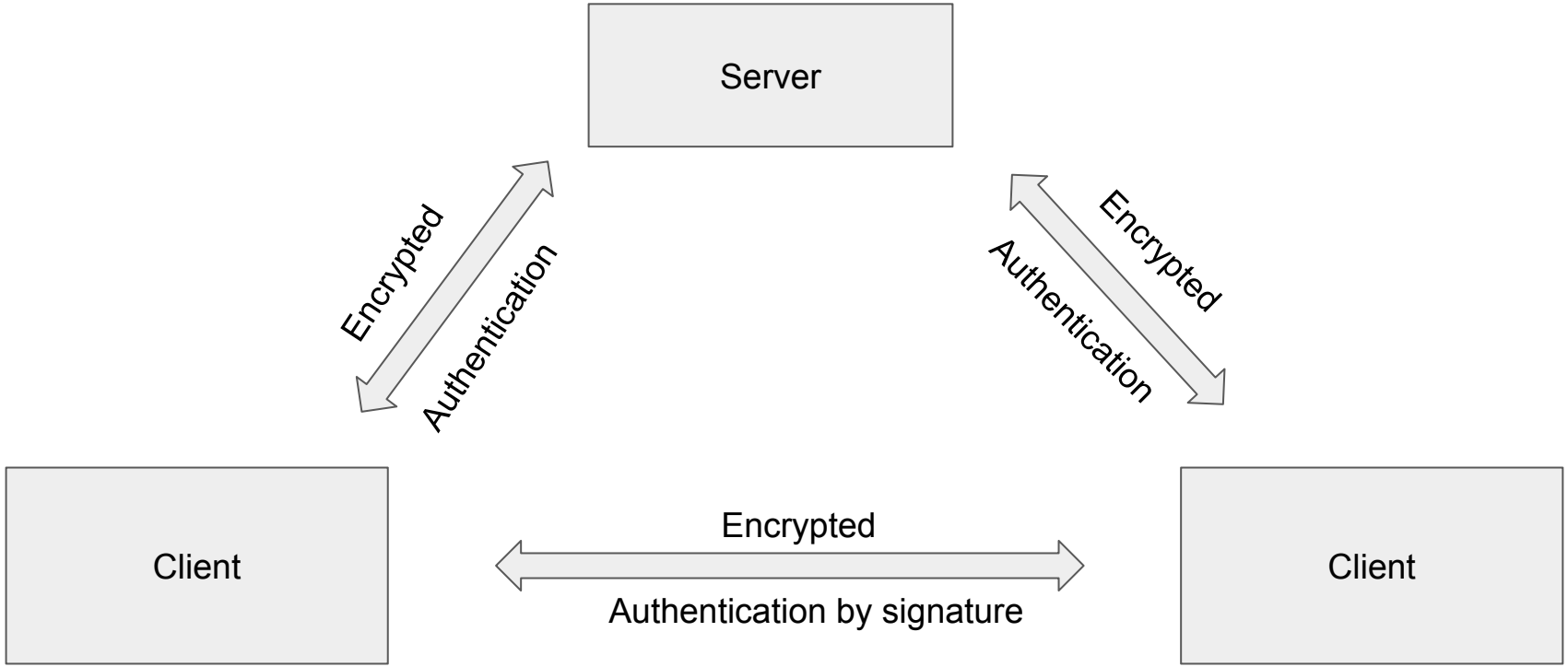
Secure Instant Messaging System

Team member: Xinwen Zhang, Yang Cai

Architecture



Before Authentication (assumptions)

Client A:

- **Password Pa**

Client can compute: W, W’

Server:

- **W: derived from Pa using PBKDF2**
- **A’s public key**
- **Y=W’{A’s private key}**

Note: All symmetric encryption use AES-GCM to provide confidentiality and data integrity

During Client-Server Authentication

Augmented Strong Password Protocol:

A->S: “Alice”

S->A: c = Hash(A’s ip, secret)

A->S: c, W{g^a mod p}

S->A: W{g^b mode p), (g^ab mode p){W’{A’s private key}}, c1

A->S:[hash(g^ab mod p, c1)]sign-A

Client to Server Communication (after authentication)

Both party: Session key: Ks = g^ab mod p

Client: private RSA key

A -> Server: Ks{“List”, Timestamp}

Server -> A: Ks{“List of log in users”,Timestamp}

A -> Server: Ks{“Tell me about B”,Timestamp}

Server -> A: Ks{B’s public key, B’s ip address,Timestamp}

A -> Server: Ks{“Log me out”, Timestamp}

Protocol Security

1. Mutual authentication.
2. Resistant to offline attack
3. If the server is compromised, hard to brute-force the password
4. If the server is compromised, attacker cannot impersonate the user, since he does not know W’.
5. Resistant to DoS attack by using cookies.
6. Resistant to man-in-the-middle by encrypting with W.
7. Perfect Forward Secrecy using Diffie-Hellman
8. Resistant to replay attack by using timestamp
9. Provides confidentiality and integrity using AES-GCM

Client to Client Key Establishment

A gets B’s ip address from the server

A->B:g^a mod p

B->A:g^b mod p

A->B:g^ab mod p{“A”, [g^a mod p]sign-A}

B verifies the signature using A’s public key retrieved from the server

B->A:g^ab mod p{“B”, [g^b mod p]sign-B}

A verifies the signature using B’s public key retrieved from the server

Client to Client Communication

Both party: Session key: Ks = g^ab mod p

A -> B: Ks{“message”, Timestamp}

B-> A: Ks{“message”,Timestamp}

Protocol Security

1. Resistant to man-in-the-middle by using signature
2. Identity hiding
3. Perfect forward Secrecy (Deffie-hellmen)
4. Mutual authentication by signature
5. Provide both confidentiality and data integrity by using AES-GCM
6. Resistant to replay attack by using timestamp.