ALLSEEN ALLIANCE

Core Working Group

October 03, 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

1. Microsoft proposal: Move Message Header Encryption security work from 14.12 to 15.04
2. Microsoft proposal: AllJoyn Core to recognize SASL-GSSAPI (RFC 4752 Kerberos V5) for Authentication
3. Technicolor contributions to Core 14.12

Proposal: Move Message Header Encryption security work from 14.12 to 15.04

Microsoft

Proposal: Move Message Header Encryption security work from 14.12 to 15.04

- Proposal
  - Upon request of the Gateway Working Group, Microsoft will postpone completion of Message Header Encryption Security 1.5 (14.12) work and move that work to Security 2.0 targeting the 15.04 release.
- Impact
  - The current plan of the Gateway working group is to provide a router node on a gateway that can be configured to effectively act as a firewall for AllJoyn messages. This is intended for retail available routers which allow 3rd party, AllJoyn-enabled, apps to be downloaded and executed on the router while providing access control to devices and device functionality in the home. There is some overlap with this and what will be available in Security 2.0.
  - The downloaded applications would be jailed and only able to communicate with the home network via an AllJoyn router node that would be consumer configurable to selectively allow the 3rd party application access to specific devices, interfaces and/or interface members. With the proposed change, the interface and interface members will not be available to the router node. This effectively reduces the available functionality to allowing filtering rules based solely upon source and destination, at least for encrypted messages.
- Benefit
  - Additional time will allow all parties to evaluate the proposed changes to encrypt message headers and determine how to mitigate impact to functionality.

Proposal: AllJoyn Core to recognize SASL-GSSAPI (RFC 4752 Kerberos V5) for Authentication

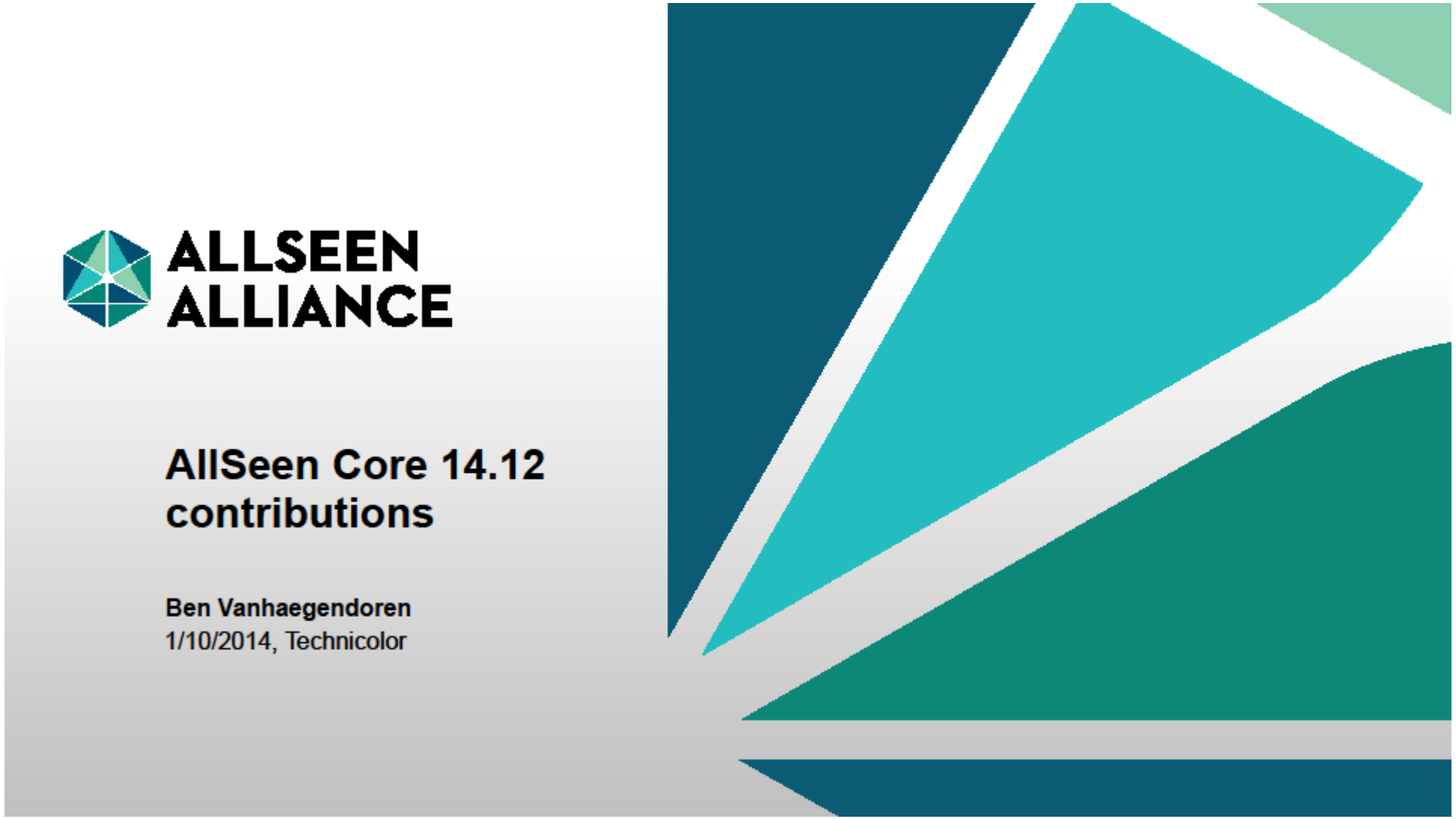
- **Summary of work:** Reserve a key exchange bit to add GSSAPI as an auth name.
- **Details:**
  - The AuthMechanisms that are supported by the AllJoyn Core are unfortunately hard coded and not dynamically extensible by the individual implementation. MSFT would like to take advantage of Kerberos authentication amongst AllJoyn peers that are domain joined. This will streamline device provisioning and simplify access control in enterprises greatly and lead to a higher acceptance of AllJoyn in managed environments.

    For that purpose MSFT is requesting to reserve a KEYX bit for GSSAPI (#define AUTH_KEYX_GSSAPI 0x00800000, #define AUTH_SUITE_GSSAPI AUTH_KEYX_GSSAPI) and add the string 'GSSAPI' as allowed AuthMechanism in CheckNames() (AuthManager.h@110) and AllJoynPeerObj::SetupPeerAuthentication(). The AllJoyn Core will by default not register a listener nor provide AuthMechanism, similar to the ALLJOYN_ECDHE_* AuthMechnisms that are currently reserved however not served in the core.
- **Benefit:**
  - This will open up the opportunity for an implementer to provide a listener and AuthMechanism that will then serve this SASL protocol. Once the authentication and authorization has been successfully completed, the shared session secret is used with SP800-180 HMAC in CTR-Mode to derive the 46 byte Master Secret.

Additional discussion points

- Discussion of AllJoyn runtime size/bloat
  - Need to establish baseline for 14.06 for each platform
  - Need to have a means to track relative code size for each core release
  - Need to agree on acceptable range (disk footprint and memory usage) of variation
- Scalability
  - How many devices can we support on an AllJoyn bus (LN?, RN?)
    - Theoretical max number; recommended max implementation?
      - How do we limit?
    - Has testing been performed?
      - If so, can you share the data

Link to Technicolor Core 14.12 contributions



Thank You

Follow Us On 

- For more information on AllSeen Alliance, visit us at: allseenalliance.org & allseenalliance.org/news/blogs