

Beyond "Web of Trust": Enabling P2P E-commerce

Karl Aberer, Anwitaman Datta, Manfred Hauswirth

Distributed Information Systems Laboratory
Swiss Federal Institute of Technology Lausanne (EPFL)
<http://lsirwww.epfl.ch/>
<http://www.p-grid.org/>



© 2003 Karl Aberer, Anwitaman Datta, Manfred Hauswirth, EPFL-IBC-11F

1

Overview

- C2C e-Commerce: Essentially peer-to-peer
 - Relevance of PKIs
 - Our long-term goal: eBay without centralized infrastructure
- Taxonomy of public key infrastructures (PKIs)
- A quorum-based decentralized PKI
 - Overview of the P-Grid P2P system
 - A PKI based on P-Grid (probabilistic quorum)
- Analysis of the approach
- Possible attacks and their impact
- A layered architecture for enabling P2P e-commerce
- Conclusions



© 2003 Karl Aberer, Anwitaman Datta, Manfred Hauswirth, EPFL-IBC-11F

2

C2C e-Commerce

- The huge success of eBay demonstrates that a need for C2C e-Commerce exists
- C2C e-Commerce is inherently decentralized
- Centralized C2C infrastructure (e.g., eBay):
 - Enforcement of policies is easy due to centralization
 - Single point of failure
 - Centralized enforcement of policies does not help if seller do not deliver or customers do not pay
- Decentralized C2C infrastructure:
 - Naturally maps onto the C2C interaction pattern
 - No single point of failure
 - Customers collaboratively provide the infrastructure
 - Security guarantees are harder to provide



© 2003 Karl Aberer, Anwitaman Datta, Manfred Hauswirth, EPFL-IBC-11F

3

C2C e-Commerce & Security

- e-Commerce requires security services and guarantees
 - Authentication
 - Non-repudiation
 - Accountability
 - Access control
- Secure identification is the basis for many of these services \Rightarrow public key infrastructure
- Standard approach: centralized PKI (e.g., VeriSign)
- Centralized PKI introduces centralization into a decentralized system through the back door \Rightarrow decentralized PKI required



© 2003 Karl Aberer, Anwitaman Datta, Manfred Hauswirth, EPFL-IBC-11F

4

Public Key Infrastructure (PKI)

- Management of certificates
 - Issuing
 - Registration
 - Retrieval
 - Revocation
 - Cross-certification
 - etc.
- A certificate securely maps an entity's identity onto its public key
- Basis for higher-level security services



© 2003 Karl Aberer, Anwitaman Datta, Manfred Hauswirth, EPFL-IBC-11F

5

Taxonomy of decentralized PKI approaches

- Web of Trust (WoT) and PGP
 - Transitive trust model: A trusts B, B trusts C \Rightarrow A trusts C
 - Trust model depends on the weakest link
 - Path discovery is inefficient
 - Lack of quantifiable guarantees
- Statistical/Probabilistic Quorum (PQ) based
 - Correctness is judged via a quorum
 - Structured P2P systems can make information discovery and thus forming a quorum inexpensive
- Hybrid
 - Combination of WoT and PQ approach
 - Hybrid PGP approach is inefficient (finding random paths) and insecure (intersecting paths)



© 2003 Karl Aberer, Anwitaman Datta, Manfred Hauswirth, EPFL-IBC-11F

6

P-Grid

<http://www.p-grid.org/>

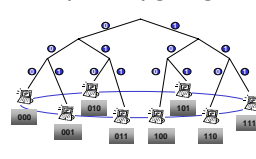
Goal
Scalability through self-organization

Properties

- Scalable, distributed search tree: distributed hash table (DHT)
- Randomized algorithms
- Purely local decisions
- Efficient search and load balancing
- Robust through massive replication
- Support for updates
- Support for identification
- Semantic integration
- Java implementation

Applications

- Trust assessment of peers
- Peer commerce
- Scalable, semantic Internet search
- Decentralized public key infrastructure



© 2003 Karl Aberer, Anwitaman Datta, Manfred Hauswirth, EPFL-IBC-IFP 7

PKI based on Probabilistic Quorum - 1

- **Bootstrap phase**
 - Peer generates UUID (P_{uuid}), public/private key
 - Insert tuple (P_{uuid} , public key, IP-address, timestamp, signature) into P-Grid at R_{min1} random peers so that R_{min2} distinct replicas receive insert
 - All replicas initiate updates
 - Update registered only if quorum of R_{min3} formed
 - P_{uuid} waits for confirmation from R_{min3} distinct replicas
- **Peer startup phase**
 - If the peer's IP address has changed after last session, insert new IP address securely into P-Grid

