Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

IFIP Summer School on Privacy and Identity Management 2017,
Ispra/Italy, 6. September 2017

Anonymity Online – Current Solutions and Challenges

Prof. Dr. Hannes Federrath
Security in distributed systems
http://svs.informatik.uni-hamburg.de

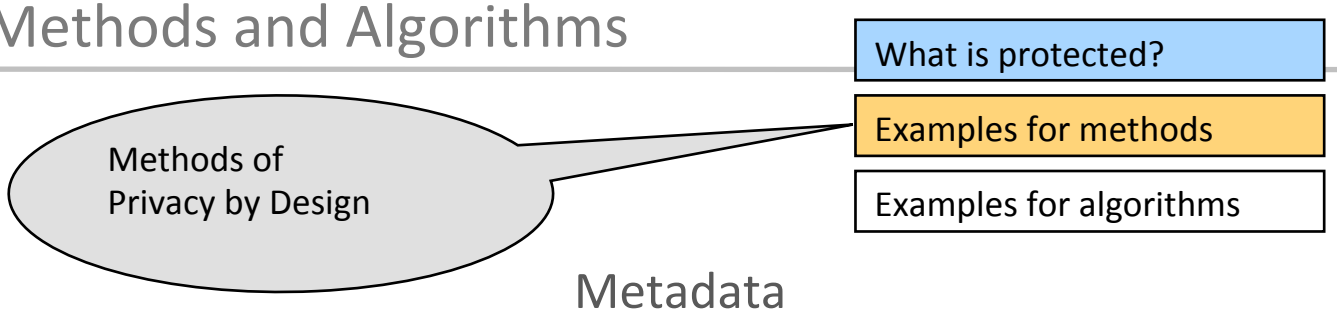
Protection goals

Voydock, Kent 1983

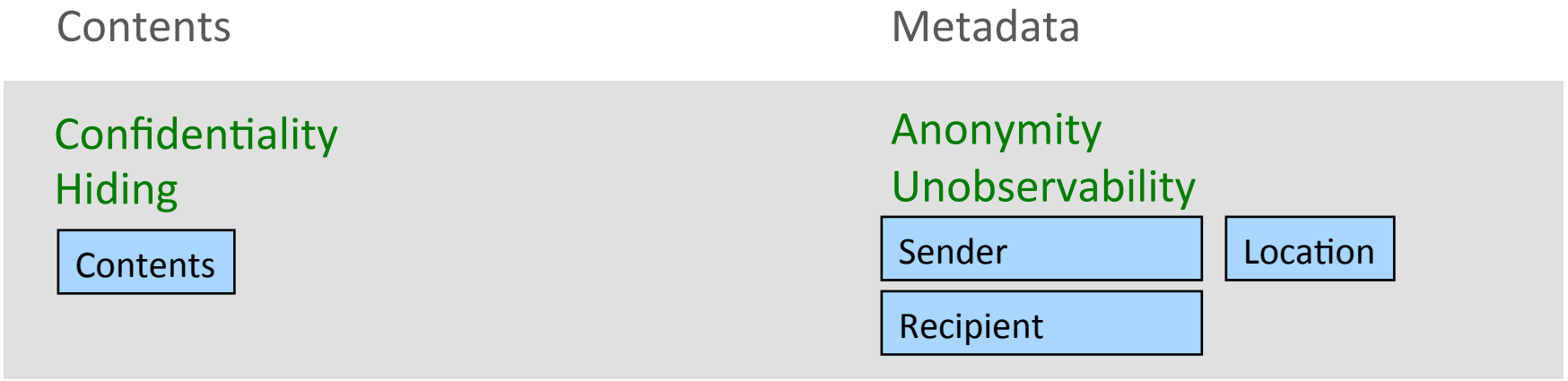
- Classical IT security follows a risk approach which addresses the violation of access rules by dishonest users.

Confidentiality	unauthorized release of information
Integrity	unauthorized modification of information
Availability	unauthorized denial of use of resources

Confidentiality: Methods and Algorithms

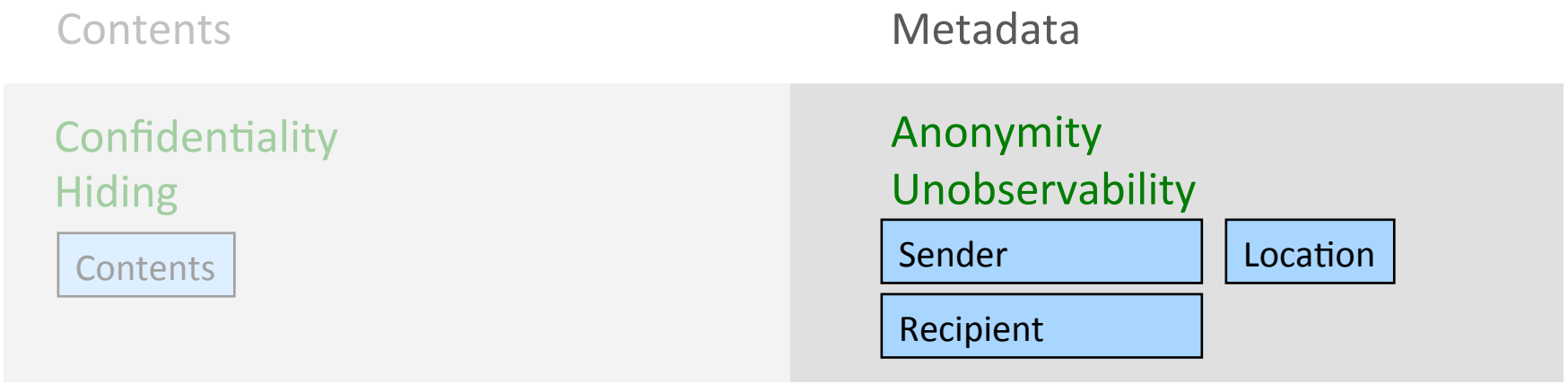


Confidentiality: Protection goals and attacker model



- Outsider
  - eavesdropping on communication lines
  - traffic analysis
- Insider
  - network operators or malicious staff
  - governmental organizations

Confidentiality: Protection goals and attacker model



- Anonymity
  - Protection of the identity of a user while using a service
- Unobservability
  - Protection of the communication relations of users
  - Users may know identity of each other

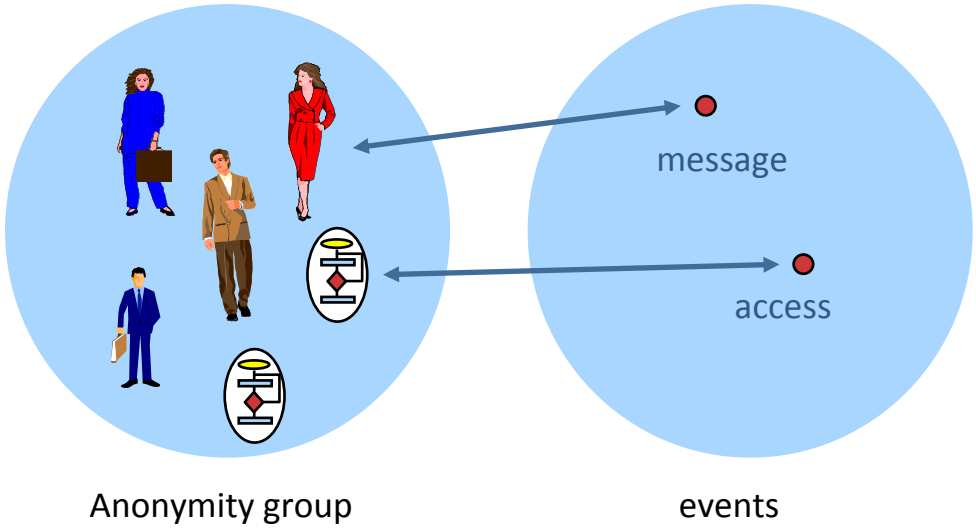
Service or users cannot link communication events to identities

Anonymity group

- A single event, caused by a single person, cannot be anonymously or unobservable.
- We need a group of persons, who behave equal:

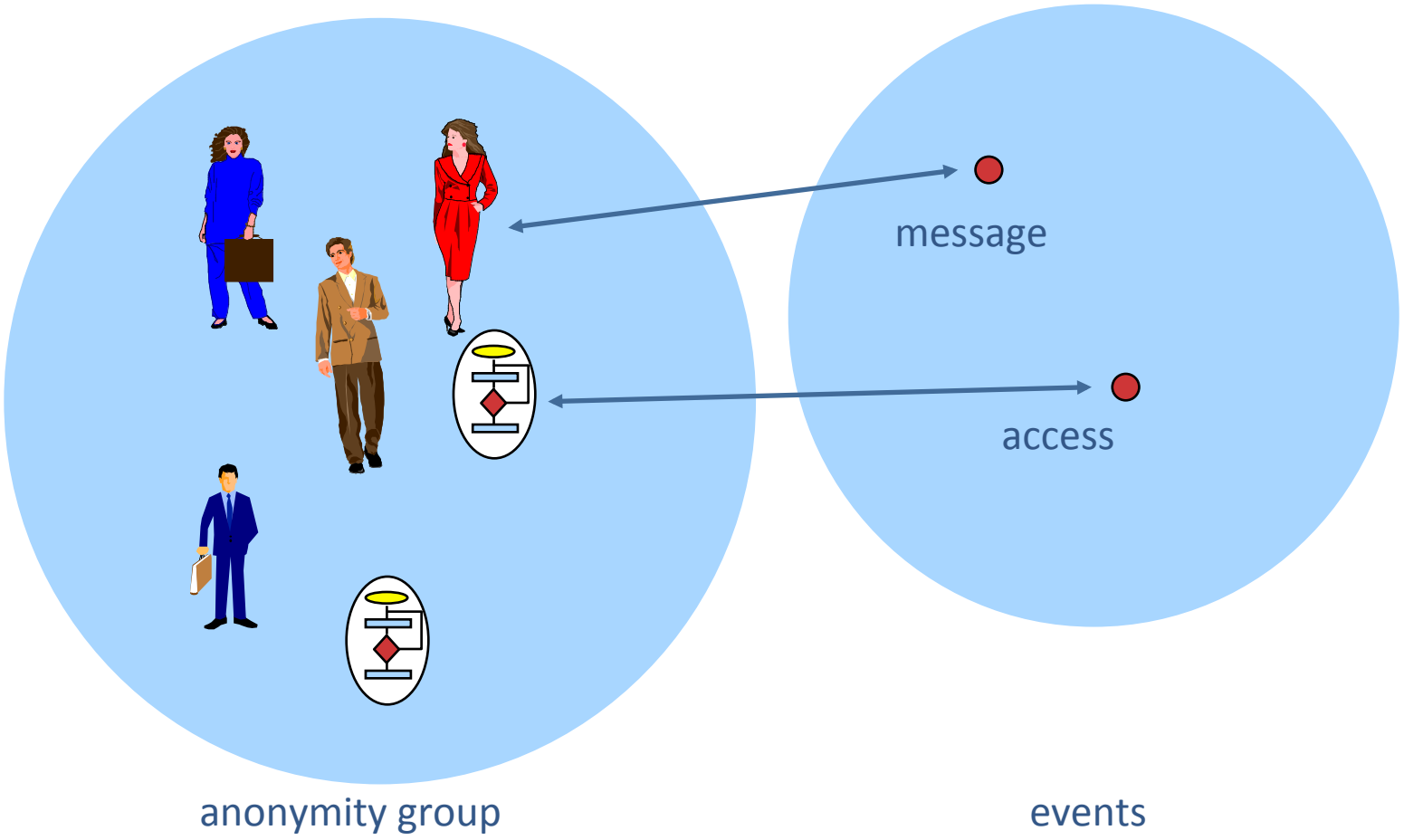
  Anonymity group

  - Each member of an anonymity group is possibly the creator of an event.
  - A public known characteristic, which all members of the anonymity group fulfill, cannot be anonymous.



Anonymity and unobservability

- Everybody can be the originator of an event with an equal likelihood



Anonymity and unobservability and ISO OSI network levels

User

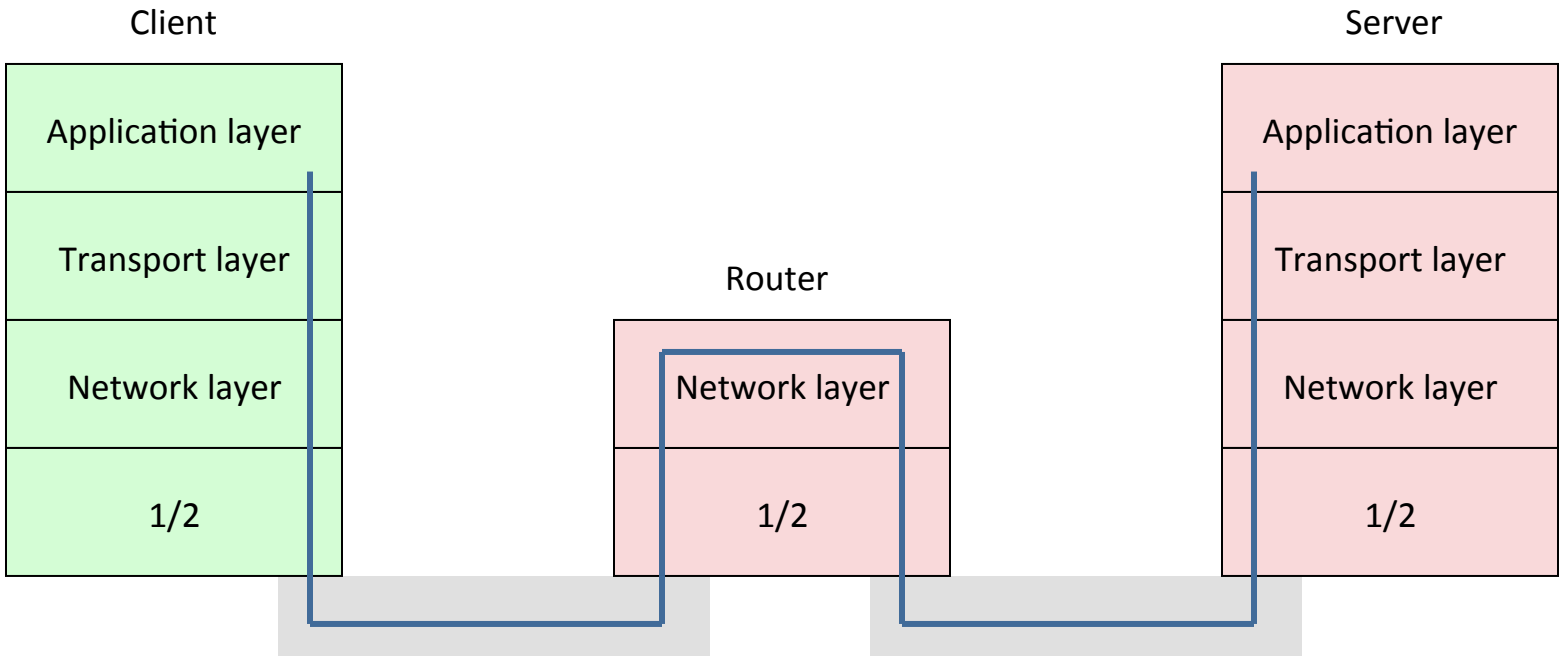
- honest
- no malicious code

Outsiders

- eavesdropping on communication lines
- traffic analysis

Insiders

- network operators or malicious staff
- governmental organizations



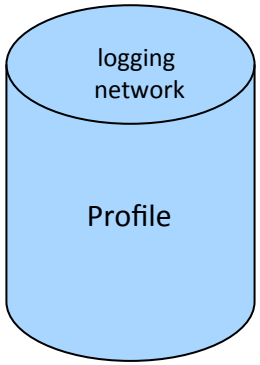
Anonymity and unobservability and ISO OSI network levels

Application layer

App 1: SN-Device, start, stop, …
82031M6UV2F, 2012-12-19T16:39:57, 2012-12-19T16:45:33

App 2: SN-Device, start, stop, address book, …
82031M6UV2F, 2012-12-20T12:19:11, 2012-12-20T12:25:01, data

App 3: SN-Device, start, stop, location info, …
82031M6UV2F, 2012-12-20T12:21:23, 2012-12-20T12:21:55, data



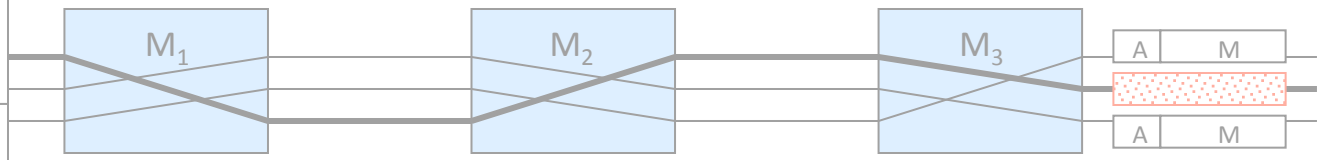
Tracking on application level

Transport layer

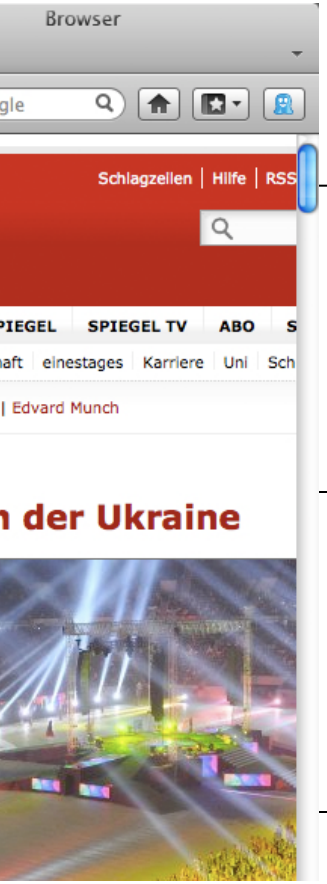
Network layer

1/2

Tracking on network level



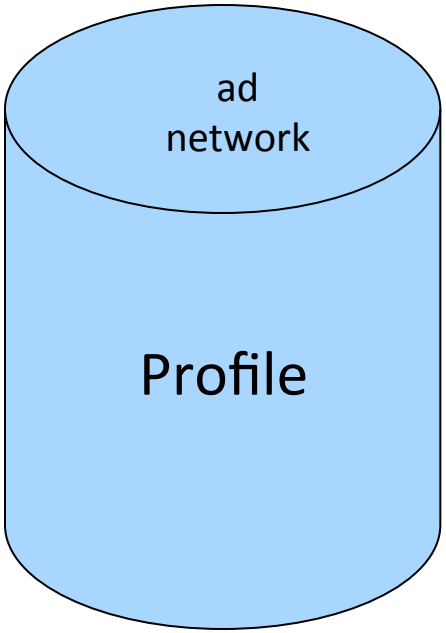
Third-Party Cookies



GET http://adnet.example.net/banner1.gif
Cookie: guid=8867563
Referer: http://www.bookshop.example

GET http://adnet.example.net/banner2.gif
Cookie: guid=8867563
Referer: http://www.healthinfo.example

GET http://adnet.example.net/banner3.gif
Cookie: guid=8867563
Referer: http://www.lifeinsurance.example



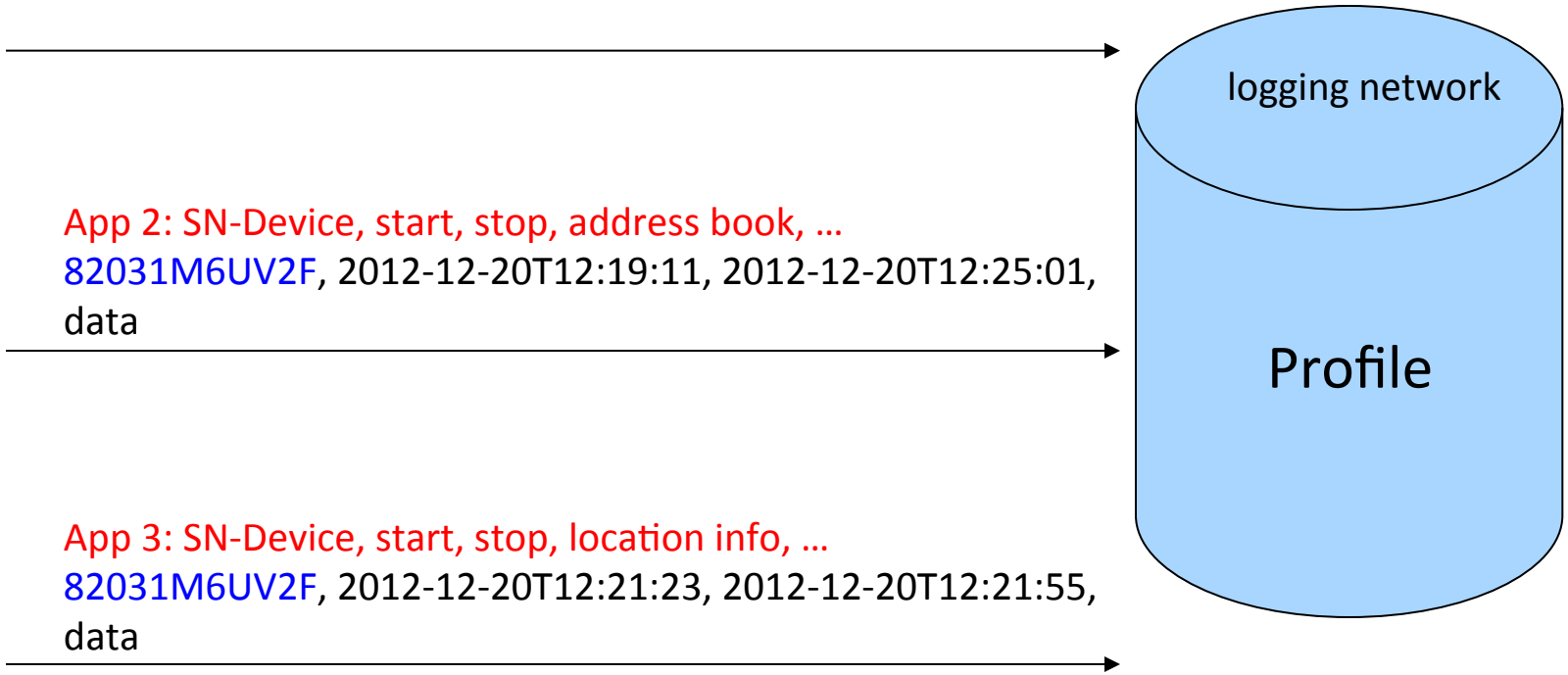
Protection: Delete cookies

Mobile logging networks

App 1: SN-Device, start, stop, …
82031M6UV2F, 2012-12-19T16:39:57, 2012-12-19T16:45:33

