Allseen Alliance
CORE working group

Security design discussion

August 12,13,14

Table of Contents

Attendees

- Microsoft (MSFT)
  - Felix Coifman felixcoi@microsoft.com
  - Rob Smith robs@microsoft.com
  - Stefan Thom stefanth@exchange.microsoft.com
  - Alain Maillot alainma@microsoft.com
  - Daniel Mihai Daniel.Mihai@microsoft.com
  - Brian Clubb Brian.Clubb@microsoft.com
- Symantec
  - Paul Sangster Paul_Sangster@symantec.com
  - Minglang Pei
- Technicolor
  - Gerrit Ruelens Gerrit.Ruelens@technicolor.com
  - Dominique Chanet Dominique.Chanet@technicolor.com
  - Joris Bleys Joris.Bleys@technicolor.com
- Qualcomm Connected Experiences (QCE)
  - Ken Swinson kens@qce.qualcomm.com
  - Phil Nguyen philn@qce.qualcomm.com
  - Greg Burns gburns@qce.qualcomm.com
  - Marcello Lioy mlioy@qce.qualcomm.com
  - Cam McDonald cameronm@qti.qualcomm.com
  - Chris Kavas ckavas@qce.qualcomm.com

Agenda

- Introductions
- Review HLD
- Deep dive on open design items from HLD and day 1
  - Separate membership policy from guild certificate
- Components and implementers
- Existing issues not identified in 2.0
- Work process
- Testing
- Scheduling

Overall statements

- Need process to develop threat models
- There is a business case where someone could offer a security service

HLD Review

2.1 Overview

- Permission system is developed outside of the application
- Security manager
  - Update description to include
    - The security manager is optional

                - The way it works is that it is about defining the relationships between devices; this can also be done directly in the device itself. Assuming that the relationships/permissions are defined, the security manager doesn't need to be there in order for the system to work
            - This is an app that assists in managing security using the security APIs
            - This is a framework
            - Membership certificates should be discussed
                - Are they required?
                - Can symmetric keys be directly provisioned into devices

Figure 2.1 Security system diagram

- There could be multiple instances of security manager
    - Design does not restrict it
    - How to maintain consistency is not defined
- Should set some rules or "best practices"
- You can have multiple admin users
    - We have considered use case when the device with admin privilege is damaged/lost so end user has a backup.
        - Considered outside of the scope of AllJoyn
- Discussed the idea of a credentials database
    - This could be a separate module from the security manager
    - For constrained devices you may not need for them to have an identity and could have a group key.
- Pre-shared secret support to be backwards compatible with security 1.0
- Instead of 48 byte master secret, use an algorithm identifier to give us crypto agility
    - Goal is not to tie ourselves to specific type of key
    - Need to determine the minimal set of algorithms
        - Agreed to support:
            - SHA256
            - AES-CMAC
    - Need a more generic algorithm exchange
- Need a mechanism to uniquely identify an asset

Additional Discussion Items

Enterprise Management

- Scale
- Permissions
- Plug in with existing infrastructure
- One option is a security manager plug in

Federated identities

- Conclusion – possible through an app
- Identity equivalence
- Today we do equivalence of a derived AllJoyn identity

X509 vs SPKI

- Question: Do we need certificates on small devices
  - What is a small device?
    - ~ 256K to 512K RAM devices
    - A standalone device that can be proximal
  - Answer is NO
- Consider decoupling what can be done from the certificate and keep the cert more static
- Enterprises use X509 extensively
- **GO for X509**
  - Pull out SPKI
- Is XACML (eXtensible Access Control Markup Language) a possible option or is this too complex?

Separate membership policy from guild certificate

- If the guild membership certificate is rarely modified, then consider moving the remaining data out of the guild membership certificate into the signed policy document.
- Will discuss more on day 2

TPM support in the certificate?

- This could be implemented in the trust zone
- Consider putting attestation in the certificate
  - Note: TPM key attestation is the ability of the user who is requesting a certificate to cryptographically prove to a CA that the RSA key in the certificate request is protected by either “a” or “the” TPM that the CA trusts.
- Need to investigate – action item created

Existing concerns with Security 1.0 and not identified in 2.0

- RN to RN communication that is not authenticated or encrypted
  - Header data is not encrypted
  - Routers are not encrypted
    - Routers are not trusted
  - No differentiation between private and open networks
  - Need to determine how to manage DoS attacks
- About interface is not authenticated and reveals info an attacker would want to know
  - Need to encrypt part of the about information
  - Broadcast signal – needs to be in the open
    - We could limit the amount of data initially sent
  - The subsequent requests after the broadcast could be encrypted
- Isolating traffic across two networks
  - Broadcast signals or multicast will span the entire tree
  - Routing nodes on multi homed devices

