Anonymization for web, fixed line, and mobile applications

Prof. Dr. Hannes Federrath

University of Regensburg · Information Systems ·
Management of Information security

Anonymization for web, fixed line, and mobile applications

- Basic concepts
  - Who is the observer?
  - Protection ideas
- Fixed line
  - Unobservability and anonymity of communication relations
- Mobile communications
  - Protection of communication relations
  - Unobservability of locations
- Internet/Web
- Conclusions

Who is the observer?

- 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

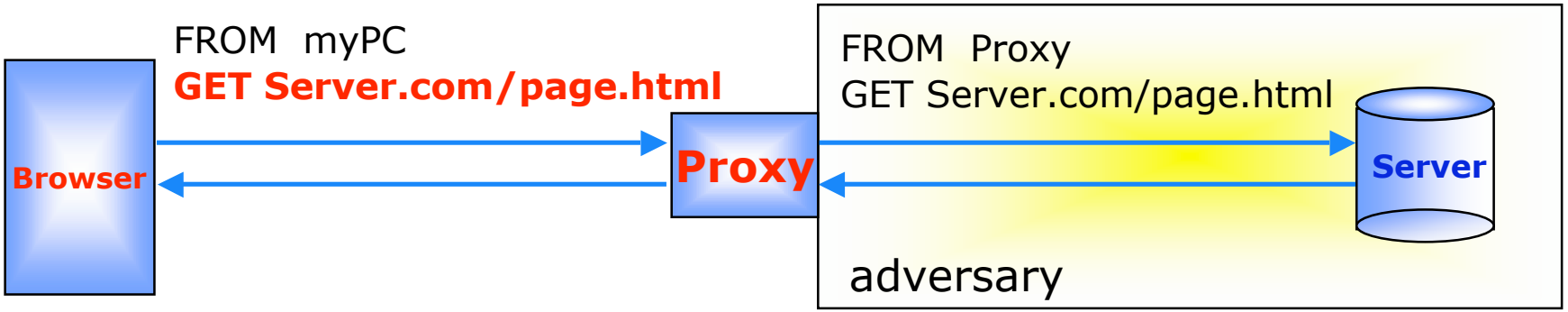
- Outsiders
  - … tapping the «line»
  - … doing traffic analysis

- Insiders
  - Network operator (or corrupt staff) reading e.g. billing data
  - Governmental organizations asking for log files

Anonymity is a prerequisite for identity management.

Protection ideas (selection)

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



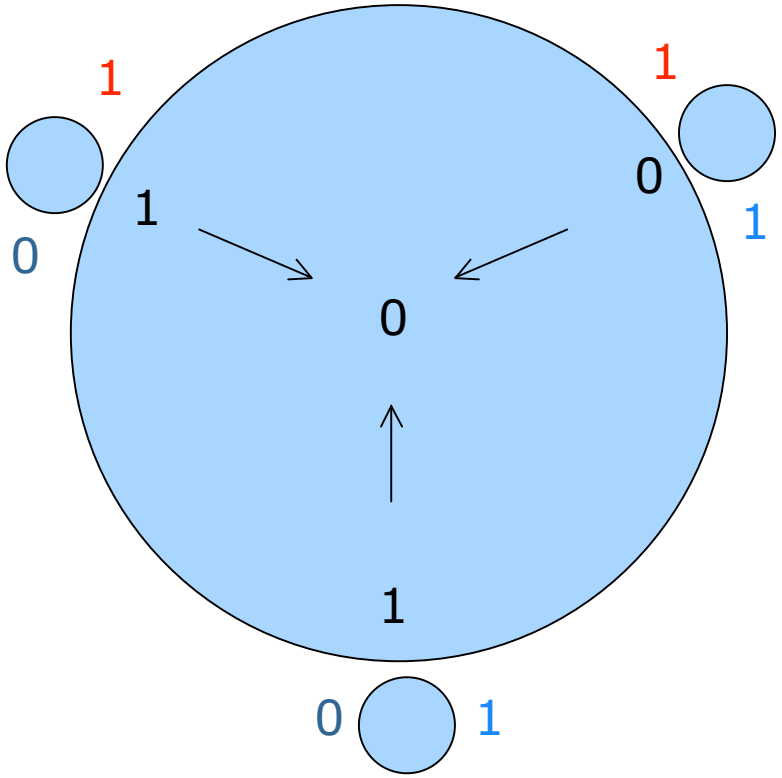
- Users need to trust the proxy
- proxy knows all communication relations

