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.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
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:

\[
\text{ssh.example.com IN SSHFP 4 2 ( a87f1b687ac0e57d2a081a2f2826723
34d90ed316d2b818ca9580ea384d924
01 )}
\]

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

\[
\text{ssh-ed25519}
\text{AAAAC3NzaC1lZDI1NTE5AAAIGPKSUTyz1HwReFVvD5obVsALAgJRNaHR4TrpNePnAS}
\]

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:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Ed25519</td>
<td>[RFC7479]</td>
</tr>
</tbody>
</table>

5. References

5.1. Normative References


5.2. Informative References

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