        - Router node should enforce separation
            - Nanny camera use case
        - This is potentially addressed with Security 2.0
            - More granular permission

Discovery of claimable devices

- Onboarding service manages this
    - Wifi configuration
    - Config service
        - All about configuration of the friendly name
- Need to resolve
    - How do I know I am claiming my device?
    - How do I know I am not onboarding my neighbor's TV?
- Onboarding service can require authentication
- Consider a C&C rule to enforce authentication?
- Should a device that is not claimed advertise itself as claimable?
    - Could be a field in About "claimable"

Revocation & Redistribution of policies/certificates

- Need to look at all the certificates and determine the method for revocation for each
- Expirations in X509 can be leveraged
- Default lifetime for certs
    - Will be determined when the profile is designed
    - The time is used to avoid having to revoke the cert
- Potential for a "revocation service" for certificates
    - May have two methods for TCL vs SCL
- Consider both push and pull policy for validating certificates
    - This would be "best effort"
- Where is the canonical data?
    - Canonical – the ACL
    - Security manager or end devices?
        - Cloud would be a requirement if one has multiple security managers
    - Current architecture does not require a security manager
    - System should recognize not all security features work without the security manager
        - Without the security manager, revocation may not work
- Could a security update be a "signed" sessionless signal?
    - Sessionless signals are not currently signed and the sender cannot guarantee that the message was delivered
- Security manager is the only one that can be reliably backed up
    - Need a way to query devices to determine policy
- Need to investigate peer nodes redistributing policy information
    - Action item set up
    - In the future, C&C may enforce this feature
    - Need to determine story for subnet to subnet routing
        - Discussion for CORE WG

        - Outside of scope of current security discussion
- OCSP (Online Certificate Status Protocol)
    - A method that we could use for cert revocation
    - An Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 6960

Federated Identities

- Cloud manager could resolve this
- You cannot use these today to do anything local
- Is there a way that the security manager can be tied to the MSA for apps to authenticate without the security manager?
    - One option - Part of the app install should be to log into the MSA to get credentials
    - This will require a prototype – Action captured

Enforcement of manifest

- Goal is, if you want to be claimed, you need to tell the security manager what interfaces you want to provide and access
- A device would potentially send a manifest to the peer and the peer would then validate the call against the manifest to ensure that the approved calls are being made
- User experience should be taken into account if this will be designed
- Do we want the idea of a manifest to be part of Security 2.0?
    - Yes, action created

XML vs JSON for policies

- No decision made – further thought needed
- Action item – QCE to Turn JSON examples into a table in HLD

Credential backup and restore

- Action item created to investigate

Scenarios Discussed

- Scenarios
    - Hotel
    - Rental
    - Sell house/appliance
    - Repossession
    - Theft
- Ideas
    - Offborarding service should be considered
    - “Crossboarding” service should be considered
    - Potentially a “cloud service” to assist
    - Need time limited permissions / certificates
        - Or a system that can wipe all the existing credentials
        - Consider a countdown timer for the small devices that do not keep track of time
        - May need a controller to host the security manager

- Small devices that are not able to save time state and power on and off and the countdown is reset
- Security manager could be built into a hub device that has a routing node

Development Process

Major component breakdown

Component	Dev Team	Dev LOE	Test LOE	Dependencies
Permission Mgmt & enforcement TC Linux	QCE			
Permission Mgmt & enforcement SC Linux	QCE			
~~Exposing Credential/Signer APIs SC Linux~~	QCE			
~~Exposing Credential/Signer APIs iOS~~	QCE			
~~Exposing Credential/Signer APIs Android~~	QCE			
~~Exposing Credential/Signer APIs Windows~~				
~~Exposing Credential/Signer APIs JavaScript~~				
Permission Mgmt TC (other platform TBD)	QCE			Target minimum: 32K RAM / 512K Flash
Security Manager API & Application SC Linux	Technicolor			Permission Mgmt and Exposing APIs in different stages. Security manager service (maintains state) can run on any device but requires a separate app for the UI.
Security Manager Sample App Android	Technicolor			Sample app for now, reference in the future
Security Manager Sample App iOS	Technicolor			Sample app for now, reference in the future
Security Manager Sample App Windows	MSFT			
~~Security Manager Sample App JavaScript~~				Requires HTML5
Provide hooks to replace default Key Store in CORE	QCE			Related to trusted platform investigation
Use hooks to replace default Key Store in Windows	MSFT			Related to trusted platform investigation
Use hooks to replace default Key Store in Android	??			Related to trusted platform investigation
Use hooks to replace default Key Store in IOS	??			Related to trusted platform investigation
Proxy distribution agent SC (Generic version)	Technicolor			Once design is done, determine if experimental for 2.0 Related to actions items #20 & #22
Proxy distribution agent SC OpenWRT	QCE			Once design is done, determine if experimental for 2.0 Related to actions items #20 & #22
Test plans	All			Plans from each contributing team regarding the test plans for their respective contributions. Need strong collaboration for crafting test plans for combined testing on the integration branch
Integration Testing	All			Requires collaboration across all teams

