Use of the SHA-256 Algorithm with RSA,
Digital Signature Algorithm (DSA),
and Elliptic Curve DSA (ECDSA) in SSHFP Resource Records

Abstract

   This document updates the IANA registries in RFC 4255, which defines
   SSHFP, a DNS Resource Record (RR) that contains a standard Secure
   Shell (SSH) key fingerprint used to verify SSH host keys using DNS
   Security Extensions (DNSSEC). This document defines additional
   options supporting SSH public keys applying the Elliptic Curve
   Digital Signature Algorithm (ECDSA) and the implementation of
   fingerprints computed using the SHA-256 message digest algorithm in
   SSHFP Resource Records.

Status of This Memo

   This is an Internet Standards Track document.

   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
   fInternet Engineering Steering Group (IESG). Further information on
   Internet Standards is available in 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/rfc6594.

Table of Contents

1. Introduction

   The Domain Name System (DNS) is the global, hierarchical distributed
   database for Internet naming. The Secure Shell (SSH) is a protocol
   for secure remote login and other secure network services over an
   insecure network. RFC 4253 [RFC4253] defines Public Key Algorithms
   for the Secure Shell server public keys.

   The DNS has been extended to store fingerprints in a DNS Resource
   Record named SSHFP [RFC4255], which provides out-of-band verification
   by looking up a fingerprint of the server public key in the DNS
   [RFC1034][RFC1035] and using Domain Name System Security Extensions
   (DNSSEC) [RFC4033][RFC4034][RFC4035] to verify the lookup.

   RFC 4255 [RFC4255] describes how to store the cryptographic
   fingerprint of SSH public keys in SSHFP Resource Records. SSHFP
   Resource Records contain the fingerprint and two index numbers
   identifying the cryptographic algorithms used:

   1. to link the fingerprinted public key with the corresponding
       private key, and

   2. to derive the message digest stored as the fingerprint in the
       record.

   RFC 4255 [RFC4255] then specifies lists of cryptographic algorithms
   and the corresponding index numbers used to identify them in SSHFP
   Resource Records.

   This document updates the IANA registry "SSHFP RR Types for public
   key algorithms" and "SSHFP RR types for fingerprint types"
   [SSHFPVALS] by adding a new option in each list:

   o the Elliptic Curve Digital Signature Algorithm (ECDSA) [RFC6090],
      which has been added to the Secure Shell Public Key list by RFC
      5656 [RFC5656] in the public key algorithms list, and

   o the SHA-256 algorithm [FIPS.180-3.2008] in the SSHFP fingerprint
      type list.

   Familiarity with DNSSEC, SSH Protocol [RFC4251][RFC4253][RFC4250],
   SSHFP [RFC4255], and the SHA-2 [FIPS.180-3.2008] family of algorithms
   is assumed in this document.

2. Requirements Language

   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 [RFC2119].

3. SSHFP Resource Records

   The format of the SSHFP RR can be found in RFC 4255 [RFC4255].

3.1. SSHFP Fingerprint Type Specification

   The fingerprint type octet identifies the message digest algorithm
   used to calculate the fingerprint of the public key.

3.1.1. SHA-256 SSHFP Fingerprint Type Specification

   SHA-256 fingerprints of the public keys are stored in SSHFP Resource
   Records with the fingerprint type 2.

3.2. SSHFP Algorithm Number Specification

   The SSHFP Resource Record algorithm number octet describes the
   algorithm of the public key.

3.2.1. ECDSA SSHFP Algorithm Number Specification

   ECDSA public keys are stored in SSHFP Resource Records with the
   algorithm number 3.

4. Implementation Considerations

4.1. Support for SHA-256 Fingerprints

   SSHFP-aware Secure Shell implementations SHOULD support the SHA-256
   fingerprints for verification of the public key. Secure Shell
   implementations that support SHA-256 fingerprints MUST prefer a SHA-
   256 fingerprint over SHA-1 if both are available for a server. If
   the SHA-256 fingerprint is tested and does not match the SSH public
   key received from the SSH server, then the key MUST be rejected
   rather than testing the alternative SHA-1 fingerprint.

4.2. Support for ECDSA

   SSHFP-aware Secure Shell implementations that also implement the
   ECDSA for the public key SHOULD support SSHFP fingerprints for ECDSA
   public keys.

5. Examples

   The following examples provide reference for both the newly defined
   value for ECDSA and the use of the SHA-256 fingerprint combined with
   both the new and the existing algorithm numbers.