App 2: SN-Device, start, stop, address book, …
82031M6UV2F, 2012-12-20T12:19:11, 2012-12-20T12:25:01, data

App 3: SN-Device, start, stop, location info, …
82031M6UV2F, 2012-12-20T12:21:23, 2012-12-20T12:21:55, data

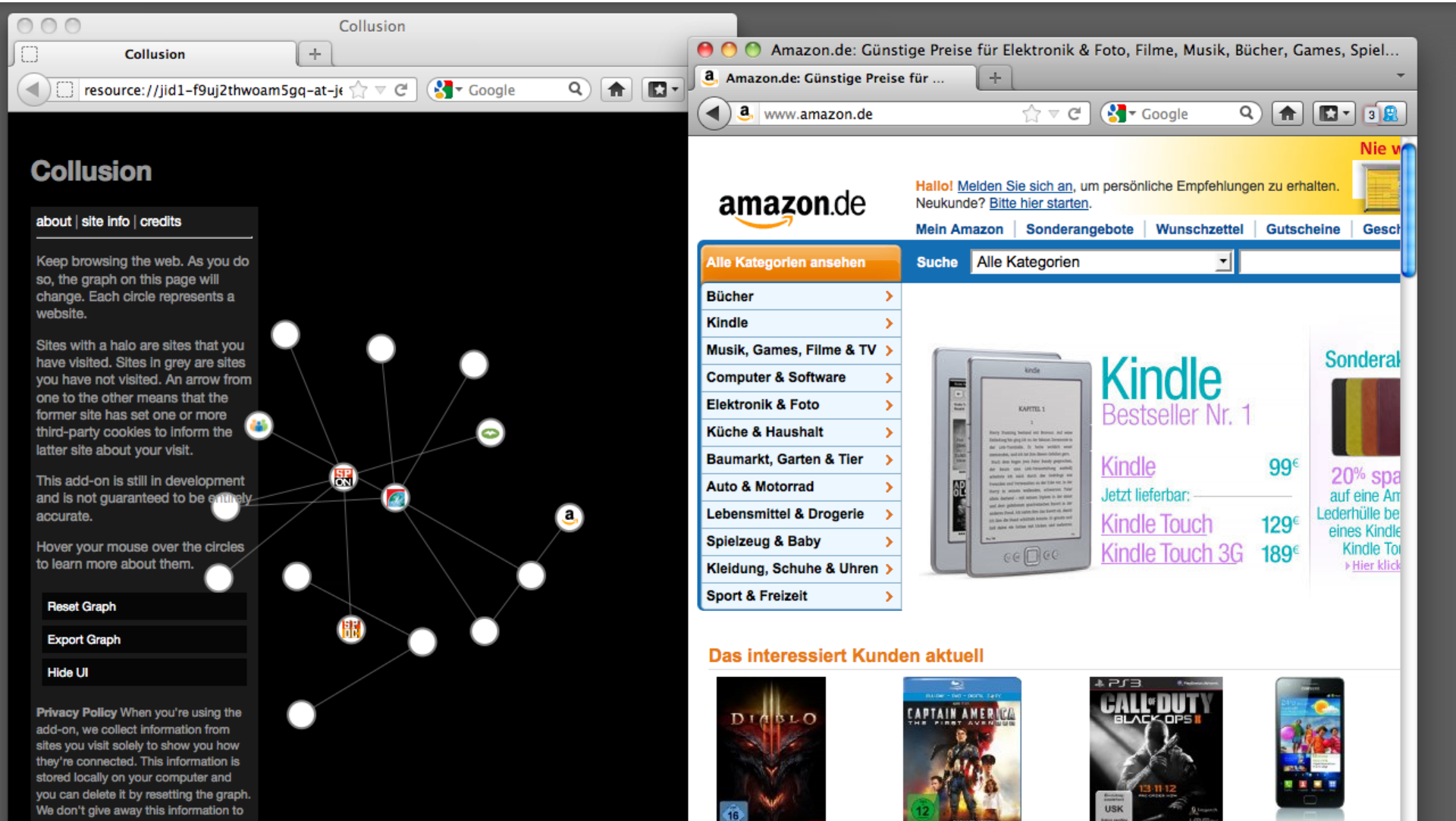


How to protect?

Lightbeam (Collusion) to visualize tracking

Left: Dependency graph

Right: Browser window



- Tracking with a «Browser Fingerprint» (without cookies)

- Tracking data and entropy:
  - User Agent: ca. 10 Bit
  - HTTP_ACCEPT Headers: ca. 7 Bit
  - Browser Plugin Details: ca. 20 Bit
  - Time Zone: ca. 2,5 Bit
  - Screen Size and Color Depth: ca. 5 Bit
  - System Fonts: >=21 Bit
  - Are Cookies Enabled? ca. 0,4 Bit
  - Limited supercookie test? ca. 1 Bit

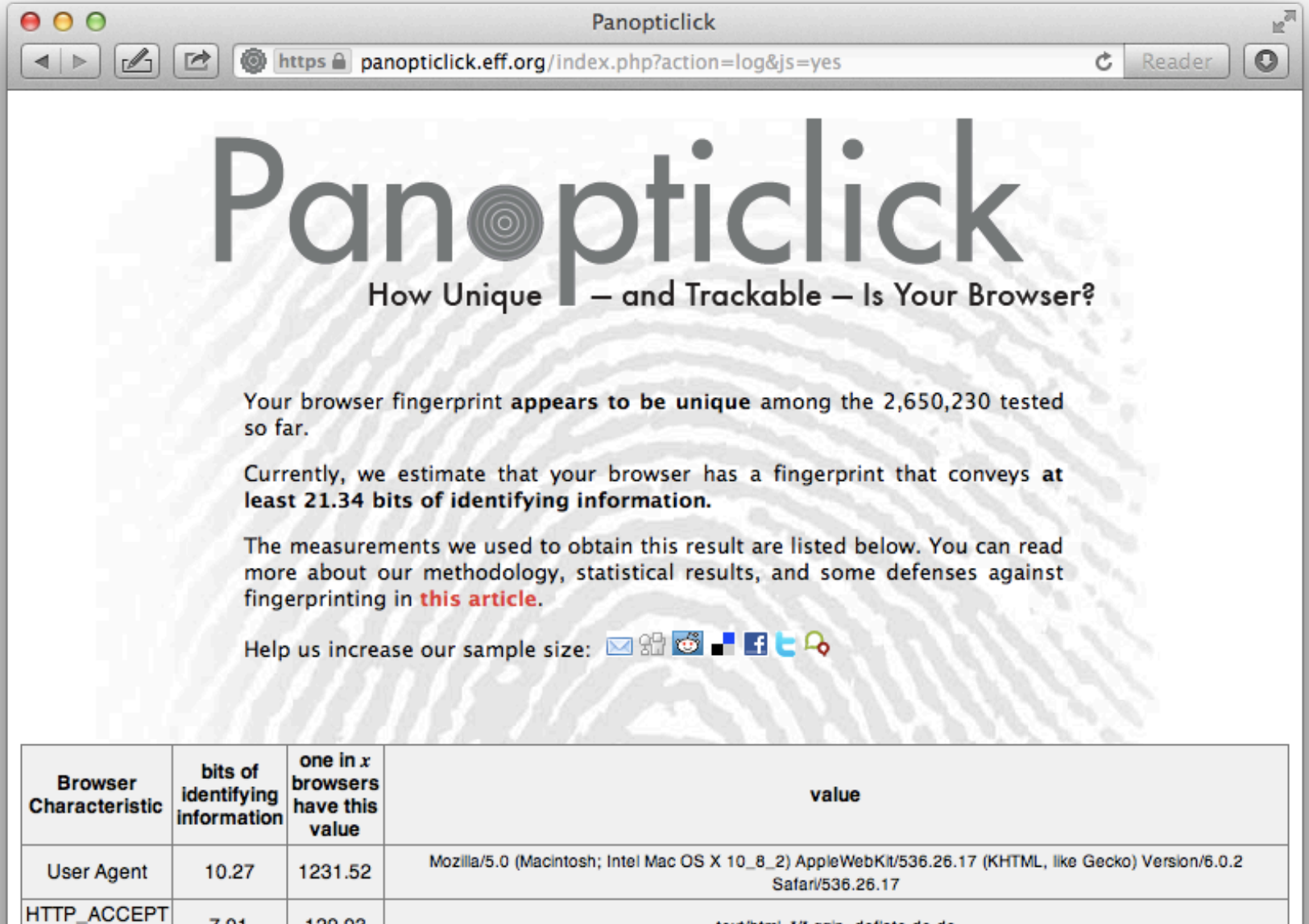
- https://panopticlick.eff.org

Panopticlick

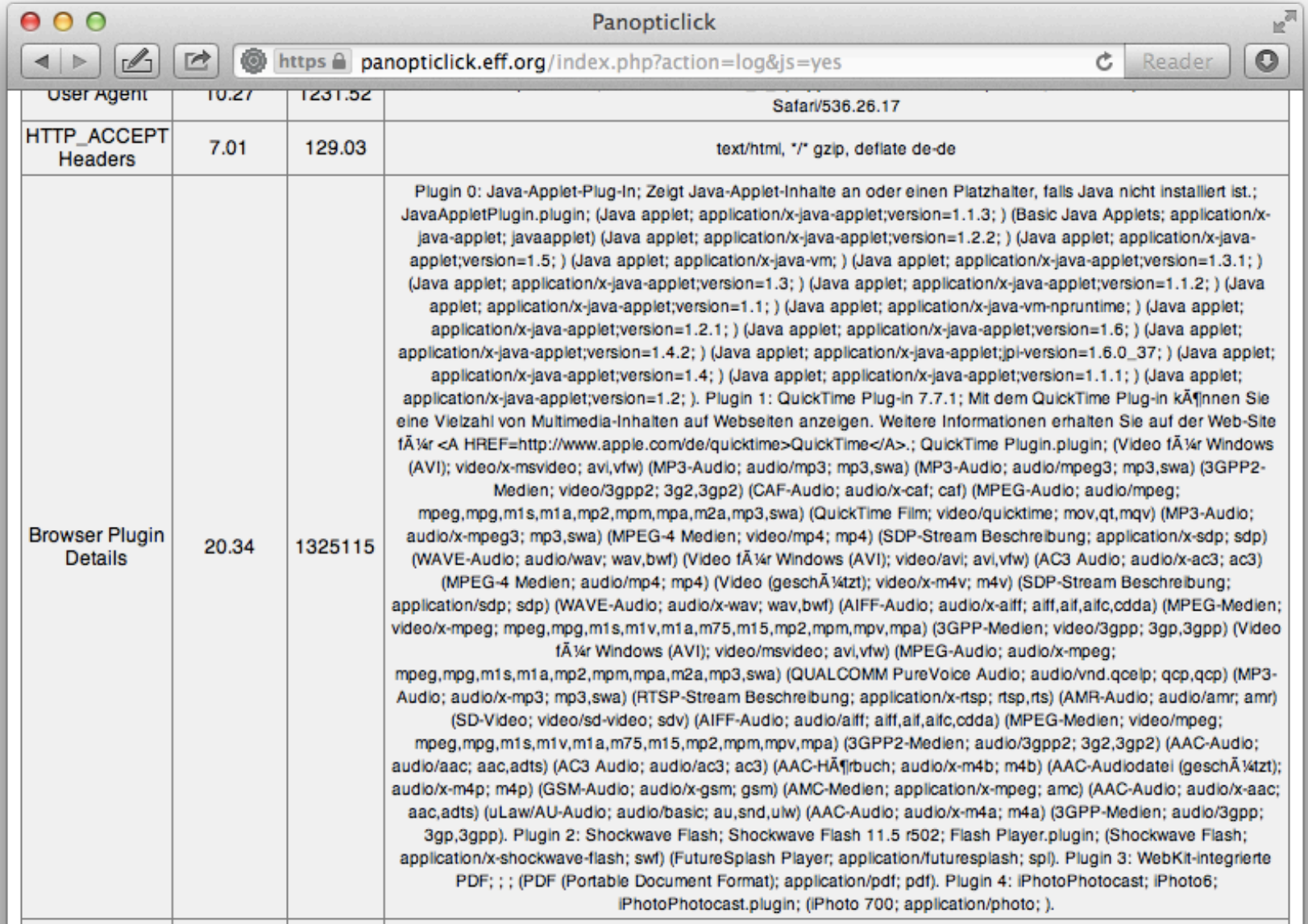
Eckersley 2010

Panopticlick

Eckersley 2010



Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
User Agent	10.27	1231.52	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_2) AppleWebKit/536.26.17 (KHTML, like Gecko) Version/6.0.2 Safari/536.26.17
HTTP_ACCEPT	7.01	129.02	



User Agent	10.27	1231.52	Safari/536.26.17
HTTP_ACCEPT Headers	7.01	129.03	text/html, */* gzip, deflate de-de
Browser Plugin Details	20.34	1325115	Plugin 0: Java-Applet-Plug-In; Zeigt Java-Applet-Inhalte an oder einen Platzhalter, falls Java nicht installiert ist.; JavaAppletPlugin.plugin; (Java applet; application/x-java-applet;version=1.1.3;) (Basic Java Applets; application/x-java-applet; javaapplet) (Java applet; application/x-java-applet;version=1.2.2;) (Java applet; application/x-java-applet;version=1.5;) (Java applet; application/x-java-vm;) (Java applet; application/x-java-applet;version=1.3.1;) (Java applet; application/x-java-applet;version=1.3;) (Java applet; application/x-java-applet;version=1.1.2;) (Java applet; application/x-java-applet;version=1.1;) (Java applet; application/x-java-vm-npruntime;) (Java applet; application/x-java-applet;version=1.2.1;) (Java applet; application/x-java-applet;version=1.6;) (Java applet; application/x-java-applet;version=1.4.2;) (Java applet; application/x-java-applet;jpi-version=1.6.0_37;) (Java applet; application/x-java-applet;version=1.4;) (Java applet; application/x-java-applet;version=1.1.1;) (Java applet; application/x-java-applet;version=1.2;). Plugin 1: QuickTime Plug-in 7.7.1; Mit dem QuickTime Plug-in kÃ¶nnen Sie eine Vielzahl von Multimedia-Inhalten auf Webseiten anzeigen. Weitere Informationen erhalten Sie auf der Web-Site fÃ¼r <A HREF=http://www.apple.com/de/quicktime>QuickTime</A>.; QuickTime Plugin.plugin; (Video fÃ¼r Windows (AVI); video/x-msvideo; avi,vfw) (MP3-Audio; audio/mp3; mp3,swa) (MP3-Audio; audio/mpeg3; mp3,swa) (3GPP2-Medien; video/3gpp2; 3g2,3gp2) (CAF-Audio; audio/x-caf; caf) (MPEG-Audio; audio/mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a,mp3,swa) (QuickTime Film; video/quicktime; mov,qt,mqv) (MP3-Audio; audio/x-mpeg3; mp3,swa) (MPEG-4 Medien; video/mp4; mp4) (SDP-Stream Beschreibung; application/x-sdp; sdp) (WAVE-Audio; audio/wav; wav,bwf) (Video fÃ¼r Windows (AVI); video/avi; avi,vfw) (AC3 Audio; audio/x-ac3; ac3) (MPEG-4 Medien; audio/mp4; mp4) (Video (geschÃ¼tzt); video/x-m4v; m4v) (SDP-Stream Beschreibung; application/sdp; sdp) (WAVE-Audio; audio/x-wav; wav,bwf) (AIFF-Audio; audio/x-aiff; aiff,aif,aifc,cdda) (MPEG-Medien; video/x-mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (3GPP-Medien; video/3gpp; 3gp,3gpp) (Video fÃ¼r Windows (AVI); video/msvideo; avi,vfw) (MPEG-Audio; audio/x-mpeg; mpeg,mpg,m1s,m1a,mp2,mpm,mpa,m2a,mp3,swa) (QUALCOMM PureVoice Audio; audio/vnd.qcelp; qcp,qcp) (MP3-Audio; audio/x-mp3; mp3,swa) (RTSP-Stream Beschreibung; application/x-rtsp; rtsp,rts) (AMR-Audio; audio/amr; amr) (SD-Video; video/sd-video; sdv) (AIFF-Audio; audio/aiff; aiff,aif,aifc,cdda) (MPEG-Medien; video/mpeg; mpeg,mpg,m1s,m1v,m1a,m75,m15,mp2,mpm,mpv,mpa) (3GPP2-Medien; audio/3gpp2; 3g2,3gp2) (AAC-Audio; audio/aac; aac,adts) (AC3 Audio; audio/ac3; ac3) (AAC-HÃ¶rbuch; audio/x-m4b; m4b) (AAC-Audiodatei (geschÃ¼tzt); audio/x-m4p; m4p) (GSM-Audio; audio/x-gsm; gsm) (AMC-Medien; application/x-mpeg; amc) (AAC-Audio; audio/x-aac; aac,adts) (uLaw/AU-Audio; audio/basic; au,snd,ulw) (AAC-Audio; audio/x-m4a; m4a) (3GPP-Medien; audio/3gpp; 3gp,3gpp). Plugin 2: Shockwave Flash; Shockwave Flash 11.5 r502; Flash Player.plugin; (Shockwave Flash; application/x-shockwave-flash; swf) (FutureSplash Player; application/futuresplash; spl). Plugin 3: WebKit-integrierte PDF; ; ; (PDF (Portable Document Format); application/pdf; pdf). Plugin 4: iPhotoPhotocast; iPhoto6; iPhotoPhotocast.plugin; (iPhoto 700; application/photo;).

