Towards an Authentication Service for Peer-to-Peer based MMVEs

Arno Wacker[*], Gregor Schiele[♦],
Sebastian Schuster[*], and Torben Weis[*]

[*]University of Duisburg-Essen
Duisburg, Germany

[♦]University of Mannheim
Mannheim, Germany

Overview

- Motivation
- Assumptions
- Moderated vs. Open MMVEs
- Requirements
- Our Approach for an Authentication Service
- Properties
- Conclusion & Future Work

Motivation

- Security crucial requirement for MMVEs
- Open (i.e. general access) network
  - Untrusted network environment (e.g. the Internet)

    → potential threats from outside the MMVE
- (Potentially) open large user base
  - Untrusted users

    → potential threats from within the MMVE
- Goal: provide authentication service
  - Once this is achieved, other services can be added

Assumptions

- **P2P communication**
  - Send/receive messages
  - Multi-hop routing using overlay
- **Distributed Hash Table (DHT)**
  - Store/retrieve/remove globally available data
  - Consistency and persistency
  - E.g. CAN, Chord
- **Honest user majority**
  - Small fraction of malicious users

Moderated vs. Open MMVEs

We distinguish between two types of environments:

- Moderated MMVE:
  - An operator, e.g. a game provider, releases a new game
  - Mandatory registration with the game provider
  - Game fee depending on playing time etc.
- Open MMVE:
  - There is no operator
  - Managed by the virtual community itself
- Both pose different challenges

Requirements

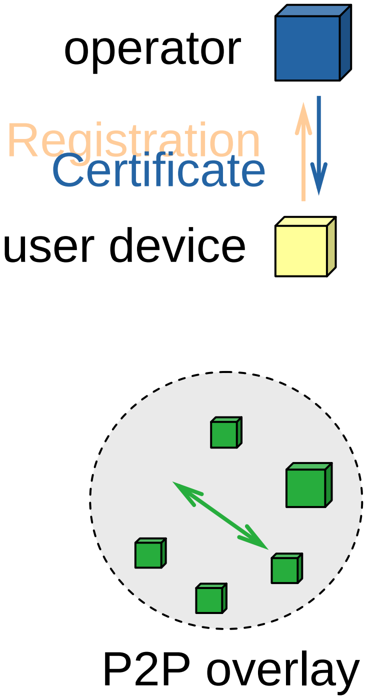
- Decentralized Operation
  - High costs for operating a server
  - No bandwidth-bottleneck
  - No single point of failure
- Privacy
  - MMVE users should remain anonymous to each other
  - However, the MMVE operator may reveal the identities
- Availability
  - Authentication is a crucial service for MMVEs
  - Log-in to the system should always be possible

Authentication Goals

- **Moderated MMVEs:**
  - Only registered users can participate in the MMVE
    - I.e. those who paid
  - Prevent identity theft
    - Personification of other users
- **Open MMVEs:**
  - Existing MMVE identity cannot be removed by other users
  - Prevent identity theft

Moderated P2P-based MMVEs

- Goal:
  - Only registered users participate
  - Prevent identity theft
- Approach:
  - Classical approach with certificates
  - Operator is CA and assigns certificate to user's MMVE identity
  - Certificate is well-known by game software
  - To access MMVE client signs messages
  - Peers can check validity through checking the certificate
  - Revocation with revocation list in the DHT

