User identification with username and password in structured P2P networks

Rodrigo Fernández
rfernand@inf.utfsm.cl

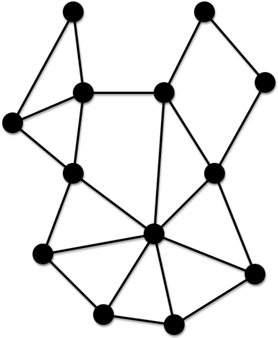
Universidad Técnica Federico Santa María

11 de septiembre de 2013

P2P Networks

Characteristics

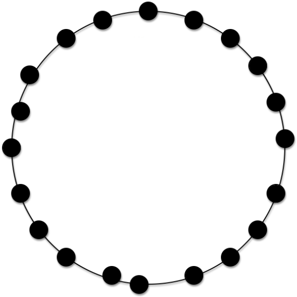
- Scalable
- Decentralized
- Self-maintained
- Robust



P2P Networks

Overlay structure

- Structured networks (CAN, CHORD)
- Unstructured networks (Gnutella, Bittorrent)



P2P Networks

Overlay structure

- Images of structured/unstructures networks
- Differences

Username / password identification

Why?

- Many complex systems require authenticated users to work.
- Most of the users has more than one device, so identification through multiple devices is needed.
- User are accostumed to username/password solutions.

Username / password identification

P2P Identification Schemes

Descentralized schemes distributes the task of public key auth to all participants.

- PGP-like scheme
  Creates web of trust to auth public keys based on their acquaintances opinions.
- Quorum-based scheme
  Multiple independent participants replicate public keys.

Identification schemes

In need of a third party

- PKI
- Username/password pair

Poor scaling, single point of failure, heavy administration overhead.

Trust in P2P networks

1. To deliver a valuable service in P2P applications, it is important to trust that the participants will act as requested.
2. We need to be sure that other peers will forward messages, and that the designated peers will indeed save the information correctly so that operations can be successful.

Trust in P2P networks

Building Trust

1. Complex since a P2P network includes untrusted nodes from an open environment.
2. Untrusted nodes may be faulty, malicious, and act together to attack the network.

Trust in P2P networks

How to detect faulty nodes?

Reputation systems: Assess the past history of a peer by gathering feedback from nodes with previous interactions with this peer.

Accountability: Detects and exposes faulty nodes by creating non-repudiable records of every node's actions.

Trust in P2P networks

Bizantine nodes

Are all nodes that not behave as expected

1. Faulty nodes
2. Malicious nodes
3. Infected nodes

Trust in P2P networks

Bizantine node tolerance

P2P networks can achieve byzantine fault tolerance under 1/3 byzantine peers
A peer is honest only if the peers executes the protocol faithfully; otherwise, the peer is faulty.

Byzantine Generals Problem

Trust in P2P networks

Bizantine node tolerance

P2P networks can achieve byzantine fault tolerance under 1/3 byzantine peers
A peer is honest only if the peers executes the protocol faithfully; otherwise, the peer is faulty.

Byzantine Generals Problem

Working Hypothesis

- It is assumed that the use of a reputation system and trusted nodes management mitigates the efectivity of malicious nodes on identity usurpation attacks.
- It is assumed that encryption schemes available today are sufficient to secure the user's private data in the P2P networks.

Goals

Main Goals

The implementation of a secure *user-name/password* based user identification scheme in structured P2P networks using:

- Secure routing
- Node trust management
- Encryption schemes

Goals

Specifics Goals

- Study the possibility of password recovery mechanisms.
- Study and use trust management to maintain a secure layer inside the P2P network.
- Use bizantine tolerant algorithms to verify and maintain the system consistency in the presence of malicious nodes.
- Study and use secure routing, search and storage mechanisms in structured P2P networks.

Results

Contributions and Expected Results

- Design of a secure and modern user identification system for structured P2P networks.
- Generate a base system to develop complex projects in P2P networks.
- Reassure that P2P distributed systems have the capabilities to offer complex and high level services.
- Paper publication.

Results

Validation procedures

- Proving that the system will have a minimal probability of error.
- Proving that the system will maintain his consistency in networks with at most 30 % of bizantine nodes.

EOF