Device Fingerprinting

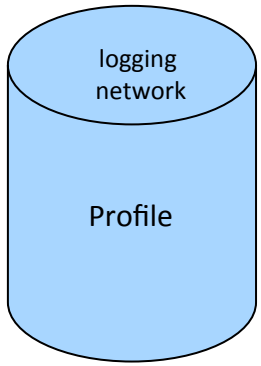
- Unique? App
  - Shows possible device identifiers
  - Developed at University of Erlangen

http://www.iphone-ticker.de/oh-mein-gott-so-eindeutig-laesst-jedes-iphone-zuordnen-66244/

App 1: SN-Device, start, stop, …
82031M6UV2F, 2012-12-19T16:39:57, 2012-12-19T16:45:33

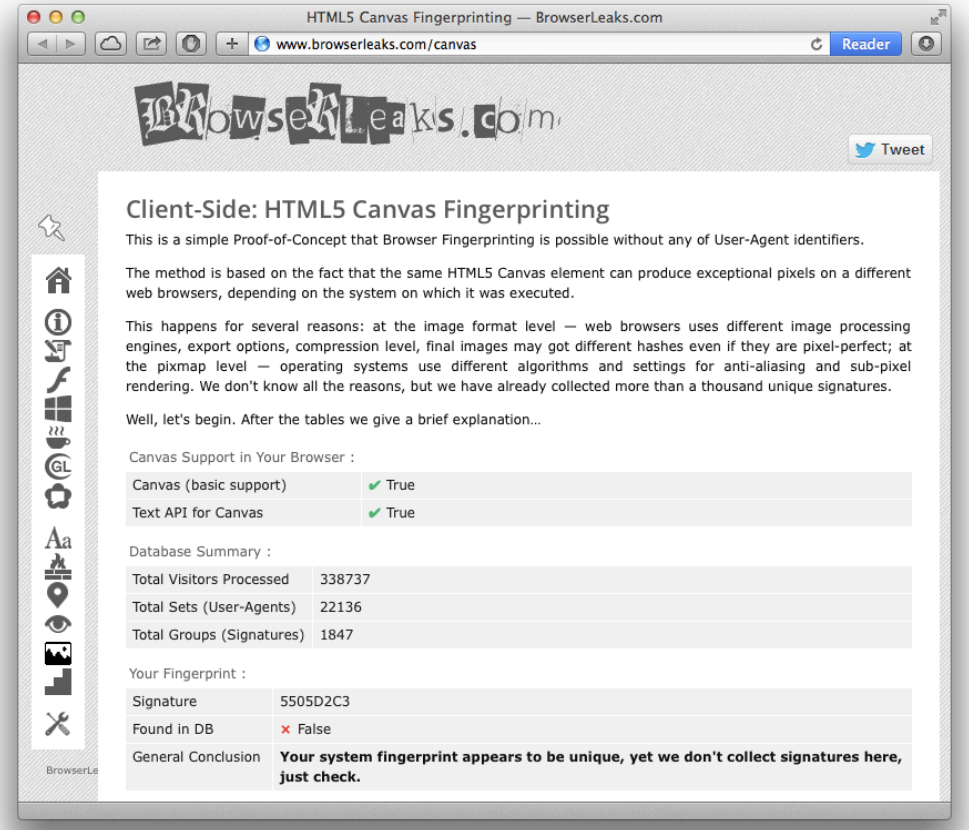
App 2: SN-Device, start, stop, address book, …
82031M6UV2F, 2012-12-20T12:19:11, 2012-12-20T12:25:01, data

App 3: SN-Device, start, stop, location info, …
82031M6UV2F, 2012-12-20T12:21:23, 2012-12-20T12:21:55, data



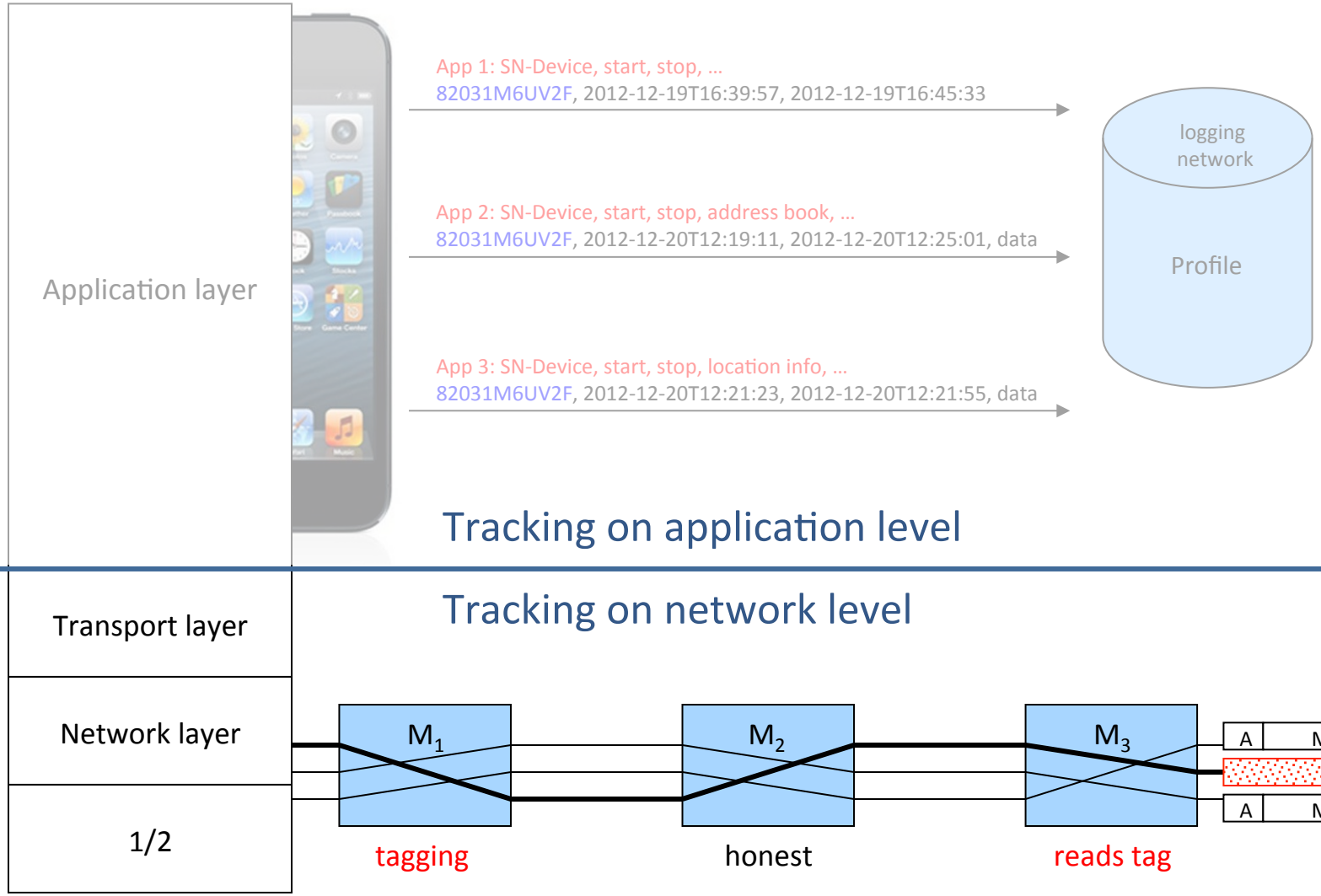
Canvas Fingerprinting

- Tracking by use of individual device visualization differences within a http canvas element

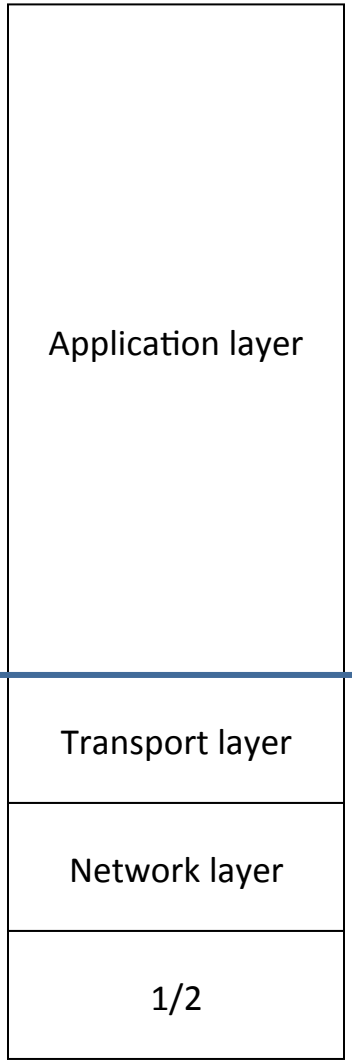


Gunes Acar, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, Claudia Diaz. The Web never forgets: Persistent tracking mechanisms in the wild. CCS 2014

Anonymity and unobservability and ISO OSI network levels



Anonymity and unobservability and ISO OSI network levels



Tracking on application level

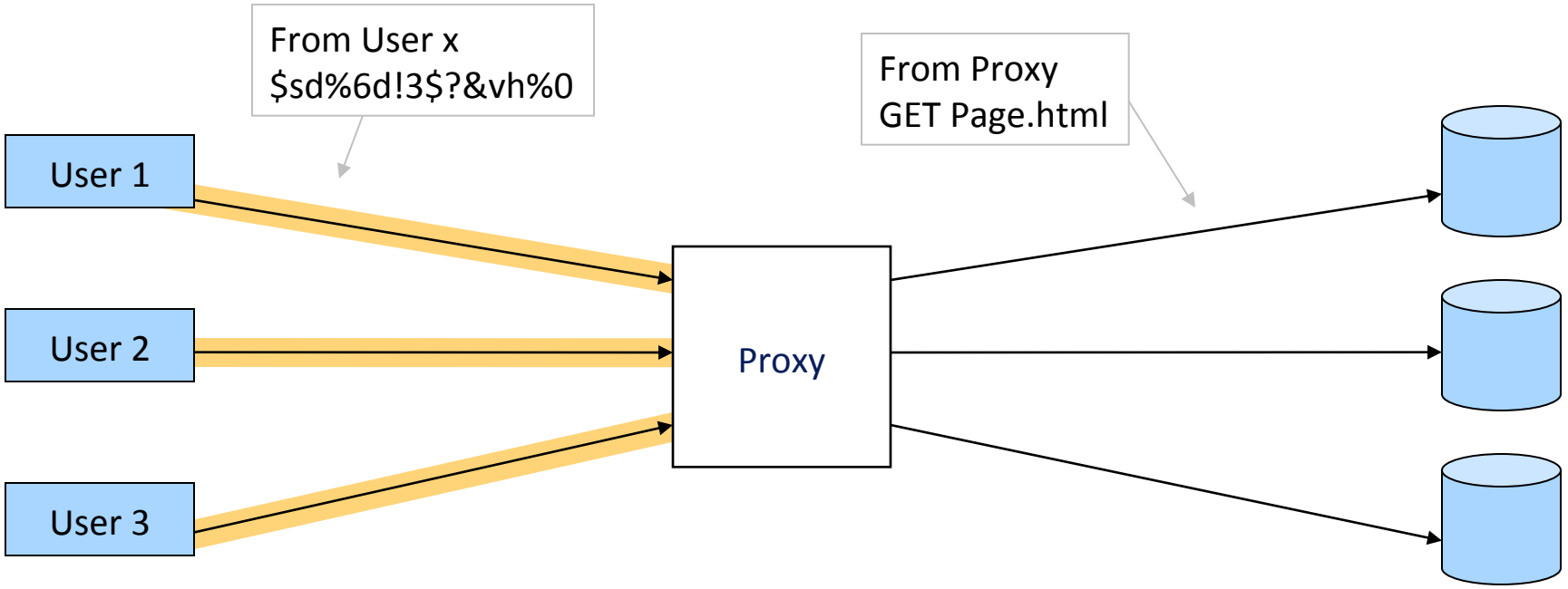
- Hiding transactions
  - Pseudonyms
  - Credentials (link properties to pseudonyms)
- Encryption

Tracking on network level against …

- outsiders
  - Proxies
- insiders
  - Broadcast
  - Blind message service
  - DC network
  - MIX network

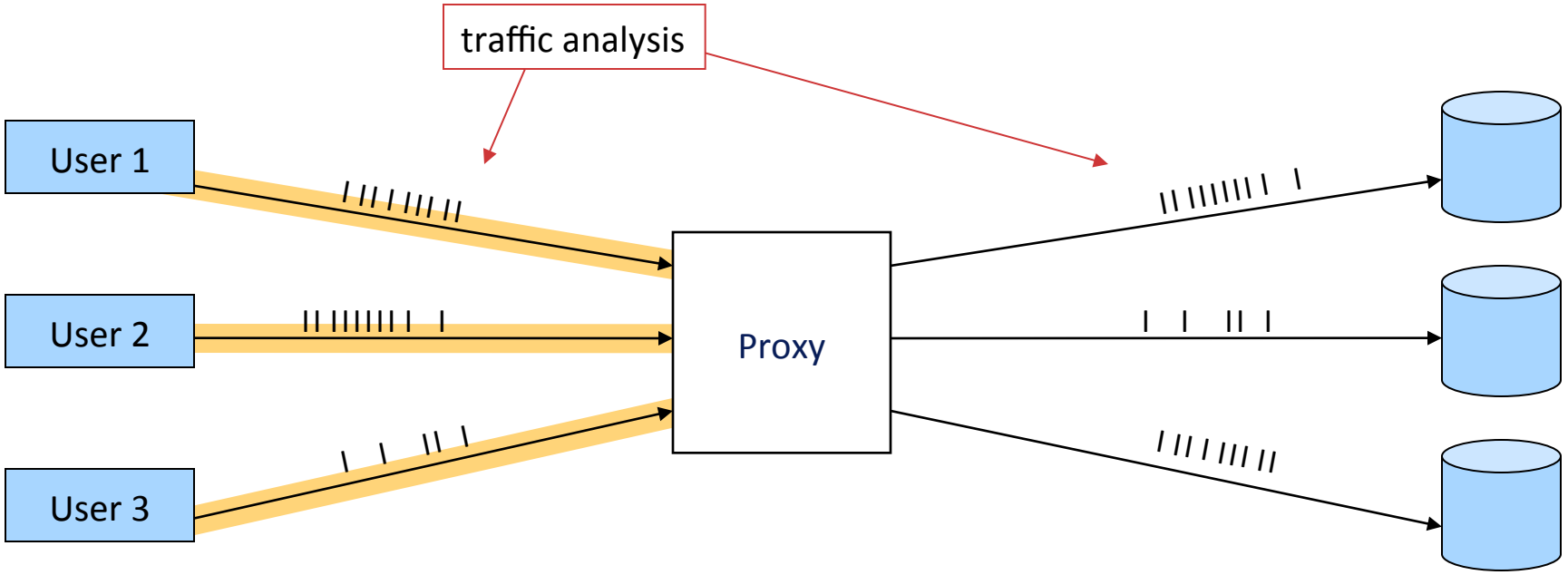
Proxies: Outsider

- Against weak outsider attacks
  - Use Proxy a mediator:
    - Users need to trust the proxy
    - proxy knows all communication relations
  - Encryption — does not protect from traffic analysis

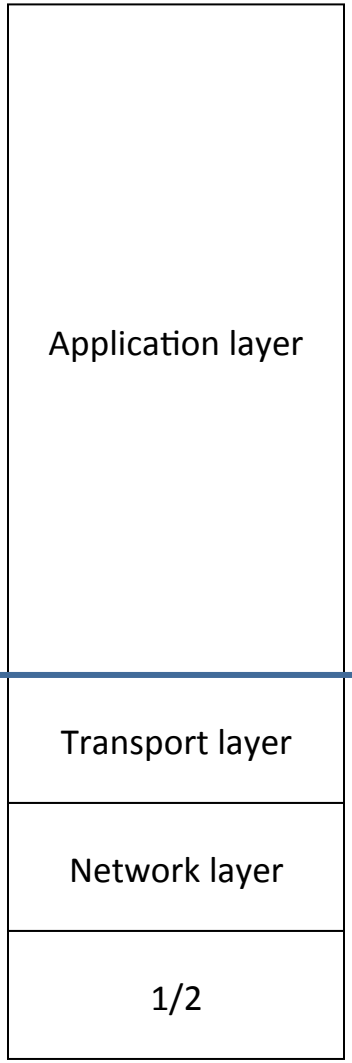


Proxies: Outsider

- Against weak outsider attacks
  - Use Proxy a mediator:
    - Users need to trust the proxy
    - proxy knows all communication relations
  - Encryption — does not protect from traffic analysis



Anonymity and unobservability and ISO OSI network levels



Tracking on application level

- Hiding transactions
  - Pseudonyms
  - Credentials (link properties to pseudonyms)
- Encryption

Tracking on network level against …

- outsiders
  - Proxies
- insiders
  - Broadcast
  - Blind message service
  - DC network
  - MIX network

Broadcast

- The past...

  - Reading newspapers
  - Radio via antenna
  - TV via broadcasting cannels (cable, antenna)

- Broadcast and implicit addressing (for point-to-point communication)
  - Protects the *recipient*
  - *All recipients* get all (encrypted) messages
  - *Locally* select content from broadcast channel
  - Hides who is interested in what

Broadcast

- Present
  - Video on Demand
  - Internet radio
  - News online
  - No privacy!
  - No protection?
- The past ... (broadcast)
  - Reading newspapers
  - Radio via antenna
  - TV via broadcasting cannels (cable, antenna)
- Broadcast and implicit addressing (for point-to-point communication)
  - Protects the *recipient*
  - *All recipients* get all (encrypted) messages
  - *Locally* select content from broadcast channel
  - Hides who is interested in what

Broadcast

- Present
  - Video on Demand
  - Internet radio
  - News online
  - No privacy!
  - No protection?
- The past ... (broadcast)
  - Reading newspapers
  - Radio via antenna
  - TV via broadcasting cannels (cable, antenna)
- The message is

Keep the broadcast channels alive!

Protection of recipient: Broadcast

Pfitzmann 1993

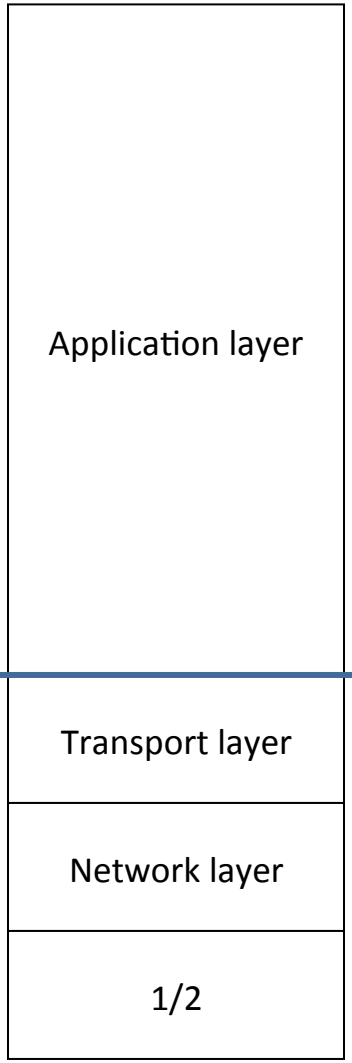
- Addressing
  - explicit addresses: Routing
  - implicit addresses: Characteristic pattern for receiver station
    - covered: (Public Key) Encryption System
    - open: (Pseudo) Random Number Generator
- Examples
  - Paging of connection requests to mobile users
  - No storage of location information

		public address	private address
implicit address	covered	very expensive, use for first contact	expensive
	open	do not used	continually change after first contact

Implicit Addresses

- First contact: covered implicit address CIA
  - Recipient publishes public encryption key c
  - Sender creates CIA := c (R , S , M)
    - Redundancy R
    - Seed S of a pseudo-random generator PRG
    - Message M (optional)
  - Recipient decrypts all received messages with private key d
    - Finds correct R for own messages only
- Following addressing: open implicit address OIA
  - OIA_{i+1} := PRG (i , S) (i = 0,1,2,…)
    - Sender calculates next OIA
    - encrypts message M (optional)
    - Sends OIA , M
  - Receiver: Associative memory with valid OIAs to recognize messages

Anonymity and unobservability and ISO OSI network levels



Tracking on application level

- Hiding transactions
  - Pseudonyms
  - Credentials (link properties to pseudonyms)
- Encryption

Tracking on network level against …

- outsiders
  - Proxies
- insiders
  - Broadcast
  - Blind message service
  - DC network
  - MIX network

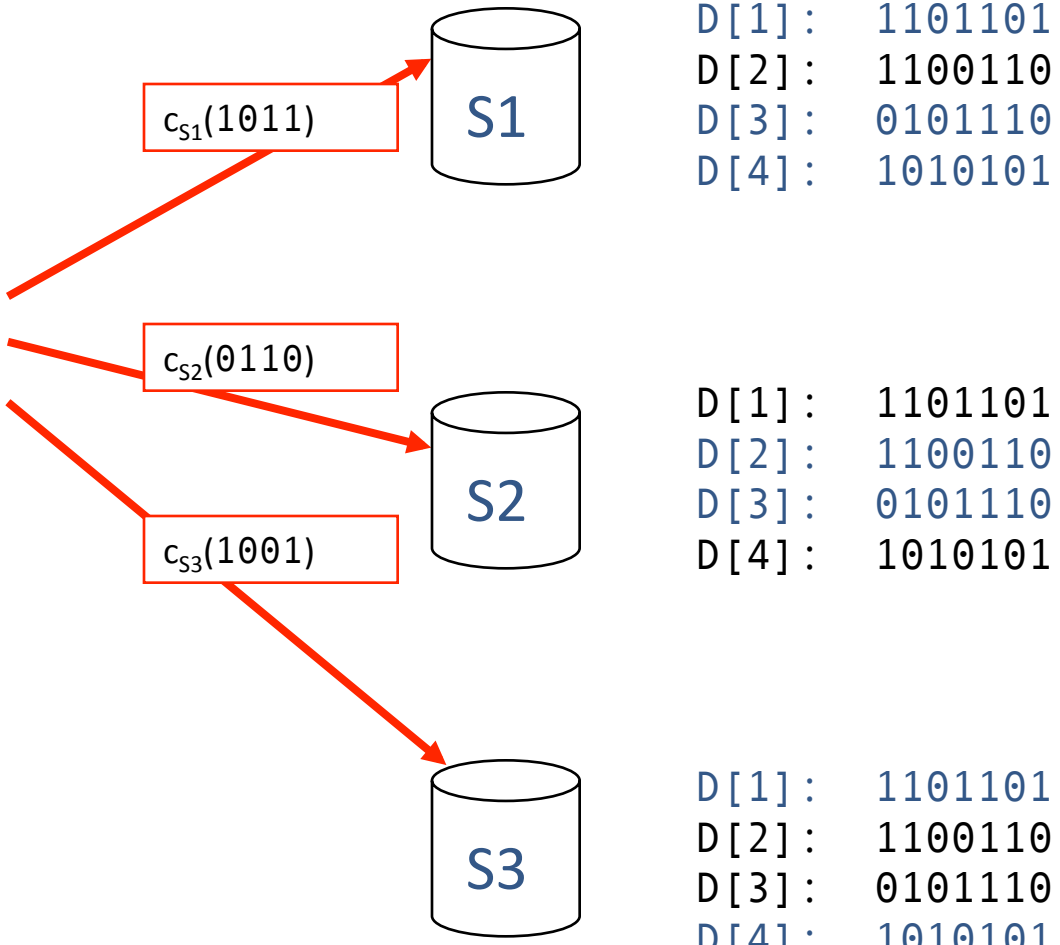
Blind-Message-Service: Query

Cooper, Birman, 1995

Client queries for D[2]:

