CoNe Freiburg

IIF INSTITUT FÜR INFORMATIK FREIBURG

Peer-to-Peer Networks

14 Security

Christian Schindelhauer
Technical Faculty
Computer-Networks and Telematics
University of Freiburg

UNI FREIBURG

CoNe Freiburg

Motivation for Anonymity

- Society
  - Free speech is only possible if the speaker does not suffer negative consequences
  - Thus, only an anonymous speaker has truly free speech
- Copyright infringement
  - Copying items is the best (and most) a computer can do
  - Copyright laws restrict copying
  - Users of file sharing systems do not want to be penalized for their participation or behavior
- Dictatorships
  - A prerequisite for any oppressing system is the control of information and opinions
  - Authors, journalists, civil rights activists like all citizens should be able to openly publish documents without the fear of penalty
- Democracies
  - Even in many democratic states certain statements or documents are illegitimate, e.g.
    - (anti-) religious statements
    - insults (against the royalty)
    - certain types of sexual contents
    - political statements (e.g. for fascism, communism, separation, revolution)
- A anonymizing P2P network should secure the privacy and anonymity of each user without endangering other users

UNI FREIBURG

CoNe Freiburg

Terms

- From
  - Danezis, Diaz, A Survey of Anonymous Communication Channels
  - Pfitzmann, Hansen, Anonymity, Unobservability and Pseudonymity – A Proposal for Terminology
- Anonymity (Pfitzmann-Hansen 2001)
  - describes the state of being not identifiable within a larger set of subjects (peers), i.e.
    - the anonymity set
  - The anonymity set can be all peers of a peer-to-peer network
    - yet can be another (smaller or larger) set

UNI FREIBURG

CoNe Freiburg

Terms

- Unlinkability
  - Absolute (ISO15408)
    - „ensures that a user may make multiple uses of resources or services without other being able to link these uses together.“
  - Relative
    - Any attacker cannot find out more about the connections of the uses by observing the system
      - a-priori knowledge = a-posteriori knowledge

UNI FREIBURG

CoNe Freiburg

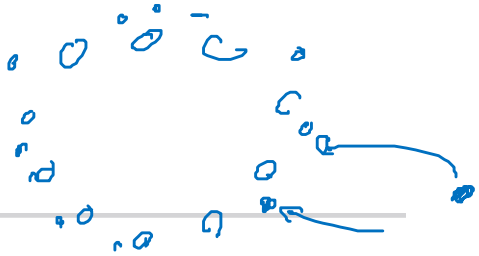
Terms

- Unobservability
  - The items of interests are protected
  - The use or non-use of any service cannot be detected by an observer (attacker)
- Pseudonymity
  - is the use of pseudonyms as IDs
  - preserves accountability and trustability while preserving anonymity

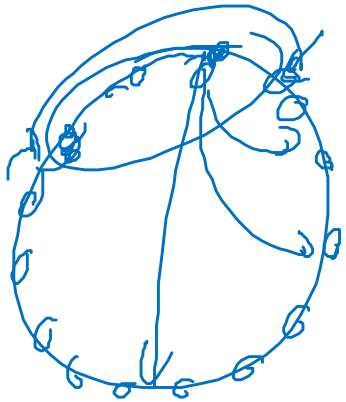
UNI FREIBURG

CoNe Freiburg

Attacks



- Denial-of-Service Attacks (DoS)
  - or distributed denial of service attacks (DDoS)
  - one or many peers ask for a document
  - peers are slowed down or blocked completely
- Sybil Attacks
  - one attacker produces many fake peers under new IP addresses
  - or the attacker controls a bot-net
- Use of protocol weaknesses
- Infiltration by malign peers
  - Byzantine Generals

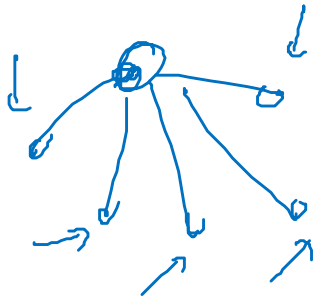


UNI FREIBURG

CoNe Freiburg

Attacks

- Timing attacks
  - messages are slowed down
  - communication line is slowed down
  - a connection between sender and receiver can be established
- Poisoning Attacks
  - provide false information
  - wrong routing tables, wrong index files etc.
- Eclipse Attack
  - attack the environment of a peer
  - disconnect the peer
  - build a fake environment
- Surveillance
  - full or partial



UNI FREIBURG

CoNe Freiburg

Cryptography in a Nutshelf

- Symmetric Cryptography
  - AES
  - Affine Cryptosystems
- Public-Key Cryptography
  - RSA
  - ElGamal
- Digital Signatures
- Public-Key-Exchange
  - Diffie-Hellman
- Interactive Proof Systems
  - Zero-Knowledge-Proofs
  - Secret Sharing
  - Secure Multi-Party Computation