

Network Working Group
Internet-Draft
Expires: July 7, 2005

B. Harris
January 6, 2005

RSA key exchange for the SSH Transport Layer Protocol
draft-harris-ssh-rsa-kex-00.txt

Status of this Memo

This document is an Internet-Draft and is subject to all provisions of [section 3 of RFC 3667](#). By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she become aware will be disclosed, in accordance with [RFC 3668](#).

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/lid-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 July 7, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This memo describes an RSA-based key-exchange method for the SSH protocol. It uses much less client CPU time than the Diffie-Hellman algorithm specified as part of the core protocol, and hence is particularly suitable for slow client systems.

1. Introduction

Secure Shell (SSH) [[SSH-ARCH](#)] is a secure remote-login protocol. The

Internet-Draft

SSH RSA key exchange

January 2005

core protocol uses Diffie-Hellman key exchange. On slow CPUs, this key exchange can take tens of seconds to complete, which can be irritating for the user. A previous version of the SSH protocol, described in [[SSH1](#)] uses an RSA-based key exchange method, which consumes an order of magnitude less CPU time on the client, and hence is particularly suitable for slow client systems such as mobile devices. This memo describes a key-exchange mechanism for the version of SSH described in [[SSH-ARCH](#)] which is similar to that used by the older version, and about as fast, while retaining the security advantages of the newer protocol.

[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.](#) Overview

The RSA key-exchange method consists of three messages. First, the server sends to the client an RSA public key, K_T , to which the server holds the private key. This may be a transient key generated solely for this SSH connection, or it may be re-used for several connections. The client generates a string of random bytes, K , encrypts it using K_T , and sends the result back to the server, which decrypts it. The client and server each hash K , K_T , and the various key-exchange parameters to generate the exchange hash, H , which is used to generate the encryption keys for the session, and the server signs H with its host key and sends the signature to the client. The client then verifies the host key as described in [[SSH-TRANS](#)].

This method provides explicit server identification as defined in section 7 of [[SSH-TRANS](#)]. It requires a signature-capable host key.

[4.](#) Details

The RSA key exchange method has the following parameters, which are defined by the method name:

HASH	hash algorithm for calculating exchange hash etc.
HLEN	output length of HASH in bits
MINKLEN	minimum transient RSA modulus length in bits

The method uses the following messages.

First, the server sends:

byte SSH_MSG_KEXRSA_PUBKEY

Harris

Expires July 7, 2005

[Page 2]

Internet-Draft

SSH RSA key exchange

January 2005

string K_T, transient RSA public key

The key K_T is encoded according to the "ssh-rsa" scheme described in section 6.6 of [[SSH-TRANS](#)]. Note that unlike an "ssh-rsa" host key, K_T is only used for encryption, and not for signature. The modulus of K_T MUST be at least MINKLEN bits long.

The client generates a random integer, K, in the range $0 \leq K < 2^{(KLEN-2HLEN-49)}$, where KLEN is the length of the modulus of K_T, in bits. The client then uses K_T to encrypt:

mpint K, the shared secret

The encryption is performed according to the RSAES-OAEP scheme of [[RFC3447](#)], with a mask generation function of MGF1-with-HASH, a hash of HASH, and an empty label. See [Appendix A](#) for a proof that the encoding of K is always short enough to be thus encrypted. Having performed the encryption, the client sends:

byte SSH_MSG_KEXRSA_SECRET
string RSAES-OAEP-ENCRYPT(K_T, K)

The server decrypts K. If a decryption error occurs, the server SHOULD send SSH_MESSAGE_DISCONNECT with a reason code of SSH_DISCONNECT_KEY_EXCHANGE_FAILED and MUST disconnect. Otherwise, the server responds with:

byte SSH_MSG_KEXRSA_DONE
string server public host key and certificates (K_S)
string signature of H

The hash H is computed as the HASH hash of the concatenation of the following:

string V_C, the client's version string (CR and NL excluded)
string V_S, the server's version string (CR and NL excluded)
string I_C, the payload of the client's SSH_MSG_KEXINIT
string I_S, the payload of the server's SSH_MSG_KEXINIT
string K_S, the host key

string K_T, the transient RSA key
mpint K, the shared secret

This value is called the exchange hash, and it is used to authenticate the key exchange. The exchange hash SHOULD be kept secret.

The signature algorithm MUST be applied over H, not the original data. Most signature algorithms include hashing and additional

Harris

Expires July 7, 2005

[Page 3]

Internet-Draft

SSH RSA key exchange

January 2005

padding - for example, "ssh-dss" specifies SHA-1 hashing. In that case, the data is first hashed with HASH to compute H, and H is then hashed with SHA-1 as part of the signing operation.

