Internet Draft
<draft-irtf-cfrg-spake2-00.txt>
Category: Informational
Expires 26 July 2015

W. Ladd
UC Berkeley

22 January 2015

SPAKE2, a PAKE
<draft-irtf-cfrg-spake2-00.txt>

Status of this Memo

Distribution of this memo is unlimited.

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), 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/shadow.html.

This Internet-Draft will expire on date.

Abstract

This Internet-Draft describes SPAKE2, a secure, efficient password

based key exchange protocol.

Table of Contents

1. Introduction

This document describes a means for two parties that share a password to derive a shared key. This method is compatible with any group, is computationally efficient, has a strong security proof.

2. Definition of SPAKE2

Let G be a group in which the Diffie-Hellman problem is hard of order ph, with p a big prime and h a cofactor. We denote the operations in the group additively. Let H be a hash function from arbitrary strings to bit strings of a fixed length. Common choices for H are SHA256 or SHA512. We assume there is a representation of elements of G as byte strings: common choices would be SEC1 uncompressed for elliptic curve groups or big endian integers of a particular length for prime field DH.

|| denotes concatenation of strings. We also let len(S) denote the length of a string in bytes, represented as an eight-byte big-endian number.

We fix two elements M and N as defined in the table in this document for common groups, as well as a generator G of the group. G is specified in the document defining the group, and so we do not recall it here.

Let A and B be two parties. We will assume that A and B are also representations of the parties such as MAC addresses or other names (hostnames, usernames, etc). We assume they share an integer w. Typically w will be the hash of a user-supplied password, truncated and taken mod p. Protocols using this protocol must define the method used to compute w: it may be necessary to carry out normalization.

A picks x randomly and uniformly from the integers in [0,ph) divisible by h, and calculates X=xG and T=wM+X, then transmits T to B.

B selects y randomly and uniformly from the integers in [0,ph),

divisible by h and calculates Y=yG, S=wN+Y, then transmits S to A.

Both A and B calculate a group element K. A calculates it as x(S-wN), while B calculates it as y(T-wM). A knows S because it has received it, and likewise B knows T.

Both A and B can now calculate a shared key as H(len(A)|| A || len(B) || B || len(S) || S || len(T) || T || len(w) || w || len(K) || K). The encoding of group elements must be decided upon based on convenience. For elliptic curve groups in short Weierstrass form, SEC1 uncompressed format is recommended due to wide support.

Note that the calculation of S=wN+yG may be performed more efficiently then by two separate scalar multiplications via Strauss's algorithm.

3. Table of points for common groups

This table was generated in the following way: A string S was hashed with the SHA-2 function matching the curve size repeatedly until a valid x coordinate for the curve was generated. The points are presented in hexdecimal SEC1 format. The string was "CURVE point generation seed (X)" with CURVE the name of the curve and X M or N accordingly.

For P256:

M =
02004F3886286C3DBEDAABC44EAE84C7D88205289AB3A6F7DFC9B055B41CDC5D71

N =
02004E10BC191275D4AEB183DB6E3385CDE56AE90BEA034FB20FE4D3E0E86B57F9

For P384:

M =
0300D96F8C84B8EB7BE566CA5B8788F6D7B71619F78DCA54C061E75FD0D5353570A
CA36EB3EB16C93C855442B66970A197

N =
020024C63E7770841FA3F1ABCF7469F6822C84F0EFCA2DAC8D7FD4B097C8291DD70
AA1CA824B2DFC4104F0D4FA0301EDFF

For P521:

M =
020000007396235440408 8E8407DE57063FE70C5F9B014531CCD09A007509193A60

F345031F8B1239F754B20CC5946C0257339314D112AFFE96EA880C3EBC074E5FF96

N =
02000000594BAFF0BEF7134EBBCC5D86670777EBC4A473D6797167BBEEFECEC11F8
863AF4CEC3A651E99F0357C59450D8E06124B099D1FBBF498546400AA80F08CFFB8

4. Security Considerations

A security proof for prime order groups is found in [REF]. Note that the choice of M and N is critical: anyone who is aware of an x such that xN=M, or xG=N or M can break the scheme above. The points in the table of points were generated via the use of a hash function to mitigate this risk.

There is no key-confirmation as this is a one round protocol. It is expected that a protocol using this key exchange mechanism provides key confirmation separately if desired.

Elements should be checked for group membership: failure to properly validate group elements can lead to attacks. In particular it is essential to verify that recieved points are valid compressions of points on an elliptic curve when using elliptic curves. This can be done by a quadratic character computation. It is not necessary to validate prime order.

The choices of random numbers should be uniformly at random. Note that to pick a random multiple of h in [0, ph) one can pick a random integer in [0,p) and multiply by h.

This PAKE does not support augmentation. As a result, the server has to store a password equivalent. This is considered a significant drawback.

5. IANA Considerations

No IANA action is required.

6. Acknowledgments

Special thanks to Nathaniel McCallum for generation of test vectors. Thanks to Mike Hamburg for advice on how to deal with cofactors. Thanks to Fedor Brunner and the members of the CFRG for comments and advice.

7. References

[REF] Abdalla, M. and Pointcheval, D. Simple Password-Based Encrypted

Key Exchange Protocols. Appears in A. Menezes, editor. Topics in Cryptography-CT-RSA 2005, Volume 3376 of Lecture Notes in Computer Science, pages 191-208, San Francisco, CA, US Feb. 14-18, 2005. Springer-Verlag, Berlin, Germany.

Author Addresses

Watson Ladd
watsonbladd@gmail.com
Berkeley, CA