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

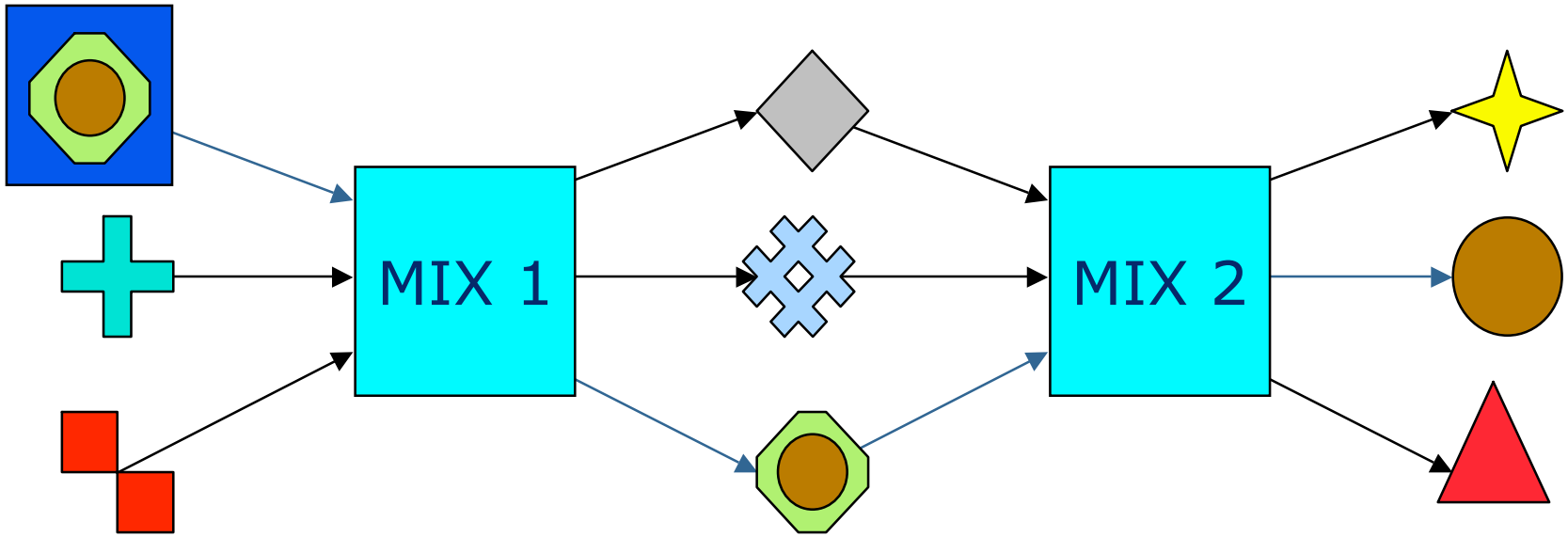
DC network (Chaum, 1988)

- 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



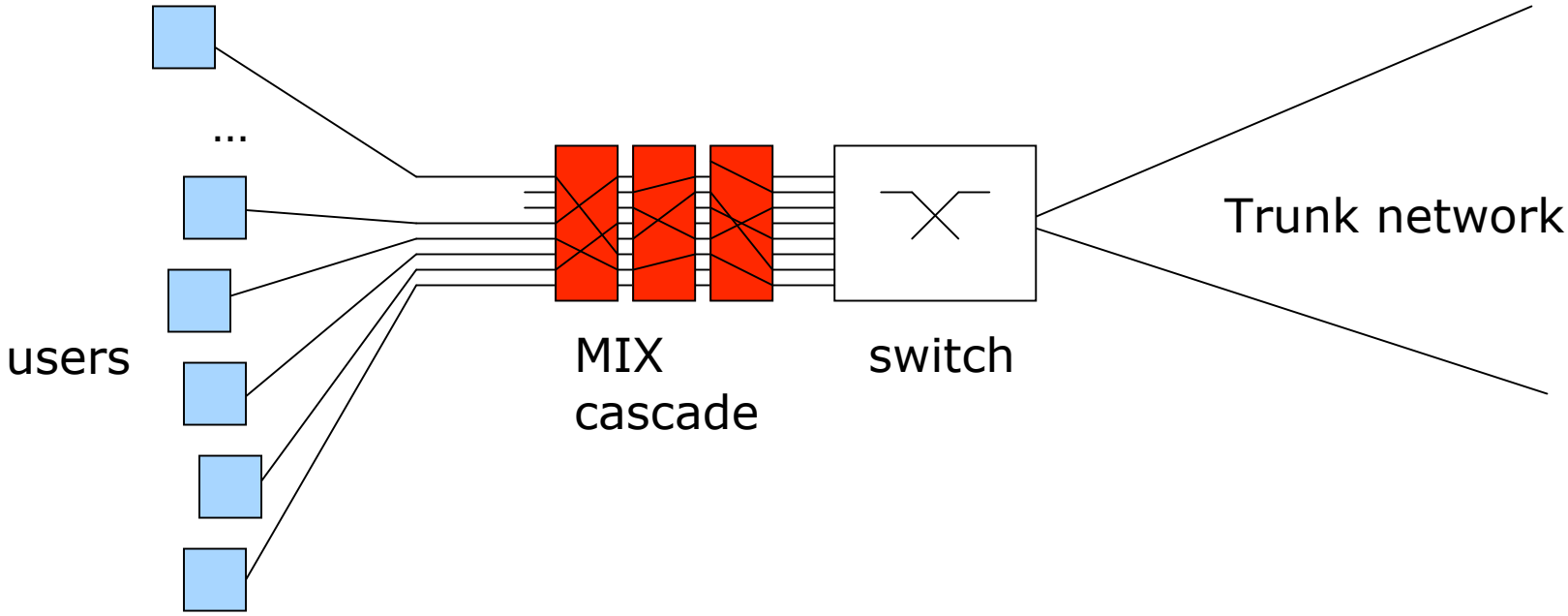
Mixes (David Chaum, 1981)