[5.](#) rsa-sha1-draft-00@putty.projects.tartarus.org

The "rsa-sha1-draft-00@putty.projects.tartarus.org" method specifies RSA key exchange as described above with the following parameters:

HASH SHA-1, as defined in [[FIPS-180-2](#)]
HLEN 160
MINKLEN 1024

[6.](#) Message numbers

The following message numbers are defined:

SSH_MSG_KEXRSA_PUBKEY 30
SSH_MSG_KEXRSA_SECRET 31
SSH_MSG_KEXRSA_DONE 32

Note that Numbers 30-49 are used for kex packets. Different kex methods may reuse message numbers in this range.

[7.](#) Security Considerations

The security considerations in [[SSH-ARCH](#)] apply.

If the RSA private key generated by the server is revealed then the session key is revealed. The server should thus arrange to erase this from memory as soon as it is no longer required. If the same RSA key is used for multiple SSH connections, an attacker who can find the private key (either by factorising the public key or by other means) will gain access to all of the sessions which used that

key.

[RFC3447] recommends that RSA keys used with RSAES-OAEP not be used with other schemes, or with RSAES-OAEP using a different hash function. In particular, this means that K_T should not be used as a host key, or as a server key in earlier versions of the SSH protocol.

The random data, K, generated by the client, is the only secret shared by client and server, so its entropy directly determines the security of the session against eavesdropping.

The size of transient key used should be sufficient to protect the encryption and integrity keys generated by the key exchange method.

Harris

Expires July 7, 2005

[Page 4]

Internet-Draft

SSH RSA key exchange

January 2005

For recommendations on this, see [[RFC3766](#)].

Unlike the Diffie-Hellman key exchange method defined by [[SSH-TRANS](#)], this method allows the client to fully determine the shared secret, K. This is believed not to be significant, since K is only ever used when hashed with data provided in part by the server (usually in the form of the exchange hash, H). If an extension to SSH were to use K directly and to assume that it had been generated by Diffie-Hellman key exchange, this could produce a security weakness. Protocol extensions using K directly should be viewed with extreme suspicion.

[8.](#) IANA Considerations

This document has no actions for IANA.

[9.](#) Acknowledgments

The author acknowledges the assistance of Simon Tatham with the design of this key exchange method.

The text of this document is derived in part from [[SSH-TRANS](#)].

[10.](#) References

[10.1](#) Normative References

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

[RFC3447] Jonsson, J. and B. Kaliski, "Public-Key Cryptography

Standards (PKCS) #1: RSA Cryptography Specifications
Version 2.1", [RFC 3447](#), February 2003.

[SSH-ARCH]

Lonvick, C., Ed., "SSH Protocol Architecture", I-D
[draft-ietf-secsh-architecture-20.txt](#), December 2004.

[SSH-TRANS]

Lonvick, C., Ed., "SSH Transport Layer Protocol", I-D
[draft-ietf-secsh-transport-22.txt](#), December 2004.

[FIPS-180-2]

National Institute of Standards and Technology (NIST),
"Secure Hash Standard (SHS)", FIPS PUB 180-2, August 2002.

[10.2](#) Informative References

[SSH1] Ylonen, T., "SSH -- Secure Login Connections over the

Harris

Expires July 7, 2005

[Page 5]

Internet-Draft

SSH RSA key exchange

January 2005

Internet", 6th USENIX Security Symposium, p. 37-42, July
1996.

[RFC3766] Orman, H. and P. Hoffman, "Determining Strengths For
Public Keys Used For Exchanging Symmetric Keys", [BCP 86](#),
[RFC 3766](#), April 2004.

Author's Address

Ben Harris
37 Milton Road
CAMBRIDGE CB4 1XA
GB

EMail: bjh21@bjh21.me.uk

[Appendix A](#). On the size of K

The requirements on the size of K are intended to ensure that it's
always possible to encrypt in under K_T. The mpint encoding of K
requires a leading zero bit, padding to a whole number of bytes, and
a four-byte length field, giving a maximum length in bytes,
 $B = (KLEN - 2HLEN - 49 + 1 + 7) / 8 + 4 = (KLEN - 2HLEN - 9) / 8$ (where "/"
represents integer division rounding down).

The maximum length of message that can be encrypted using RSAEP-OAEP is defined by [RFC3447] in terms of the key length in bytes, which is $(KLEN+7)/8$. The maximum length is thus $L = (KLEN+7-2HLEN-16)/8 = (KLEN-2HLEN-9)/8$. Thus, the encoded version of K is always small enough to be encrypted under K_T.

Harris

Expires July 7, 2005

[Page 6]

Internet-Draft

SSH RSA key exchange

January 2005

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

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

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

Acknowledgment

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