INTERNET-DRAFT
Intended Status: Informational
Expires: July 28, 2014

S. Moonesamy

January 24, 2014

Using ED25519 in SSHFP Resource Records
draft-moonesamy-sshfp-ed25519-00

Abstract

The Ed25519 signature algorithm has recently been implemented in OpenSSH. This document updates the IANA "SSHFP RR Types for public key algorithms" registry by adding an algorithm number for Ed25519.

Status of this Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

1. Introduction

The Ed25519 [Ed25519] signature algorithm has recently been implemented in OpenSSH. RFC 4255 [RFC4255] defines a new DNS resource record, "SSHFP", which can be used to publish a fingerprint of the SSH server public key in the DNS. This document updates the IANA "SSHFP RR Types for public key algorithms" registry by adding an algorithm number for Ed25519 [Ed25519].

2. ED25519 Public Key

A SSHFP-aware Secure Shell implementation of the the Ed25519 signature algorithm should support SHA-256 fingerprints [FIPS180-4][RFC6594] for verification of the ED25519 public key. A SSHFP-aware Secure Shell implementation which also supports SHA1 fingerprints [FIPS180-4][RFC6594] must choose a SHA-256 fingerprint over a SHA1 fingerprint if both fingerprints are available. If the SHA-256 fingerprint does not match the SSH public key received from the SSH server, it is recommended that the public key be rejected instead of testing the SHA1 fingerprint.

2.2. ED25519 Public Key with SHA1 Fingerprint

The SSHFP Resource Record for the ED25519 public key with SHA1 fingerprint would, for example, be:

```
ssh.example.com IN SSHFP [TBD] 1 ( 06a2de9a2d0f034701d67917e49cfc4
                                   5a03c2e61 )
```

2.2. ED25519 Public Key with SHA-256 Fingerprint

The SSHFP Resource Record for the ED25519 public key with SHA-256 fingerprint would, for example, be:

```
ssh.example.com IN SSHFP [TBD] 2 ( a87f1b687ac0e57d2a081a2f2826723
                                   34d90ed316d2b818ca9580ea384d924
                                   01 )
```

RFC Editor Note: Please replace TBD with the value assigned by IANA.

3. Security Considerations

The overall security of using SSHFP for SSH host key verification is dependent on the security policies of the SSH host administrator and DNS zone administrator (in transferring the fingerprint), detailed aspects of how verification is done in the SSH implementation, and in the client's diligence in accessing the DNS in a secure manner.

Please refer to RFC 4255 [RFC4255] for a discussion of the security considerations.

4. IANA Considerations

IANA is requested to add the following entry to the "SSHFP RR Types for public key algorithms" registry:

Value	Description	Reference
[TBD]	ED25519	[RFCXXXX]

RFC Editor Note: Please replace TBD with the value assigned by IANA and RFCXXXX to refer to this document.

5. Acknowledgements

Some of the text in this document is from RFC 6594 which was written by Ondrej Sury. The author would like to thank Damien Miller for his feedback.

6. References

6.1. Normative References

[RFC4255] Schlyter, J. and W. Griffin, "Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints", RFC 4255, January 2006.

[RFC6594] Sury, O., "Use of the SHA-256 Algorithm with RSA, Digital Signature Algorithm (DSA), and Elliptic Curve DSA (ECDSA) in SSHFP Resource Records", RFC 6594, April 2012.

[FIPS180-4] National Institute of Standards and Technology, "Secure Hash Standard (SHS)", FIPS PUB 180-4, March 2012, <http://csrc.nist.gov/publications/fips/fips180-4/fips180-4_final.pdf>.

6.2. Informative References

[Ed25519] <http://ed25519.cr.yp.to/ed25519-20110926.pdf>

Authors' Addresses

S. Moonesamy
76, Ylang Ylang Avenue
Quatres Bornes
Mauritius

Email: sm+ietf@elandsys.com