

## The Secure Remote Password Protocol

Thomas Wu  
Computer Science Department  
Stanford University  
Tjw@cs.Stanford.EDU

November 11, 1997

## Quote of the day:

*" Well begun is half done. "*

*Aristotle, Politics*

4/11/02

ilkay Cubukcu

2

## Purpose:

Presenting a new password authentication and key-exchange protocol that is suitable for:

- authenticating users and
- exchanging keys
- over an untrusted network

4/11/02

ilkay Cubukcu

3

## Categories of authentication methods:

Something that:

- The user *is* (voiceprint identification, retinal scanners)
- The user *has* (ID cards, smartcards)
- The user *knows* (password, PINs)
  - Direct password authentication (*used in this paper*)

4/11/02

ilkay Cubukcu

4

## Direct Password Authentication

- **Client:** No persistent stored information
- **User's password:** memorized quantity. Only secret that available to client software
- **Network(C-S):** vulnerable to both eavesdropping and deliberate tampering by the enemy.
- No trusted third party (key server or arbitrator). Only original two parties.

4/11/02

ilkay Cubukcu

5

## AKE (Asymmetric Key Exchange):

- New family of authentication protocols
- Generalized form for a third class of verifier-based protocols.
- Uses **swapped-secret** instead of traditional **shared-secret**.
- Do not use **symmetric encryption**.

4/11/02

ilkay Cubukcu

6

## Secure Remote Password(SRP): interpretation of AKE

- Simple, fast and highly secure
- Uses Simplified **MAC (Message Authentication Code)** that is based on one-way hash functions: For verifying the session keys by two parties in a secure manner.
- Resists **dictionary attacks** that mounted by passive or active network intruders.
- Offers perfect **forward secrecy** (protects past session and passwords against the future compromises)
- Stores user passwords stored in a form that not **plaintext equivalent** to the password (an attacker captures the password database cannot use it directly to compromise security and access to the host)
- Combines the techniques of **zero-knowledge** proofs with **asymmetric key exchange protocol**
- Offers better performance than **Augmented EKE (A-EKE)**, digital signatures) or **B-SPEKE**(secondary one-sided key exchange).

4/11/02

ilkay Cubukcu

7

## Mathematical notation of SRP

$n$  : a large prime number (All computations are performed modulo  $n$ )  
 $g$  : a primitive root modulo  $n$  (**generator** in  $GF(n)$ )  
 $s$  : a random string (**user's salt**)  
 $P$  : The user's **password**  
 $x$  : a **private key** derived from  $P$  and  $s$   
 $v$  : the host's **password verifier**  
 $u$  : **Random scrambling parameter**, publicly revealed  
 $K$  : **session key**  
 $H()$  : one-way **hash function**  
 $a, b$  : **Ephemeral private keys**, generated randomly, not publicly revealed  
 $A, B$  : corresponding **public keys**  
 $m, n$  : the two quantities (strings)  $m$  and  $n$  concatenated  
 $GF(n)$  : **Finite field** (All computations are performed in a finite field)

4/11/02

ilkay Cubukcu

8

## Mathematical notation of SRP(cont.)

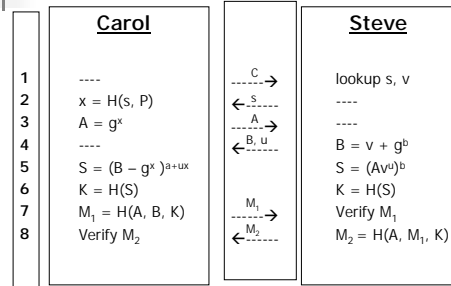
- $P(x) = g^x$  (one way verifier-generating function)
- $Q(w, x) = w + ux$  (mixing functions for private and public parameters)
- $R(w, x) = ux^u$
- $S(w, x) = w^x$  (session key generation function)
- $x = H(s, P)$
- $V = g^v$

4/11/02

ilkay Cubukcu

9

## SRP Protocol



4/11/02

ilkay Cubukcu

10

## SRP Protocol (cont.)

- C sends  $S$  her username.
- $S$  looks up  $C$ 's password entry and fetches her  $v$  and  $s$ . He sends  $s$  to  $C$ .  $C$  computes her long-term key  $x$  using  $s$  and her real password  $P$ .
- $C$  sends the random number  $a$ , computes her ephemeral public key  $A$  and sends it to  $S$  ( $A = g^a, 1 < a < n$ ).
- $S$  generates his own random number  $b$ , computes his ephemeral public key  $B$  and sends it back to  $C$  along with  $u$ , randomly generated parameter ( $B = v + g^b, 1 < b < n$ ).
- $C$  and  $S$  compute the common exponential value  $S$ . If  $C$ 's password  $P$  entered in step-2 matches the one she used to generate  $v$ , then both values of  $S$  will match ( $S = g^{ab+bus}$ ).
- Both sides hash the exponential  $S$  into a cryptographically strong session key.
- $C$  sends  $M_1$  as evidence that she has the correct key.  $S$  also computes  $M_1$  himself and verifies that it matches the one that  $C$  sent.
- $S$  sends  $M_2$  as evidence that he has the correct key.  $C$  also verifies  $M_2$  herself and accepts only if it matches  $S$ 's value.

4/11/02

ilkay Cubukcu

11

## Reduction to Diffie-Helman(DH)

- Mathematical notation of SRP protocol is similar to the DH problem.
- The algorithm used to compromise the session key in SRP through a passive attack can be used to break a DH key exchange in polynomially-equivalent time.
- This proof shows that SRP resists passive attack at least as well as DH protocol.
- The algorithm can be:
  - Oracle  $Q$  that accepts the values  $A, B, u, g, n$ , and  $x$  and computes session key  $S$ .
    - $S = g^{ab+bus}$
    - $Q(g^a, g^b + g^x, u, g, n, x) = g^{ab+bus}$
  - It is difficult to compute  $g^{ab}$  in  $GF(n)$  where  $g^a$  and  $g^b$  are given (as claimed in DH). Therefore let  $u = 2$  and  $x = (n-1)/2$ . DH oracle  $Q$  in terms of SRP oracle  $Q$  is:
    - $Q(A, B, g, n) = Q(A, B, g^{(n-1)/2}, 2, g, n, (n-1)/2)$  and  $A = g^a, B = g^b$  then
    - $Q(g^a, g^b, g, n) = g^{ab}$

4/11/02

ilkay Cubukcu

12

## Resistance to Denning-Sacco Attack

- An intruder captures the session key from an evasdropped session and uses it to gain ability to access the user directly or conduct a brute-force search against the user's password.
- A-EKE requires the user to send a message which is dependent on both long term private key and the session key. This message enables the Denning-Sacco attack.

4/11/02

ilkay Cubukcu

13

## Optimization of SRP

- Less message rounds (instead of 3 round messages, 2 with Optimized SRP and 1.5 with One-Way Optimized SRP)
- Less execution speed (fastest verified-based protocol)

4/11/02

ilkay Cubukcu

14

## Benefits of SRP:

An attacker,

- with neither user's password nor the host's password file, cannot mount a dictionary attack on the password
- captures the host's password file, cannot directly compromise user-to-host authentication and gain access to the host without an expensive dictionary search.
- compromises the host, does not obtain the password from legitimate authentication attempt.
- captures the session key, cannot use it to mount a dictionary attack on the password
- captures the user's password, cannot use it to compromise the session keys of past sessions.

4/11/02

ilkay Cubukcu

15