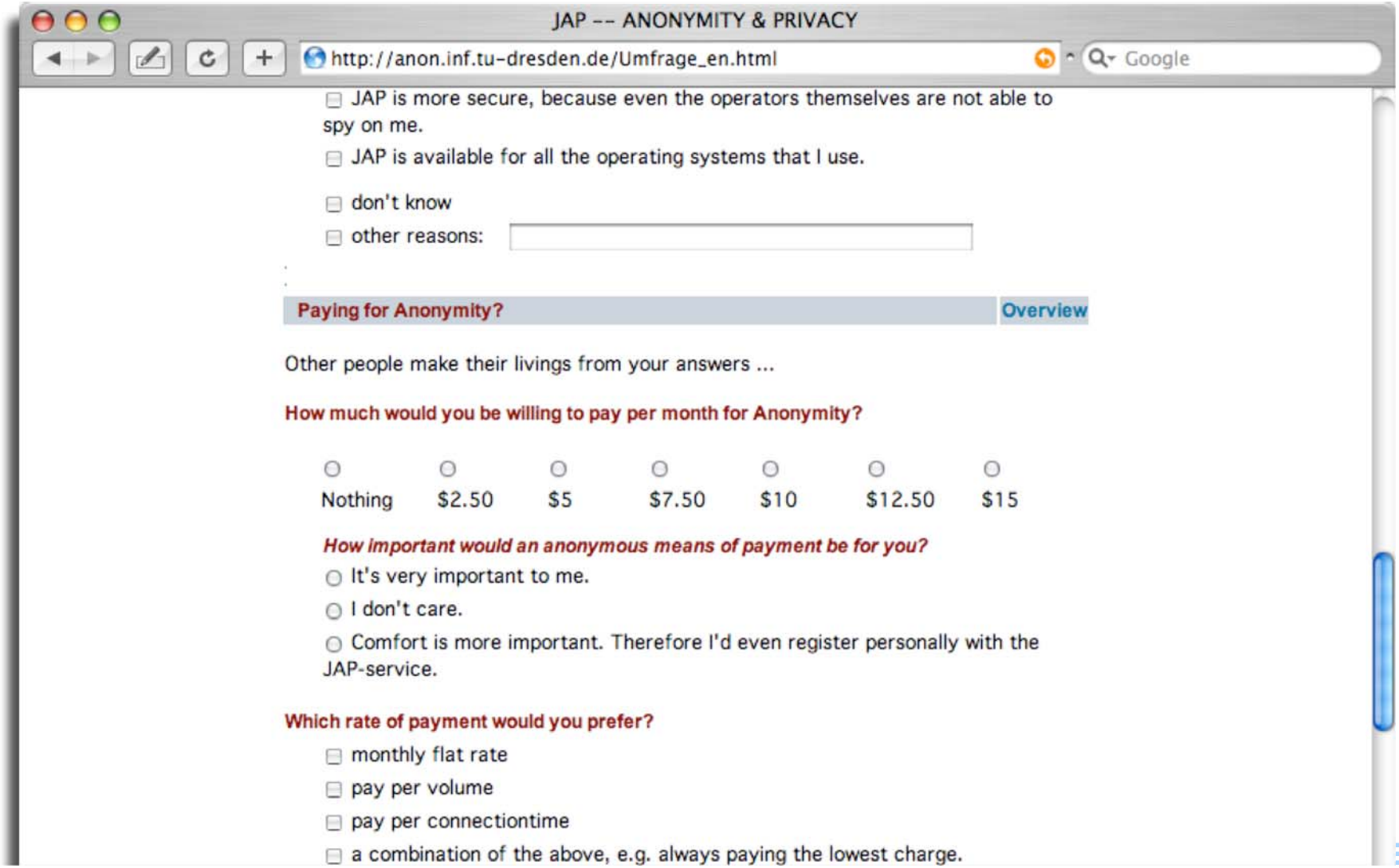
For free at www.anon-online.de

First test version has been launched in October 2000

Full service has been running since February 2001

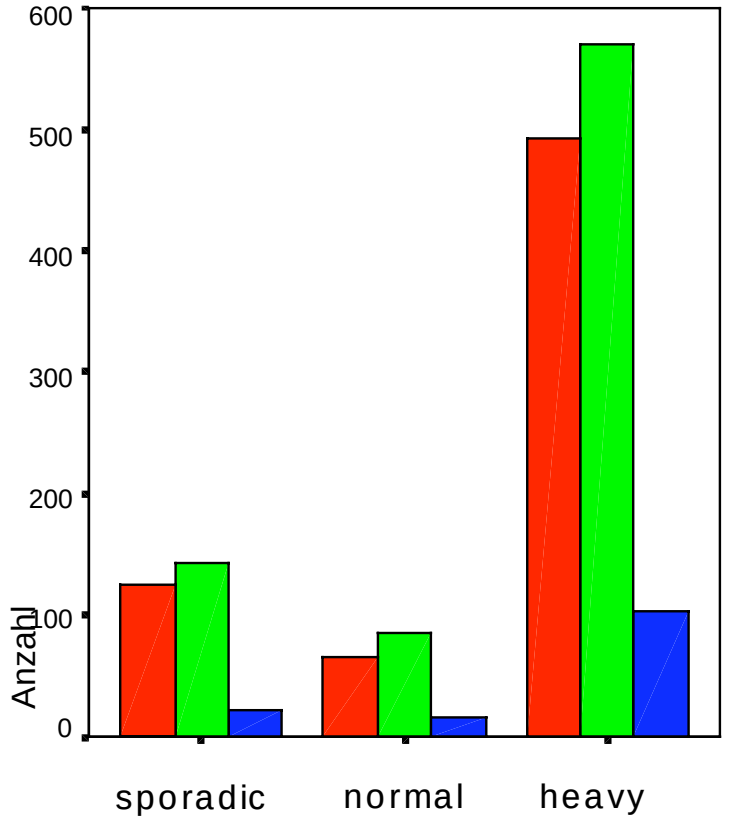
Public survey (Spiekermann 2003)

