Network Working Group
Internet-Draft
Intended status: Informational
Expires: May 9, 2016

A. Adamantiadis
libssh
S. Josefsson
SJD AB

November 6, 2015

Secure Shell (SSH) Key Exchange Method using Curve25519 and Curve448 draft-josefsson-ssh-curves-00

Abstract

How to implement the Curve25519 and Curve448 key exchange methods in the Secure Shell (SSH) protocol is described.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on May 9, 2016.

Table of Contents

1. Introduction

In [Curve25519], a new elliptic curve function for use in cryptographic applications was introduced. In [Ed448-Goldilocks] the Ed448-Goldilocks curve (also known as Curve448) is described. In [I-D.irtf-cfrg-curves], the Diffie-Hellman functions using Curve25519 and Curve448 are specified.

Secure Shell (SSH) [RFC4251] is a secure remote login protocol. The key exchange key exchange protocol described in [RFC4253] supports an extensible set of methods. In [RFC5656] it is described how elliptic curves are integrated in SSH, and this document re-use those protocol messages.

This document describe how key exchange is achieved based on Curve25519 and Curve448 in SSH. For Curve25519 what we described is identical to an already implemented (in libssh and OpenSSH) and widely deployed proposal registered in the private namespace ("curve25519-sha256@libssh.org"). The Curve448 key exchange method is novel but similar in spirit.

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].

2. Key Exchange Methods

The key exchange procedure is identical to the one described RFC 5656 chapter 4 of [RFC5656]. Public ephemeral keys are transmitted over SSH encapsulated into standard SSH strings.

The method names registered by this document are "curve25519-sha256" and "curve448-sha256".

The whole method is based on the Curve25519 and Curve448 scalar multiplication, as described in [I-D.irtf-cfrg-curves]. Private and public keys are generated as described therein, and no special validation is required beyond what is discussed there. Public keys are defined as strings of 32 bytes for Curve25519 and 56 bytes for Curve448. The derived shared secret is is 32 bytes when Curve25519 is used and 56 bytes when Curve448 is used.

The shared secret, k, is defined in SSH specifications to be a big integer. This number is calculated as follows. X is the 32 bytes point obtained by the scalar multiplication of the other side's public key and the local private key scalar. The whole 32 bytes of the number X are then converted into a big integer k. This conversion follows the network byte order. This step differs from [RFC5656].

3. Acknowledgements

The "curve25519-sha256" key exchange method is identical to the "curve25519-sha256@libssh.org" key exchange method created by Aris Adamantiadis and implemented in libssh and OpenSSH.

4. Security Considerations

The security considerations of [RFC4251], [RFC5656], and [I-D.irtf-cfrg-curves] are inherited.

5. IANA Considerations

IANA is requested to add "curve25519-sha256" and "curve448-sha256" to the "Key Exchange Method Names" registry for SSH that was created in RFC 4250 section 4.10 [RFC4250].

6. References

6.1. Normative References

[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, Ed., "The Secure Shell (SSH) Protocol Assigned Numbers", RFC 4250, DOI 10.17487/RFC4250, January 2006, <http://www.rfc-editor.org/info/rfc4250>.

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

[RFC4253] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Transport Layer Protocol", RFC 4253, DOI 10.17487/RFC4253, January 2006, <http://www.rfc-editor.org/info/rfc4253>.

[RFC5656] Stebila, D. and J. Green, "Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer", RFC 5656, DOI 10.17487/RFC5656, December 2009, <http://www.rfc-editor.org/info/rfc5656>.

[I-D.irtf-cfrg-curves] Langley, A. and M. Hamburg, "Elliptic Curves for Security", draft-irtf-cfrg-curves-10 (work in progress), October 2015.

6.2. Informative References

[Curve25519] Bernstein, J., "Curve25519: New Diffie-Hellman Speed Records", LNCS 3958, pp. 207-228, February 2006, <http://dx.doi.org/10.1007/11745853_14>.

[Ed448-Goldilocks] Hamburg, , "Ed448-Goldilocks, a new elliptic curve", June 2015, <https://eprint.iacr.org/2015/625>.

Appendix A. Copying conditions

Authors' Addresses

Aris Adamantiadis
libssh

Email: aris@badcode.be

Simon Josefsson
SJD AB

Email: simon@josefsson.org