Network Security Project Design Overview

Nimisha Peddakam

Sree Siva Sandeep Palaparthi

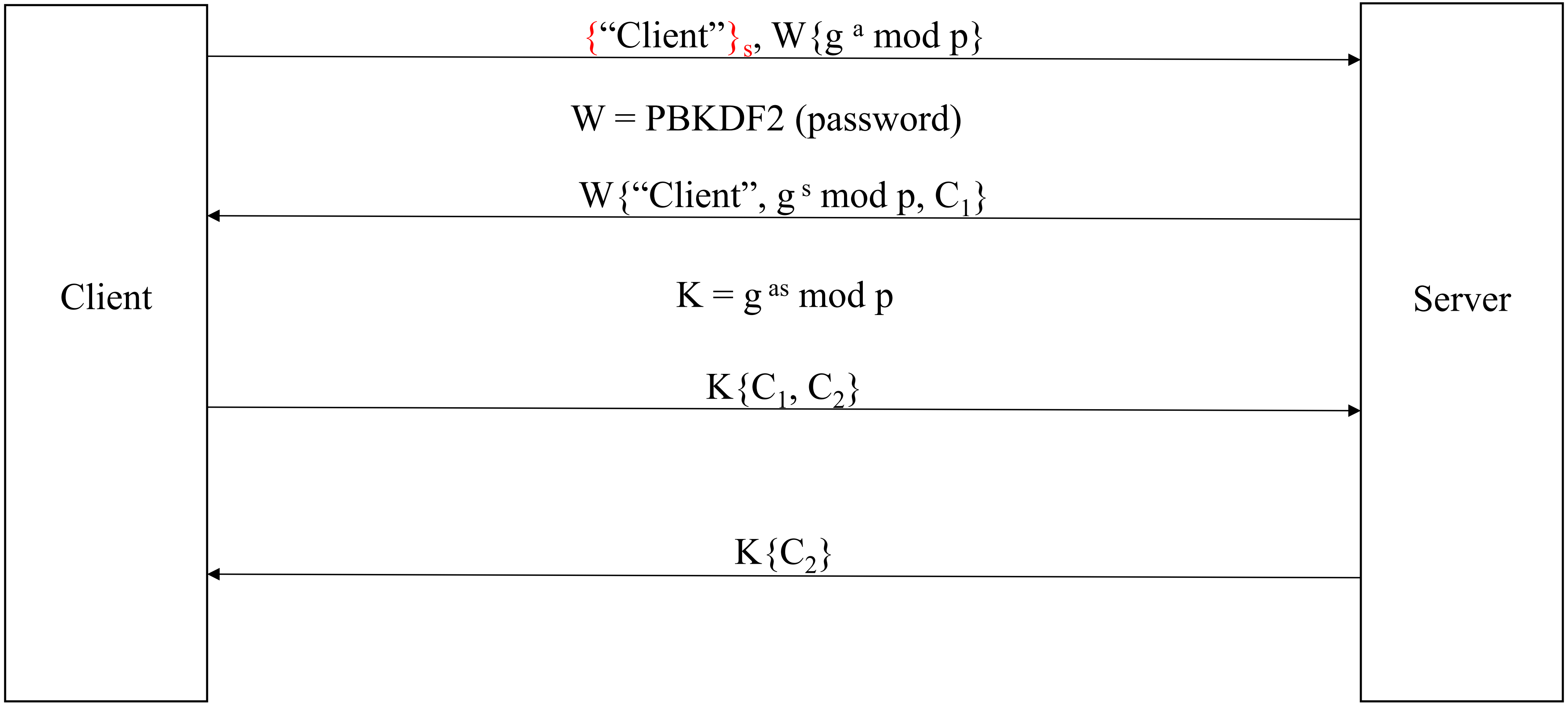
Assumptions

- Server is trusted and available
- Users are pre-registered

Architecture

- One server-multiple client architecture
- Client is authenticated with server
- Messages are communicated between clients