- Sample size:
  - 1800 users of the JAP anonymizer



Public survey

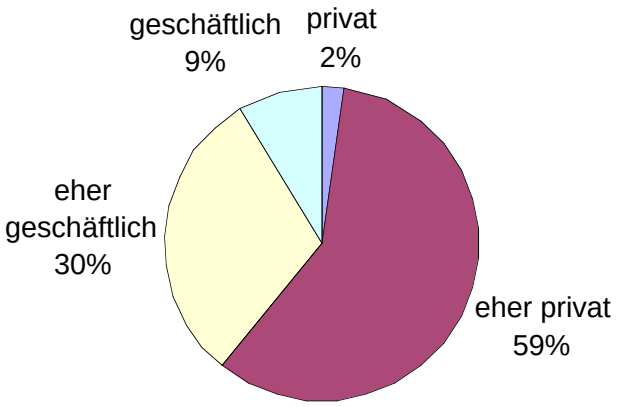
- Willingness to pay for anonymity
  - ≈ 40% absolutely not
  - ≈ 50% monthly service fee of about € 2,5 ... € 5
  - ≈ 10% more than € 5 per month
- Willingness is independent of the heaviness of usage
- Heaviness of usage
  - ≈ 73% heavy users (use the system at least daily)
  - ≈ 10% use it at least twice the week)
  - ≈ 17% spradic (less than twice the week)



Public survey

- Reasons for using an anonymizing service
  - ≈ 31% Free speech
  - ≈ 54% protect from secret services
  - ≈ 85% protect from profiling
  - ≈ 64% protect against observation by my ISP

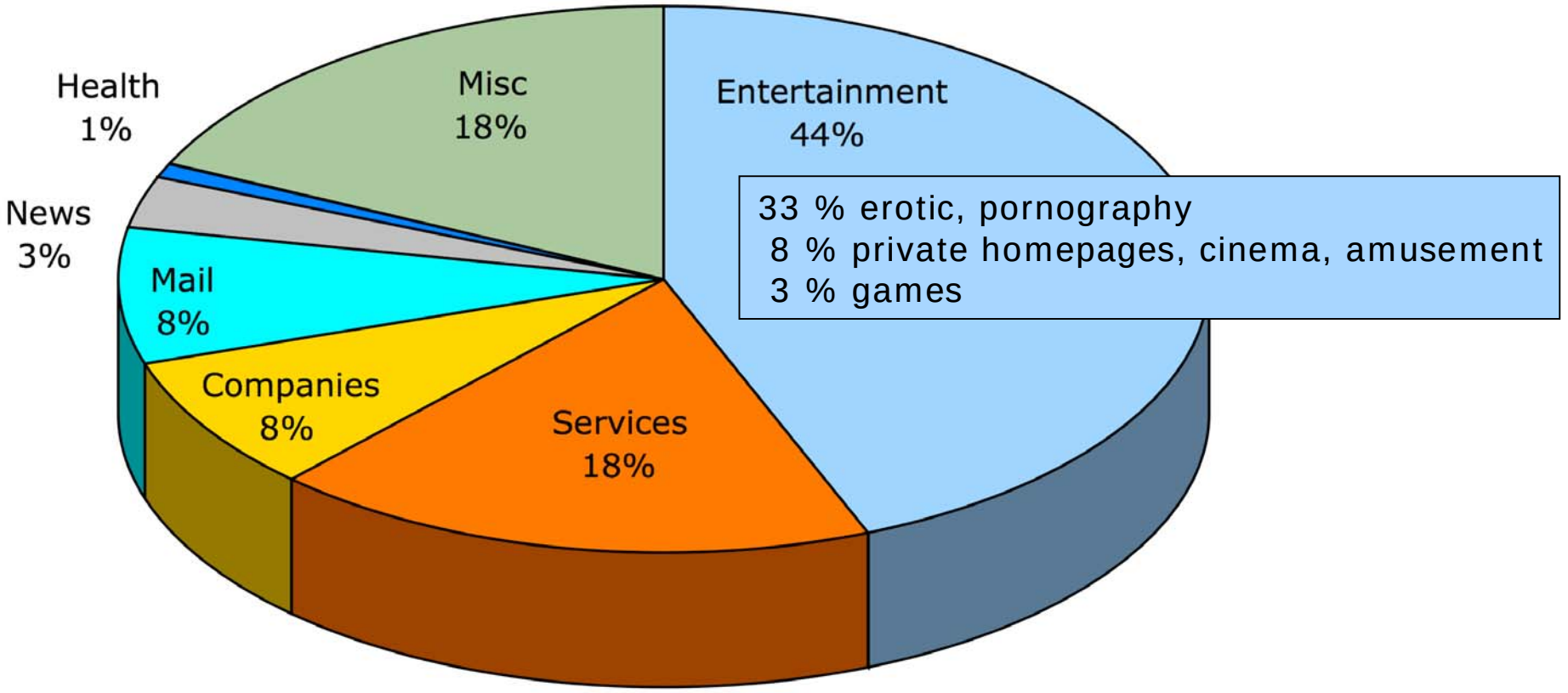
- Do you use it for private or business?
  - ≈ 2% private only
  - ≈ 59% mainly for private things
  - ≈ 30% mainly for business things
  - ≈ 9% business only