- Basic idea:
  - Sample messages in a batch, change their coding and forward them all at the same point oftime 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.



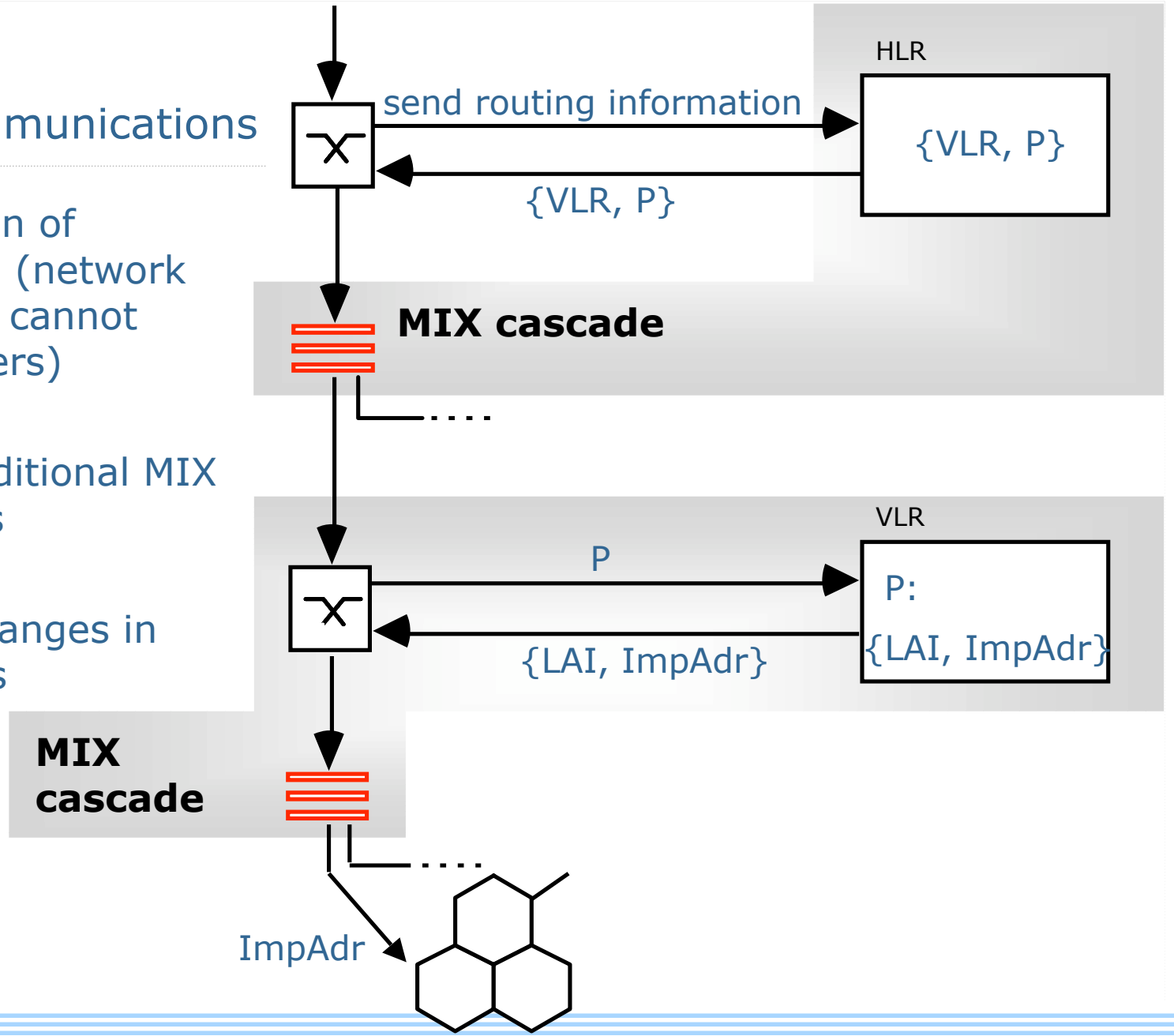
Fixed line

- Idea
  - Based on MIX networks
  - Pfitzmann et. al. 1989
  - All users served by a switching center communicate via a MIX cascade in front of the switch



Mobile communications

- Protection of locations (network operator cannot track users)
- Need additional MIX cascades
- Small changes in protocols

