Anonymity on the web
Agenda

1. Motivation
2. Definitions
3. Privacy Enhancing Technologies (PET)
   1. Mix Cascade
   2. JAP
   3. TOR
Motivation

- User leaves data tracks at the internet
  - For example log data on the www
- Many analysis options
  - Marketing analysis
  - Identity theft
- Results of current studies:
  - “Internet-user have fear of data abuse”
- Requirements of:
  - Protecting personal data
  - Private space like in the “real world”
Unlinkability

- **ensures** that a user may make multiple uses of resources or services without others being able to link these uses together
- **requires** that users and/or subjects are unable to determine whether the same user caused certain specific operations in the system

[Common Criteria: ISO15408 1999]
identity of a single or several people at an anonym process of joining an instance is not definable

• Don’t know other part of instance
• Don’t make an appearance to the other part of instance or
• Act without a name at the anonym process.
3 Anonymity types:

- Transmitter – Anonymity:
  Transmitter and Messages is unlinkable

- Receiver – Anonymity:
  Receiver and Messages is unlinkable
  For Example: Broadcast

- Relation – Anonymity:
  Transmitter and Receiver is unlinkable
  For Example: Mixe

Unlinkability → Anonymity
Unobservability

- Sending and receiving of a message is indistinguishable by third parties
- Ensure anonymity to third parties
- Existence of a Message is indeterminable
- Connections can’t be established

Unobservability $\rightarrow$ Anonymity
Pseudonymity

- Being pseudonymous is the **state of using** a pseudonym as ID.

- That makes data minimization possible, because we can **reduce** with a **pseudonym** personal data to an ID.

  \[ \text{–> Anonymity} \]
Privacy Enhancing Technologies (PET)

- Realize especially privacy properties:
  - Anonymity, Unobservability
- Strengthen user and operator similarly
Mix Cascade (Mixe) I

- Based on a Idea of David Chaum 1981
- Realize Transmitter – and Relation – Anonymity
- Main Idea:
  - Collection, ignore repeats, recode, re-sort, common display of Messages
  - All Messages have the same length
  - Use more then one Mix (interstations) and different operator
  - At least one Mix which don’t attack
Mix Cascade (Mixe) II

- The aim:
  - The perfect unlinkability of Transmitter and Receiver

- Procedure:
  - Transmitter don’t send a Message directly to a Receiver
  - The Transmitter send the Message through intermediate stations
  - The Transmitter cipher the Message (incl. the address of the Receiver) and a random number with the public key of the Mixes.
  - This cryptographic message will be send
    Input message !≠ Output message
Mix Cascade (Mixe) III

Transmitter

Mix-Network

Receiver
Mix Cascade (Mixe) IV

Conclusion:
- Just public information will be send
  - Transmitter have to know all public keys of Mixe
  - Every single Mix know there own private key
- But there are some *practical* problems:
  - Public key ciphering is slow
  - Replay – attacks (restore of available packages)
JAP I

- Develop since 2000 of AN.ON Project
  - Uni Regensburg, TU Dresden are supported by funds of German Research Foundation and Federal Ministry of economy and technology
  - http://anon.inf.tu-dresden.de

- Aim:
  - Transmitter–Anonymity by demand of websites
    (note: Difference to TOR is that TOR cipher the internet–communication)
  - Simple usability: easy installation, configuration and operation
  - Quality of service: network performance (Throughput, latency and so on) and Security (Anonymity)
In contrast to Mix-Cascade there are constant channels with symmetrical ciphering.
- Symmetrical ciphering is more efficient than public key.

- Graphical Client-Component
  - Proxy in Webbrowser.

- Additional: Info-Service informs you of keys and active Mixe.
JAP III

- Architecture of JAP
JAP IV

Boundary:
- Just mask the IP – address
- Static cascades
  - If the attacker guess, which cascade the target subject use, so he just need to attack the computers
- Confined to website – access
  - More a reason of performance, not a problem of this concept
- Performance, Availability
  - Mix–Server of a cascade are single point of failure and Bottleneck for many user
TOR I

- Project of Electronic Frontier Foundation, Developed since 2004
- In contrast to JAP here is a more modern background
  - Onion Routing (nearly the same like the Mixe)
  - Hidden Services: Anonymous Server-Addresses
  - Supports any TCP-based protocol
    - Http, P2P or ICQ
  - Random Connection to each network connection
    - Access will new chosen, when the server close an Access
    - No static Mix-Cascades

- Aims:
  - Relation – Anonymity by cipher the internet-communication
Boundary:
  ◦ Like JAP: Just mask the IP – address
  ◦ Some practical problems:
    • Infiltrate of Tor – nodes with many free recourses (or manipulation of this data), those will preferred used of this network
    • In control of less computers a big part of the traffic can completely eavesdrop
    • Every OS setting the TCP–time stamp in an other way, it depends on the computer hardware
    • Statistic attacks are possible
Conclusion

- Anonymity is essential for democracy
  - For example: elections, freedom of expression
- A 100% of anonymity is not possible
  - Examples for reasons:
    - Pseudonyms have a relation to an identity
    - Since 9/11/2001 it is very important for the government to trace every connection of an internet-user (in Germany: a provider have to save this information over a period of a year)
      - Against child pornography
      - Against right wing radicalism
Thank you for your attention!