Index = 1234

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



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

Blind-Message-Service: Answer

Cooper, Birman, 1995

Client queries for D[2]:

Index = 1234

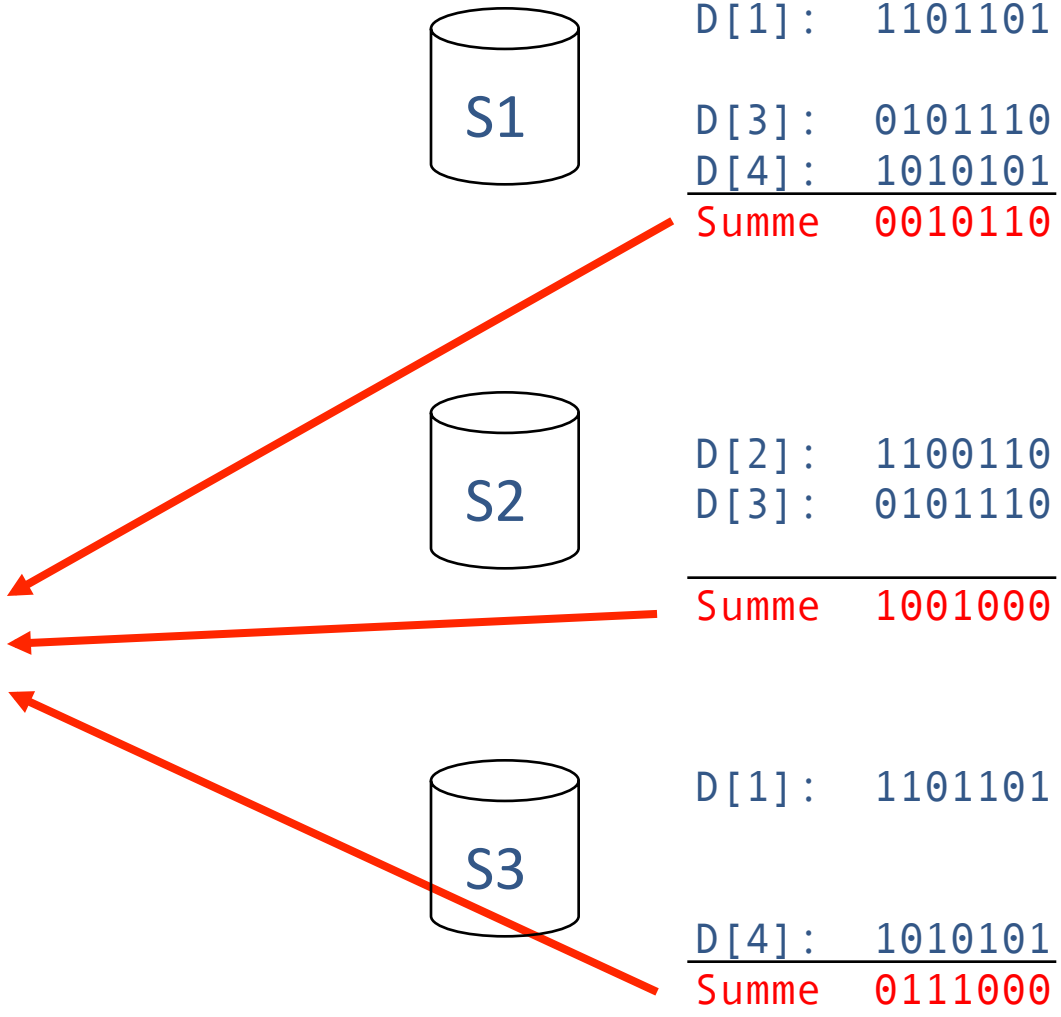
Set vector = 0100
Choose randomly request(S1) = 1011
Choose randomly request(S2) = 0110
Calculate (xor) request(S3) = 1001

Answers from

S1: 0010110
S2: 1001000
S3: 0111000

xor of the sums from
S1, S2 and S3 equals to D[2]: 1100110

- Link encryption between client and databases

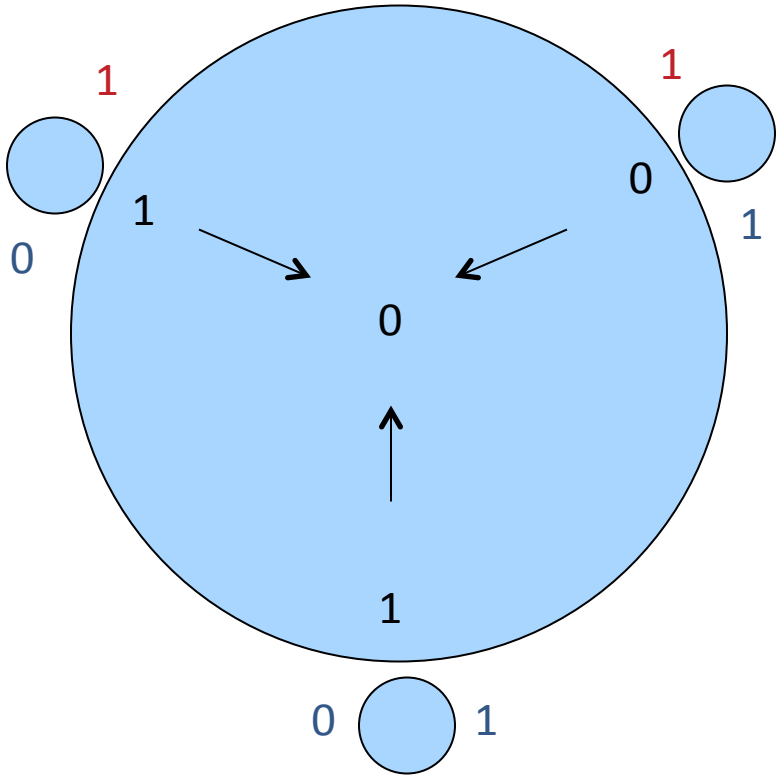


DC network

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

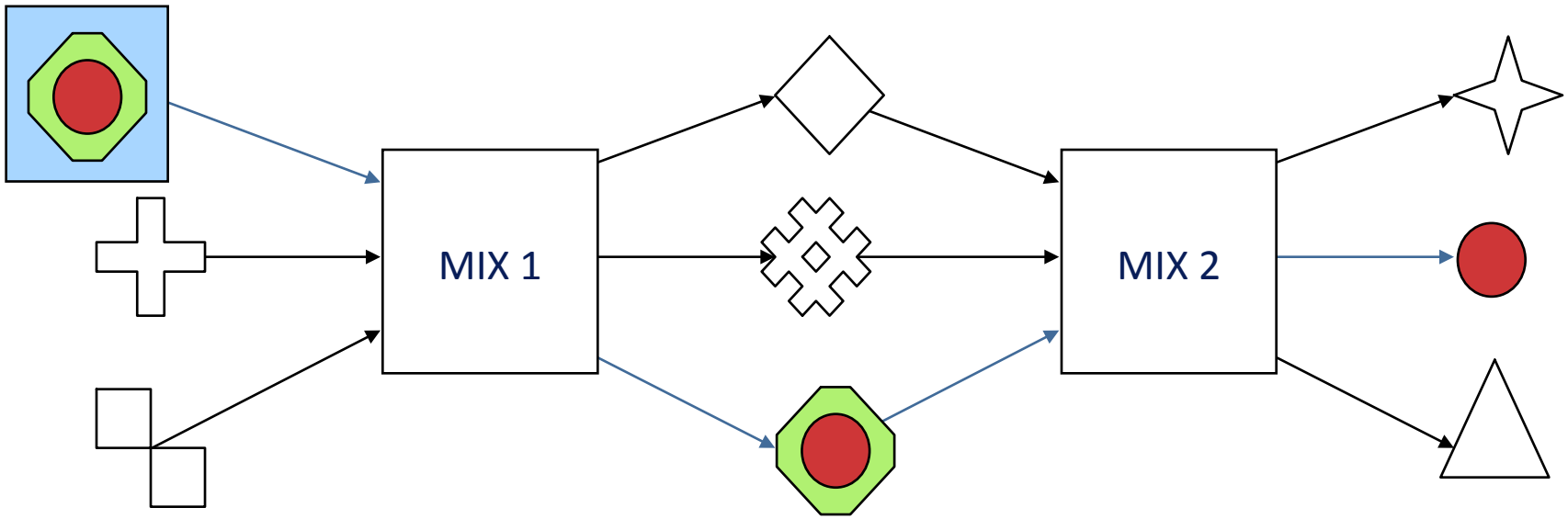


Who has paid?

Mix network

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

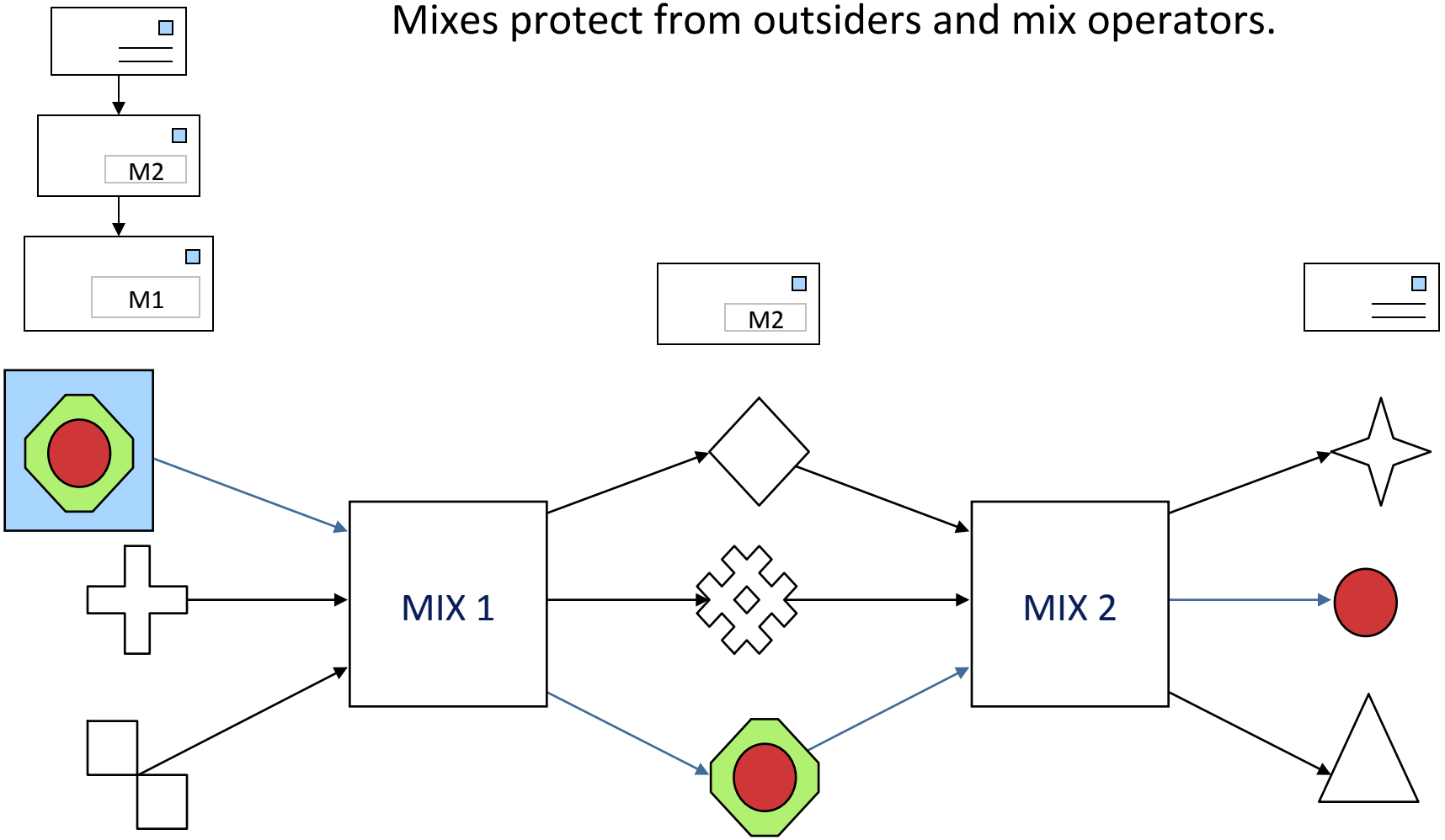


Mix network

Chaum, 1981

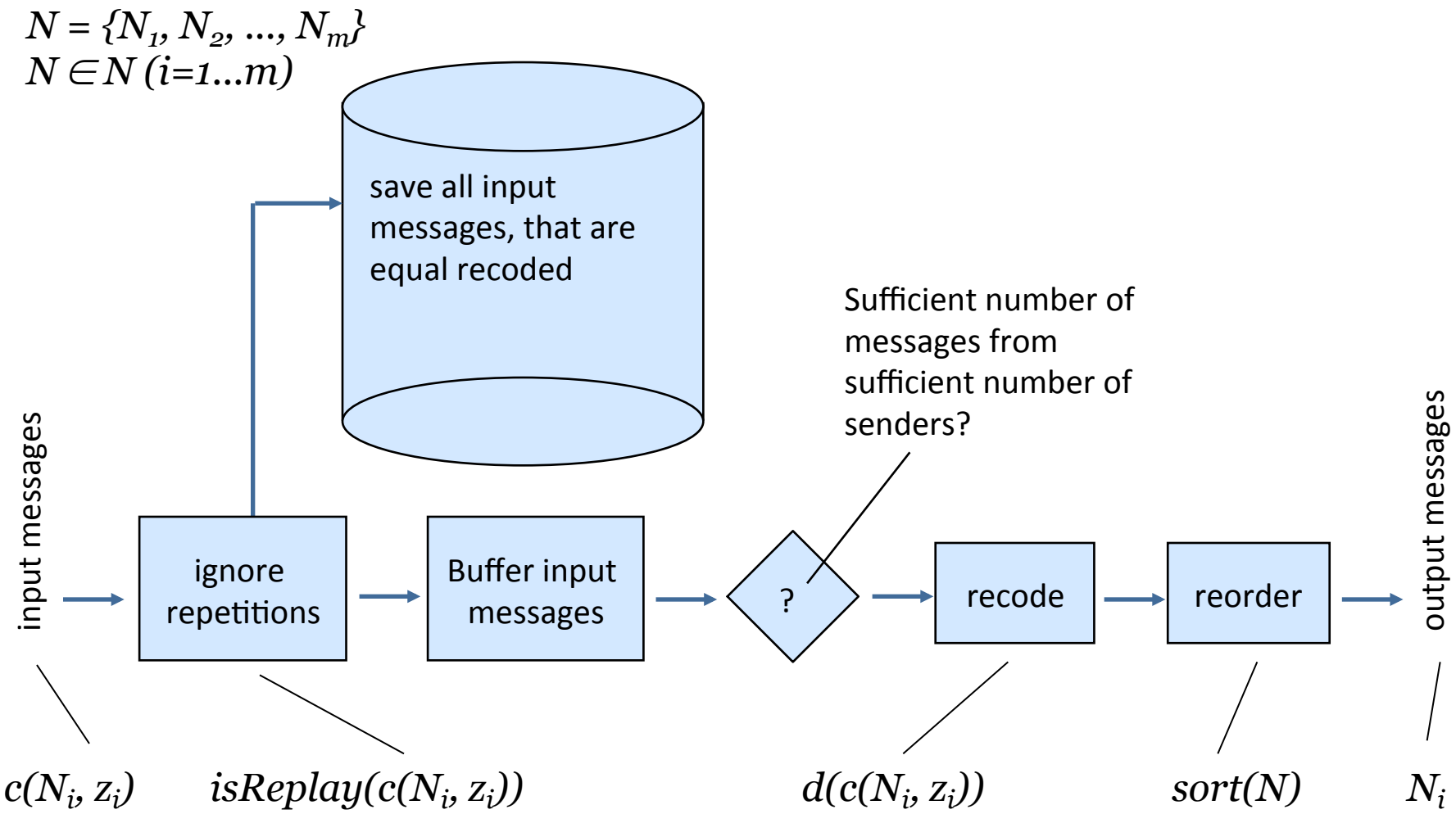
- Perfect unlinkability of sender and recipient

Mixes protect from outsiders and mix operators.

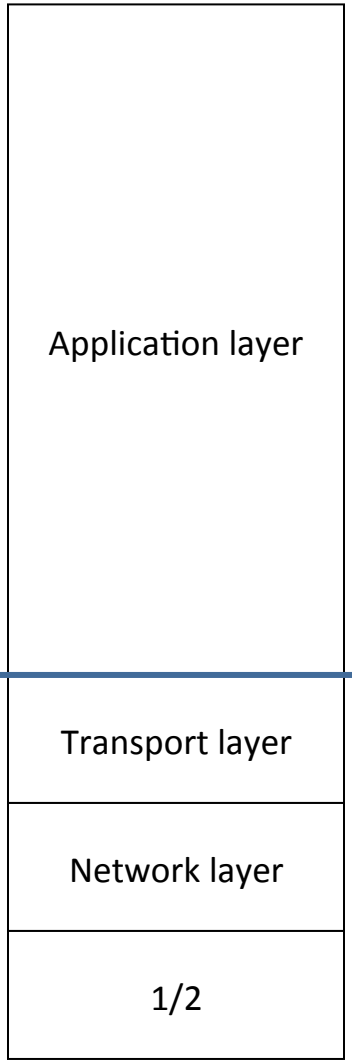


Block diagram of mix

Chaum, 1981



Anonymity and unobservability and ISO OSI network levels



Tracking on application level

- Hiding transactions
  - Pseudonyms
  - Credentials (link properties to pseudonyms)
- Encryption

Tracking on network level against …

- outsiders
  - Proxies
- insiders
  - Broadcast
  - Blind message service
  - DC network
  - MIX network

Timeline of development of Privacy Enhancing Technologies

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
1999 Zeroknowledge Freedom Anonymizer
2000 AN.ON/JAP Anonymizer
2004 TOR

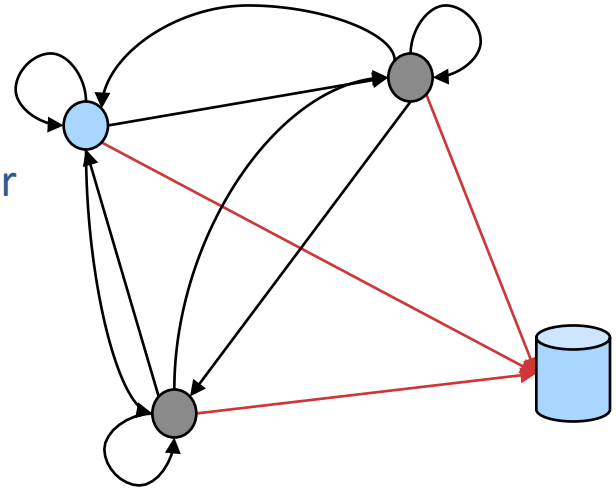
Basic concepts

Applications

Crowds

Mike Reiter, Avi Rubin, AT&T, 1997

- Web request is directly sent to the server with a probability P or alternatively (with 1-P) to other participants (Jondo)
  - Symmetric encryption connection between the users
- Embedded objects (images etc.) requested by last Jondo
  - Prevent request-bursts
- Security characteristics
  - User can always say, his Jondo received the request for forwarding
- Weaknesses
  - Traffic analysis possible
  - Jondos can read and track contents (problematic for personalized sites)



Timeline of development

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
1999 Zeroknowledge Freedom Anonymizer
2000 AN.ON/JAP Anonymizer
2004 TOR

David Chaum (*1955)

