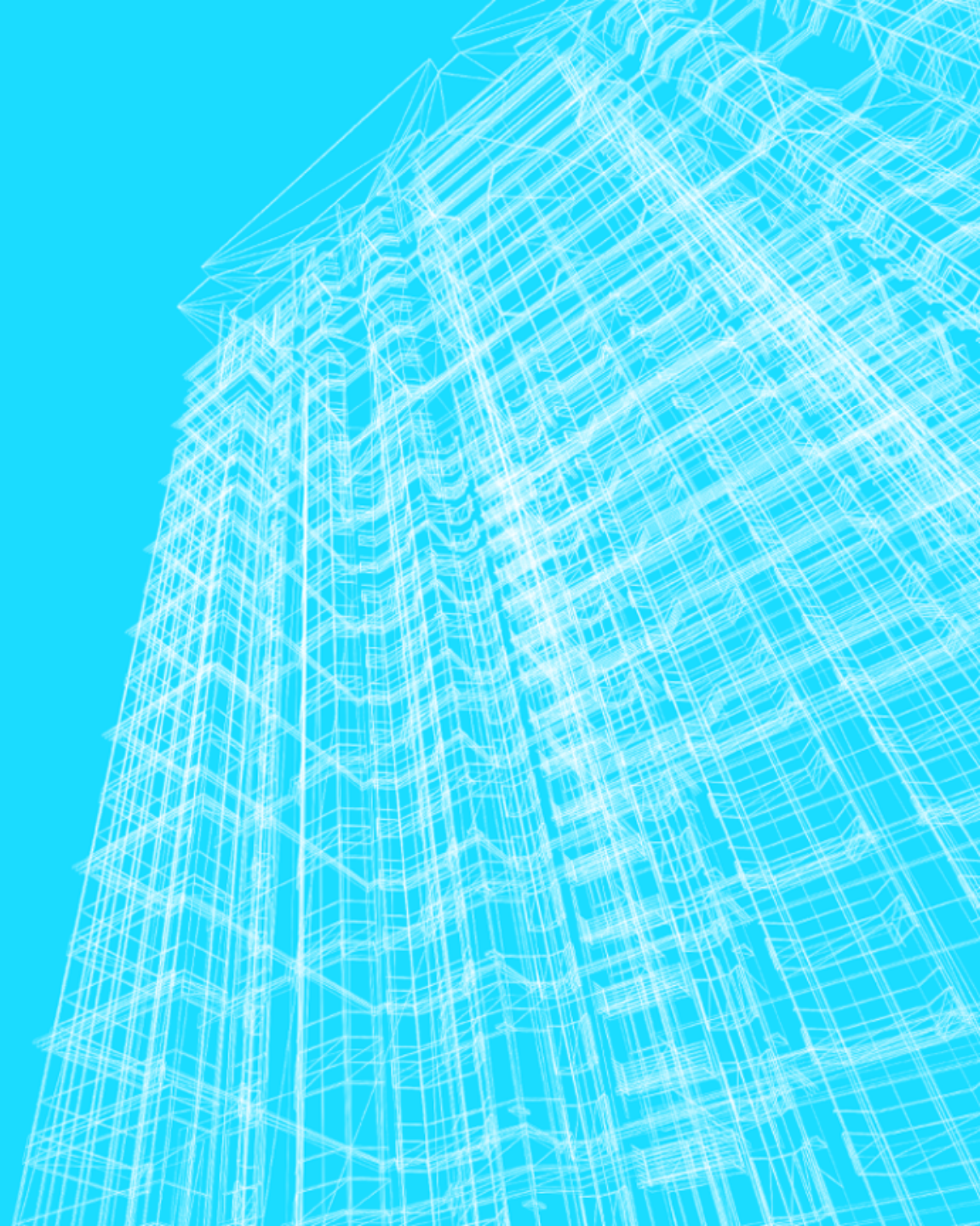
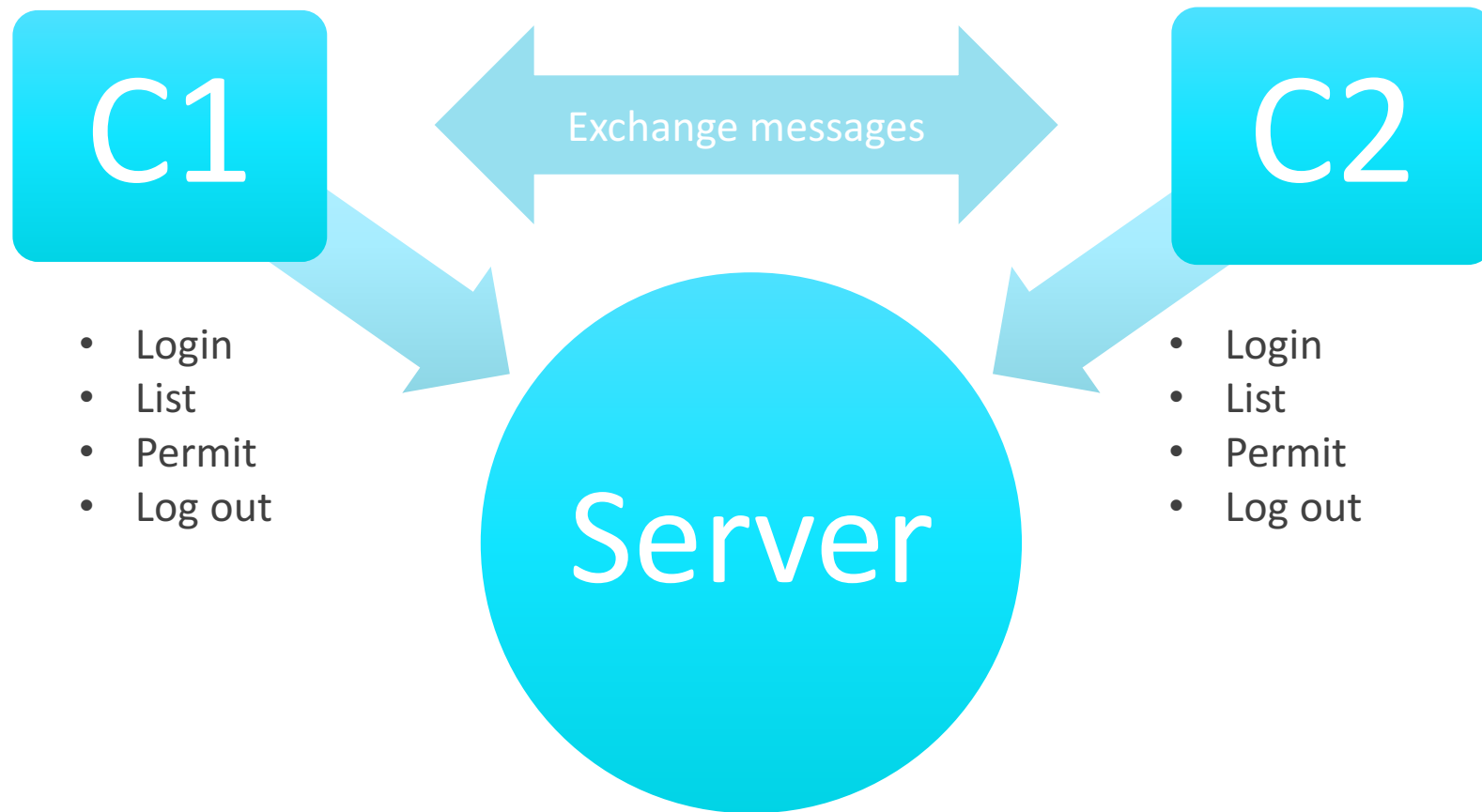