Login Protocol



Client

Server

$\{\text{“Client”}\}_s$, $W\{g^{a} \bmod p\}$

$W = \text{PBKDF2}(\text{password})$

$W\{\text{“Client”}, g^{s} \bmod p, C_1\}$

$K = g^{as} \bmod p$

$K\{C_1, C_2\}$

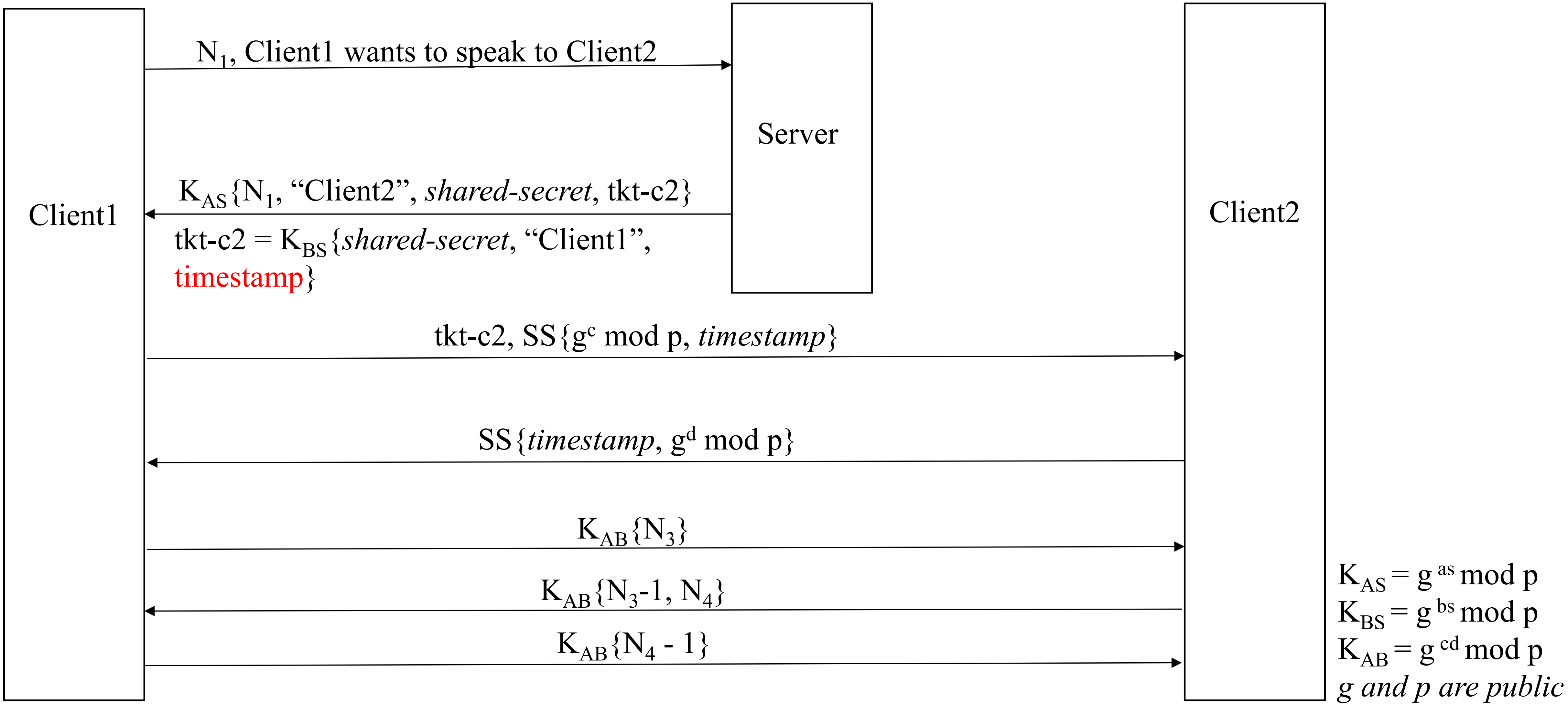
$K\{C_2\}$

g and p are public

- Based on EKE protocol
- When implementing, we will be choosing p in order to eliminate the offline attack vulnerability.