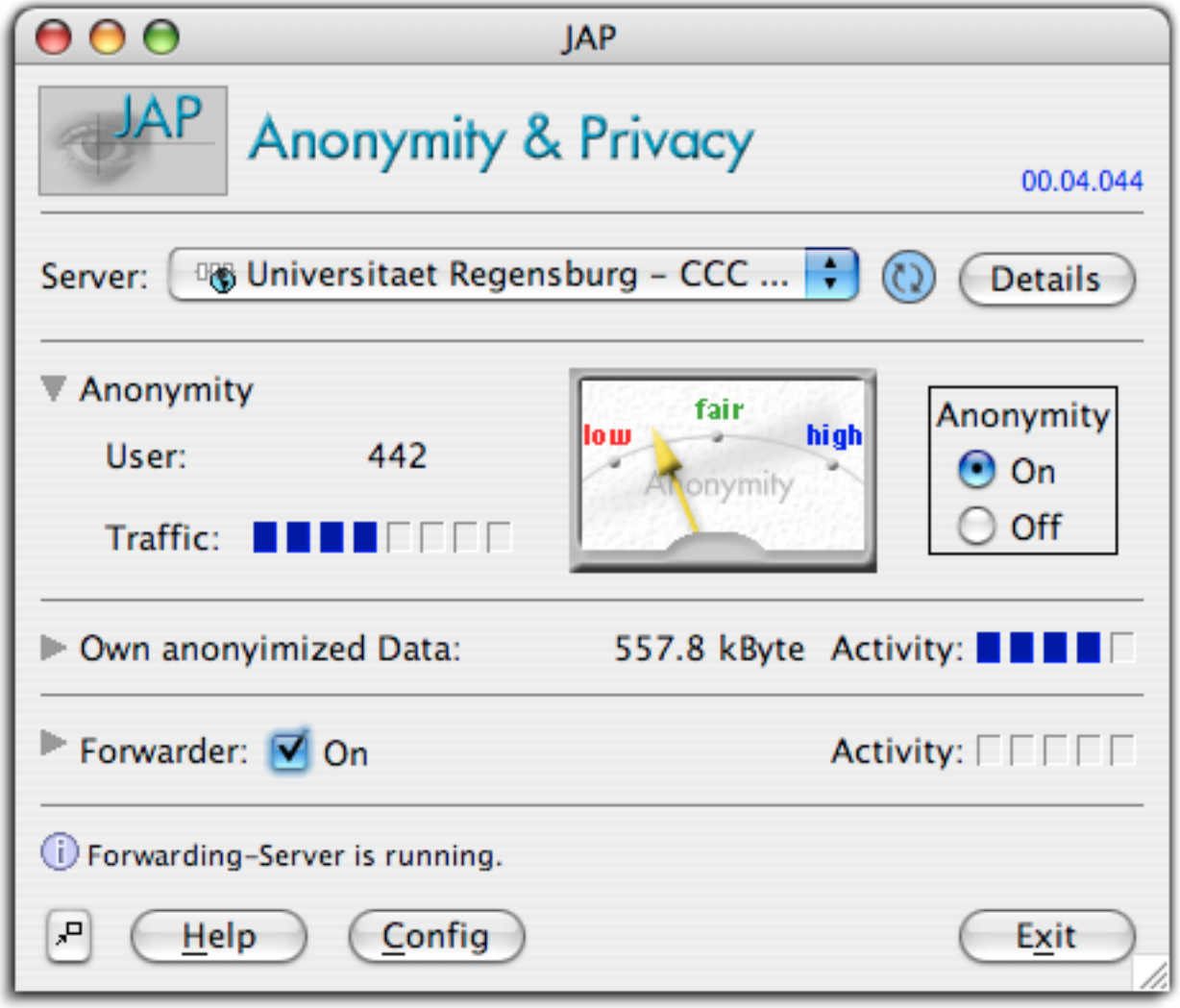
Source: Wikipedia

Timeline of development

Andreas Pfitzmann (1958-2010)

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
1999 Zeroknowledge Freedom Anonymizer
2000 AN.ON/JAP Anonymizer
2004 TOR

AN.ON/JAP anonymizer



For free at www.anon-online.de

First test version has been launched in October 2000

Full service has been running since February 2001

AN.ON/JAP anonymizer

Sponsor: BMWA, Partners: TU Dresden, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, FU Berlin, HU Berlin, Universität Regensburg, Medizinische Universität Lübeck, Chaos Computer Club, Ulmer Akademie für Datenschutz und IT-Sicherheit, RWTH Aachen, New York University