© 2003 Karl Aberer, Anwitaman Datta, Manfred Hauswirth, EPFL-IBC-IFP 8

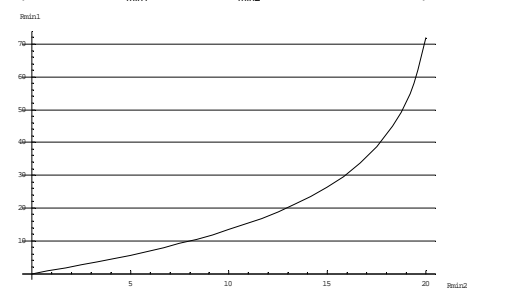
PKI based on Probabilistic Quorum - 2

- **Operation phase**
 - Routing of queries includes authentication of peers before forwarding requests using a challenge/response scheme and the stored public keys
 - Requestor collects all answers received from replicas and trusts the result if it can form a quorum of R_{min3} distinct replicas
 - Optimization
 - Peers store the public keys they learn about
- R_{min1} , R_{min2} , R_{min3} are design parameters and can be defined individually by any peer \Rightarrow individual level of security

© 2003 Karl Aberer, Anwitaman Datta, Manfred Hauswirth, EPFL-IBC-IFP 9

Finding distinct replicas

Expected effort R_{min1} to contact R_{min2} distinct and random replicas



© 2003 Karl Aberer, Anwitaman Datta, Manfred Hauswirth, EPFL-IBC-IFP 10

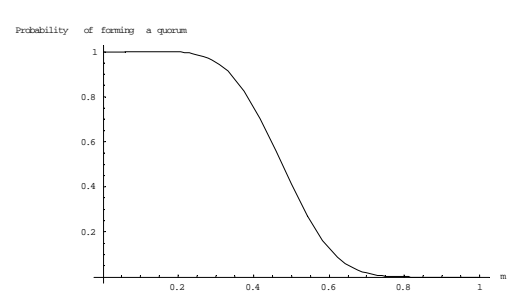
Some possible Attacks

- **Bootstrap phase**
 - Malicious replica propagates tampered tuple
 - In a predominantly well-behaving population the use of a quorum compensates for this
- **Peer startup**
 - DOS attack by malicious replica returning wrong public key
 - Quorum based authentication & randomized routing thwart this attack
- **Operation phase**
 - Impersonation
 - Quorum based authentication & randomized routing thwart this attack

© 2003 Karl Aberer, Anwitaman Datta, Manfred Hauswirth, EPFL-IBC-IFP 11

Malicious peers vs. finding a quorum

Probability of forming a quorum

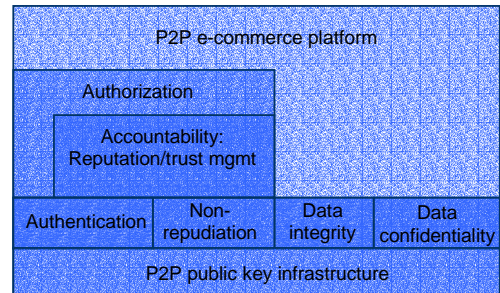


© 2003 Karl Aberer, Anwitaman Datta, Manfred Hauswirth, EPFL-IBC-IFP 12

Enabling P2P e-Commerce

- Our PKI can be used as a basis for:
 - Authentication
 - Non-repudiation
 - Accountability (reputation/trust management)
 - Authorization/access control
 - Data integrity and privacy
- Open issues
 - Payment model
 - Trust to do business (not possible even with centralized solutions)
 - Enforcement (not possible even with centralized solutions)

P2P e-Commerce Architecture



Related Work

- New approach \Rightarrow little related work exists
- PKI
 - PGP/Web of trust
- Structured P2P systems
 - DHT based systems (Chord, CAN, Pastry) cannot be applied
 - No explicit statement on the management of replicas
 - Update not addressed
 - Freenet: analysis of guarantees for update propagation required
- Unstructured P2P systems
 - Gnutella: inefficient

Conclusions

- PKIs are key to support any of e-commerce
- C2C e-commerce is inherently decentralized \Rightarrow decentralized PKIs
- Decentralized PKIs can offer similar QoS as centralized QoS but require no additional infrastructure and overcome the problem of a single point of failure
- Our decentralized PKI can provide probabilistic guarantees and works fine in a predominantly well-behaving environment
- Further research and practical tests are required
 - Exploration of hybrid systems
 - Incorporate trust in P-Grid's routing strategy

References

- **Improving Data Access in P2P Systems**, Karl Aberer, Manfred Hauswirth, Magdalena Puceva, Roman Schmidt. IEEE Internet Computing 6(1), January/February 2002.
- **Beyond "Web of Trust": Enabling P2P E-commerce**, Anwitaman Datta, Manfred Hauswirth, Karl Aberer. CEC'03, IEEE Conference on E-Commerce, June 24-27 2003, Newport Beach, California, USA.
- **Handling Identity in Peer-to-Peer Systems**, Manfred Hauswirth, Anwitaman Datta, Karl Aberer. 6th International Workshop on Mobility in Databases and Distributed Systems, MDDS'2003, in conjunction with the 14th International Conference on Database and Expert Systems Applications DEXA'2003, September 1-5, 2003, Prague, Czech Republic. A longer version is also available as EPFL Technical Report: IC-2003-67
- **Efficient, self-contained handling of identity in Peer-to-Peer systems**, Manfred Hauswirth, Anwitaman Datta, Karl Aberer. EPFL Technical Report: IC-2003-36. Submitted to IEEE Transactions on Knowledge and Data Engineering.
- <http://www.p-grid.org/>