Security and Privacy

Password Agreed Key Exchanges (PAKE)

12.03.2019

Ph. Oechslin

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Introduction

Introduction

- In Homework 2 you will be implementing the Secure Remote Passoword protocol (SRP), a Password Agreed Key Exchanges (PAKE)

- A PAKE allows to
  - verify the password of a remote party and
  - exchange a key (e.g. for encryption)

- We saw in TLS, that the server can sign its half of the Diffie Hellman key exchange to prove possession of the private key of the certificate, thus proving its identity

- PAKE is similar, but authentication is based on a symmetric key, the password.

- To help with the homework, here is a short explanation of SRP

SRP Overview

- SRP is like Diffie Hellman with some additional elements that depend on the password

- It uses exponentiations of a generator g (e.g. g^k) and a modulo N

- For each user, the server stores three elements:
  1. the username U
  2. a salt s
  3. the password verifier v (the exponentiation of a salted hash of the password p):

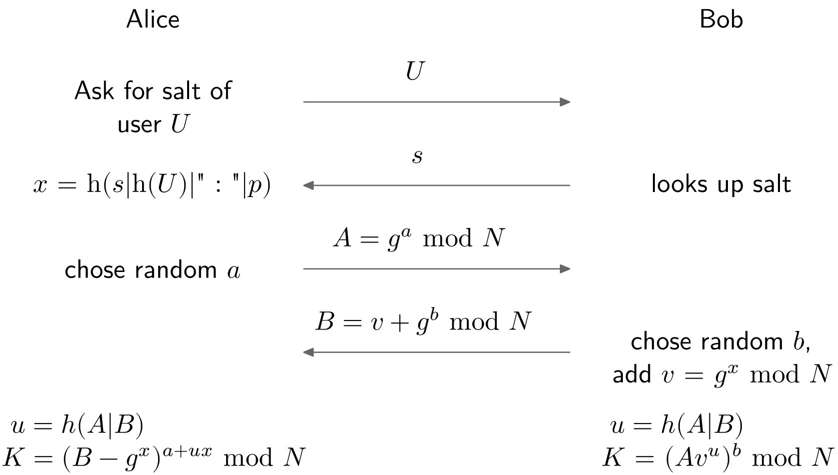
     $x = \mathrm{h}(s|\mathrm{h}(U)|" : "|p)$

     $v = g^x \mod N$

- The server adds v to its part of the Diffie-Hellman exchange
  - it contributes to the calculation of the key

- The client will need to know the salt to calculate x, so it first asks for this.

SRP Exchange



Alice

Bob

Ask for salt of user U $\xrightarrow{\quad U \quad}$

$x = \mathrm{h}(s|\mathrm{h}(U)|" : "|p)$ $\xleftarrow{\quad s \quad}$ looks up salt

chose random a $\xrightarrow{A = g^a \bmod N}$

$\xleftarrow{B = v + g^b \bmod N}$ chose random b, add $v = g^x \bmod N$

$u = h(A|B)$
$K = (B - g^x)^{a+ux} \bmod N$

$u = h(A|B)$
$K = (Av^u)^b \bmod N$

They both get $K = g^{b(a+ux)} \bmod N$

SRP Conclusions

- Alice and Bob have only exchanged public values: g^a and $g^b + g^x$
- Eavesdroppers can not learn anything from these values
- The resulting key depends on a, b and x (x depends on the password)
- Before continuing, they can send each other an encrypted message or a MAC to prove that they succeeded in calculating the key