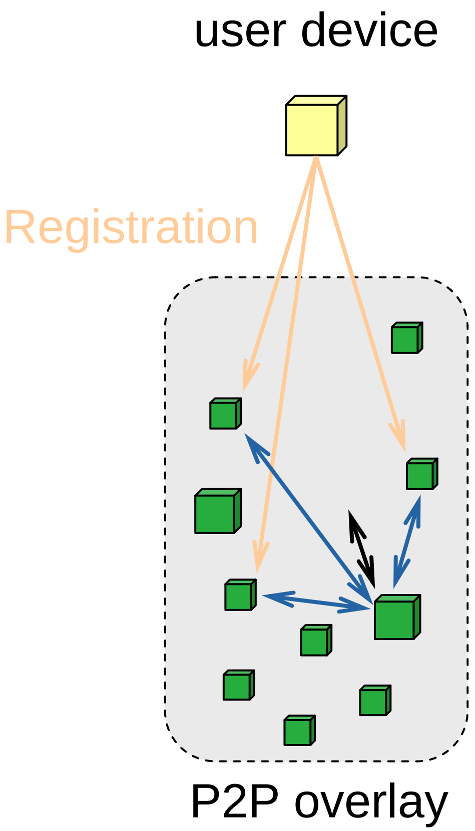


Open P2P-based MMVEs (1/2)

- Goal:
  - Prevent identity theft
- Certificates not applicable, thus:
  - Public keys stored on set of peers in DHT
  - Set size selectable (security level *s*) ➔ tolerate *s* attackers
  - Majority voting to determine valid public key
- Note:
  - Risk inversely proportional to network size
  - Evenly distributing DHT hash function required
  - Peer-id must not be selectable by user

Open P2P-based MMVEs (2/2)

1. **Registration of a new user**
   - Stores own public key in the DHT
   - Replicated 2s+1 times
   - Well know positions, e.g. derived from MMVE identity
2. **Log-In/Communication**
   - Other users can find public key
   - At least (s+1) retrieved values must match (majority)
   - Proceed with signing each message



Properties

- Decentralized Operation:
  - Moderated MMVEs: no server needed at runtime
  - Open MMVEs: no server needed at any time
- Privacy:
  - Achieved through usage of an MMVE identity
- Availability:
  - Registration in mod. MMVEs depends on operator's server
  - Registration in open MMVEs always available
  - Log-in always available (moderated and open)

Conclusion

- Authentication Service for P2P-based MMVEs
  - For moderated MMVEs:
    - Resembles closely PKI mechanism (operator as CA)
  - For open MMVEs:
    - Uses the DHT to store public keys
    - Uses replication to prevent manipulation
    - Tolerates up to *s* compromised peers (security level)
- Current & future work:
  - Implementation underway in the peers@play project
- Open issues:
  - Secure relocation of DHT content (open MMVEs)

Thank you for your attention!

Arno Wacker

arno.wacker@uni-duisburg-essen.de

- **Towards an Authentication Service for Peer-to-Peer based Massively Multiuser Virtual Environments**
  Arno Wacker, Gregor Schiele, Sebastian Schuster, and Torben Weis
  To appear in: Proceedings of the 1st International Workshop on Massively Multiuser Virtual Environments, organized at the IEEE Virtual Reality 2008, Reno, Nevada, USA, March 2008
- **Consistency Management for Peer-to-Peer-based Massively Multiuser Virtual Environments**
  Gregor Schiele, Richard Süselbeck, Arno Wacker, Tonio Triebel, and Christian Becker
  To appear in: Proceedings of the 1st International Workshop on Massively Multiuser Virtual Environments, organized at the IEEE Virtual Reality 2008, Reno, Nevada, USA, March 2008
- **Decentralized bootstrapping in pervasive applications**
  Mirko Knoll, Arno Wacker, Gregor Schiele, Torben Weis
  In: Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications (PerCom 07), Work in Progress Session, White Plains, NY, USA, March 2007
- **Requirements of Peer-to-Peer-based Massively Multiplayer Online Gaming**
  Gregor Schiele, Richard Sueselbeck, Arno Wacker, Joerg Haehner, Christian Becker, Torben Weis
  In: Proceedings of the Seventh International Workshop on Global and Peer-to-Peer Computing, organized at the IEEE/ACM International Symposium on Cluster Computing and the Grid 2007 (CCGRID 2007), Rio de Janeiro, Brazil, May 2007