Anonymity in the Internet

Hannes Federrath

University of Regensburg
Management of Information security
http://www-sec.uni-regensburg.de

ZISC Information Security Colloquium SS 2006, ETH Zurich, 20.06.2006
http://www.zisc.ethz.ch/events/infseccolloquium2006
### Protection Goals

<table>
<thead>
<tr>
<th>Subject of communication WHAT?</th>
<th>Circumstances of comm. WHEN?, WHERE?, WHO?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
<td><strong>Anonymity</strong> Unobservability</td>
</tr>
<tr>
<td>Contents</td>
<td></td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td><strong>Accountability</strong> Legal Enforcement</td>
</tr>
<tr>
<td>Contents</td>
<td></td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Contents**
- Sender
- Location
- Recipient

**Billing**
- Recipient
### Protection Goals

<table>
<thead>
<tr>
<th>Subject of communication WHAT?</th>
<th>Circumstances of comm. WHEN?, WHERE?, WHO?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
<td><strong>Anonymity</strong></td>
</tr>
<tr>
<td><strong>Contents</strong></td>
<td><strong>Unobservability</strong></td>
</tr>
<tr>
<td><strong>Sender</strong></td>
<td><strong>Location</strong></td>
</tr>
<tr>
<td><strong>Recipient</strong></td>
<td></td>
</tr>
</tbody>
</table>

- 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 likelihood.
### Protection Goals

<table>
<thead>
<tr>
<th>Subject of communication</th>
<th>Circumstances of comm.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WHAT?</td>
<td>WHEN?, WHERE?, WHO?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Anonymity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>Unobservability</td>
</tr>
</tbody>
</table>

- **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 in the Internet

Prof. Dr.-Ing. Hannes Federrath

Why encryption is not enough

Observation of communication relations may give information about contents

Attorney Miller, specialized in mergers
**Anonymity in the Internet**

**Protection Goals**

<table>
<thead>
<tr>
<th>Subject of communication</th>
<th>Circumstances of comm.</th>
</tr>
</thead>
<tbody>
<tr>
<td>WHAT?</td>
<td>WHEN?, WHERE?, WHO?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Anonymity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>Unobservability</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sender</td>
</tr>
<tr>
<td></td>
<td>Location</td>
</tr>
<tr>
<td></td>
<td>Recipient</td>
</tr>
</tbody>
</table>

- **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 in the Internet

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 vector = 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

D[1]: 1101101
D[2]: 1100110
D[3]: 0101110
D[4]: 1010101
Blind-Message-Service (Cooper, Birman, 1995): Answer

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 equals D[2]: 1100110

Link encryption between client and databases
Anonymity in the Internet

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

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

Internet/Web

- JAP acts as a local proxy on the local machine
For free at www.anon-online.de

First test version has been launched in October 2000

Full service has been running since February 2001
Anonymity in the Internet

AN.ON/JAP

Mix based solution for anonymous Internet access

OpenSource

>10,000 users

>6 TByte per month

www.anon-online.de

Public survey (Spiekermann 2003)

- **Sample size:**
  - 1800 users of the JAP anonymizer
Anonymity in the Internet

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% sporadic (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
Anonymity in the Internet

Prof. Dr.-Ing. Hannes Federrath

Anonymized content

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

- Entertainment 44%
  - 33% erotic, pornography
  - 8% private homepages, cinema, amusement
  - 3% games

- Services 18%
- Companies 8%
- Mail 8%
- News 3%
- Health 1%
- Misc 18%
Regions of users

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

- Europe: 60%
- Asia: 27%
- America: 12%
- Rest of the world: 1%
Regions of users

- Dayline of May 27, 2005
Regions of users

- Dayline of Aug 1, 2005
Anonymity in the Internet

Censor-free Internet access

JAPs act as a forwarder node for the Anonymizer

Blocking by government

WWW Server

Also blocked

Blocked

MIX MIX MIX

JAPs act as a forwarder node for the Anonymizer

Blocking by government
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.
Anonymity in the Internet

Censor-free Internet access

Blocking by government

Web request or send e-mail
Provide forwarder information after passing a Turing test

JAP

... JAP

? MIX MIX MIX

JAP Information Service

JAP Information Service

WWW Server

JAP

JAP

JAP

JAP
Censor-free Internet access

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