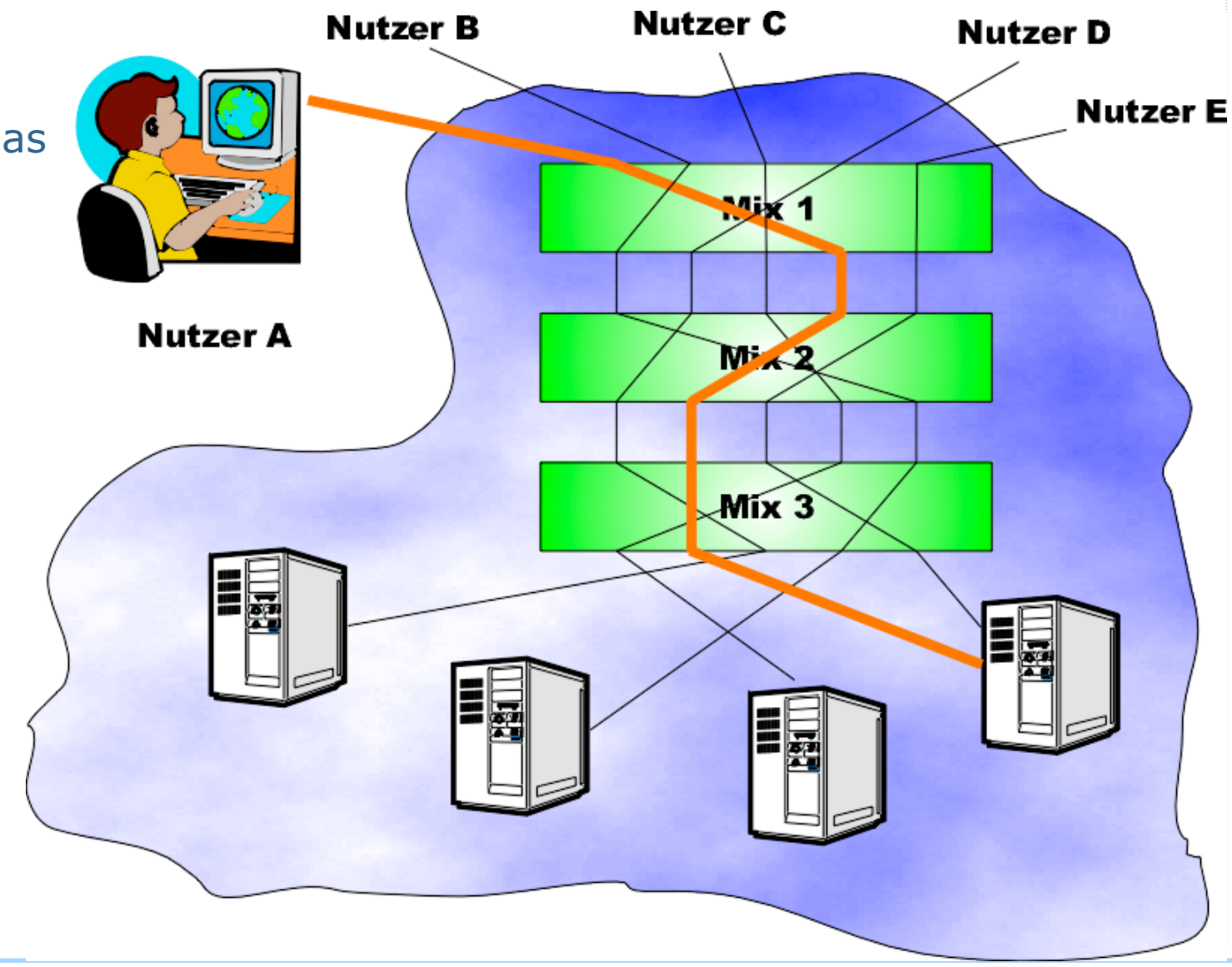


Internet/Web

- 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

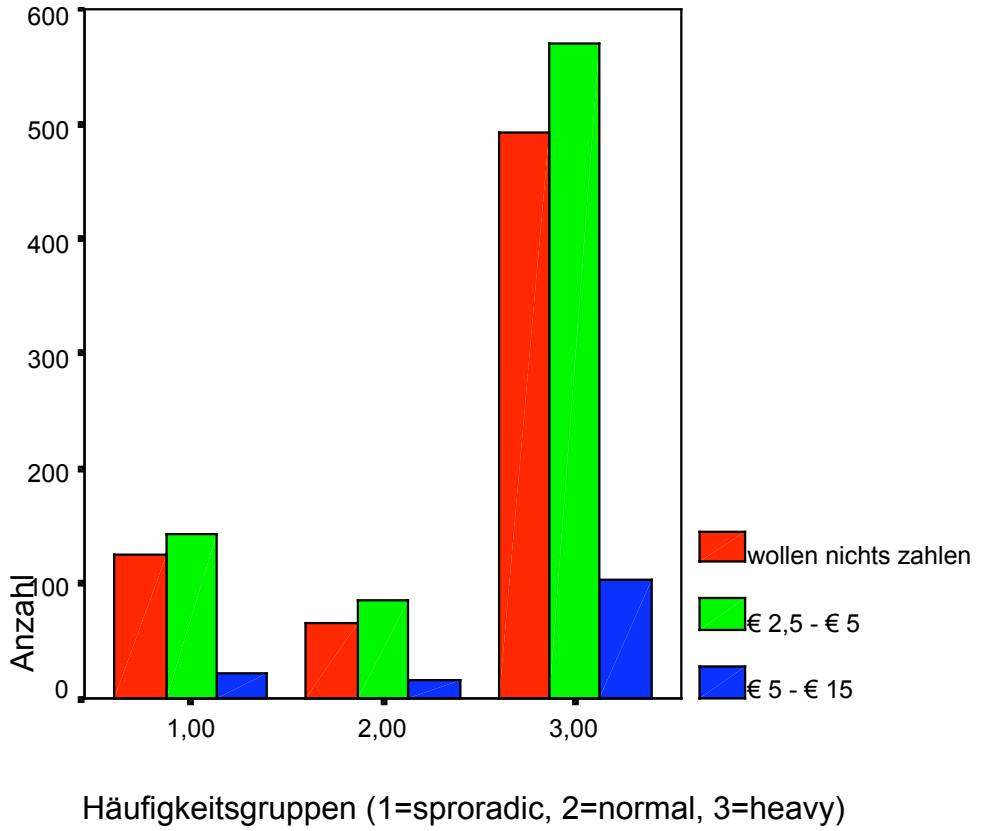


Internet/Web

- For free at www.anon-online.de

Public survey

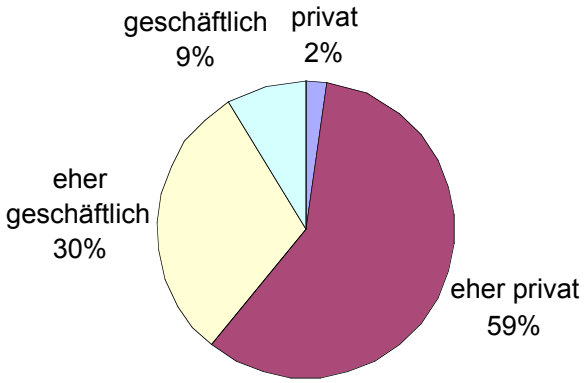
- Willingness to pay for anonymity
  - ≈ 40% absolutely not
  - ≈ 50% monthly service fee of about € 2,5 … € 5
  - ≈ 10% more than € 5 per month
- Sample size:
  - 1800 users of the JAP anonymizer
- Spiekermann 2003



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

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 true identity management.
  - 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

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

Management of information security

Information security management tries to protect the processes of organizations using information technology from intended attacks and accidental events.

- Our research topics
  - IT Security in distributed systems and multilateral security
  - Privacy enhancing technologies
  - Security on the Internet
  - Digital Rights Management Systems
  - Security in electronic markets
  - Security in mobile communication systems
- More information
  - http://www-sec.uni-regensburg.de