Internet Draft
<draft-ladd-spake2-00.txt>
Category: Informational
Expires 9 July 2015

W. Ladd
UC Berkeley

9 October 2014

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

Status of this Memo

Copyright Notice

Abstract

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

based key exchange

Table of Contents

1. Introduction

This document describes a means for two parties that share a password to derive a shared key.

2. Definition of SPAKE2

Let G be a group in which the Diffie-Hellman problem is hard of prime order p, written 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.

|| denotes concatenation of strings. We also let len(S) denote the length of a string in bytes, rrepresented 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.

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 element of Zp w. Typically w will be the hash of a user-supplied password, truncated and taken mod p. Protocols using this protocol must define w.

A picks x randomly and uniformly from the integers in [0,p), and calculates X=xg and T=wM+X, then transmits T to B.

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

Both A and B can now calculate a shared key as H(len(A)||len(B)||len(S)||len(T)||A||B||S||T||K).

3. Table of points

[TODO]

4. Security Considerations

A security proof 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 picked in standard ways to eliminate 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.

5. IANA Considerations

No IANA action is required.

6. 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