Internet Engineering Task Force (IETF)
Request for Comments: 7479
Category: Informational
ISSN: 2070-1721

S. Moonesamy

March 2015

Using Ed25519 in SSHFP Resource Records

Abstract

The Ed25519 signature algorithm has 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 document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7479.

Table of Contents

1. Introduction

The Ed25519 [Ed25519] signature algorithm, specifically Ed25519-SHA-512, has been implemented in OpenSSH. RFC 4255 [RFC4255] defines a 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 with SHA-256 Fingerprint

The encoding of Ed25519 public keys is described in [Ed25519]. In brief, an Ed25519 public key is a 32-octet value representing a 255-bit y-coordinate of an elliptic curve point, and a sign bit indicating the corresponding x-coordinate.

The SSHFP Resource Record for the Ed25519 public key with SHA-256 fingerprint [FIPS180-4] would, for example, be:

```
ssh.example.com IN SSHFP 4 2 ( a87f1b687ac0e57d2a081a2f2826723
                               34d90ed316d2b818ca9580ea384d924
                               01 )
```

The following body of the public key file was used as input to generate the above fingerprint:

```
ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIGPKSUTyz1HwHReFVvD5obVsALAgJRNarH4TRpNePnAS
```

The opaque octet string output produced is placed as is in the RDATA fingerprint field.

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 has added the following entry to the "SSHFP RR Types for public key algorithms" registry:

Value	Description	Reference
4	Ed25519	[RFC7479]

5. References

5.1. Normative References

[Ed25519] Bernstein, D. J., Lange T., Schwabe P., and B-Y. Yang, "High-Speed High-Security Signatures", Journal of Cryptographic Engineering, Vol. 2, September 26, 2011.

[RFC4255] Schlyter, J. and W. Griffin, "Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints", RFC 4255, January 2006, <http://www.rfc-editor.org/info/rfc4255>.

5.2. Informative References

[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/fips-180-4.pdf>.

Acknowledgements

Some of the text in this document was written by Ondrej Sury. The author would like to thank Richard Barnes, Damien Miller, Yoav Nir, and Paul Wouters for their feedback. Rene Struik provided advice about the usage of Ed25519. Stephen Farrell, as Security Area Director, reviewed the code point request.

Author's Address

S. Moonesamy
76, Ylang Ylang Avenue
Quatres Bornes
Mauritius

EMail: sm+ietf@elandsys.com