PFS CHAT

Matt Brandman
Ibrahim Aleidan



ARCHITECTURE





ASSUMPTIONS

- Client knows the public key of the server
- Server knows the password for the client
- Clients are preregistered with the server and persist through restart
- Shared Secret is used to key a AES-GCM encryption

Client

Server

I am C1, $g^a \bmod p$

$g^b \bmod p, N_1$

DHK = $g^{ab} \bmod p$

$K_{\text{DHK}}\{H\{N_1, \text{DHK}\}\}$

$K_{\text{DHK}}\{ [H\{N_1, \text{DHK}\}]_S \}$

$K_{\text{DHK}}\{\text{PASSWORD}, \text{PUK}_c\}$

$K_{\text{DHK}}\{\text{LOGIN ACCEPTED}\}$

LOGIN PROTOCOL

PUK_x = Public Key of x.

Client

Server

$K_{DHK}\{LIST\}$

$K_{DHK}\{USERS\ LIST\}$

$K_{DHK}\{PERMIT\ C_2\}$

$K_{DHK}\{ADDRESS_C2, C2, PUK_{c2}, K_{c1-c2}, K_{c2}\{C1, PUK_{c1}, K_{c1-c2}\}\}$

LIST & PERMIT PROTOCOL

Changed

Added C2 to reply and C1 to ticket.

Client1

Client2

$K_{c2} \{ \text{PUK}_{c1}, K_{c1-c2} \}, K_{c1-c2} \{ g^a \bmod p \}$

$K_{c1-c2} \{ g^b \bmod p, N_1 \}$

$\text{DHK} = g^{ab} \bmod p$

$K_{\text{DHK}} \{ [H\{N_1, \text{DHK}\}]_{c1} \}$

$K_{\text{DHK}} \{ [H\{N_1, \text{DHK}\}]_{c2} \}$

$K_{\text{DHK}} \{ \text{MESSAGE}, [\text{MESSAGE}]_{c1} \}$

$K_{\text{DHK}} \{ \text{MESSAGE}, [\text{MESSAGE}]_{c2} \}$

CLIENT-CLIENT PROTOCOL

Client

Server

$K_{\text{DHK}}\{\text{LOG-OUT}\}$

$K_{\text{DHK}}\{\text{OKAY}\}$

LOGOUT PROTOCOL



DISCUSSION

- The use AES throughout keyed with a DH shared key means that even if the private key of the server is cracked they will never be able to decrypt past messages.
- Shared Secret is used to key a AES-CBC encryption
- SHA-2 is used as hashing algorithm



NOT IMPLEMENTED IN CODE

- Delete the key between Client-Server and Client-Client after some time, and ask to start a new key if key expired.



CHANGES FROM PS4

- Used AES-GCM instead of AES-CBC.
- One more change shown in PERMIT Protocol.