5.1. RSA Public Key

   A public key with the following value in OpenSSH format [RFC4716]
   would appear as follows:

       ---- BEGIN SSH2 PUBLIC KEY ----
       AAAAB3NzaC1yc2EAAAADAQABAAABAQDCUR4JOhxTinzq7QO3bQXW4jmPCCulFsnh
       8Yi7MKwpMnd96+T7uV7nEwy+6+GWYu98IxFJByIjFXX/a6BXDp3878wezH1DZ2tN
       D/tu/eudz6ErpTFYmnVLyEDARYSzVBNQuIK1UDqvvB6KffJcyt78FpwW27euGkqE
       kam7GaurPRAgwXehDB/gMwRtXVRZ+13zYWkAmAY+5OAWVmdXuQVm5kjlvcNzto2H
       3m3nqJtD4J9L1lKPuSVVqwJr4/6hibXJkQEvWpUvdOAUw3frKpNwa932fXFk3ke4
       rsDjQ/W8GyleMtK3Tx8tE4z1wuowXtYe6Ba8q3LAPs/m2S4pUscx
       ---- END SSH2 PUBLIC KEY ----

5.1.1. RSA Public Key with SHA1 Fingerprint

   The SSHFP Resource Record for this key would be:

       server.example.net IN SSHFP 1 1 (dd465c09cfa51fb45020cc83316fff
                                         21b9ec74ac)

5.1.2. RSA Public Key with SHA-256 Fingerprint

   The SSHFP Resource Record for this key would be:

       server.example.net IN SSHFP 1 2 (b049f950d1397b8fee6a61e4d14a9a
                                         cdc4721e084eff5460bbed80cfaa2c
                                         e2cb)

5.2. DSA Public Key

   A public key with the following value in OpenSSH format would appear
   as follows:

       ---- BEGIN SSH2 PUBLIC KEY ----
       AAAAB3NzaC1kc3MAAACBAPVFrc0U36gWaywbfJzjcv8ef13qAX4EJl8Na6xqvXh1
       t+aCJEdS7soRjtvK4KsNhk78DjdtnfhEhyFKHHNz3i6/c/s9lP0UjV7mRAo6nA7A
       3Gs6iQElb6O9Fqm6iVSC6bYWilTSB0tYencEEJUoaAua8YQF/uxRzPrReXxGqHnj
       AAAAFQDC9M/pli8VIVmEGOO0wC1TeUTN4wAAAIEAgA2Fbkbbeo0+u/qw8mQFOFWZ
       pTaqNo7d7jov3majbh5LqEVD7yT3MS1GSGhjgvvhus/ehMTqzYbjTc0szUM9JnwT
       7xq15P2ZYDK98IVxrw31jMtsUUEmBqB4DUjTurtcaWmJ9LNaP1/k4bMo0/hotnOc
       OVnIPsTLBFWVvdNRxUAAACAOZcDcK01NTM1qIIYbBqCffrwjQ+9PmsuSKI6nUzf
       S4NysXHkdbW5u5VxeXLcwWj5PGbRfoS2P3vwYAmakqgq502wigam18u9nAczUYl+
       2kOeOiIRrtSmLfpV7thLOAb8k1ESjIlkbn35jKmTcoMFRXbFmkKRTK8OEnWQ8AVg
       6w8=
       ---- END SSH2 PUBLIC KEY ----

5.2.1. DSA Public Key with SHA1 Fingerprint

   The SSHFP Resource Record for this key would be:

       server.example.net IN SSHFP 2 1 (3b6ba6110f5ffcd29469fc1ec2ee25
                                         d61718badd)

5.2.2. DSA Public Key with SHA-256 Fingerprint

   The SSHFP Resource Record for this key would be:

       server.example.net IN SSHFP 2 2 (f9b8a6a460639306f1b38910456a6a
                                         e1018a253c47ecec12db77d7a0878b
                                         4d83)

5.3. ECDSA Public Key

   A public key with the following value in OpenSSH format would appear
   as follows:

       ---- BEGIN SSH2 PUBLIC KEY ----
       AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAD+9COUiX7W
       YgcvIOdI8+djdoFDVUTxNrcog8sSYdbIzeG+bYdsssvcyy/nRfVhXC5QBCk8IThq
       s7D4/lFxX5g=
       ---- END SSH2 PUBLIC KEY ----

5.3.1. ECDSA Public Key with SHA1 Fingerprint

   The SSHFP Resource Record for this key would be:

        server.example.net IN SSHFP 3 1 (c64607a28c5300fec1180b6e417b92
                                          2943cffcdd)

5.3.2. ECDSA Public Key with SHA-256 Fingerprint

   The SSHFP Resource Record for this key would be:

        server.example.net IN SSHFP 3 2 (821eb6c1c98d9cc827ab7f456304c0
                                          f14785b7008d9e8646a8519de80849
                                          afc7)

6. IANA Considerations

   This document updates the IANA registry "SSHFP RR Types for public
   key algorithms" and "SSHFP RR types for fingerprint types"
   [SSHFPVALS].