Functional/Compatibility Testing	All			Requires collaboration across all teams
Performance Testing	All			Requires collaboration across all teams May be platform specific (e.g. MSFT may do Windows testing)
E2E System Testing	All			Requires collaboration across all teams May be platform specific (e.g. MSFT may do Windows testing)
Threat Analysis for CORE	QCE			Cam
Threat Analysis for Windows	MSFT			Felix
Threat Analysis Generic	Technicolor			TBD

Collaboration Mechanics

- Code contribution
    - Each contributing team will have their own feature branch
    - The Security feature will have an integration branch
    - The integration branch will then be the branch merged with master

Schedule Discussion

- Each contributing team needs to plan the items they have claimed
- Milestone for teams to communicate their plans
    - Meeting week of Aug 25th to discuss the plans

Communication Process

- Email
    - Leverage CORE WG mail list
        - https://wiki.allseenalliance.org/core/overview
- Conference Calls
    - How often?
        - Weekly calls with each appointed lead from the contributing teams
            - 7am PT
            - TBD (Preferred Tues)
        - Required attendees:
            - QCE: Chris Kavas
            - MSFT: Brian Clubb
            - Technicolor: Ben Vanhaegendoren
            - Symantec: Paul Sangster
        - Larger calls as needed
    - Will be managed by the Alliance
        - Calls will be announced in mail list
        - Calls will be recorded
- Ad-hoc discussions
    - Decisions from any ad-hoc discussions are posted to mail list
    - Trivial discussions are not required to be posted

Next Steps

- Schedules

Actions

ID	Action	2.0	Owner
1	Define a crypto agility exchange	Y	QCE
2	Define a plug in model/Enterprise mgmt./ Optional credential manager	N	MSFT
3	~~Optional credential manager~~	N	N/A
4	Review the key identifier – need a fixed size handle	Y	QCE
5	Need to develop threat models	N	SYMC?
6	~~Consider showing examples of what is in a certificate in the HLD~~		
7	~~Profile spec on how to code into a certificate~~		
8	Implement X509	Y	QCE
9	Identify the X509 profile for AllJoyn	Y	SYMC/MSFT
10	Remove SPKI	Y	QCE
11	Investigate TPM in 1.0 security model / defining interfaces to expose TPM functionality	Y	QCE
12	Encrypt a portion of the About information	?	MSFT
13	Determine what info in About should be restricted	?	MSFT
14	Add “claimable” field in About	Y	QCE
15	Investigate offboarding/crossboarding/claimable state options define use cases for “device churn”	?	MSFT
16	Security manager should have a mechanism to query devices to determine policy – Update HLD	Y	QCE
17	Security manager should be able to push updates– Update HLD	Y	QCE
18	End nodes need to be able to pull policy updates– Update HLD	Y	QCE
19	Policies need a revision number – Update HLD	Y	QCE
20	Determine how peer devices send policy updates between peers – This could OBE #22	Y	Worksplit discussion
21	In CORE WG, begin discussion to determine story for subnet to subnet routing	N	?
22	Determine if a proxy could work for policy distribution – this could OBE #20	Y	Worksplit discussion
23	Federated use identity prototype		MSFT
24	Manifest enforcement feature – HLD updates & propose implementation	Y	Technicolor
25	Pre-shared secret support to be backwards compatible with security 1.0	Y	QCE
26	Turn JSON examples into a table in HLD	Y	QCE
27	Begin discussion in CORE WG regarding scenarios for transfer/ temp access/ repossessing a device	N	MSFT
28	Update revocation in HLD/LLD	Y	QCE
29	Update LLD regarding granted permissions	Y	QCE

30	Team should decide on a TC platform. Target minimum 32K RAM 512 Flash	Y	QCE
31	Need to follow up on Test coordination. Specifically coordinating on the plan and implementation of Functional and performance testing across all features in the integration branch	Y	Worksplit discussion
32	Test plan fuzzing – will require coordination with all test leads from each contributing team	Y	MSFT
33	Identify POC for Threat Analysis effort	Y	Technicolor
34	Identify POC for programmatics from each team QCE: Chris Kavas MSFT: Brian Clubb Technicolor: Ben Vanhaegendoren Symantec: Paul Sangster	Y	All
35	Determine time and set up weekly calls through Alliance	Y	QCE