Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 25, 2020

P. Hallam-Baker
October 23, 2019

Mathematical Mesh 3.0 Part X: Considerations for Quantum Cryptanalysis Resistance
draft-hallambaker-mesh-quantum-01

Abstract

The Mathematical Mesh 'The Mesh' is an infrastructure that facilitates the exchange of configuration and credential data between multiple user devices and provides end-to-end security. This document describes.

[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.

This document is also available online at http://mathmesh.com/Documents/draft-hallambaker-mesh-quantum.html [1] .

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 25, 2020.

Table of Contents

1. Introduction

One of the core goals of the Mesh is to move the state of the art in commercial cryptography beyond that achieved in the 1990s when PKIX, S/MIME and OpenPGP were first developed. While each of these infrastructures and protocols has been subject to incremental improvement, none has seen widespread adoption of new cryptographic approaches.

o Quantum Resistant Signatures.

2. 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.

2.1. 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 [RFC2119] .

2.2. Defined Terms

The terms of art used in this document are described in the Mesh Architecture Guide [draft-hallambaker-mesh-architecture] .

2.3. Related Specifications

The architecture of the Mathematical Mesh is described in the Mesh Architecture Guide [draft-hallambaker-mesh-architecture] . The Mesh documentation set and related specifications are described in this document.

2.4. Implementation Status

The implementation status of the reference code base is described in the companion document [draft-hallambaker-mesh-developer] .

3. Recommended and Required Algorithms

4. Quantum Resistant Signatures.

Quantum computing has made considerable advances over the past decade and the field has now reached the point where a machine weighing many tons can apply Shor's algorithm to factor numbers as large as 35 before decoherence occurs.

Should construction of a large-scale device prove practical, it will in principle be possible to break all of the public key cryptosystems currently in use. While public key cryptosystems that resist quantum cryptanalysis are currently in development, none has yet reached a sufficient state of maturity for the field to reach consensus that they are resistant to ordinary cryptanalysis, let alone offer a replacement.

The consequence of successful quantum cryptanalysis for encryption systems is that all material encrypted under existing public key

systems could be decrypted by a quantum capable attacker. Nor is mitigation of this consequence practical since it is not the adoption of new cryptographic algorithms that make a system more secure, it is the elimination of weak options that provides improvement.

The Mesh does not currently provide an infrastructure that is Quantum Resistant but could in principle be used as the basis for deploying a Needham-Schroeder style symmetric key infrastructure or a future PKI based on an as yet undecided quantum cryptanalysis resistant public key algorithm.

Mesh profiles MAY include a Quantum Resistant Signature Fingerprint (QRSF). This contains the UDF fingerprint of an XMSS signature public key [RFC8391] together with the parameters used to derive the private key set for the public key from a 256 bit master secret.

Should it ever become necessary to make use of the QRSF, the user first recovers the master secret from whatever archival mechanism was used to protect it. The use of secret sharing to protect the secret is RECOMMENDED. The master secret is then used to reconstruct the set of private keys from which the public key set is reconstructed. The profile owner can now authenticate themselves by means of their XMSS public key.

4.1. Example: Creating a Quantum Resistant Signature Fingerprint

Alice decides to add a QRSF to her Mesh Profile. She creates a 256 bit master secret.

TBS:

To enable recovery of the master key, Alice creates five keyshares with a quorum of three:

TBS:

Alice uses the master secret to derrive her private key values:

TBS:

These values are used to generate the public key value:

TBS:

The QRSF contains the UDF fingerprint of the public key value plus the XMSS parameters:

TBS:

Alice adds the QRSF to her profile and publishes it to a Mesh Service that is enrolled in at least one multi-party notary scheme.

5. Security Considerations

The security considerations for use and implementation of Mesh services and applications are described in the Mesh Security Considerations guide [draft-hallambaker-mesh-security] .

6. IANA Considerations

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

7. Acknowledgements

A list of people who have contributed to the design of the Mesh is presented in [draft-hallambaker-mesh-architecture] .

8. References

8.1. Normative References

[draft-hallambaker-mesh-architecture]
Hallam-Baker, P., "Mathematical Mesh 3.0 Part I: Architecture Guide", draft-hallambaker-mesh-architecture-10 (work in progress), August 2019.

[draft-hallambaker-mesh-security]
Hallam-Baker, P., "Mathematical Mesh Part VII: Security Considerations", draft-hallambaker-mesh-security-01 (work in progress), July 2019.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997.

8.2. Informative References

[draft-hallambaker-mesh-developer]
Hallam-Baker, P., "Mathematical Mesh: Reference Implementation", draft-hallambaker-mesh-developer-08 (work in progress), April 2019.

[RFC8391] Huelsing, A., Butin, D., Gazdag, S., Rijneveld, J., and A. Mohaisen, "XMSS: eXtended Merkle Signature Scheme", RFC 8391, DOI 10.17487/RFC8391, May 2018.

8.3. URIs

[1] http://mathmesh.com/Documents/draft-hallambaker-mesh-quantum.html

Author's Address

Phillip Hallam-Baker

Email: phill@hallambaker.com