6.1. SSHFP RR Types for Public Key Algorithms

   The following entries have been added to the "SSHFP RR Types for
   public key algorithms" registry:

                    +-------+-------------+------------+
                    | Value | Description | Reference |
                    +-------+-------------+------------+
                    | 3 | ECDSA | [This doc] |
                    +-------+-------------+------------+

6.2. SSHFP RR Types for Fingerprint Types

   The following entries have been added to the "SSHFP RR types for
   fingerprint types" registry:

                    +-------+-------------+------------+
                    | Value | Description | Reference |
                    +-------+-------------+------------+
                    | 2 | SHA-256 | [This doc] |
                    +-------+-------------+------------+

7. Security Considerations

   Please see the security considerations in [RFC4255] for SSHFP
   Resource Records and [RFC5656] for the ECDSA.

   Users of SSHFP are encouraged to deploy SHA-256 as soon as
   implementations allow for it. The SHA-2 family of algorithms is
   widely believed to be more resilient to attack than SHA-1, and
   confidence in SHA-1's strength is being eroded by recently announced
   attacks [IACR2007/474]. Regardless of whether or not the attacks on
   SHA-1 will affect SSHFP, it is believed (at the time of this writing)
   that SHA-256 is the better choice for use in SSHFP records.

   SHA-256 is considered sufficiently strong for the immediate future,
   but predictions about future development in cryptography and
   cryptanalysis are beyond the scope of this document.

8. References

8.1. Normative References

   [FIPS.180-3.2008]
               National Institute of Standards and Technology, "Secure
               Hash Standard (SHS)", FIPS PUB 180-3, October 2008,
               <http://csrc.nist.gov/publications/fips/fips180-3/
               fips180-3_final.pdf>.

   [RFC1034]   Mockapetris, P., "Domain names - concepts and
               facilities", STD 13, RFC 1034, November 1987.

   [RFC1035]   Mockapetris, P., "Domain names - implementation and
               specification", STD 13, RFC 1035, November 1987.

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
               Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC4250]   Lehtinen, S. and C. Lonvick, "The Secure Shell (SSH)
               Protocol Assigned Numbers", RFC 4250, January 2006.

   [RFC4251]   Ylonen, T. and C. Lonvick, "The Secure Shell (SSH)
               Protocol Architecture", RFC 4251, January 2006.

   [RFC4253]   Ylonen, T. and C. Lonvick, "The Secure Shell (SSH)
               Transport Layer Protocol", RFC 4253, January 2006.

   [RFC4255]   Schlyter, J. and W. Griffin, "Using DNS to Securely
               Publish Secure Shell (SSH) Key Fingerprints", RFC 4255,
               January 2006.

   [RFC5656]   Stebila, D. and J. Green, "Elliptic Curve Algorithm
                Integration in the Secure Shell Transport Layer",
                RFC 5656, December 2009.

8.2. Informative References

   [IACR2007/474]
                Cochran, M., "Notes on the Wang et al. 2^63 SHA-1
                Differential Path", IACR 2007/474,
                <http://eprint.iacr.org/2007/474.pdf>.

   [RFC4033]   Arends, R., Austein, R., Larson, M., Massey, D., and S.
                Rose, "DNS Security Introduction and Requirements",
                RFC 4033, March 2005.

   [RFC4034]   Arends, R., Austein, R., Larson, M., Massey, D., and S.
                Rose, "Resource Records for the DNS Security Extensions",
                RFC 4034, March 2005.

   [RFC4035]   Arends, R., Austein, R., Larson, M., Massey, D., and S.
                Rose, "Protocol Modifications for the DNS Security
                Extensions", RFC 4035, March 2005.

   [RFC4716]   Galbraith, J. and R. Thayer, "The Secure Shell (SSH)
                Public Key File Format", RFC 4716, November 2006.

   [RFC6090]   McGrew, D., Igoe, K., and M. Salter, "Fundamental
                Elliptic Curve Cryptography Algorithms", RFC 6090,
                February 2011.

   [SSHFPVALS] IANA, "DNS SSHFP Resource Records Parameters",
                <http://www.iana.org/assignments/
                dns-sshfp-rr-parameters>.

Author's Address

   Ondrej Sury
   CZ.NIC
   Americka 23
   120 00 Praha 2
   Czech Republic

   Phone: +420 222 745 110
   EMail: ondrej.sury@nic.cz