- Why do you use the JAP system?
  - ≈ 76% free of charge
  - ≈ 56% secure against the operator
  - ≈ 51% easy to use

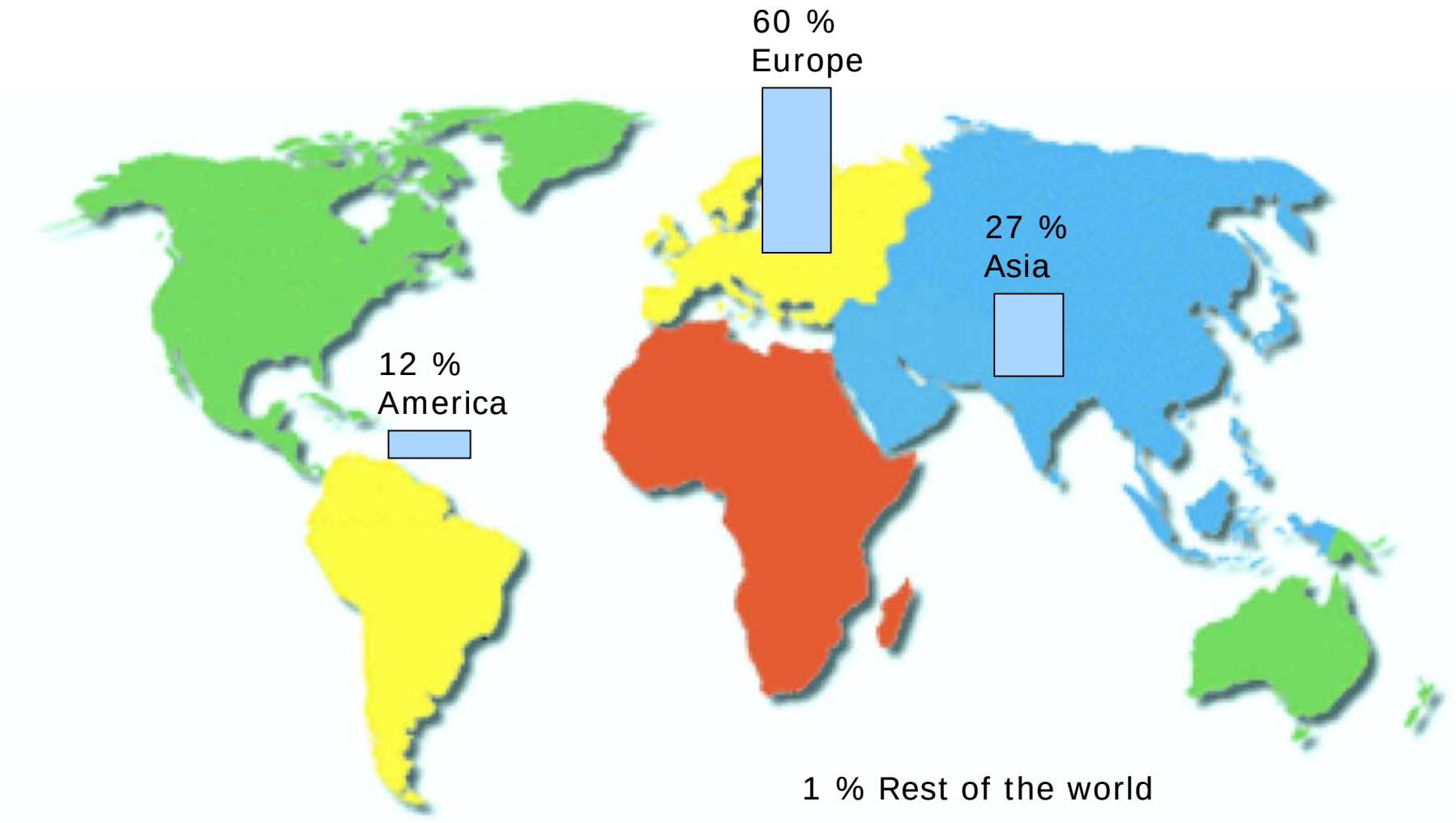
Anonymized content

- 150 requests randomly picked from millions of requests of June 2005



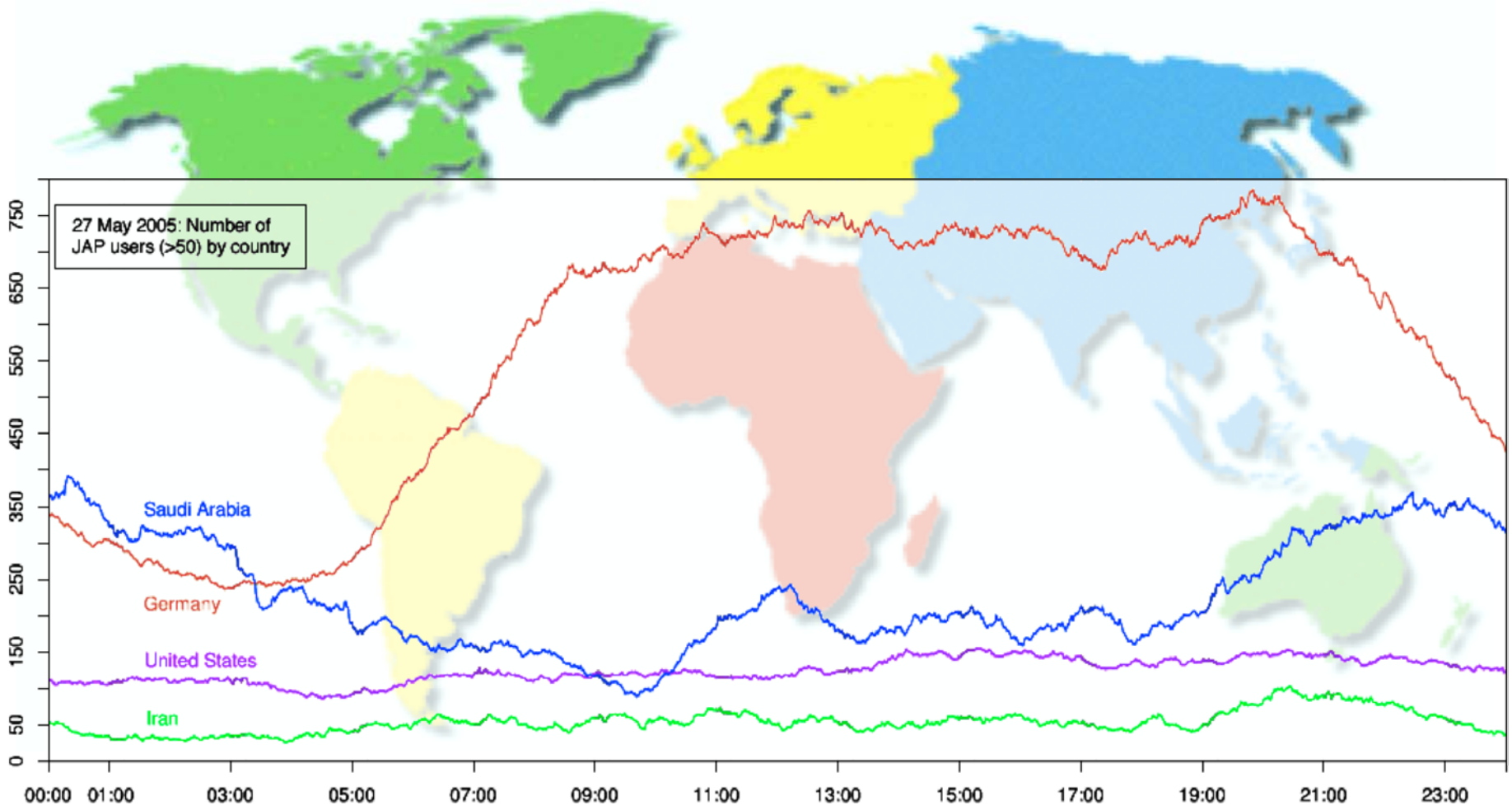
Regions of users

