Towards a Secure Rendezvous Network for Future Publish/Subscribe Architectures

Nikos Fotiou, Giannis F. Marias and George C. Polyzos
Athens University of Economics and Business
Mobile Multimedia Laboratory
{fotiou,marias,polyzos}@aueb.gr

3rd Future Internet Symposium
Berlin, Germany, September 20-22, 2010

Outline

- Publish/Subscribe Architectures
- Security Requirements
- Security Threats
- Existing Solutions
- Conclusions, Future Work

Publish/Subscribe Architectures

- 3 Basic Components
  - Publishers : Information providers that advertise information using "publications"
  - Subscribers : Information consumers that express their interest in particular pieces of information using "subscriptions"
  - A rendezvous network
- Rendezvous Network is a network of brokers
  - Responsible for matching subscriptions with publications
  - The ideal place for applying security mechanisms
- Information oriented, publisher/subscriber decouple
  - Mobility, multicast, multihoming can be easily achieved

Security Requirements

Requirements	Impact on the RN design
Publication confidentiality • Hide that a publication exists • Hide the structure of a publication • Hide the contents of a publication	Access control, Encryption, Trust Mechanisms
Integrity • Information Integrity • Subscription Integrity	Digital Signatures, Encryption, Access control
Authentication	Should be able to indentify other entities and itself.
Anonymity	Anonymity mechanisms (Open issue)
Accountability	Reports, User charging
Scoping	Access control
Availability	Load balancing, Fault tolerance, DoS resistance

Security threats

- …or lessons learned from DNS and DHTs
- Pure design and lack of cryptography led to DNS spoofing and DNS cache poisoning attacks
- Reliance in poor transitive trust led to failures caused in other administrative domains
- DHTs have been found to be vulnerable to Route attacks, Storage and retrieval attacks, Sybil attacks, Eclipse attacks

→ Efficient trust mechanisms, Fault tolerance as there will always be bad implementations, Strong identities

Security threats

- …or threats that exist in a publish/subscribe architecture
- Publish/Subscribe architectures are vulnerable to DoS attacks, which differ from the traditional DoS
- Publish/Subscribe architectures can be vulnerable to spam

➡ Distinguish of malicious messages, Isolation of bad publishers and subscribers, Assure users' privacy

Security solutions

- EventGuard: authentication for publications, confidentiality, privacy, integrity for publications and subscriptions,
  - but… subscription privacy is not so effective, before any action communication with a meta-service is needed
- Key Management Centers: message confidentiality and integrity
  - but…each topic is handled by a single KMC, scalability issues
- Various solutions for access control, based on positive access rights, OASIS role-based access control system, Attribute based encryption …
- Puzzles, micro-payments offer a layer of resistance against DoS attacks

Conclusions – Future Work

- Rendezvous network is the most critical part of the publish/subscribe architecture therefore it has to be secured
- Lessons learned from similar systems have to be taken into consideration
- Rendezvous network is the place in which various security mechanisms can be applied in order to secure publish/subscribe architecture
- PURSUIT (http://www.fp7-pursuit.eu/) project will investigate the possibilities for a world wide scale rendezvous network

Thank you