SRP Protocol for Auth

…

Introduction

- Secure Remote Password (SRP) protocol is a password-authenticated key exchange protocol

- Developed by Thomas Wu at Stanford University

- Standardized in RFC 2945

- Provides mutual authentication between client and server

- Zero-knowledge proof: Server never stores actual password

- Resistant to dictionary attacks, man-in-the-middle attacks, and replay attacks

Why SRP ?

- Traditional password authentication has vulnerabilities
    - Password storage on server
    - Transmission of password or hash over network
- SRP advantages:
    - Server stores verifier, not password
    - Immune to passive dictionary attacks
    - No trusted third party required
    - Mutual authentication
    - Perfect forward secrecy

Application for Web Authentication

Client-server architecture implementation

- Used by:
  - 1Password password manager
  - Apple iCloud
  - ProtonMail

- Benefits for web applications:
  - Enhanced security without SSL/TLS
  - Protection against phishing
  - Simplified key management
- Can be implemented in JavaScript for browser clients

Core Concepts : Mathematical Notations

n	A large prime number. All computations are performed modulo n.
g	A primitive root modulo n (often called a *generator*)
s	A random string used as the user's *salt*
P	The user's password
x	A private key derived from the password and salt
v	The host's password verifier
u	Random scrambling parameter, publicly revealed
a, b	Ephemeral private keys, generated randomly and not publicly revealed
A, B	Corresponding public keys
$H()$	One-way hash function
m, n	The two quantities (strings) m and n concatenated
K	Session key

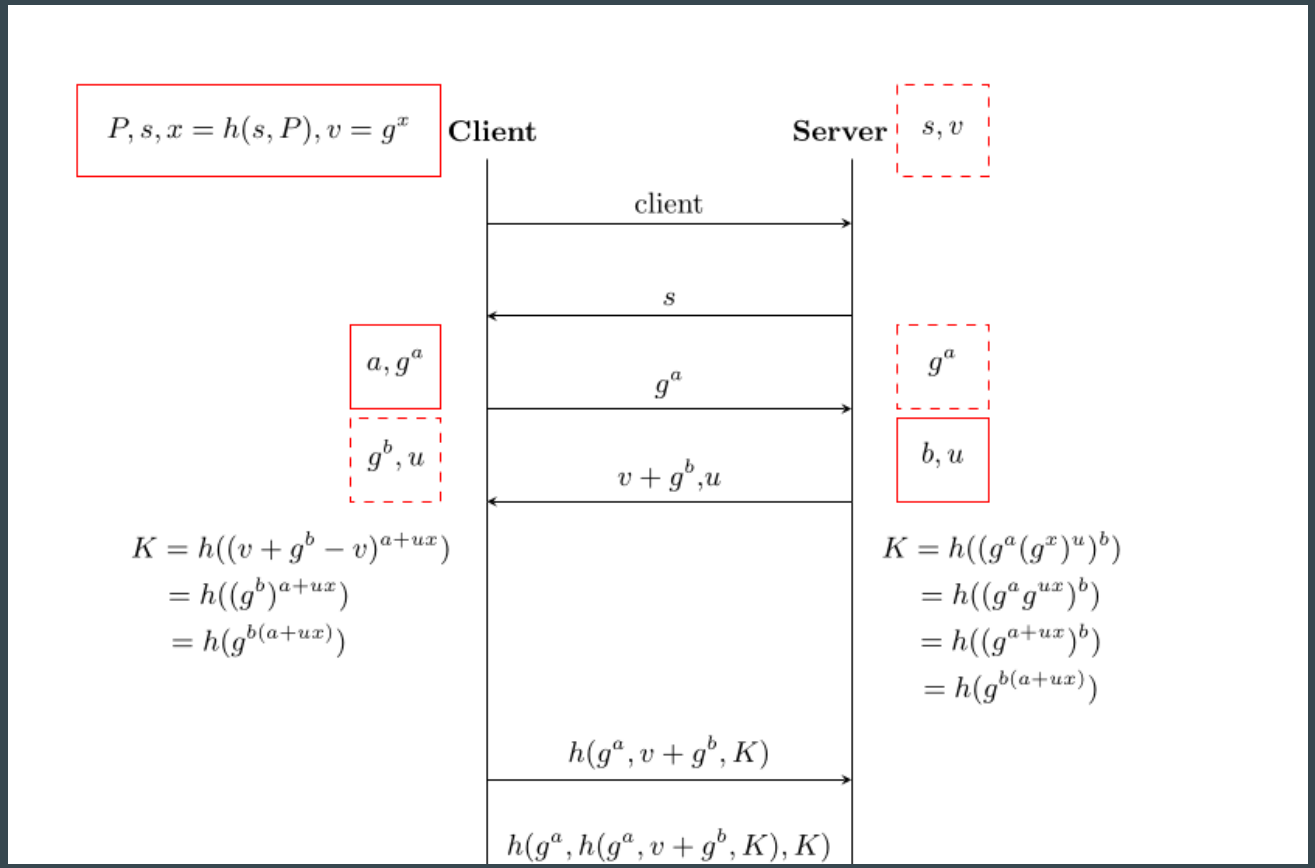
Table 3: Mathematical Notation for SRP

Core Concepts : Authentication Flow

Two Phases:

I. Key Establishment

II. Key Verification.



Security Analysis

- Resistant to various attacks:
  - Dictionary attacks
  - Man-in-the-middle attacks
  - Replay attacks
- Security proofs based on:
  - Diffie-Hellman problem
  - Discrete logarithm problem
- Known limitations and considerations