

Secure Shell Working Group
Internet-Draft
Expires: March 5, 2004

J. Schlyter
OpenSSH
W. Griffin
SPARTA
September 5, 2003

Using DNS to Securely Publish SSH Key Fingerprints
draft-ietf-secsh-dns-05.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 March 5, 2004.

Copyright Notice

Copyright (C) The Internet Society (2003). 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.

Internet-Draft

DNS and SSH Fingerprints

September 2003

Table of Contents

1.	Introduction	3
2.	SSH Host Key Verification	3
2.1	Method	3
2.2	Implementation Notes	3
2.3	Fingerprint Matching	4
2.4	Authentication	4
3.	The SSHFP Resource Record	4
3.1	The SSHFP RDATA Format	5
3.1.1	Algorithm Number Specification	5
3.1.2	Fingerprint Type Specification	5
3.1.3	Fingerprint	5
3.2	Presentation Format of the SSHFP RR	6
4.	Security Considerations	6
5.	IANA Considerations	7
	Normative References	8
	Informational References	8
	Authors' Addresses	9
A.	Acknowledgements	9
	Intellectual Property and Copyright Statements	10

[1](#). Introduction

The SSH [\[6\]](#) 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 as well as the user authenticating itself to the server.

If a connection is established to a server whose public key is not already known to the client, a fingerprint of the key is presented to the user for verification. If the user decides that 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 verify the fingerprint out-of-band before accepting the key, many users blindly accept the presented key.

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, "SSHFP", 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 match the algorithm and fingerprint of one of the SSHFP resource record(s) returned from DNS, the client MAY accept the identity of the server.

[2.2](#) Implementation Notes

Client implementors SHOULD provide a configurable policy used to select the order of methods used to verify a host key. This document defines one method: Fingerprint storage in DNS. Another method defined in the SSH Architecture [\[6\]](#) uses local files to store keys for comparison. Other methods that could be defined in the future might include storing fingerprints in LDAP or other databases. A

configurable policy will allow administrators to determine which methods they want to use and in what order the methods should be prioritized. This will allow administrators to determine how much trust they want to place in the different methods.

One specific scenario for having a configurable policy is where clients do not use fully qualified host names to connect to servers. In this scenario, the implementation SHOULD verify the host key against a local database before verifying the key via the fingerprint returned from DNS. This would help prevent an attacker from injecting a DNS search path into the local resolver and forcing the client to connect to a different host.

[2.3](#) Fingerprint Matching

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

The public key algorithm and the SSHFP algorithm number MUST match.

A message digest of the public key, using the message digest algorithm specified in the SSHFP fingerprint type, MUST match the SSHFP fingerprint.

[2.4](#) Authentication

A public key verified using this method MUST NOT be trusted if the SSHFP resource record (RR) used for verification was not authenticated by a trusted SIG RR.

Clients that do validate the DNSSEC signatures themselves SHOULD use standard DNSSEC validation procedures.

Clients that do not validate the DNSSEC signatures themselves MUST use a secure transport, e.g. TSIG [9], SIG(0) [10] or IPsec [8], 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.

```

1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
0 1 2 3 4 5 6 7 8 9 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:

Value	Algorithm name
-----	-----
0	reserved
1	RSA
2	DSS

Reserving other types requires IETF consensus [4].

[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:

Value	Fingerprint type
-----	-----
0	reserved
1	SHA-1

Reserving other types requires IETF consensus [4].

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 [7].

The message-digest algorithm is presumed to produce an opaque octet string output which is placed as-is in the RDATA fingerprint field.

[3.2](#) Presentation Format of the SSHFP RR

The RDATA of 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
```

The use of mnemonics instead of numbers is not allowed.

[4.](#) Security Considerations

Currently, the amount of trust a user can realistically place in a server key is proportional to the amount of attention paid to verifying that the public key presented actually corresponds to the private key of the server. If a user accepts a key without verifying the fingerprint with something learned through a secured channel, the connection is vulnerable to a man-in-the-middle attack.

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.

