Secure Instant Messaging System

Binbin Lu

Architecture

1. A server keeps records of registered users, authentication, client discovery, key distribution

2. Multiple clients

Assumptions

1. Users only need to remember username and password

2. Client workstation knows server's public key

3. All users are already registered

Authentication protocol (login)

a) $A \rightarrow S$: Request Login

b) $S \rightarrow A$: $Cookie - Hash(IP_A, \ timestamp)$

c) $A \rightarrow S$: $Cookie, \{A\}_{PK_S}, g^a \bmod p$

d) $S \rightarrow A$: $g^b + g^W \bmod p, u, C_1$

The shared key between client and server is $K = g^{b(a+uW)} \bmod p$

e) $A \rightarrow S$: $K\{C_1\}, C_2$

f) $S \rightarrow A$: $K\{C_2\}$

Key Establishment Protocol

a) $A \rightarrow S: K_{AS}\{A, B, N_1\}$

b) $S \rightarrow A: K_{AS}\{B, IP_B, port_B, N_1, K_{AB}, t-to-B\}$

$t-to-B_1 = K_B\{A, K_{AB}, TTL\}$

c) $A \rightarrow B: t-to-B, K_{AB}\{N_2\}$

d) $B \rightarrow A: K_{AB}\{N_2 - 1, N_3, g^b \bmod p\}$

e) $A \rightarrow B: K_{AB}\{N_3 - 1, g^a \bmod p\}$

Key used between A and B is $K = g^{ab} \bmod p$

Messaging Protocol

a) $A \rightarrow B: K_{AB'}\{M_1, HMAC(M_1)\}$

b) $B \rightarrow A: K_{AB'}\{M_2, HMAC(M_2)\}$

Logout Protocol

a) $A \rightarrow S: K_{AS}\{FIN,\ N_1\}$

b) $S \rightarrow A: K_{AS}\{FIN - ACK,\ N_1 - 1, N_2\}$

c) $A \rightarrow S: K_{AS}\{ACK, N_2 - 1\}$

Services

1. DoS resiliency
2. Perfect forward secrecy
3. Identity hiding
4. Mutual authentication
5. Confidentiality
6. Integrity
7. Non repudiation
8. Replay resistance
9. Break in tolerance
10. MITM resistance
11. Dictionary attack
12. Offline attack
13. Impersonation