Mix based solution for anonymous Internet access

OpenSource

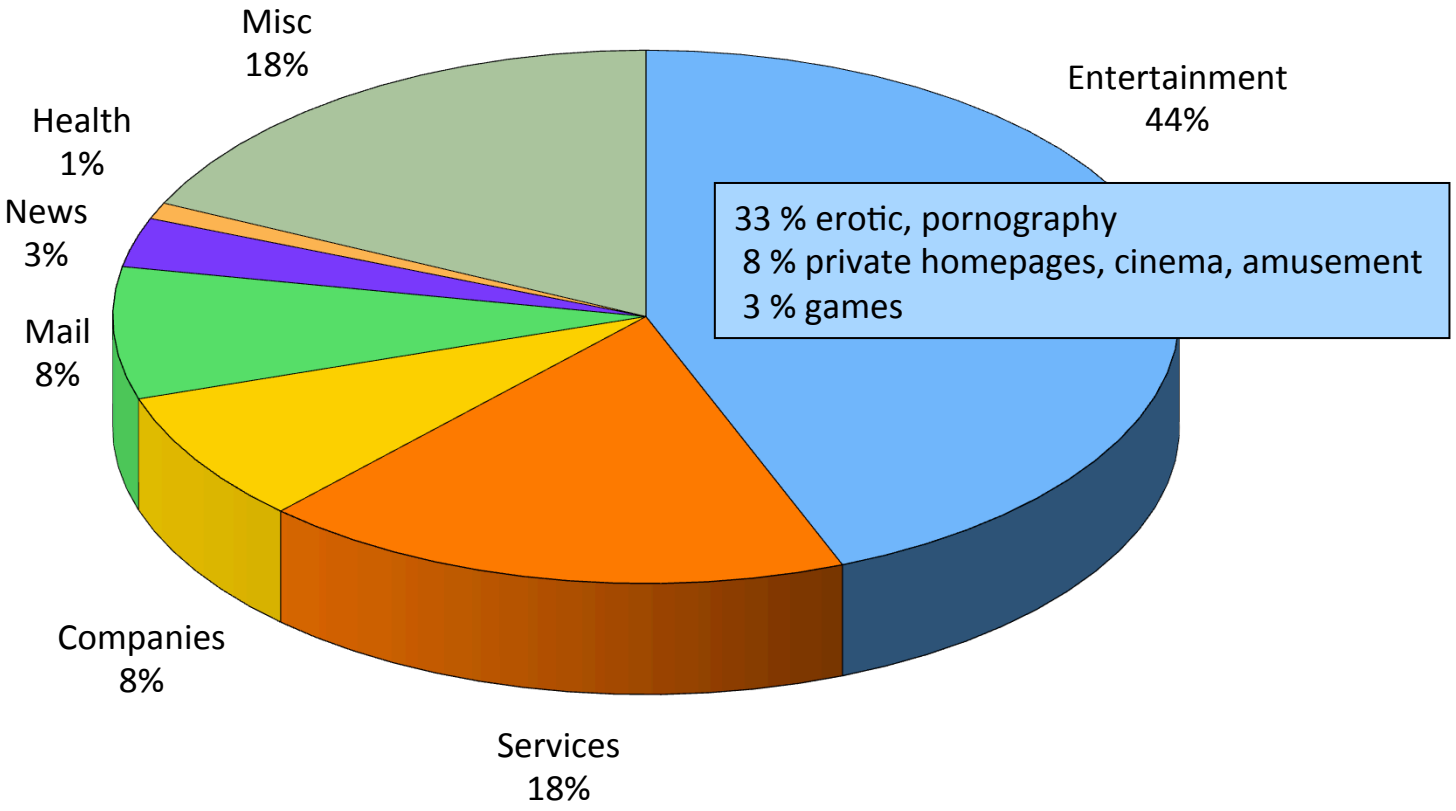
>10.000 users

>6 TByte per month

www.anon-online.de

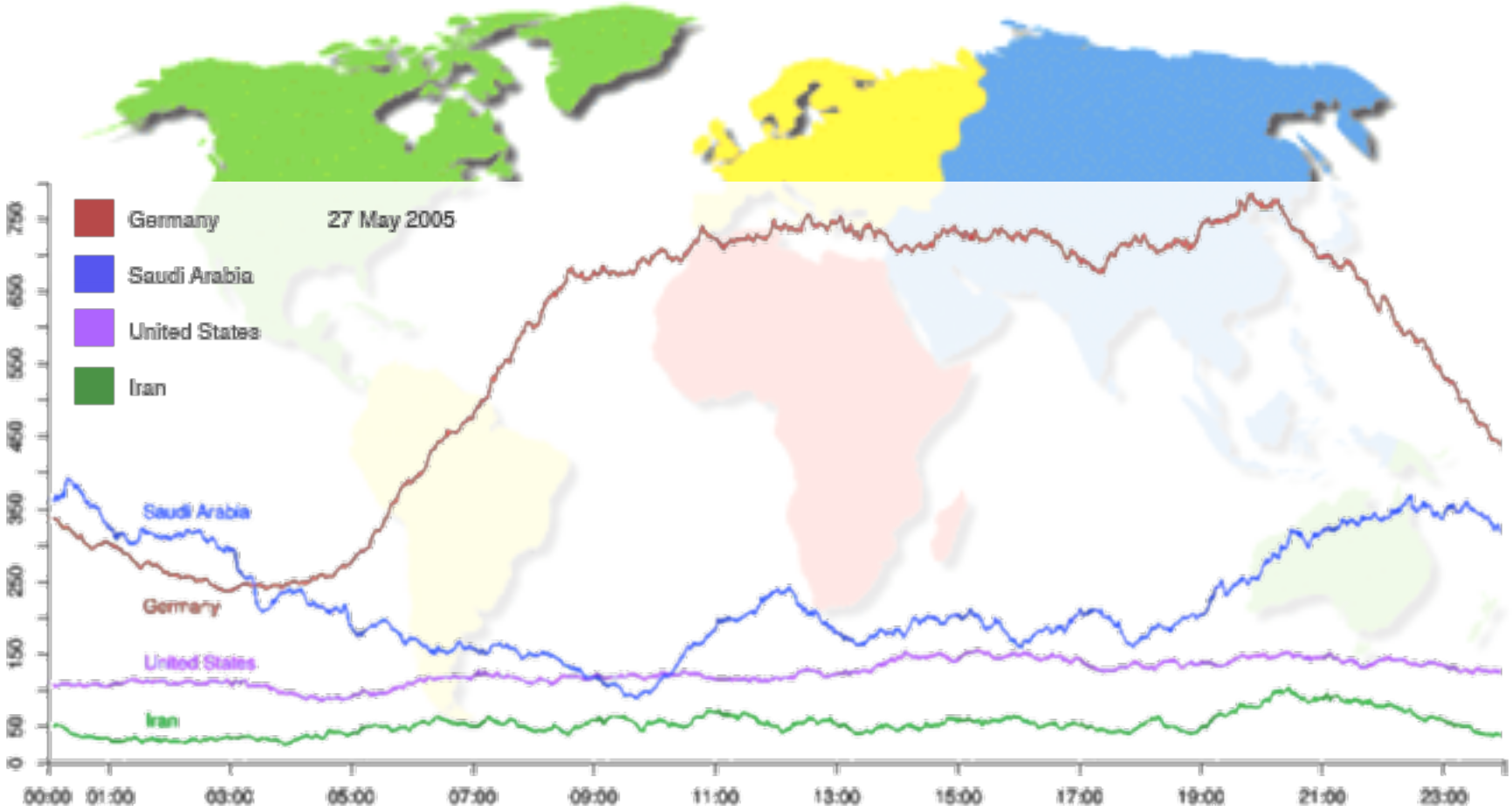
Anonymized content

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



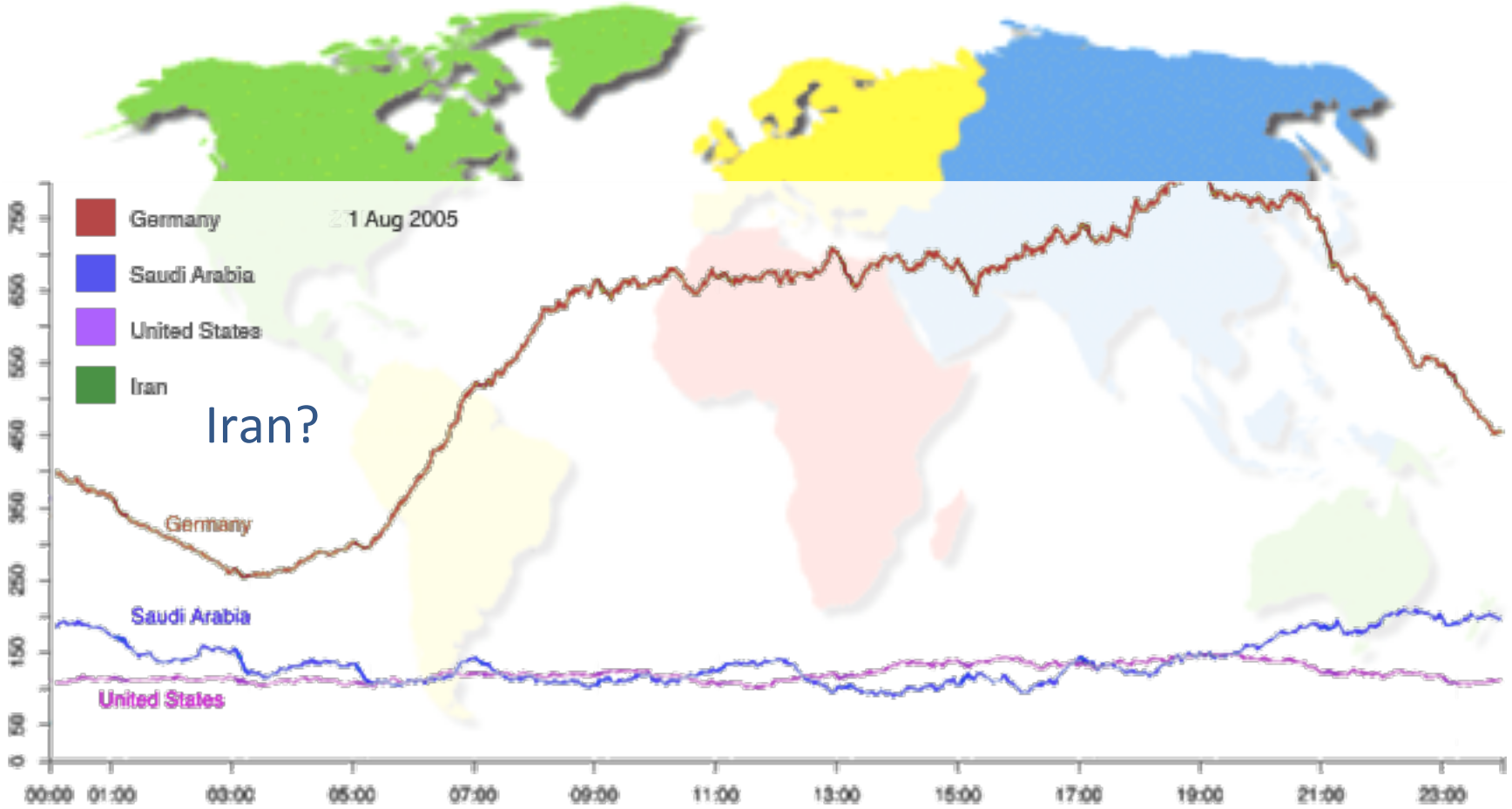
Regions of users

- Dayline of 27 May 2005

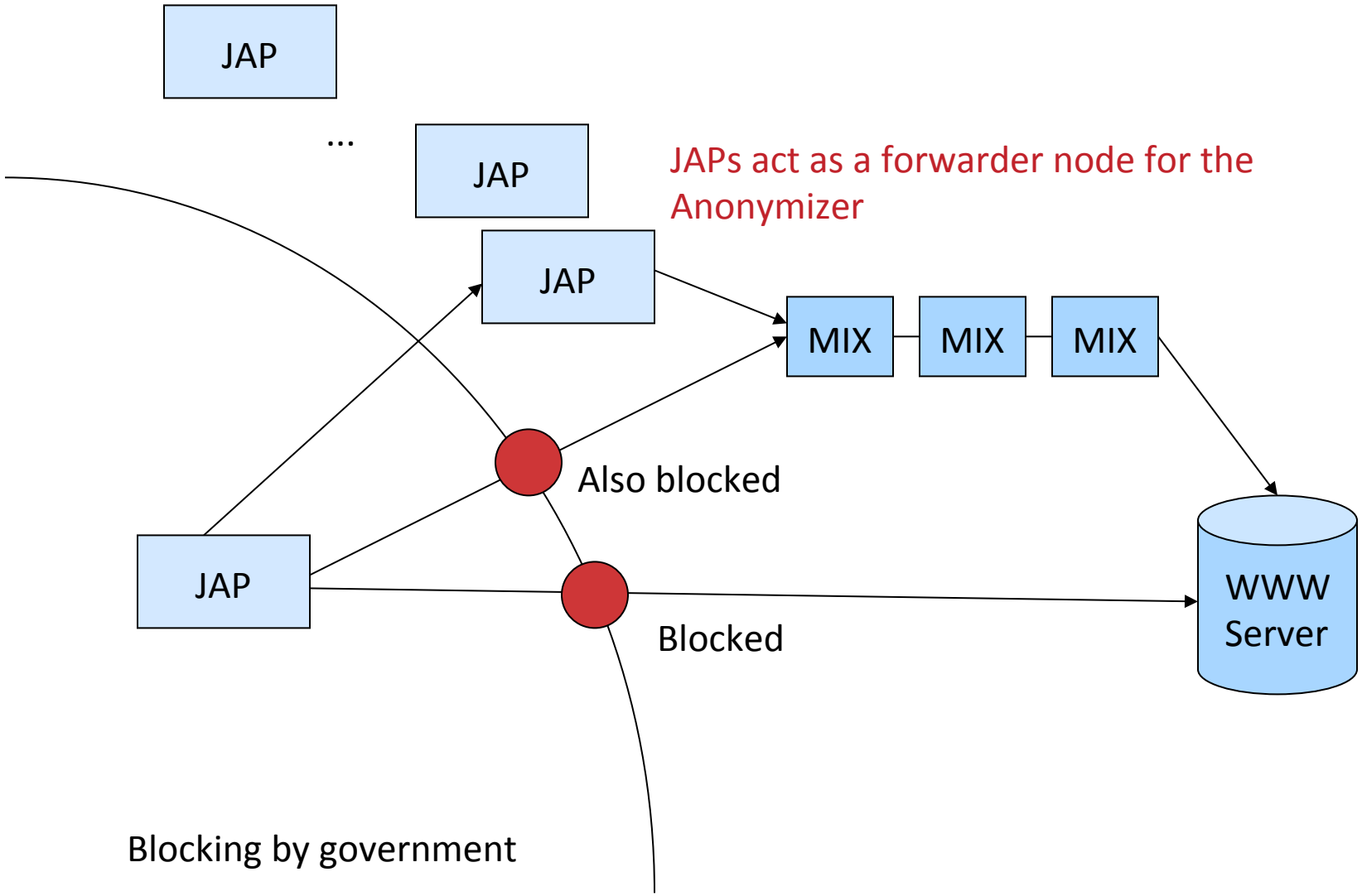


Regions of users

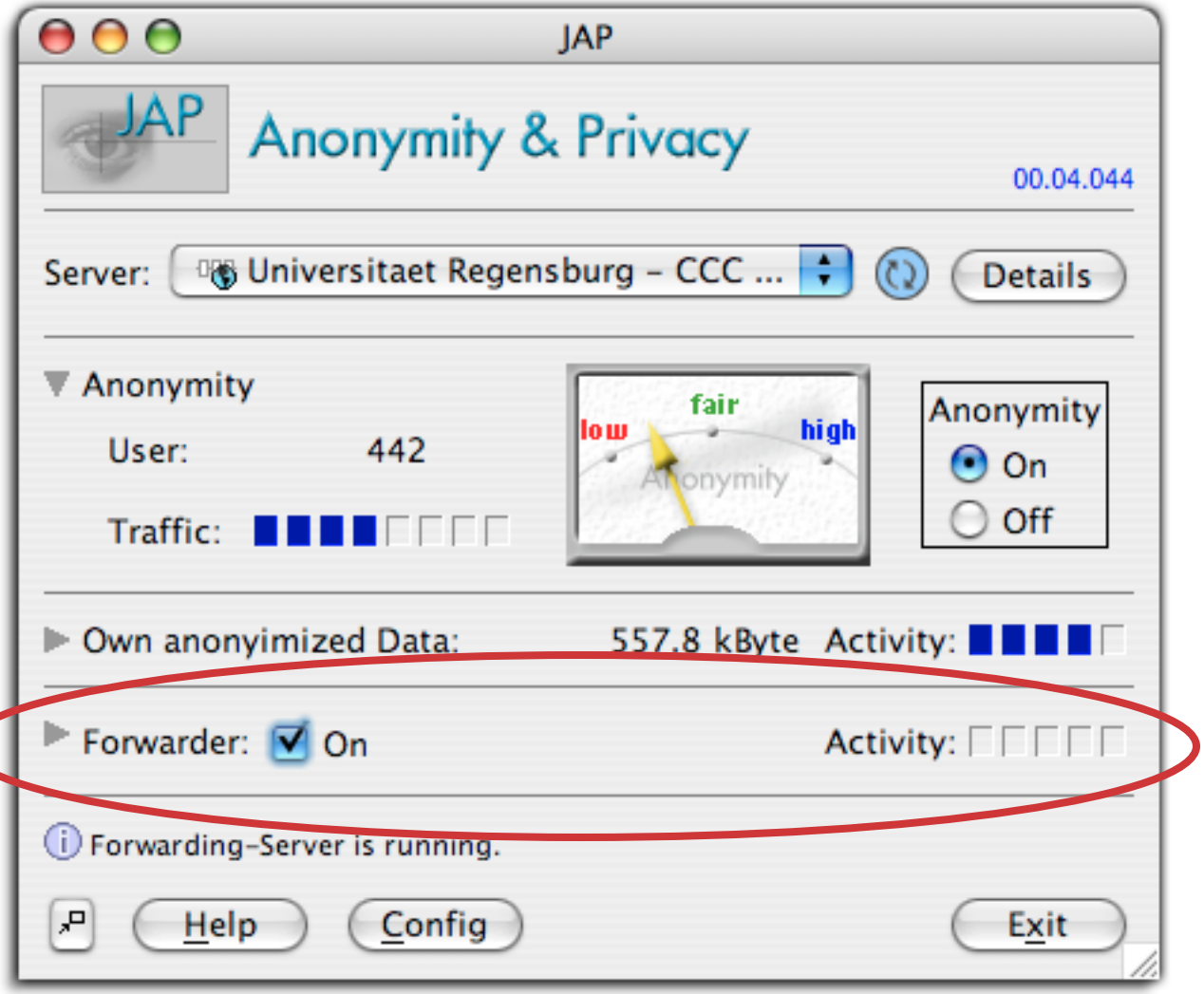
- Dayline of 1 Aug 2005



Censor-free Internet access



Censor-free Internet access

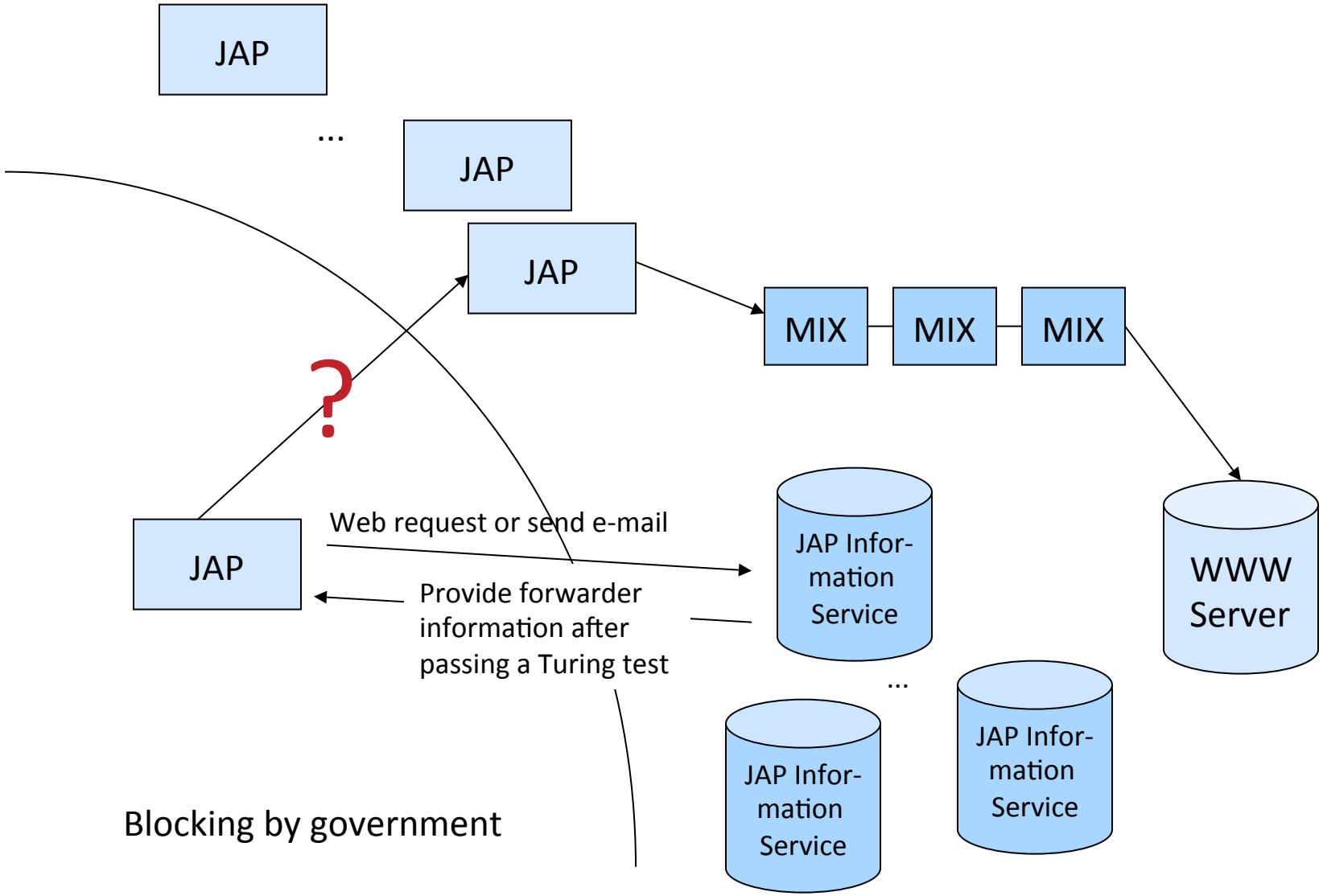


JAP users can share their bandwidth with blocked JAP users

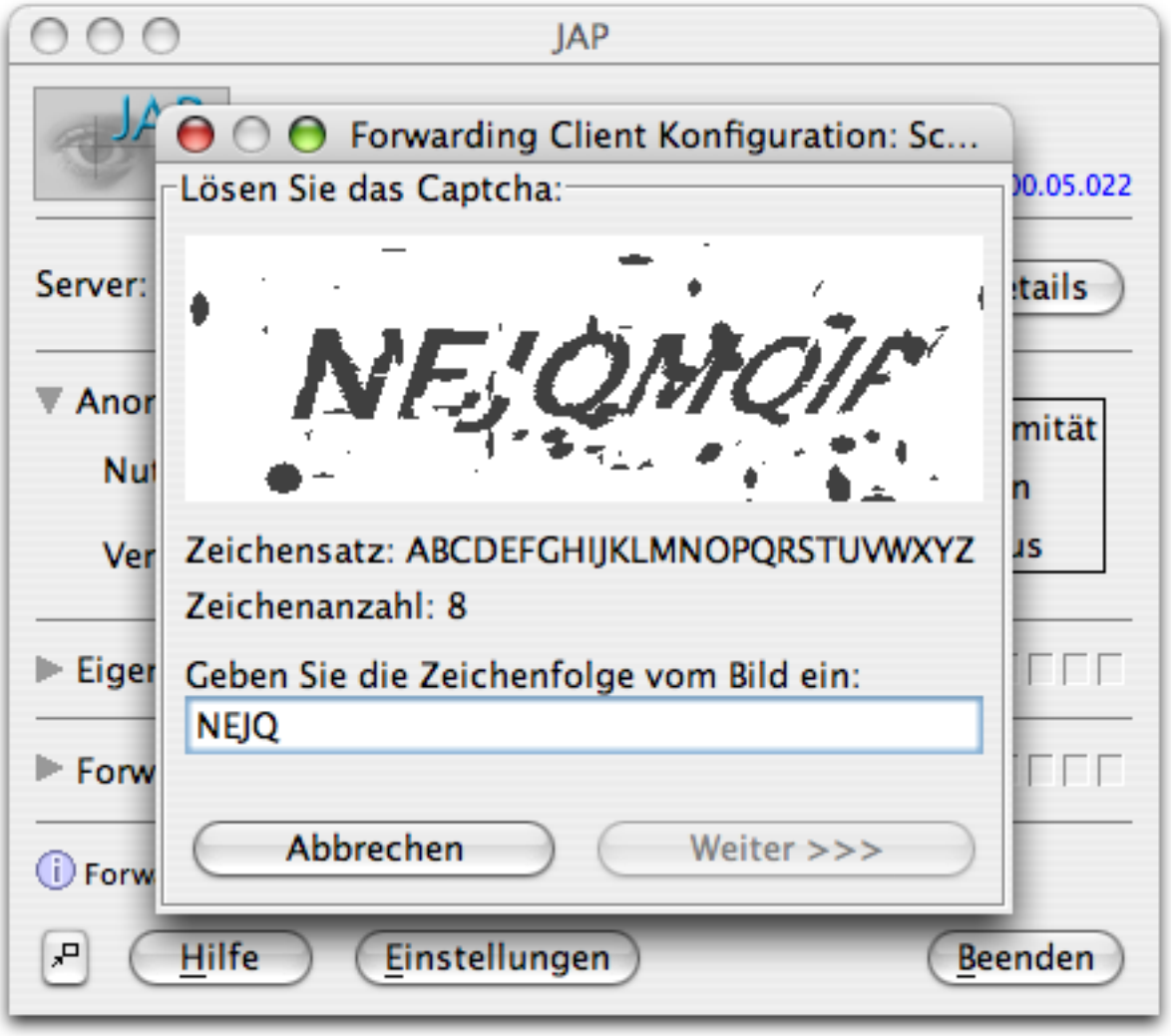
Requests are anonymized through the Mix network

Forwarders gain no information about contents of forwarded requests

Censor-free Internet access



Censor-free Internet access



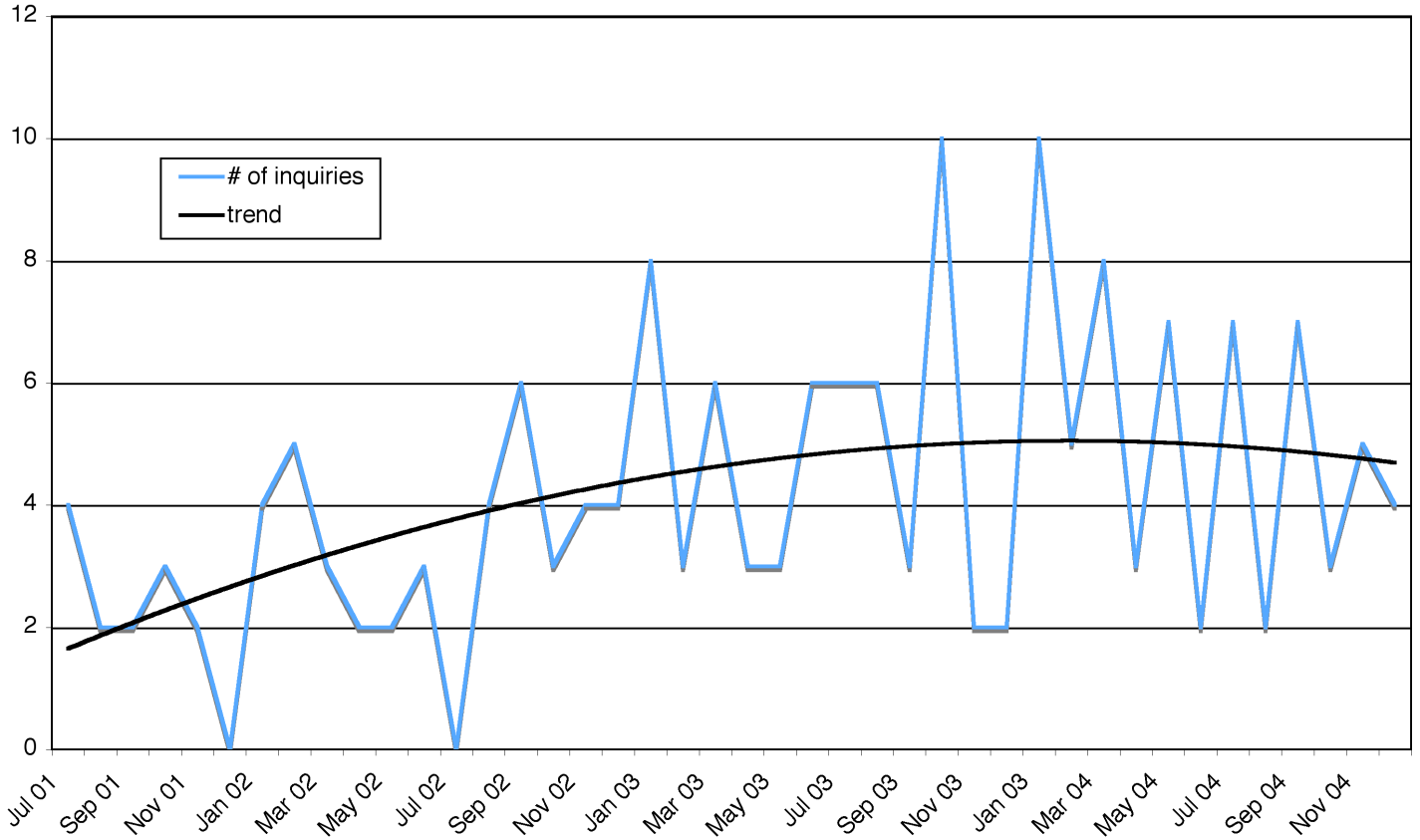
InfoService is sending the IP number of one forwarder after passing a Turing test

Challenges and Problems

- Blocking possible – censorship resistance
- Criminal misuse – data retention?
- Correlation attacks still possible – improved algorithms needed
- Traffic overload – lightweight anonymity

Misuse

- JAP project (2000-2010)
  - Avg. 4-5 inquiries per month by law enforcement agencies and private persons



Misuse

- JAP project (2000-2010)
  - Avg. 4-5 inquiries per month by law enforcement agencies and private persons
  - > 6 Terabytes per month of anonymized data

- Typical inquiry
  - Date and time of access, IP address anonymizing service
  - Inquiry: Identification request (name, address) for user behind that IP address
    - Anonymizer is misunderstood as an Internet Service Provider (ISP)

Misuse

- Typical crimes committed by use of JAP (suspicion)
  - credit card fraud,
  - computer fraud,
  - sending malicious code to vulnerable web servers,
  - insult,
  - defamation,
  - death thread,
  - access to child pornography

- Observation
  - While the traffic anonymized by the system increased over the time the number of inquiries did not

Challenges and Problems

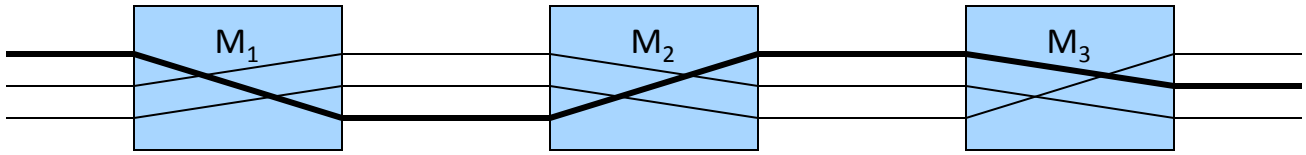
- Blocking possible – censorship resistance
- Criminal misuse – data retention?
- Correlation attacks still possible – improved algorithms needed
- Traffic overload – lightweight anonymity

Tagging attack on anonymous channels

Raymond, 2000 (Wei Dai, 1999)

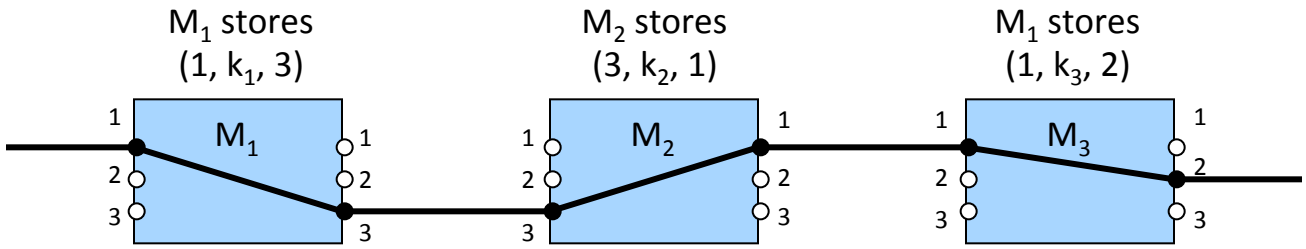
Phase 1: Asymm. Channel setup message: $N_1=c_1(k_1, c_2(k_2, c_3(k_3)))$

No Attacker



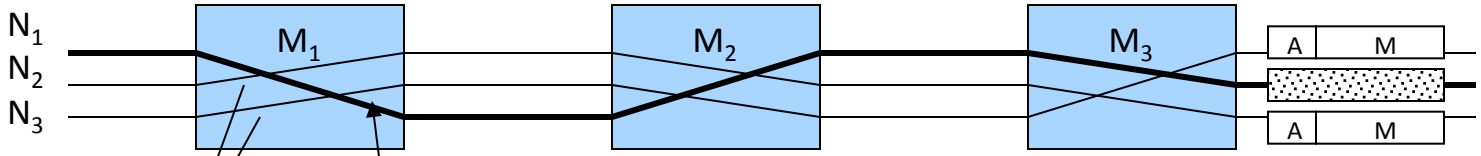
Leads to storage of I/O-allocation in each mix, e.g. for N_1:

No Attacker



Phase 2: Symm. Messages: $k_1(k_2(k_3(A_i,M_i)))$

Attack:
M_1 and M_3
attacks



Remain unchanged

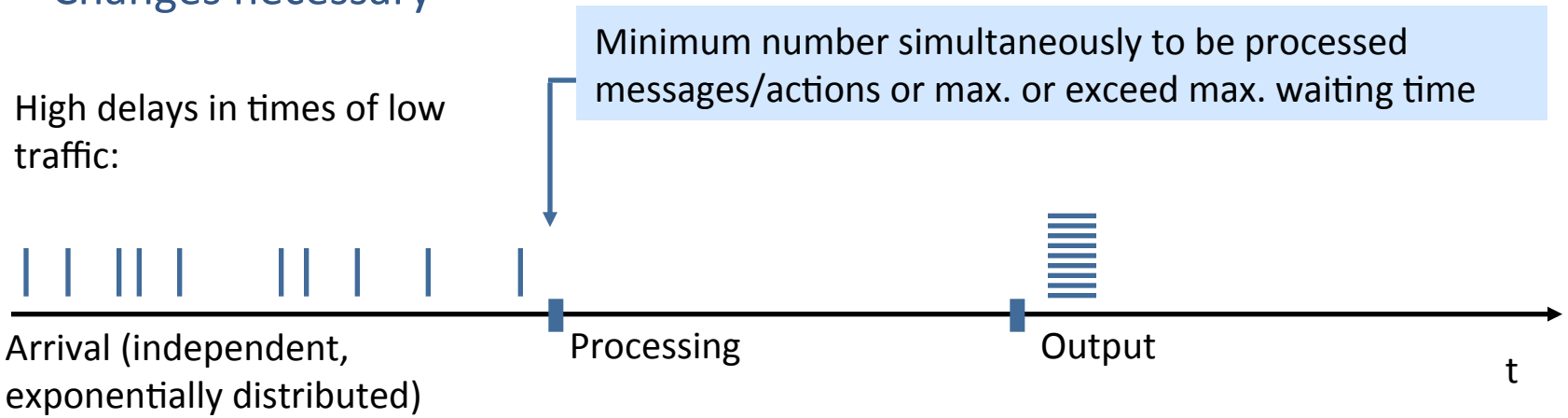
Mix change message(tagging)

Does not attack

Mix „read“ messages, if no existing redundancy (i.e. not consistent message format), then this is the searched message

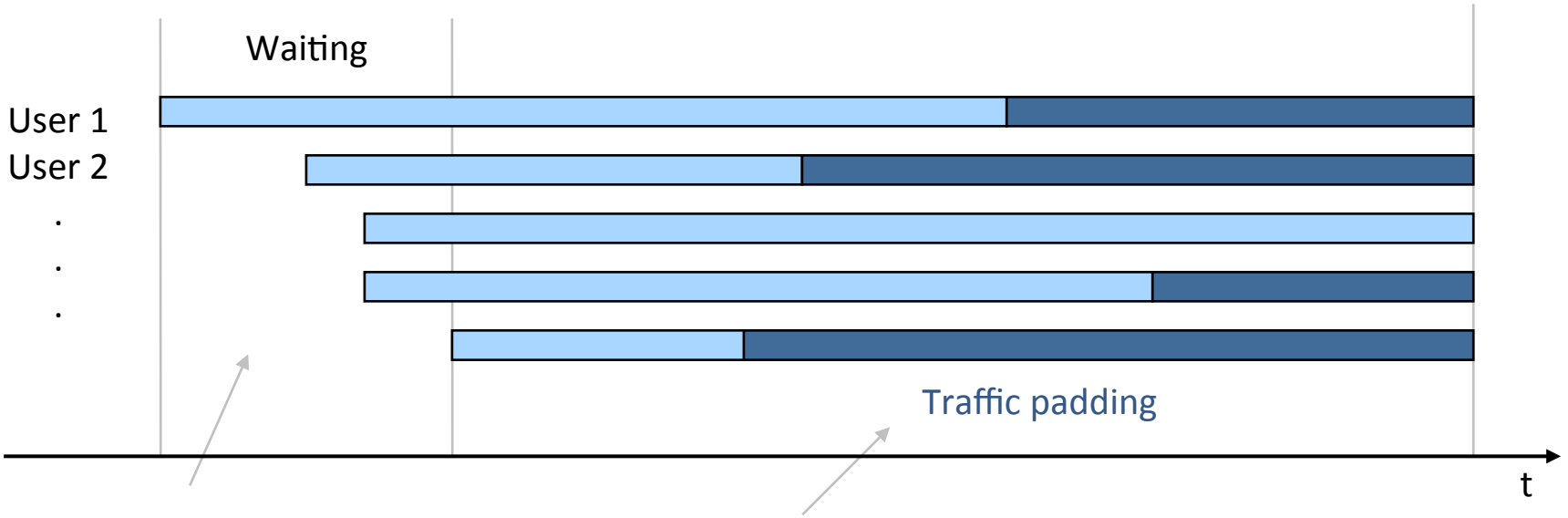
Real-time communication and mixes

- Mixes are well suited for non-real-time services:
  - E-Mail
- Modifications are necessary for real-time communication
  - Collecting messages leads to strong delays, because most of the time a mix is waiting for other messages
  - Messages lenghts and communication time vary greatly at connection-oriented services
- Changes necessary