Key establishment & Messaging Protocol

Based on Needham-Schroeder



Client1

Server

Client2

N_1, Client1 wants to speak to Client2

K_{AS}\{N_1, “Client2”, *shared-secret*, tkt-c2\}

tkt-c2 = K_{BS}\{*shared-secret*, “Client1”, timestamp\}

tkt-c2, SS\{g^c mod p, *timestamp*\}

SS\{*timestamp*, g^d mod p\}

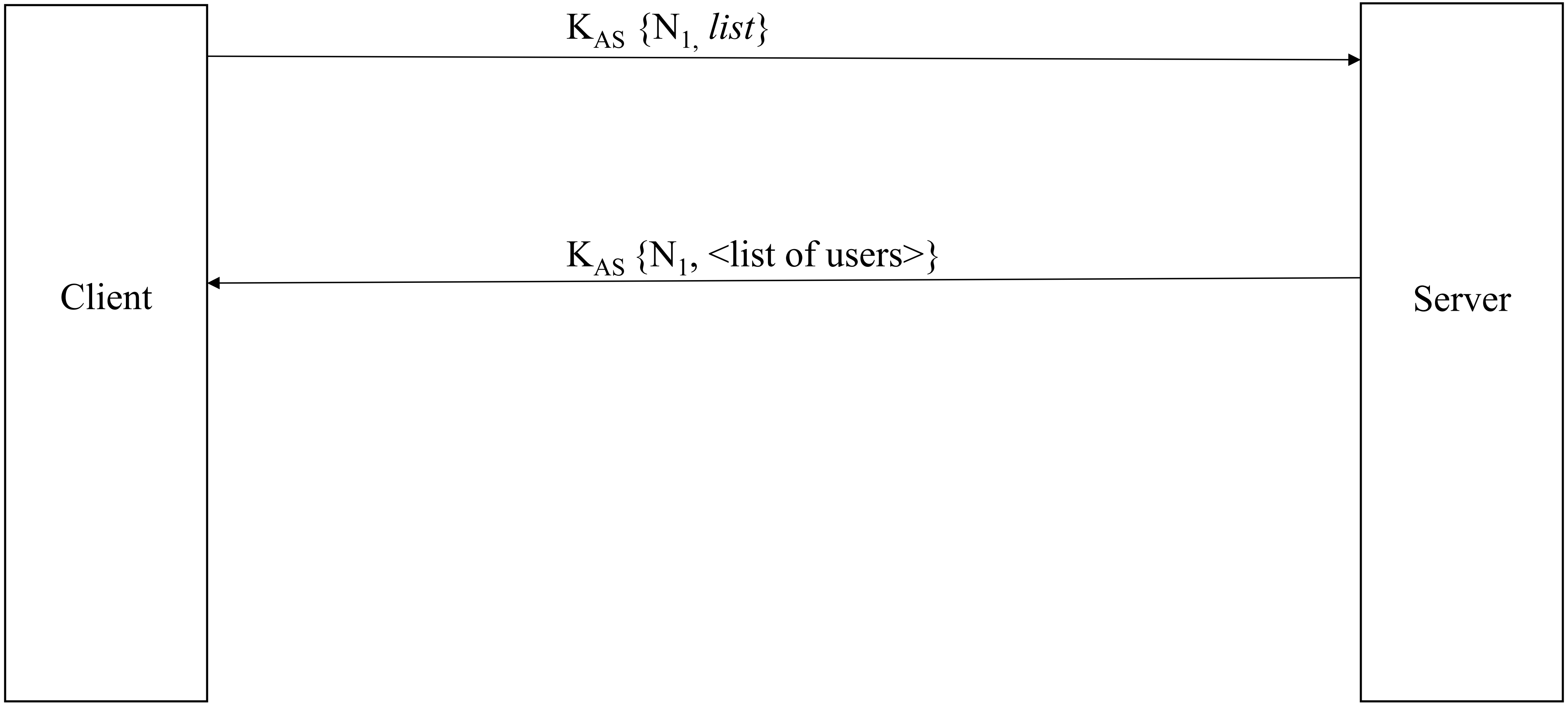
K_{AB}\{N_3\}

K_{AB}\{N_3-1, N_4\}

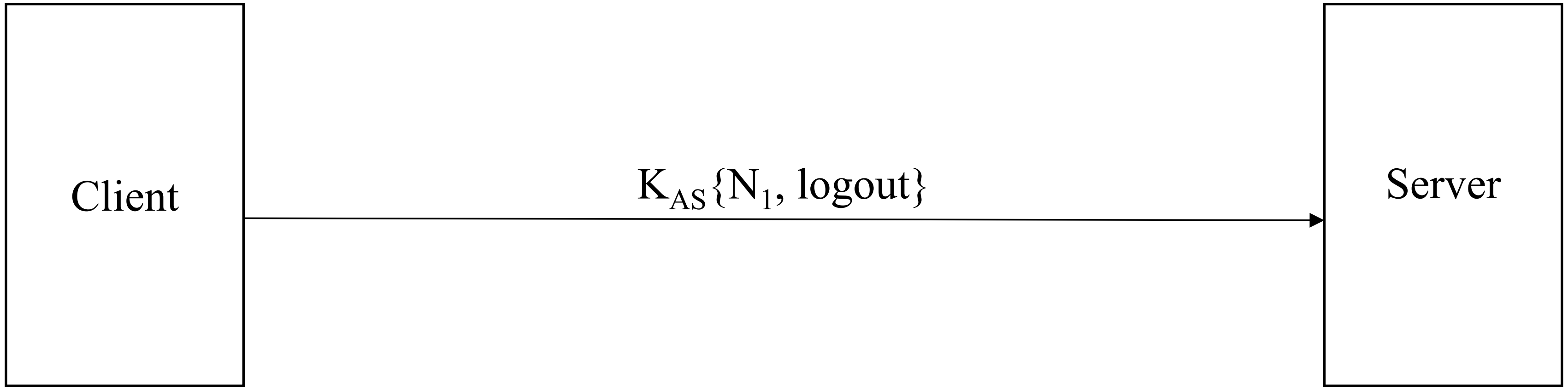
K_{AB}\{N_4 - 1\}

$K_{AS} = g^{as}$ mod p
$K_{BS} = g^{bs}$ mod p
$K_{AB} = g^{cd}$ mod p
g and p are public

List Command



Logout protocol



Client

$K_{AS}\{N_1, \text{logout}\}$

Server

$K_{AS} = g^{as} \bmod p$

Algorithms used

- PBKDF2 used to derive W from password
- Symmetric encryption AES in GCM mode.
- RSA

Services

- Perfect forward secrecy – Diffie-Hellman key exchange
- Confidentiality – Encryption using AES
- Integrity – AES in GCM mode
- Mutual authentication – Challenge response
- Identity hiding
- Weak password protection