Mathematical Mesh 3.0 Part XI: Security Considerations

Mathematical Mesh Reference

<series>draft-hallambaker-mesh-security

<status>informational

<stream>independent

<ipr>trust200902

<author>Phillip Hallam-Baker

<surname>Hallam-Baker

<initials>P. M.

<firstname>Phillip

<email>phill@hallambaker.com

<organization>ThresholdSecrets.com

<also>http://mathmesh.com/Documents/draft-hallambaker-mesh-security.html

The Mathematical Mesh ‘The Mesh’ is an end-to-end secure infrastructure that facilitates the exchange of configuration and credential data between multiple user devices. The core protocols of the Mesh are described with examples of common use cases and reference data.

[Note to Readers]

Discussion of this draft takes place on the MATHMESH mailing list (mathmesh@ietf.org), which is archived at https://mailarchive.ietf.org/arch/search/?email\_list=mathmesh.

# Introduction

# Definitions

This section presents the related specifications and standard, the terms that are used as terms of art within the documents and the terms used as requirements language.

## Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in <norm="RFC2119"/>.

## Defined Terms

The terms of art used in this document are described in the *Mesh Architecture Guide* <norm="draft-hallambaker-mesh-architecture"/>.

## Related Specifications

The architecture of the Mathematical Mesh is described in the *Mesh Architecture Guide* <norm="draft-hallambaker-mesh-architecture"/>. The Mesh documentation set and related specifications are described in this document.

## Implementation Status

The implementation status of the reference code base is described in the companion document <info="draft-hallambaker-mesh-developer"/>.

<include=..\Generated\SchemaMesh.md>

<include=..\Generated\MeshProtocol.md>

# Assets

## Data

## Credentials

## Reputation

### Outbound Messaging Abuse ()

# Risks

## Confidentiality

Is a regulatory requirement GDPR/HIPPA

### Privacy

Stronger requirement, given data but with restrictions on use

Unintended use within an organization may put it in default

GDPR

HIPPA

## Integrity

Modification of data enables control breaches

## Availability

### Data loss

Loss of the pictures of the kids at 5

### Partial data survivability

Where they buried Aunt Agatha’s jewelry but not where they buried Aunt Agatha.

## Inbound Messaging Abuse (Spam)

# Threats

## End point Compromise

# Controls

## Cryptographic

### Triple lock

#### Transport Security

Traffic analysis protection

#### Message Security

Access control

Authentication / Integrity

#### Data Level Security

Data Confidentiality

Non-Repudiation

### Key Protection

Use of platform provided facilities to bind private keys in the Device profile to the device is highly desirable. Ideally, private keys should be protected against extraction by hardware techniques presenting a high degree of resistance.

#### Windows

Use encrypted key store

Preferably use BitLocker

#### OSX

Use Key Ring

#### iOS

Use ???

#### Linux

Use the DBUS mechanism

#### Android

Hope and prayers.

### Key and Nonce Generation

Use strong mechanisms as described in RFC???

Use of key co-generation as described in part 8 is advised

### Key Escrow and Recovery

Master profile keys should be escrowed

Escrow strategies for DARE should take account of the fact that users may want some but not all their data assets to survive them.

### Profile Verification

Check that the device credential has been signed by an administration device and that the administration device was properly authorized by the master profile.

Device catalog MUST be signed by the admin device.

Future – provide protection against rollback attacks.

### Identity Validation

See the separate document on the trust model

### Trust Broker Accountability

Cert transparency type techniques

## Mesh Messaging

### Ingress Control

Every message is subject to access control

Mesh Services should perform abuse filtering on inbound mail

Mesh Services MUST apply user specified ingress control as specified in their contacts catalog.

### Egress Control

Some applications may require egress control

For example, classified environments

Mail too stupid to send

### Security Signal

Confirmation messages requiring payments

Need Accountability

Need to know the source of the accountability assertions

Should be distinguished from sender controlled part of a message

#### Brand

If messages are being sent on behalf of a corporate entity, this should be signaled to both sender and receiver

Sender – remind them that they are speaking on behalf of another party

Receiver – establish who is speaking by the familiar technique.

### Accountability

Authentication and consequences

# Security Considerations

This document comprises the security considerations for the use and implementation of the Mathematical Mesh.

## Integrity

### DNS Spoofing

### TLS Downgrade

### TLS Service Impersonation

### Request Replay Attack

### Response Replay Attack

## Confidentiality

### Side Channel Attack

### Session Key Leakage

# IANA Considerations

All the IANA considerations for the Mesh documents are specified in this document

# Acknowledgements

A list of people who have contributed to the design of the Mesh is presented in <norm="draft-hallambaker-mesh-architecture"/>.