Secure Shell Working Group J. Galbraith
Internet-Draft VanDyke Software
Expires: January 16, 2006 O. Saarenmaa
F-Secure Corporation
July 15, 2005

X.509 authentication in SSH2
draft-ietf-secsh-x509-02.txt

Status of this Memo

Copyright Notice

Abstract

The X.509 extension specifies how X.509 keys and signatures are used within the SSH2 protocol.

Table of Contents

1. Introduction 3
2. Conventions Used in This Document 3
3. Certificate validation 3
3.1 Host Authentication 3
3.2 User Authentication 3
4. Use in SSH2 Protocol 4
4.1 x509v3-sign-rsa-sha1 4
4.2 x509v3-sign-dss-sha1 4
4.3 x509v3-sign 5
5. Implementation Considerations 5
6. IANA Considerations 5
7. Security Considerations 6
8. References 6
8.1 Normative References 6
8.2 Informative References 7
Authors' Addresses 7
Intellectual Property and Copyright Statements 8

1. Introduction

The SSH protocol can use public keys for both host and user authentication. However, particularly for host authentication, plain public keys lack a good method of verifying that the the key provided really does belong to the host asserting ownership. X.509v3 certificates can address this problem in environments where a PKI infrastructure is available.

2. Conventions Used in 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 [RFC2119].

3. Certificate validation

Implementations are expected to follow the basic certificate and certificate path validation guidelines described in [RFC3280]. No SSH specific X.509 certificate extensions are defined in this document.

3.1 Host Authentication

The client MAY verify that the serverAuth option, as specified in [RFC3280], is present in the host certificate's extendedKeyUsage field.

Implementations SHOULD validate the host certificates by matching the host's fully qualified domain name [RFC1034] against the host certificate's subjectAltName extension's dNSName entries. If the certificate does not contain dNSName subjectAltName extensions, the (most specific) Common Name field in the certificate Subject is to be used. This is similar to host validation in [RFC2818].

3.2 User Authentication

The server MAY verify that the clientAuth option, as specified in [RFC3280], is present in the user certificate's extendedKeyUsage field.

No constraints are placed on the presence of user account information in the certificates used for user authentication. Their validation and mapping is left as an implementation and configuration detail for the implementors and deployers.

4. Use in SSH2 Protocol

Key type names are of the form "x509v3-sign*". Keys are encoded as follows:

```
    string    key-type-name
    string    DER encoded x.509v3 certificate data
```

4.1 x509v3-sign-rsa-sha1

Certificates that use the RSA public key algorithm SHOULD use the "x509v3-sign-rsa-sha1" key-type-name.

Signing and verifying using this key format, uses the certificate's private key, in exactly the same manner specified for "ssh-rsa" public keys in [I-D.ietf-secsh-transport]. That is to say, signing and verifying using this key format is performed according to the RSASSA-PKCS1-v1_5 scheme in [RFC3447] using the SHA-1 hash.

The signature format for x509v3-sign-rsa-sha1 certificates is the "ssh-rsa" signing format specified in [I-D.ietf-secsh-transport]. This format is as follows:

```
    string    "ssh-rsa"
    string    rsa_signature_blob
```

The value for 'rsa_signature_blob' is encoded as a string containing s (which is an integer, without lengths or padding, unsigned and in network byte order).

4.2 x509v3-sign-dss-sha1

Certificates that use the DSA public key algorithm SHOULD use the "x509v3-sign-dss-sha1" key-type-name.

Signing and verifying using this key format, uses the certificate's private key, in exactly the same manner specified for "ssh-dss" public keys in [I-D.ietf-secsh-transport]. That is to say, signing and verifying using this key format is done according to the Digital Signature Standard [FIPS-186-2] using the SHA-1 hash [FIPS-180-2].

The signature format for x509v3-sign-dss-sha1 certificates is the "ssh-dss" signing format specified in [I-D.ietf-secsh-transport]. This format is as follows:

```
    string    "ssh-dss"
    string    dss_signature_blob
```

The value for 'dss_signature_blob' is encoded as a string containing r followed by s (which are 160-bit integers, without lengths or padding, unsigned and in network byte order).

4.3 x509v3-sign

Certificates that use another algorithm other than the two specified above, MUST use the "x509v3-sign" key-type-name.

Signing and verifying is done according to the specification associated with the public-key algorithm oid encoded in the certificate.

The signature, and description of the signature algorithms is encoded as specified in [PKCS.7.1993]. The signature MUST be detached (the signed data MUST NOT be included in the pkcs7 data).

The pkcs7 data is encoded in the SSH protocol as follows:

```
    string    "pkcs7"
    string    DER encoded PKCS7 data
```

5. Implementation Considerations

Implementations should be careful when using x.509v3 certificates as hostkeys. If the peer does not implement the required algorithms to validate both the x.509v3 certificate and all certificates in the chain, it MUST disconnect. There is no way to renegotiate the key during key exchange.

This is especially true when using the "x509v3-sign" key type, since in this case the peer has no knowledge whatsoever of required algorithms.

6. IANA Considerations

This document reserves all key types beginning with "x509v3-sign" in the SSH publickey type registry.

This document specifically adds "x509v3-sign-rsa-sha1", "x509v3-sign-dss-sha1", and "x509v3-sign" to the SSH publickey type registry.

This document adds "x509v3-sign-rsa" and "x509v3-sign-dss" to the SSH publickey type registry as "poisoned" by historical use.

7. Security Considerations

PKI is an extremely complex topic, and care must be taken by both implementors and deployers to understand the complex interactions involved.

Implementations should carefully validate the certificate, including, but not limited to, certificate expiration, certificate signature, certificate revocation lists, etc.

For more information, implementors should refer to [ITU.X509.2000] and [RFC3280].

8. References

8.1 Normative References

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

[RFC3280] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[I-D.ietf-secsh-transport] Lonvick, C., "SSH Transport Layer Protocol", draft-ietf-secsh-transport-24 (work in progress), March 2005.

[PKCS.7.1993] RSA Laboratories, "Cryptographic Message Syntax Standard. Version 1.5", PKCS 7, November 1993.

[FIPS-180-2] National Institute of Standards and Technology, "Secure Hash Standard (SHS)", Federal Information Processing Standards Publication 180-2, August 2002.

[FIPS-186-2] National Institute of Standards and Technology, "Digital Signature Standard (DSS)", Federal Information Processing Standards Publication 186-2, January 2000.

[ITU.X509.2000]
International Telecommunications Union, "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks", ITU-T Recommendation X.509, ISO Standard 9594-8, March 2000.

8.2 Informative References

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

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

Authors' Addresses

Joseph Galbraith
VanDyke Software
4848 Tramway Ridge Blvd
Suite 101
Albuquerque, NM 87111
US

Phone: +1 505 332 5700
Email: galb-list@vandyke.com

Oskari Saarenmaa
F-Secure Corporation
Tammasaarenkatu 7
Helsinki 00180
FI

Email: oskari.saarenmaa@f-secure.com

Trademark notice

"ssh" is a registered trademark in the United States and/or other countries.

Intellectual Property Statement

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Acknowledgment

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