One such aspect is in which order fingerprints are looked up (e.g. first checking local file and then SSHFP). We note that in addition to protecting the first-time transfer of host keys, SSHFP can optionally be used for stronger host key protection.

If SSHFP is checked first, new SSH host keys may be distributed by replacing the corresponding SSHFP in DNS.

If SSH host key verification can be configured to require SSHFP, SSH host key revocation can be implemented by removing the corresponding SSHFP from DNS.

As stated in [Section 2.2](#), we recommend that SSH implementors provide a policy mechanism to control the order of methods used for host key verification. One specific scenario for having a configurable policy is where clients use unqualified host names to connect to servers. In this case, we recommend that SSH implementations check the host key

against a local database before verifying the key via the fingerprint returned from DNS. This would help prevent an attacker from injecting a DNS search path into the local resolver and forcing the client to connect to a different host.

A different approach to solve the DNS search path issue would be for clients to use a trusted DNS search path, i.e., one not acquired

through DHCP or other autoconfiguration mechanisms. Since there is no way with current DNS lookup APIs to tell whether a search path is from a trusted source, the entire client system would need to be configured with this trusted DNS search path.

Another dependency is on the implementation of DNSSEC itself. As stated in [Section 2.4](#), we mandate the use of secure methods for lookup and that SSHFP RRs are authenticated by trusted SIG RRs. This is especially important if SSHFP is to be used as a basis for host key rollover and/or revocation, as described above.

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 [[11](#)] between the SSH server and the nameserver. We note that this is no different from other key enrollment situations, e.g. a client sending a certificate request to a certificate authority for signing.

[5](#). IANA Considerations

IANA needs to allocate a RR type code for SSHFP from the standard RR type space (type 44 requested).

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 [[4](#)].

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 [[4](#)].

Normative References

- [1] Mockapetris, P., "Domain names - concepts and facilities", STD 13, [RFC 1034](#), November 1987.
- [2] Mockapetris, P., "Domain names - implementation and specification", STD 13, [RFC 1035](#), November 1987.
- [3] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [4] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", [BCP 26](#), [RFC 2434](#), October 1998.
- [5] Eastlake, D., "Domain Name System Security Extensions", [RFC 2535](#), March 1999.
- [6] Ylonen, T., Kivinen, T., Saarinen, M., Rinne, T. and S. Lehtinen, "SSH Protocol Architecture", [draft-ietf-secsh-architecture-14](#) (work in progress), July 2003.
- [7] Ylonen, T., Kivinen, T., Saarinen, M., Rinne, T. and S. Lehtinen, "SSH Transport Layer Protocol", [draft-ietf-secsh-transport-16](#) (work in progress), July 2003.

Informational References

- [8] Thayer, R., Doraswamy, N. and R. Glenn, "IP Security Document Roadmap", [RFC 2411](#), November 1998.
- [9] Vixie, P., Gudmundsson, O., Eastlake, D. and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", [RFC 2845](#), May 2000.
- [10] Eastlake, D., "DNS Request and Transaction Signatures (SIG(0)s)", [RFC 2931](#), September 2000.
- [11] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", [RFC 3007](#), November 2000.

Internet-Draft

DNS and SSH Fingerprints

September 2003

Authors' Addresses

Jakob Schlyter
OpenSSH
812 23rd Avenue SE
Calgary, Alberta T2G 1N8
Canada

E-Mail: jakob@openssh.com
URI: <http://www.openssh.com/>

Wesley Griffin
SPARTA
7075 Samuel Morse Drive
Columbia, MD 21046
USA

E-Mail: wgriffin@sparta.com
URI: <http://www.sparta.com/>

[Appendix A](#). Acknowledgements

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

Martin Fredriksson

Olafur Gudmundsson

Edward Lewis

Bill Sommerfeld

Internet-Draft

DNS and SSH Fingerprints

September 2003

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in [BCP-11](#). Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of

developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION

Schlyter & Griffin

Expires March 5, 2004

[Page 10]

Internet-Draft

DNS and SSH Fingerprints

September 2003

HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

