                   Storing SSH Host Keys in DNS

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/ietf/shadow.html.

   This draft expires on October 30, 2001

   Copyright Notice

Abstract

   DNS Security Extensions enables the secure distribution of public
   keys over the Internet. This is a desirable feature for the SSH
   protocol. This document defines the format for storing SSH host keys
   in KEY resource records.

---

1. Introduction

   Key distribution, whether shared secret or public key, is a lingering
   issue in many security-aware protocols, and the SSH protocol [SSH-
   ARCH] is not an exception. DNS Security Extensions [RFC-2535] can
   provide one form of a key infrastructure on the Internet. By allowing
   the client to verify the server key, even without prior knowledge of
   said key, and out of band of the SSH protocol, the security of the
   SSH protocol has increased.

   Familiarity with DNS Security Extensions and the SSH protocol is
   assumed.

2. SSH Key Resource Records

   SSH Host Keys are stored as KEY RRs. The following sections describe
   how the flags, protocol, and algorithm are set.

   2.1 The KEY RR Flag Field

      The "flags" field is set as follows:

      Key "type" (bits 0 and 1): 00 (This key can be used for both
      authentication and confidentiality.)

      Key "name" (bits 6 and 7): 10 (This key is an "entity" or host
      key.)

   2.2 The Protocol Octect

      The protocol value is TBA by IANA.

   2.3 The KEY Algorithm Number Specification

      The algorithm is set as described in Section 3.2 of [RFC-2535].
      SSH does not place any additional restrictions on SSH host keys.
      RSA/MD5 keys use an algorithm value of 1, RSA/SHA1 keys use 5,
      and DSA keys use 3.

   2.4 KEY RDATA format

      Section 4.6 of the SSH transport layer protocol document [SSH-
      TRANS] describes the encoding format for SSH public keys. The DNS

KEY encoding format is described in [RFC-2536] for DSA public
keys and [RFC-2537] for RSA/MD5 public keys.

The KEY RDATA format itself consists of the Flags Field, Protocol
Octect, Algorithm, and public key, which can be converted from

the SSH encoding to the DNS encoding using the descriptions
mentioned.

3. Security Considerations

Placing SSH host keys in DNS allows ssh programs and users to perform
additional checks that may help foil man in the middle attacks. With
DNSSEC deployed, SSH programs can rely on DNS as a secure key
distribution mechanism, as discussed in the SSH architecture document
[SSH-ARCH].

There are 2 possible ways an SSH client can trust keys from DNS. The
first is to perform full DNSSEC verification on the host key and all
the zones containing the domain name up to a trusted zone. This
requires the client to be configured with a trusted zone key and
following the steps for SIG verification outlined in Sections 4 and
6.3 of [RFC-2535].

The other method is for the client to perform a SIG(0) or TSIG
secured query to a nameserver. This method pushes the zone
verification off to the nameserver, but uses SIG(0), defined in
[RFC-2931], or TSIG, defined in [RFC-2845], to verify the query to
the nameserver.

This document only describes the format of the DNS KEY Resource
Record. Outlined above are two simple methods for trusting keys from
DNS, however the more detailed and in-depth key trust discussion will
appear in another document.

4. IANA Considerations

This document specifies how SSH host keys can be placed in DNS, it
also requests an assignment of a DNS KEY protocol value for this use.
Guidance to IANA can be found in Section 3.1.3 of [RFC-2535].

5. Acknowledgements

   Olafur Gudmundsson and Edward Lewis were instrumental in motivating
   and shaping this document.

6. Trademark Issues

   As of this writing, SSH Communications Security Oy claims ssh as its
   trademark. As with all IPR claims the IETF takes no position
   regarding the validity or scope of this trademark claim.

7. References

[RFC-2535]
   Eastlake, D., "Domain Name System Security Extensions", RFC 2535,
   March 1999.

[RFC-2536]
   Eastlake, D., "DSA KEYs and SIGs in the Domain Name System (DNS)",
   RFC 2536, March 1999.

[RFC-2537]
   Eastlake, D., "RSA/MD5 KEYs and SIGs in the Domain Name System
   (DNS)", RFC 2537, March 1999.

[RFC-2845]
   Vixie, P., et al, "Secret Key Transaction Authentication for DNS
   (TSIG)", RFC 2845, May 2000.

[RFC-2931]
   Eastlake, D., "DNS Request and Transaction Signatures (SIG(0)s)",
   RFC 2931, September 2000.

[SSH-ARCH]
   Ylonen, T., et al, "SSH Protocol Architecture", Internet Draft,
   November 2000.

[SSH-TRANS]
   Ylonen, T., et al, "SSH Transport Layer Protocol", Internet Draft,
   November 2000.

Author's Address

       Wesley Griffin
          NAI Labs
          Network Associates, Inc.
          3060 Washington Rd. (Rt. 97)
          Glenwood, MD 21738
          USA
          +1 443 259 2388
          wgriffin@tislabs.com

Full Copyright Statement

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 defines 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 assigns.