Traffic padding

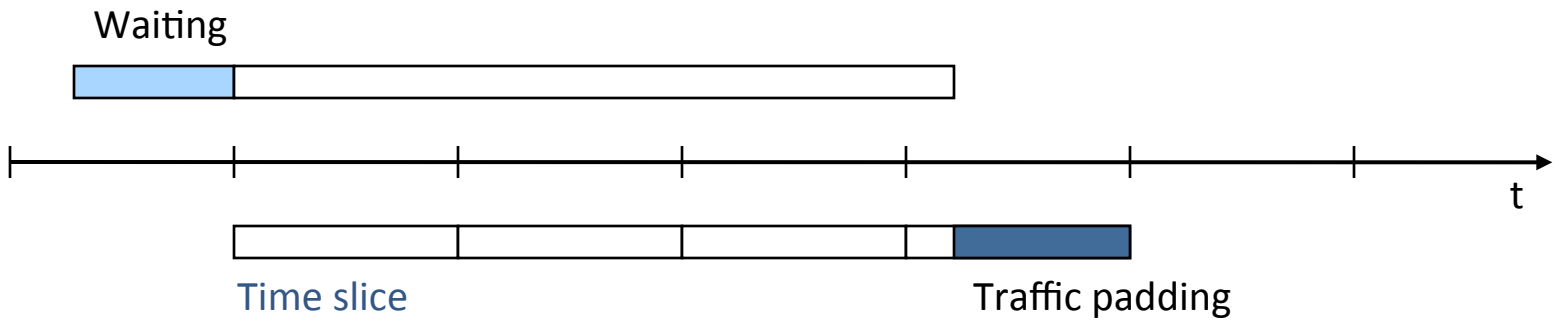
- Objective: Hide, when to start and end a communication
- Problem: Nobody knows, when the last user wants to terminate his communication



1. Users have to wait until enough users want to communicate (creation of the anonymity group)
   Example: 5 users
2. End of communication, but users have to send random data until the last user has finished his connection
3. Problem: Nobody knows when the last user wants to end his communication – because nobody can distinguish real traffic from traffic padding

Disassemble communication in time-/volume slices

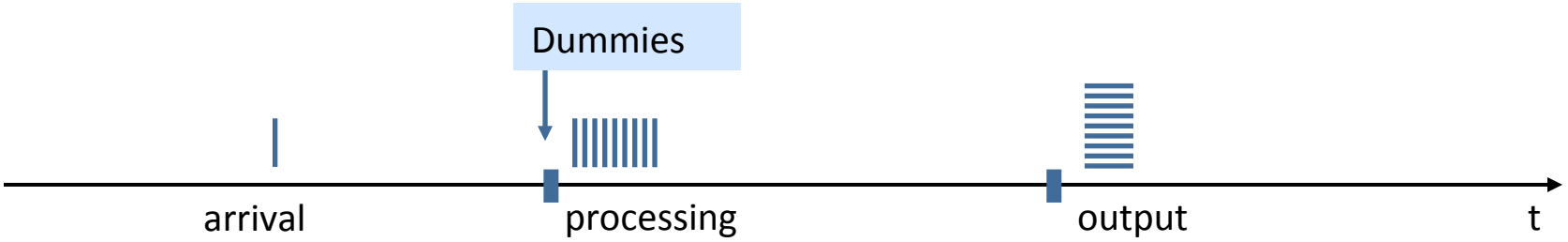
- Time slices (Pfitzmann et. al. 1989)
  - Unobservability within the group of all messages of a time slice
  - Extended communication links are made up of multiple time slices
  - Time slices are not linkable for attacker



- Volume slice (Federrath et. al. 2000)
  - adaptive adjustment of the disc size, depending on the current traffic situation
  - Minimize the overhead

Dummy traffic

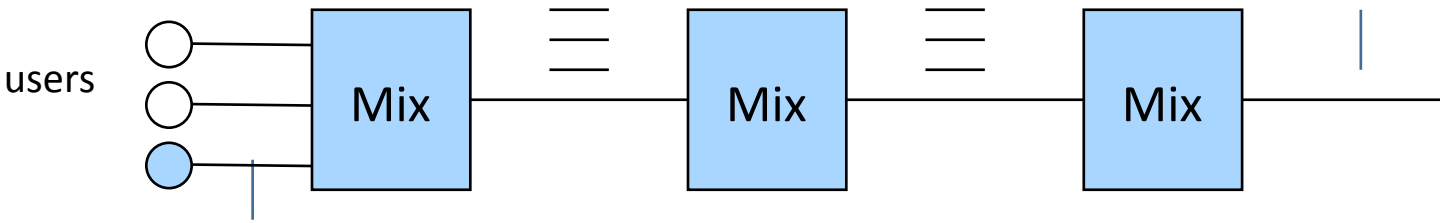
- Def.: Dummy traffic. A user sends data continously. If user has no (encrypted) messages to send, send random numbers, which can not be distinguished from real encrypted messages.
  - Goal: artificially increase traffic load in low traffic situations, to increase anonymity group



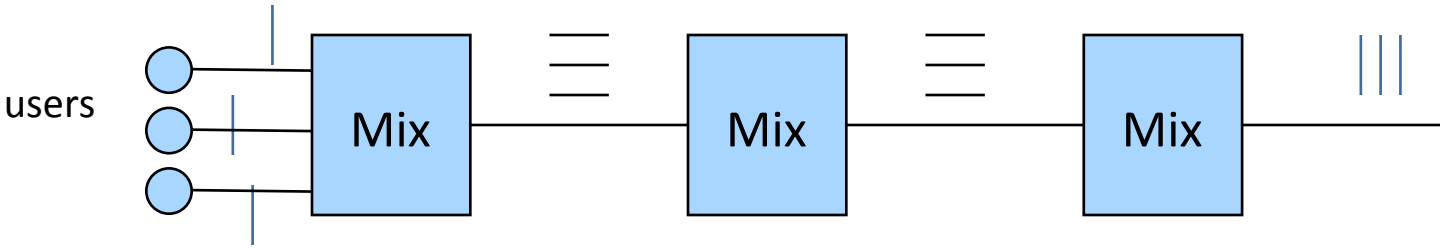
- Alternatives to dummy traffic:
  - Wait, until more messages arrive (lead to further delays)
  - Accept, that anonymity group remains small
  - User who have nothing to send, send meaningless messages

Dummy traffic

- Dummy traffic only between mixes is not sufficient (First-Hop-Last-Hop-Attack)



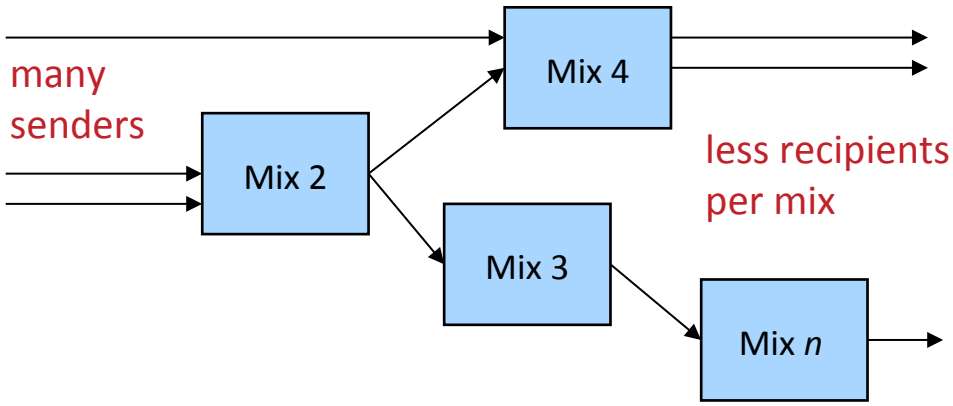
- Dummy traffic must be generated end-to-end



Random mix sequence vs. fixed mix cascade

random mix sequence

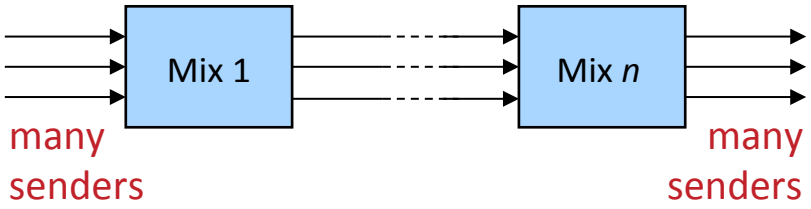
User or system selects mix sequence



- variable recipients per mix
- less recipients per route

fixed mix cascade

Operator selects mix sequence



- constant nr of routes
- constant nr of users per route
- nr of users spread over nr of cascades

Problem with long term monitoring

- Example
  - A user shows a very constant online-offline behaviour (e.g. Online from 20:00-22:00 daily)
  - During this time, he requests certain contents regularly (web pages, his e-mail account)
  - A large number of other users is also active at this time.

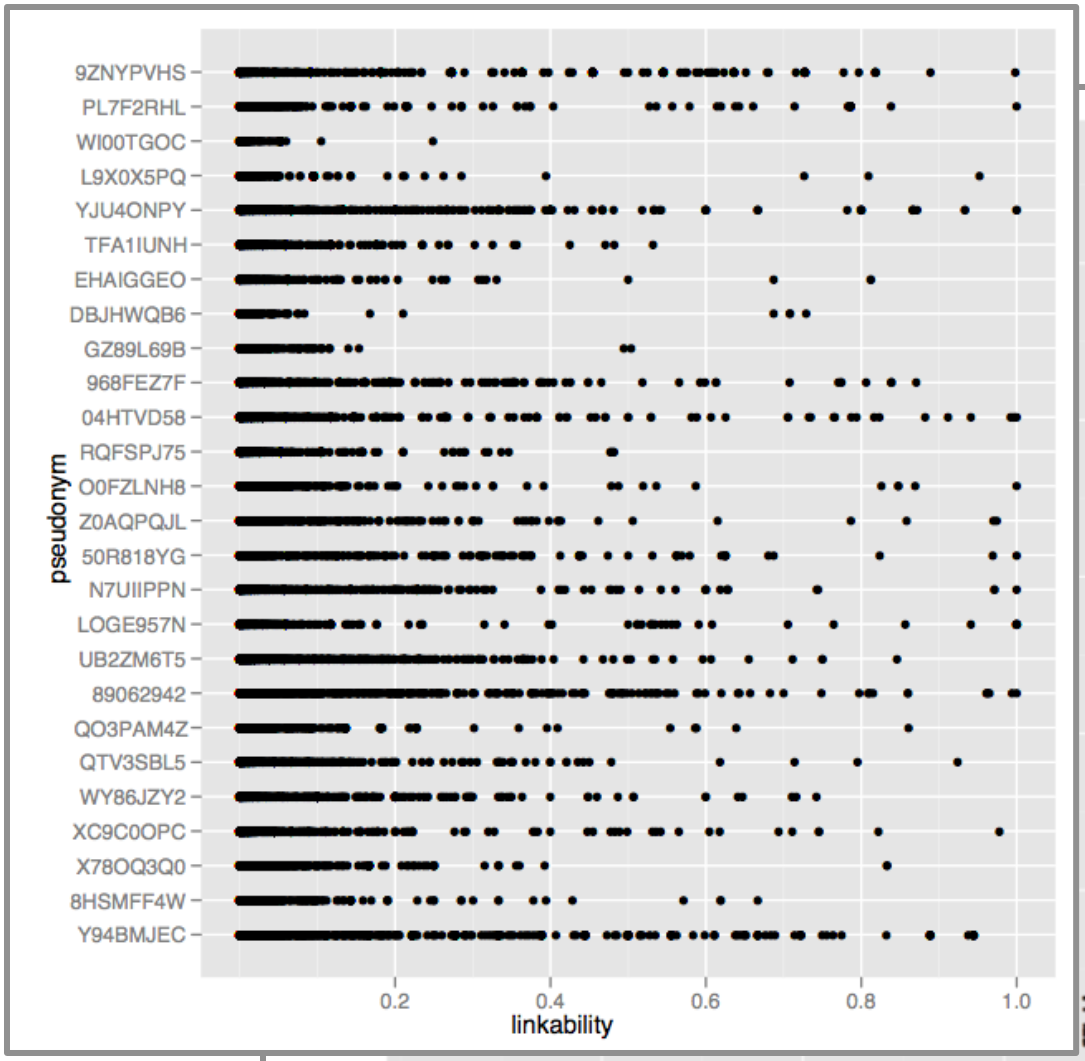
- How long does it take to chain the user actions?
  - depends on the group size and the user behaviour

Intersection attack

- Attacker gets to know by traffic analysis:
  - At t1 messages from 3 senders A,B,C to 3 recipients S,T,U
  - At t2 messages von 3 senders C,D,E an 3 recipients T,V,W
    - t1: {A,B,C} → {S,T,U}
    - t2: {C,D,E} → {T,V,W}
    - X → Y: A certain participant from set X is communicating with a certain participant of set Y. X and Y are anonymity groups.
- Intersection attack:
    - {A,B,C}∩{C,D,E} → {S,T,U}∩{T,V,W} = {C} → {T}
- Interpretation:
  - Attack leads to reduced anonymity set {C,T}
  - T attacks; T learns that C is the sender Sender of the received message

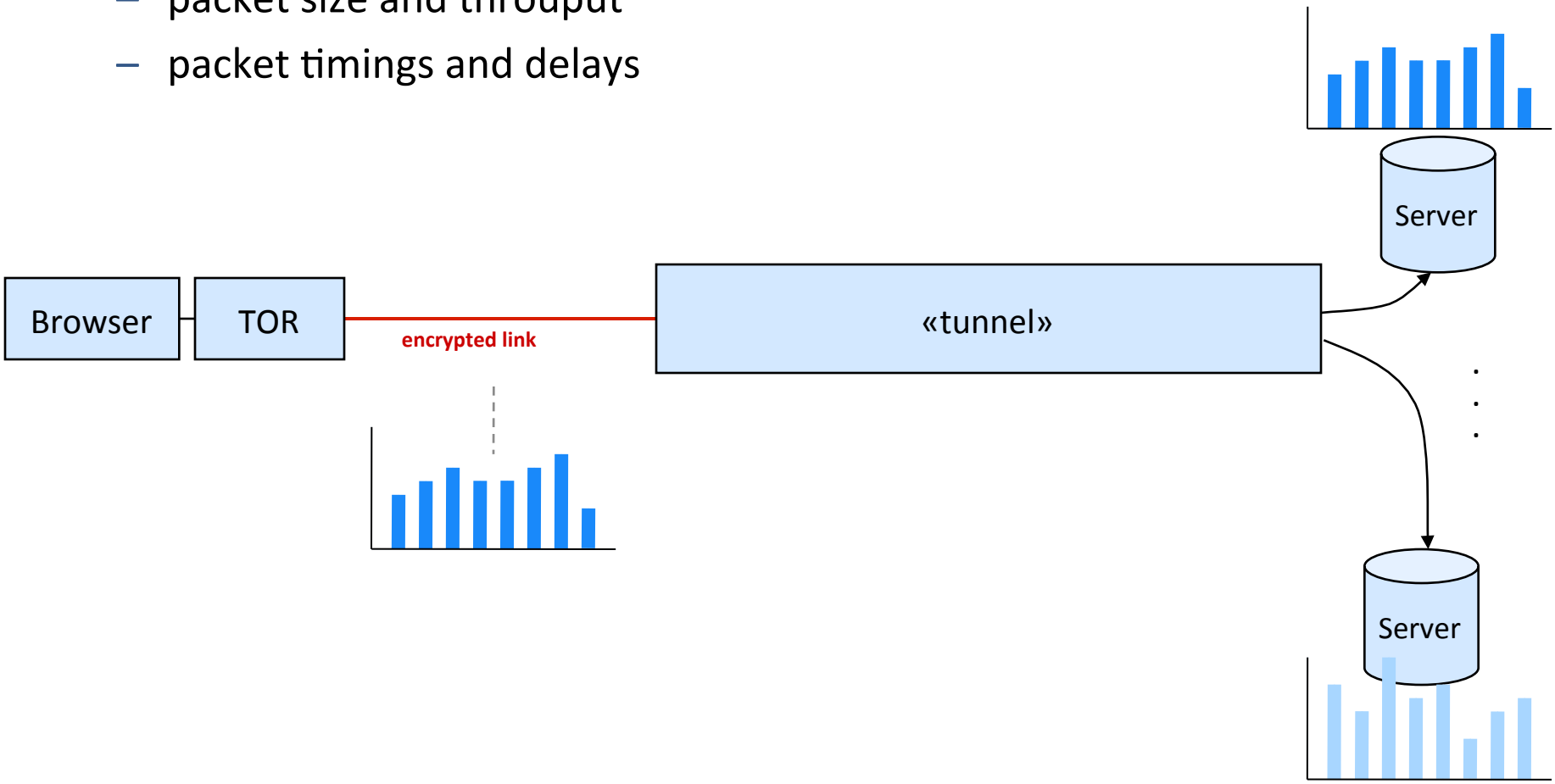
Website and DNS fingerprinting

Gerber, 2009



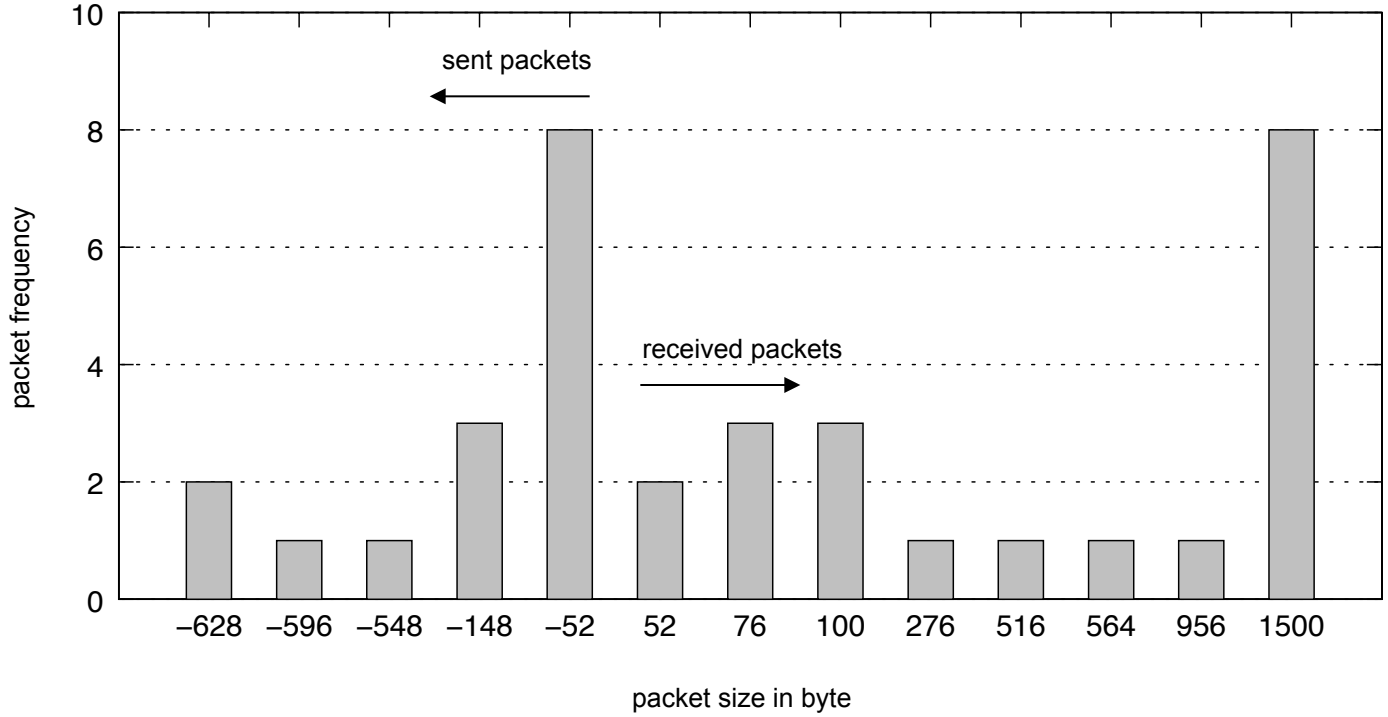
Traffic analysis by packet fingerprinting

- Characteristic properties of packets allow tracking
  - Probabilities and frequencies of packets or connection
  - packet size and throuput
  - packet timings and delays



