

draft-moran-suit-mud-00

Brendan Moran

The big question

- Who is qualified to define what a device should do when connected to your network?

Problem Domain

- MUD describes rules for a device's communication
- Devices announce MUD URLs.
 - Unauthenticated:
 - LLDP
 - DHCP
 - Authenticated:
 - 802.1X, embedded in client certificate
- Unauthenticated model is not resilient
- Service hosting MUD URL can set network policies.
 - MUD policies are subject to change.
- For MUD signatures, Root of Trust requires an audit.
 - See RFC8520 section 13.2

Complexities

- Device could report wrong MUD URL (excluding 802.1X)
 - MUD manager must track devices changes
- The server hosting the MUD URL can set network policy
 - Requires audit
 - RFC8520 => check web reputation
 - MUD Signature
- Rogue CA can authorize MUD signer
- Device communication may be altered by configuration
 - May require multiple MUD URLs for single class of devices

Simplifying the trust model

- The entity that creates IoT device software:
 - Signs firmware updates
 - Knows how the device communicates
 - Knows what policies are required
- The entity that creates IoT device configuration
 - Knows how that alters device communication
 - Knows how that changes device policies
 - E.g. IPv4 / IPv6
- These entities could specify a MUD file, or explicitly authorize a signer

MUD + SUIT + EAT

- SUIT manifest specifies a MUD file
 - Early delivery of MUD files
 - Binds firmware/configuration to MUD file
- Or, SUIT manifest specifies a MUD signer:
 - Normal MUD URL
 - Delivers Trust Anchor for MUD Signatures
- Attest several values to reduce complexity
 - SUIT Manifest digest
 - MUD URL
 - MUD Digest
 - MUD Signer ID
- MUD Manager can be a Relying Party
 - Verify correspondence between cached SUIT Manifest & reported MUD info

Advantages

- Reduces number of actors
 - Provides explicit link from Firmware Authority to MUD
 - Simplifies/Eliminates audit for MUD Signer
 - Makes Firmware Authority responsible for MUD Signer
 - No CA needed => Devices reject Firmware Authority changes
 - Removes MUD File hosting from threat model
- Multiple MUD files possible
 - Composition required
 - Augment static MUD file with dynamic MUD file
 - Use lookup from database based on attestation information rather than URI
- Reduces need for explicit onboarding flow
- Provides option for explicit version binding
- Provides alternative to 802.1X for MUD URL reporting with authentication

Next Steps

- Send to working group?
 - SUIT?
 - RATS?
 - Other?