ALLSEEN ALLIANCE

Technical Steering Meeting

May 05, 2014

Antitrust Compliance Notice

- AllSeen Alliance meetings involve participation by industry competitors, and it is the intention of AllSeen Alliance to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of and not participate in any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

- Examples of types of actions that are prohibited at AllSeen Alliance meetings and in connection with AllSeen Alliance activities are described in the AllSeen Alliance Antitrust Policy. If you have questions about these matters, please contact your company counsel, or if you are a member of AllSeen Alliance, feel free to contact Lee Gesmer or Andrew Updegrove, of the firm of Gesmer Updegrove LLP, which provides legal counsel to AllSeen Alliance.

Reminder:

This call is being recorded

Agenda

- Approve minutes from last call
- Gateway working group proposal
  - Vote required
- Hackfest Recap
- AllJoyn 14.06 release
  - Dates, Status, Risks, and new features in AllSeen Alliance git repository
- Thin client security
  - Thin Client Release 14.06 Compatibility

Gateway working group proposal

Gateway Working Group Proposal Objectives

- Provide a standard and secure, remote access method for Alljoyn devices and applications
  - The remote access method should not require specific Internet firewall or port mapping configurations, so that it robustly supports most Internet connections
- Provide an extensible and standard means to connect AllJoyn devices to external/cloud services by providing:
  - A secure services discovery and provisioning node
  - Managed by the proximal network owner or with granted authority by a services provider
  - The external services to be provisioned through a hardened gateway node
  - Support multiple independent services providers – where the network owner has easy control of which are allowed to connect to the proximal network Alljoyn devices and applications.

Initial Contributors

- Affinegy
  - Art Lancaster, CTO – contributor and proposed as W.G. chair
  - Committers
    - Josh Spain, Director of Embedded Client Applications
    - Kevin Sandifer, Software Developer
    - Jim Howard, Sr. Software Developer
- Qualcomm
  - Shane Dewing, Senior Director Product Management – contributor
  - Committers
    - Tsahi Asher, Engineer Sr. Staff/Manager
    - Tali Messing, Engineer Sr.
    - Josh Hershberg, Engineer Sr. Staff

Hackfest Recap

Full House At HackFest

AllJoyn 14.06 release

Dates, Status, Risks, and new features in AllSeen Alliance git repository

Release status

- Important Dates:
  - Development Complete: May 23
  - Source Code Release to AllSeen Alliance June 30

- Status:
  - Project plan approved
  - New feature test plans reviewed and testing is underway
  - Project is proceeding according to schedule

- Risk items:
  - Next Generation Name Service (NGNS) is considered the highest schedule risk, due to the extensive development and test effort

New Features in AllSeen Alliance git repository

- Merged
  - Policy DB
  - About Integration with Thin Library
- Feature branch publicly available
  - Next Generation Name Service (NGNS)
- Awaiting branch point creation
  - UDP transport
  - Security Enhancements
  - WMI SPI Layer (WSL)
  - Events & Actions

Thin client security

Thin Client Release 14.06 Compatibility

Supported Key Exchanges

- ECC Diffie-Hellman key exchange
- Three suites of authentication
  - ECDHE_NULL is an anonymous
    - No PIN or passphrase required
  - ECDHE_PSK is a key agreement authenticated with a pre-shared key like a PIN, passphrase, or symmetric key
  - ECDHE_ECDSA is a key agreement authenticated with an asymmetric key validated with an ECDSA signature
- No longer supported PIN code key exchange
  - Since SASL was replaced by an AllJoyn handshake protocol

Compatibility

- Thin Client 14.06 can exchange encrypted messages with the following clients:
  - Thin Client 14.06
  - Standard Client 14.06
- Thin Client 14.06 can exchange non encrypted messages with any other client
- Thin Client 14.06 can establish connection with any routing node that allows anonymous clients
  - Standard Client 14.06
  - Standard Client (prior to 14.06) with configuration that allows anonymous clients

Accommodating Thin Client release 14.02

- The Thin Client 14.06 will have ECHDE_PSK as default
  - Thin Client 14.02 codes using PIN key exchange just need to be recompiled

Thank You.