Traffic analysis by packet fingerprinting

- Example of a characteristic frequency of IP packets



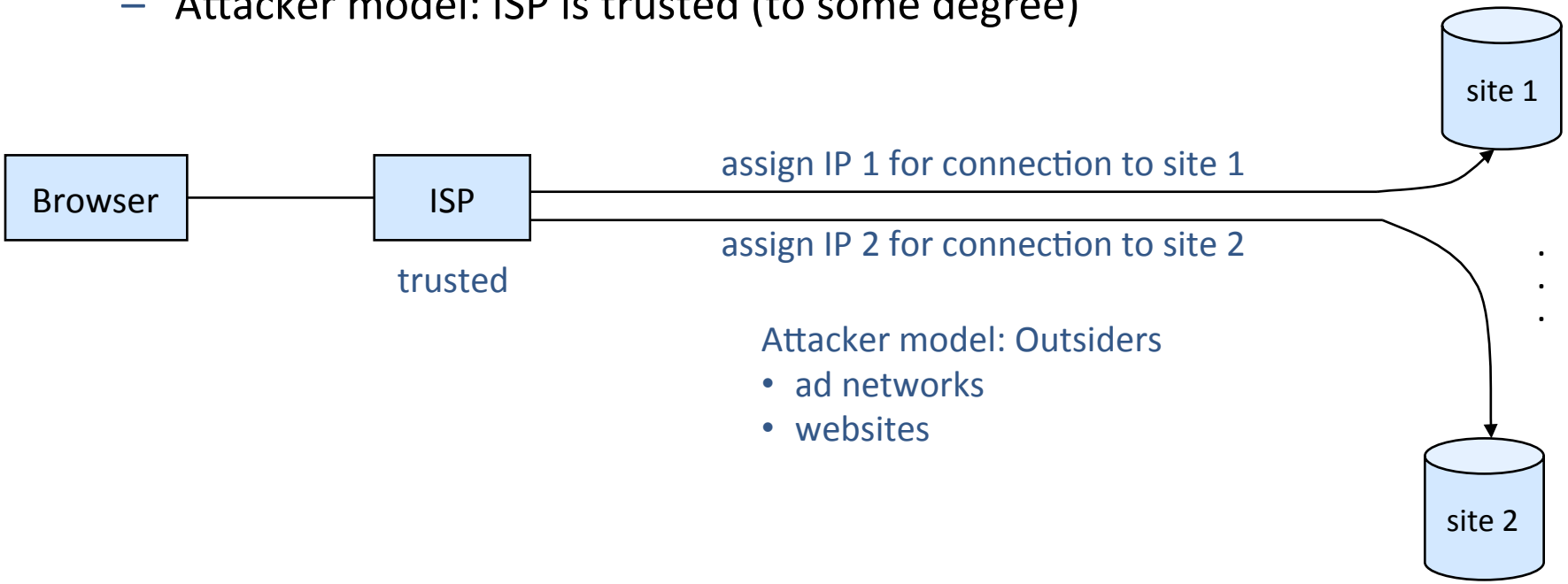
- Protection level gained by Privacy Enhancing Technologies
  - small: SSH tunnel and VPNs; detection rate 90-97% of connections
  - moderate: Tor anonymizers; detection rate < 20% of connections

Challenges and Problems

- Blocking possible – censorship resistance
- Criminal misuse – data retention?
- Correlation attacks still possible – improved algorithms needed
- Traffic overload – lightweight anonymity

IPv6 traffic pseudonymization

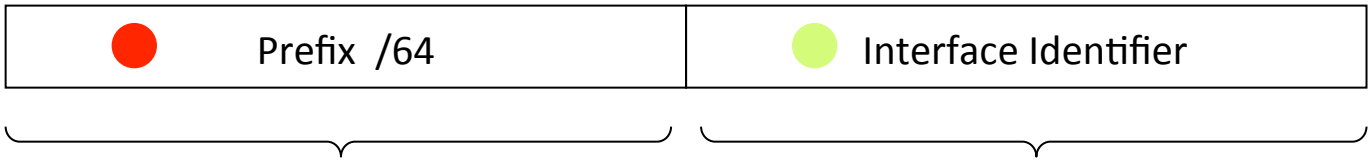
- Lightweight anonymity
  - If unlinkability of actions is sufficient (against ad networks and websites), ISPs can offer anonymity with a new approach to IP address assignment.
- Approach
  - Delegating «anonymization» to the Internet Service Provider (ISP)
  - Less effort for users, no special (TOR or mix-based) router needed
  - Attacker model: ISP is trusted (to some degree)



IPv6 traffic pseudonymization

Hermann, Arndt, Federrath, 2012

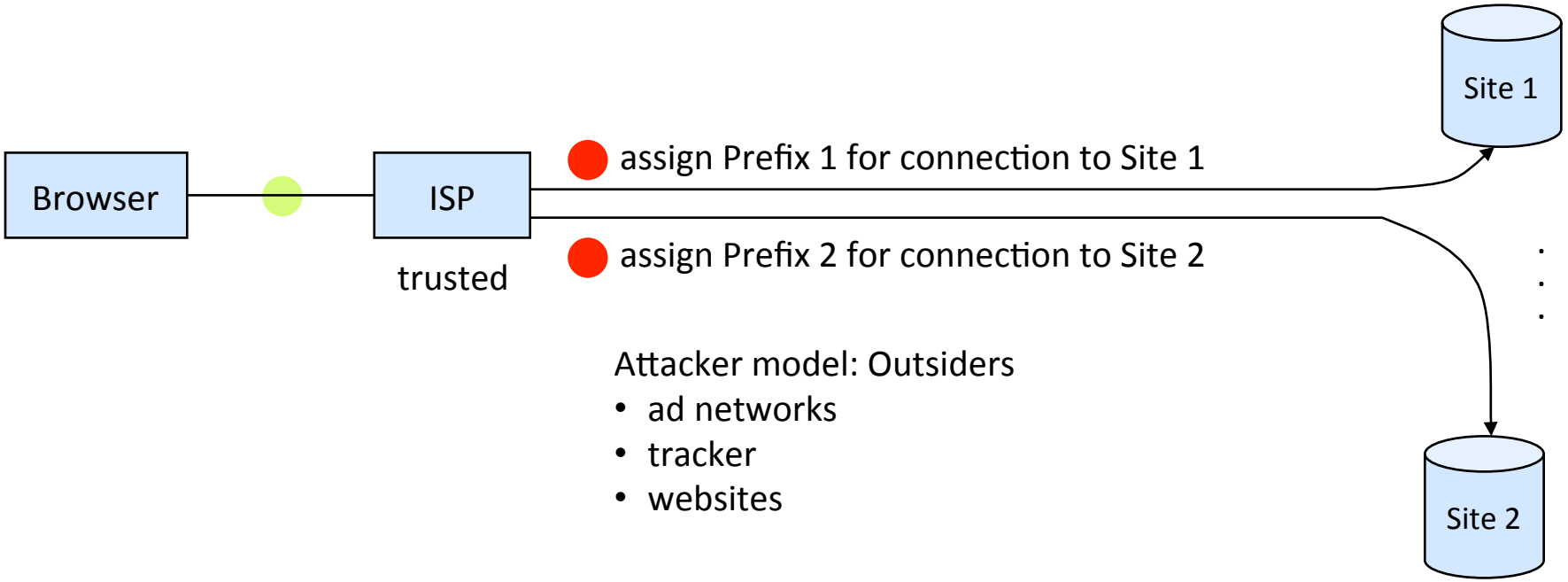
IPv6 Address = 128 Bit = 16 Byte



Prefix Alteration Strategies:

- **Prefix Hopping**
- **Prefix Bouquets**
- **Prefix Sharing**

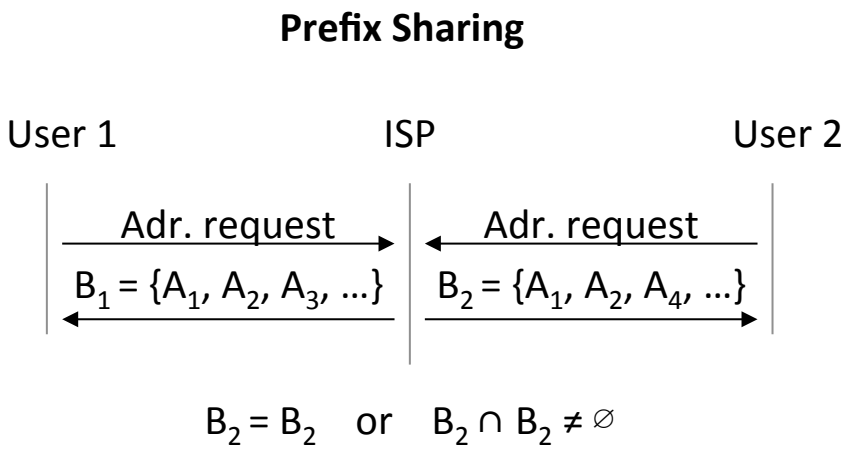
Privacy Extensions
RFC 4941 (RFC 3041)
relevant in the Local Area Network only
NATify before routing ouside



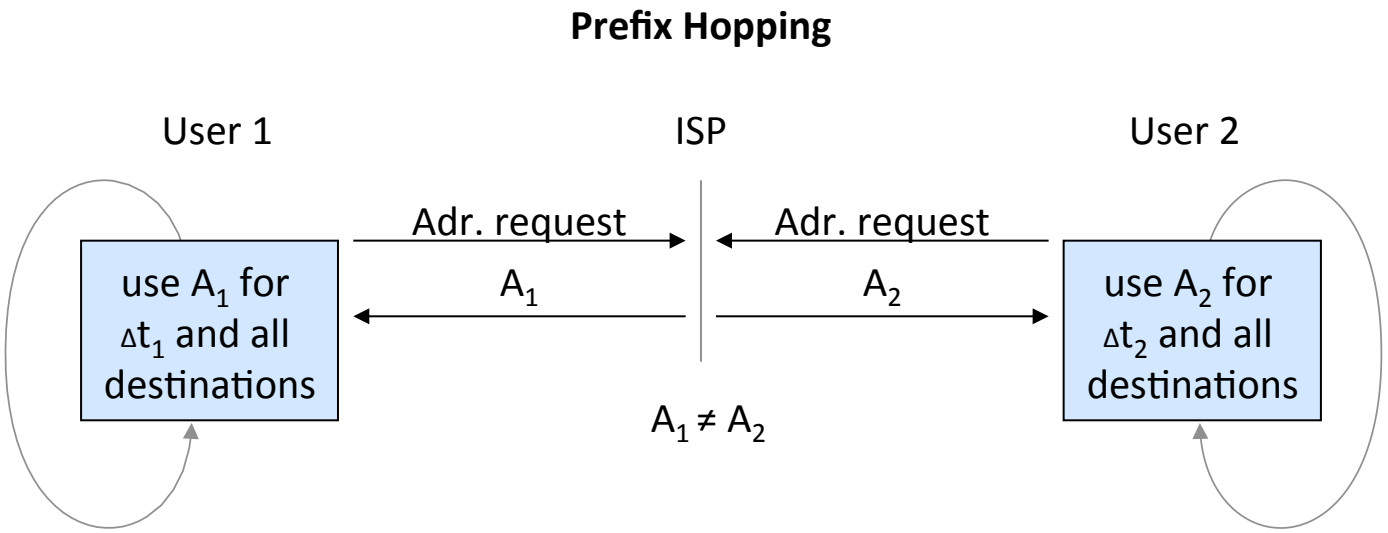
Attacker model: Outsiders

- ad networks
- tracker
- websites

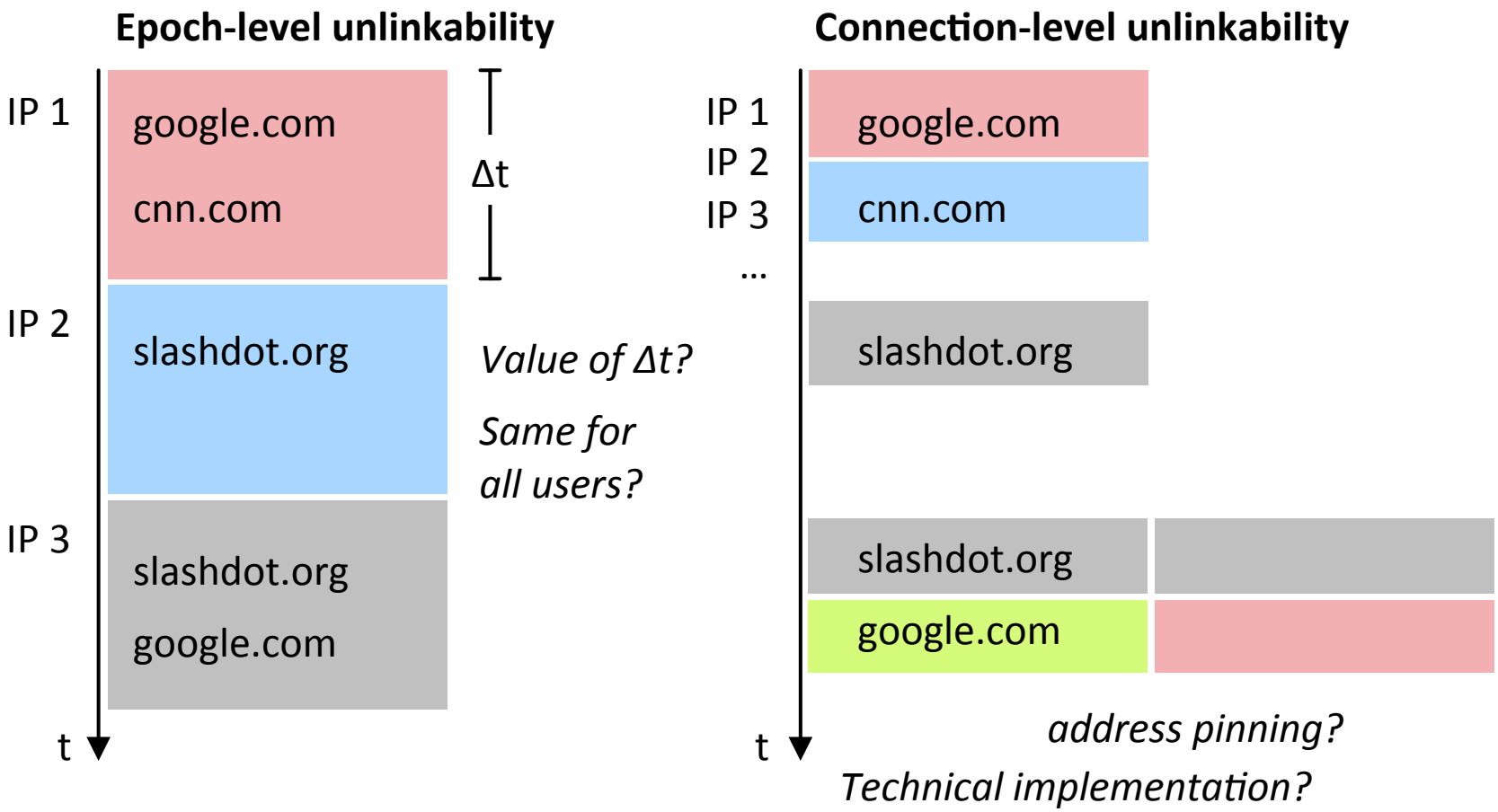
- Prefix Sharing: One IP address (or prefix) is shared among multiple users at a given point in time
  - customers using the same IP address (or prefix) form an anonymity group
  - trackers cannot distinguish customers based on their IP address anymore



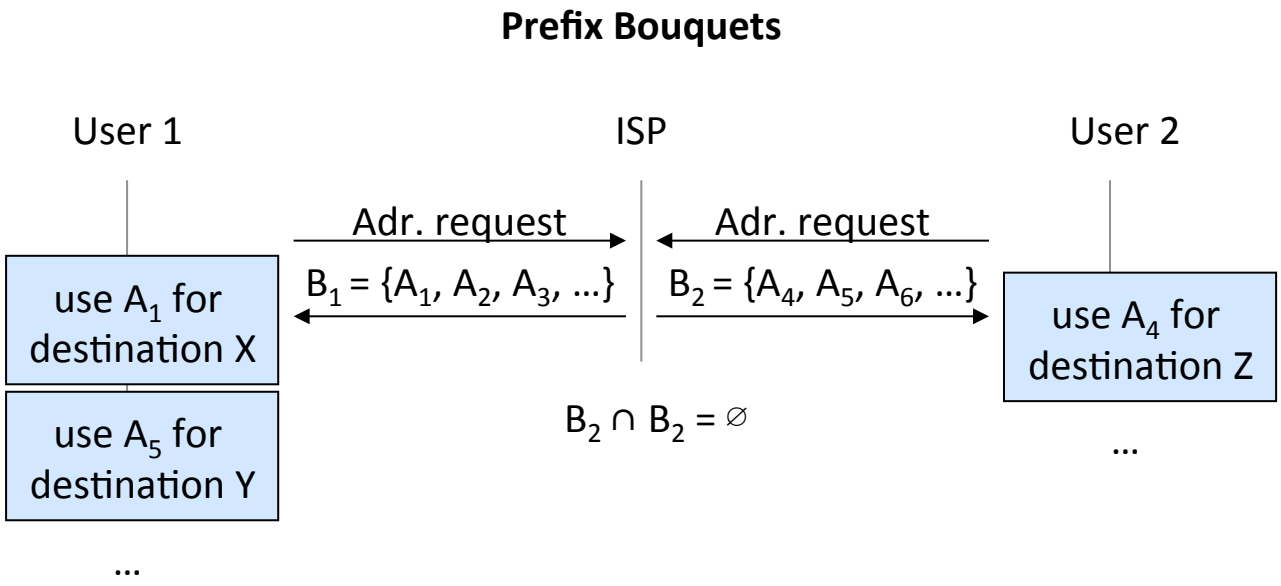
- Prefix Hopping: Each customer spreads his/her traffic over multiple addresses (or prefixes) within a short period of time
  - trackers can link all activities for which the same address is used
  - trackers cannot link activities when the address (or prefix) is changed



IPv6 traffic pseudonymization

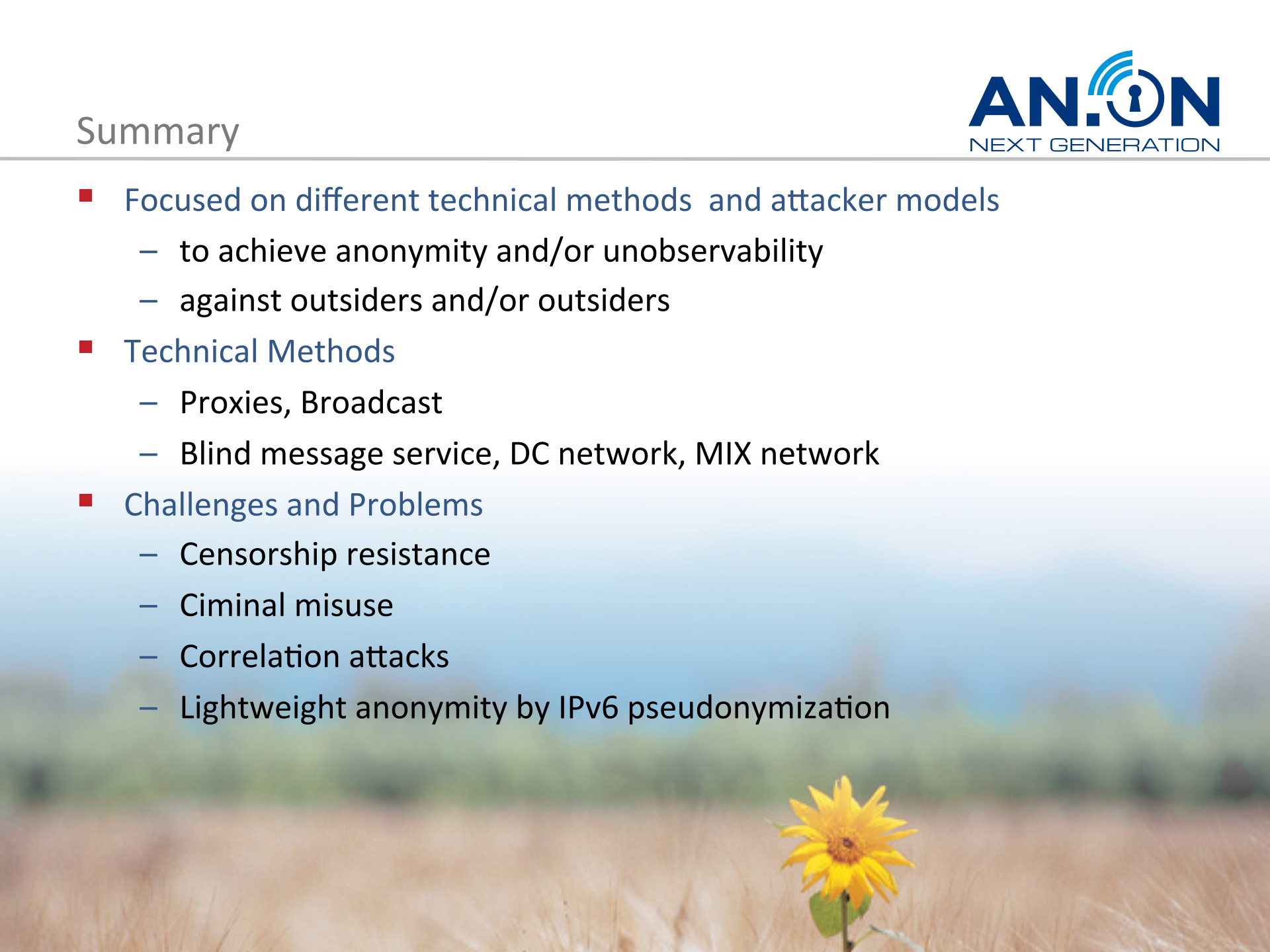


- Prefix Bouquets: each customer uses a new address (or prefixes) for a different destination
  - trackers can link all activities for which the same address is used
  - trackers cannot link activities when the address (or prefix) is changed



Summary

- Focused on different technical methods and attacker models
  - to achieve anonymity and/or unobservability
  - against outsiders and/or outsiders
- Technical Methods
  - Proxies, Broadcast
  - Blind message service, DC network, MIX network
- Challenges and Problems
  - Censorship resistance
  - Ciminal misuse
  - Correlation attacks
  - Lightweight anonymity by IPv6 pseudonymization



Universität Hamburg
Fachbereich Informatik
Arbeitsbereich SVS
Prof. Dr. Hannes Federrath
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

https://svs.informatik.uni-hamburg.de