- Incoming IP adresses have been classified into regions from May-June 2005



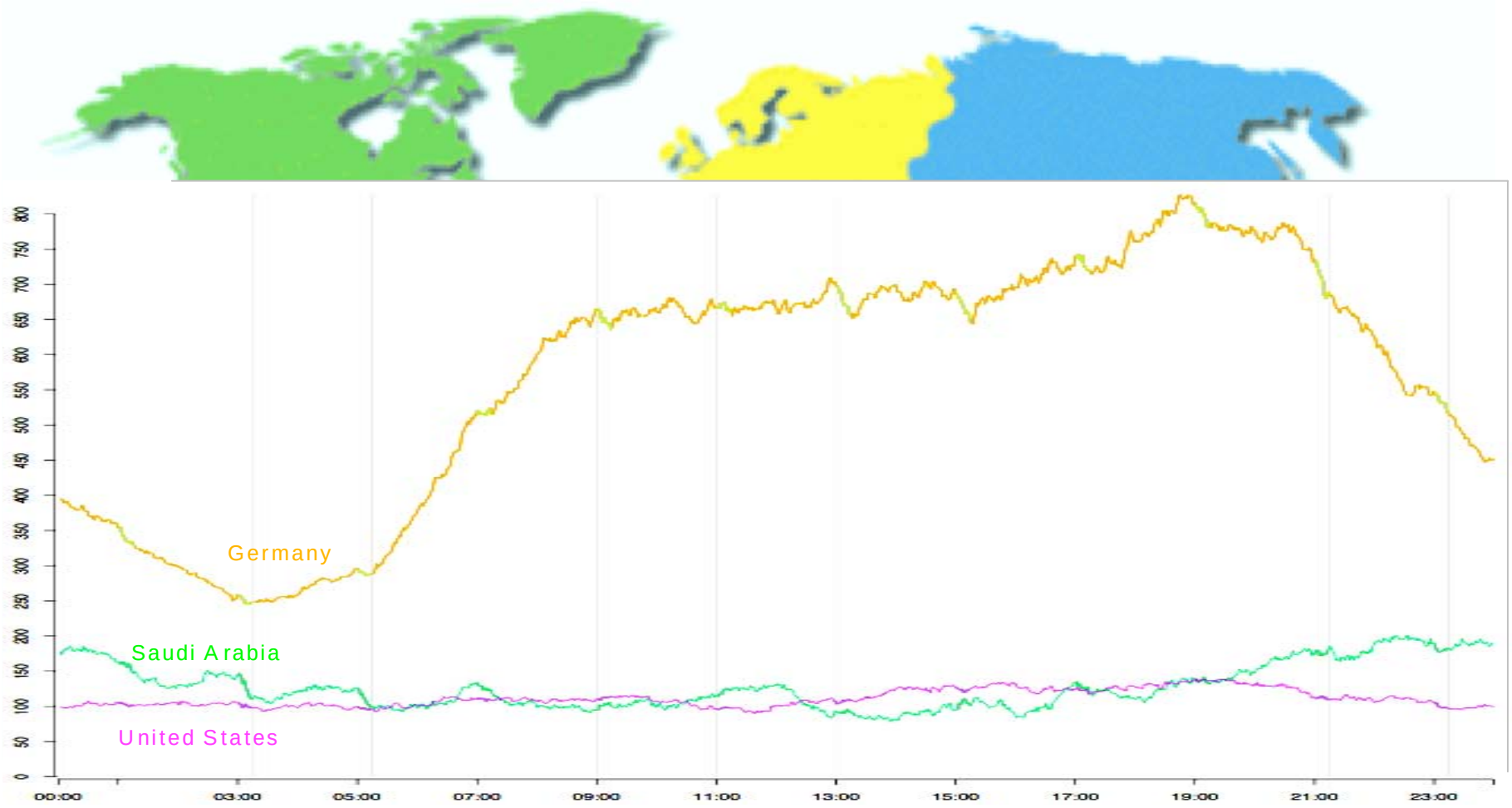
Regions of users

- Dayline of May 27, 2005

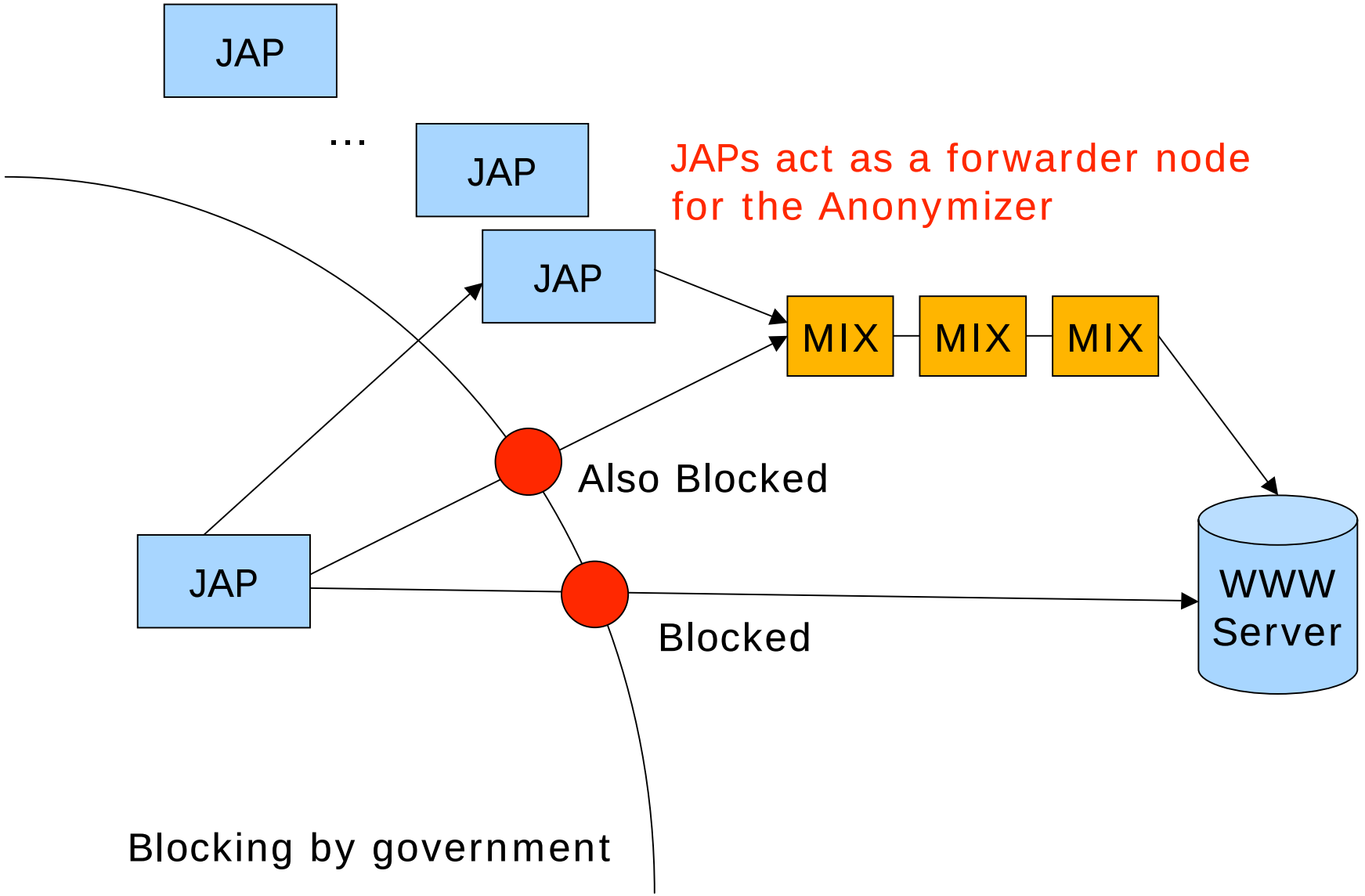


Regions of users

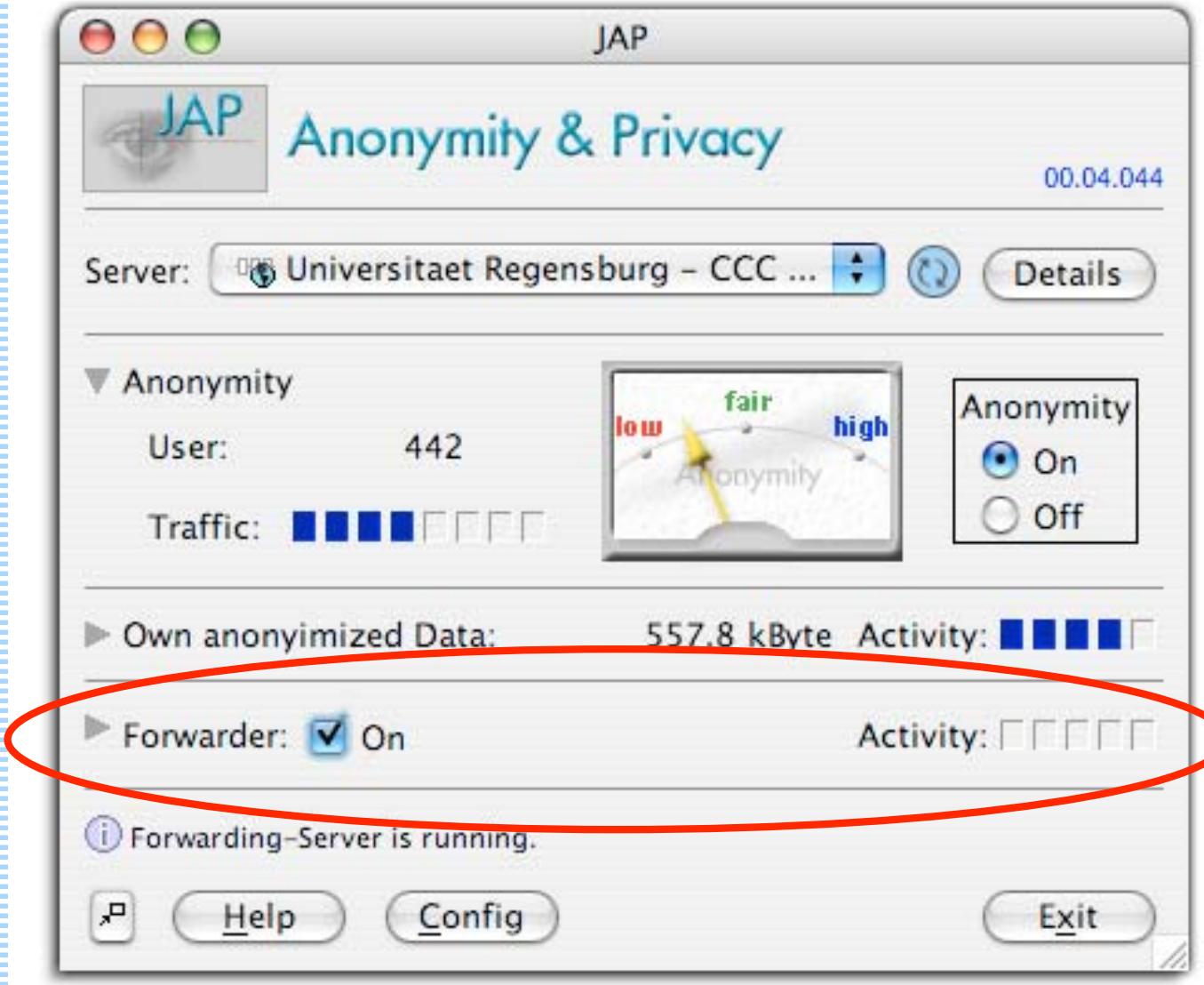
- Dayline of Aug 1, 2005



Cencor-free Internet access



Cencor-free Internet access

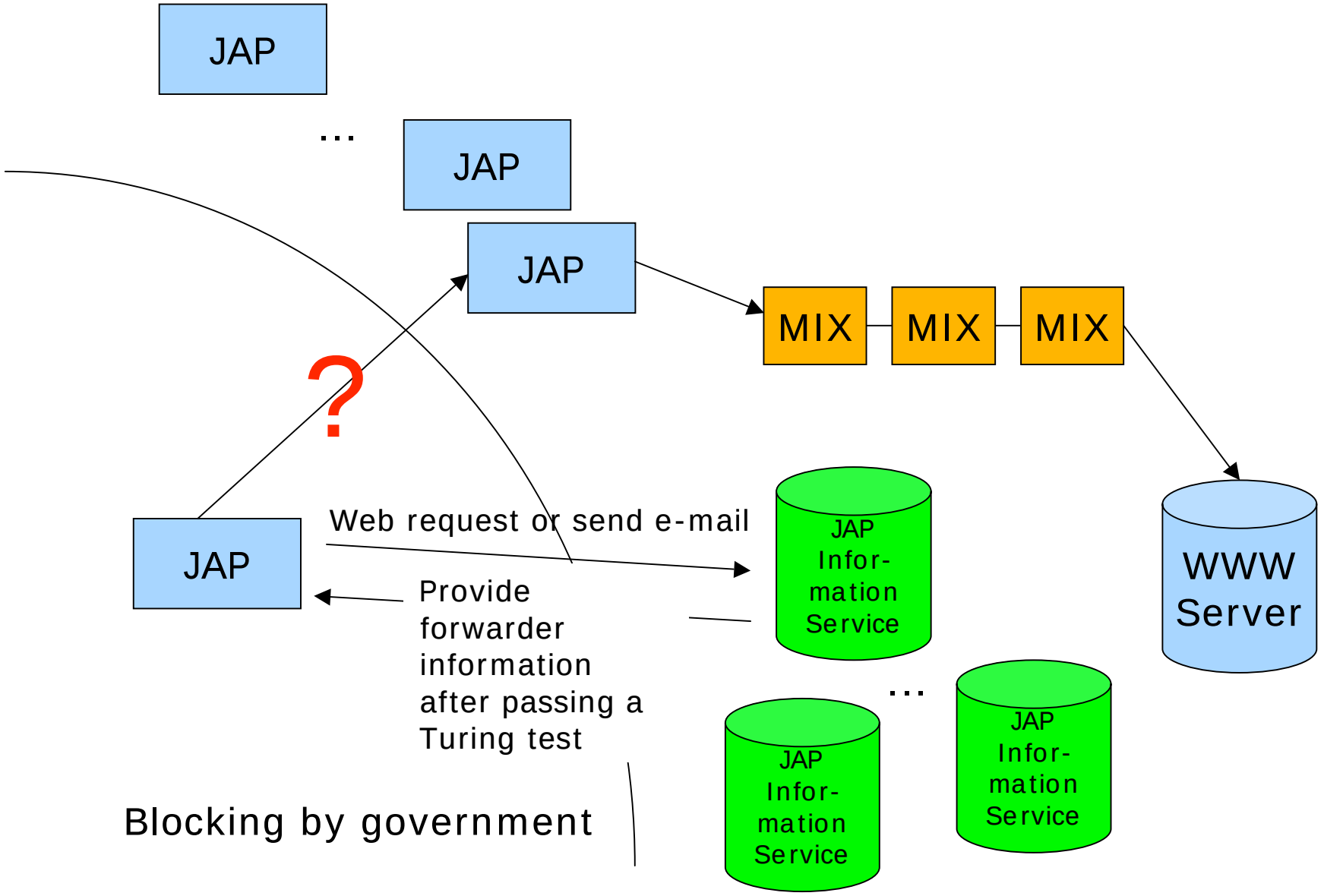


