Using DNS to securely publish SSH key fingerprints
draft-ietf-secsh-dns-00.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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/ietf/1id-abstracts.txt.

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

This Internet-Draft will expire on February 10, 2003.

Copyright Notice

Copyright (C) The Internet Society (2002). All Rights Reserved.

Abstract

This document describes a method to verify SSH host keys using DNSSEC. The document defines a new DNS resource record that contains a standard SSH key fingerprint.
Table of Contents

1. Introduction ........................................... 3
2. SSH Host Key Verification ............................... 3
   2.1 Method .............................................. 3
   2.2 Fingerprint matching ................................. 3
   2.3 Authentication ...................................... 3
3. The SSHFP resource record .............................. 4
   3.1 The SSHFP RDATA format ............................... 4
   3.1.1 Algorithm number specification ...................... 4
   3.1.2 Fingerprint type specification ...................... 4
   3.1.3 Fingerprint ........................................ 5
3.2 Presentation format of the SSHFP RR .................. 5
4. Security considerations .................................. 5
   4.1 Backend transport integrity ............................ 5
   4.2 Effects on the SSH trust model ....................... 5
5. IANA considerations ..................................... 5
References .................................................. 6
Authors’ Addresses ......................................... 7
A. Acknowledgements ....................................... 7
Full Copyright Statement .................................. 8
1. Introduction

The SSH [9] protocol provides secure remote login and other secure network services over an insecure network. The security of the connection relies on the server authenticating itself to the client.

Server authentication is normally done by presenting the fingerprint of an unknown public key to the user for verification. If the user decides the fingerprint is correct and accepts the key, the key is saved locally and used for verification for all following connections. While some security-conscious users do verify the fingerprint out-of-band before accepting the key, the average user usually blindly accepts the key presented.

The method described here can provide out-of-band verification by looking up a fingerprint of the server public key in the DNS [1][2] and using DNSSEC [5] to verify the lookup.

In order to distribute the fingerprint using DNS, this document defines a new DNS resource record to carry the fingerprint.

Basic understanding of the DNS system [1][2] and the DNS security extensions [5] is assumed by this document.

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 RFC 2119 [3].

2. SSH Host Key Verification

2.1 Method

Upon connection to a SSH server, the SSH client MAY look up the SSHFP resource record(s) for the host it is connecting to. If the algorithm and fingerprint of the key received from the SSH server matches the algorithm and fingerprint of one of the SSHFP resource record(s) returned from DNS, the client MAY accept the identity of the server. It is RECOMMENDED that the client ask the user for confirmation before accepting the identity of the server.

2.2 Fingerprint matching

The public key and the SSHFP resource record are matched together by comparing algorithm number and fingerprint.

2.3 Authentication

A public key verified using this method MUST only be trusted if the
SSHFP RR used for verification was authenticated by a trusted SIG RR.

Clients that do not validate the DNSSEC signatures themselves MUST use a secure transport, e.g. TSIG [6], SIG(0) [7] or IPsec [4], between themselves and the entity performing the signature validation.

3. The SSHFP resource record

The SSHFP resource record (RR) is used to store a fingerprint of a SSH public host key that is associated with a Domain Name System (DNS) name.

The RR type code for the SSHFP RR is TBA.

3.1 The SSHFP RDATA format

The RDATA for a SSHFP RR consists of an algorithm number, fingerprint type and the fingerprint of the public host key.

```
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----------------------------------------------
|   algorithm   |    fp type    |                               |
+-----------------------------------------------
|                                           /  |
|                                           /  |
|                                           /  |
|                                           /  |
|                                           /  |
|                                           /  |
+-----------------------------------------------
```

3.1.1 Algorithm number specification

This algorithm number octet describes the algorithm of the public key. The following values are assigned:

<table>
<thead>
<tr>
<th>Value</th>
<th>Algorithm name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>reserved</td>
</tr>
<tr>
<td>1</td>
<td>RSA</td>
</tr>
<tr>
<td>2</td>
<td>DSS</td>
</tr>
</tbody>
</table>

Reserving other types requires IETF consensus.

3.1.2 Fingerprint type specification

The fingerprint type octet describes the message-digest algorithm used to calculate the fingerprint of the public key. The following
values are assigned:

<table>
<thead>
<tr>
<th>Value</th>
<th>Fingerprint type</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>reserved</td>
</tr>
<tr>
<td>1</td>
<td>SHA-1</td>
</tr>
</tbody>
</table>

Reserving other types requires IETF consensus. For interoperability reasons, as few fingerprint types as possible should be reserved. The only reason to reserve additional types is to increase security.

3.1.3 Fingerprint

The fingerprint is calculated over the public key blob as described in [10].

3.2 Presentation format of the SSHFP RR

The presentation format of the SSHFP resource record consists of two numbers (algorithm and fingerprint type) followed by the fingerprint itself presented in hex, e.g:

```
host.example. SSHFP 2 1 123456789abcdef67890123456789abcdef67890
```

4. Security considerations

4.1 Backend transport integrity

Since DNSSEC only protects the integrity of the host key fingerprint after it is signed by the DNS zone administrator, the fingerprint must be transferred securely from the SSH host administrator to the DNS zone administrator. This could be done manually between the administrators or automatically using secure DNS dynamic update [8] between the SSH server and the nameserver.

4.2 Effects on the SSH trust model

... to be written ...

5. IANA considerations

IANA needs to allocate a RR type code for SSHFP from the standard RR type space.

IANA needs to open a new registry for the SSHFP RR type for public key algorithms. Defined types are:
0 is reserved
1 is RSA
2 is DSA

Adding new reservations requires IETF consensus.

IANA needs to open a new registry for the SSHFP RR type for fingerprint types. Defined types are:

0 is reserved
1 is SHA-1

Adding new reservations requires IETF consensus.

References


Appendix A. Acknowledgements

The authors gratefully acknowledges, in no particular order, the contributions of the following persons:

Bill Sommerfeld

Olafur Gudmundsson

Edward Lewis