JAP users can share their bandwith with blocked JAP users

Requests are anonymized through the Mix network

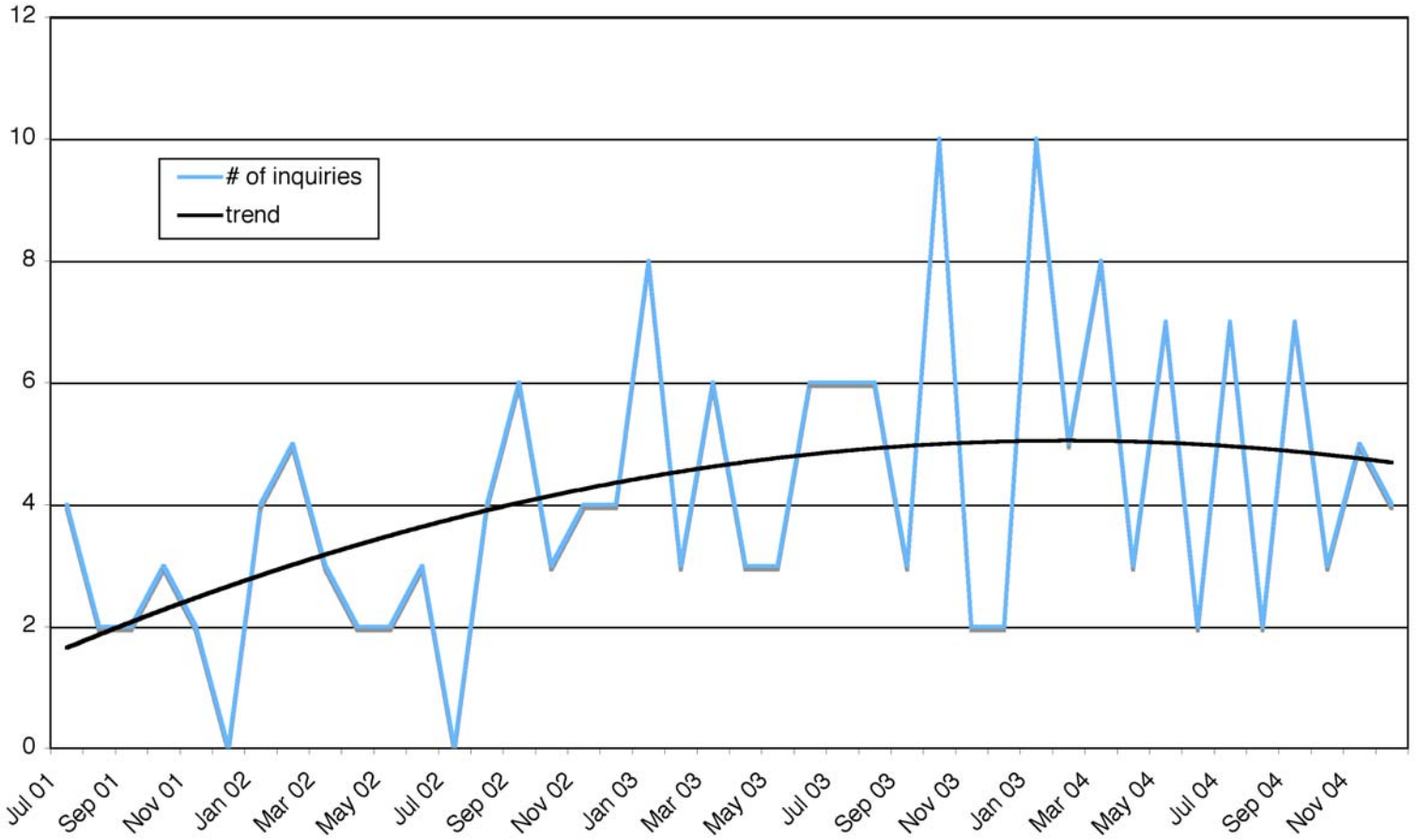
Forwarders gain no information about contents of forwarded requests

Cencor-free Internet access



Misuse

- JAP project
  - Avg. 4-5 inquiries per month by law enforcement agencies and private persons



Misuse

- JAP project
  - Avg. 4-5 inquiries per month by law enforcement agencies and private persons
  - Between 3 and 6 Terabytes per month of anonymized data
- Typical inquiry
  - Date and time of access, IP address anonymizing service
  - Inquiry: Identification request (name, addresss) for user behind that IP address
    - Anonymizer is misunderstood as an Internet Service Provider (ISP)
- Observation
  - While the traffic anonymized by the system increased over the time the number of inquiries did not

Conclusions

- Economical
  - There is a market for identity protection.
  - Users are willing to pay for it.
- Technical
  - Anonymity on the network is necessary as a basic technology for providing freedom and democracy.
  - Prototypes exist at least for Internet/Web

Prof. Dr. Hannes Federrath
Lehrstuhl Management der Informationssicherheit
Universität Regensburg
D-93040 Regensburg

E-Mail: hannes.federrath@wiwi.uni-regensburg.de
WWW: http://www-sec.uni-regensburg.de

Phone +49-941-943-2870
Telefax +49-941-943-2888