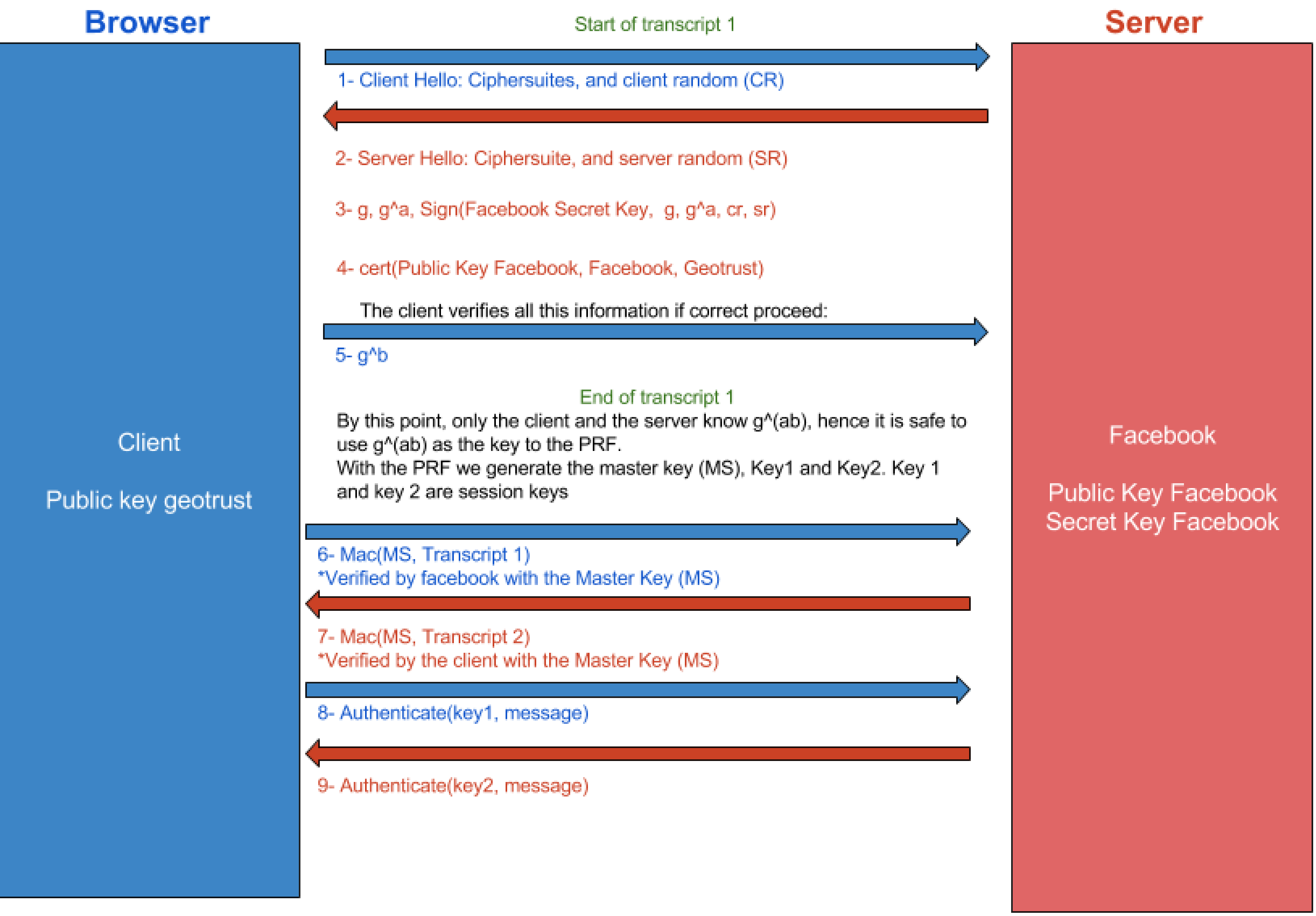
scribe: Ezequiel Gomez

TLS (Most popular) encryption protocol



Browser

Client

Public key geotrust

Server

Facebook

Public Key Facebook
Secret Key Facebook

Start of transcript 1

1- Client Hello: Ciphersuites, and client random (CR)

2- Server Hello: Ciphersuite, and server random (SR)

3- g, g^a, Sign(Facebook Secret Key, g, g^a, cr, sr)

4- cert(Public Key Facebook, Facebook, Geotrust)

The client verifies all this information if correct proceed:

5- g^b

End of transcript 1

By this point, only the client and the server know g^(ab), hence it is safe to use g^(ab) as the key to the PRF.
With the PRF we generate the master key (MS), Key1 and Key2. Key 1 and key 2 are session keys

6- Mac(MS, Transcript 1)
*Verified by facebook with the Master Key (MS)

7- Mac(MS, Transcript 2)
*Verified by the client with the Master Key (MS)

8- Authenticate(key1, message)

9- Authenticate(key2, message)

Vocabulary

- ❏ Ciphersuites: When you give the server a preference of your cypher.
- ❏ Ciphersuite: The suite the server decided to use from your Ciphersuites.
  - ❏ Note: If the server and the client can’t both decide on one ciphersuite then the browser will notify the user that the connection is not secure.

- ❏ We need TLS because, before we login, the server doesn’t know who we are. All we know at the beginning is Geotrust public key, but we need to setup session keys.
  - ❏ Key Establishment

        - ❏ At the start we know Public Key Geotrust
        - ❏ TLS Handshake
        - ❏ Setup session key K
    - ❏ The client doesn’t know Facebook’s public key, and facebook can’t just send it over because the client can’t tell if it’s actually coming from Facebook.
        - ❏ Hence Facebook has to send over the certificate in step 4, to make sure the client can verify the signature and g^a of step 3.

Security:

- ❏ If Facebook Secret key gets compromised:
    - ❏ Forward Secrecy: The person who compromised the key won’t be able to decrypt previous messages, hence he doesn’t have g^(ab).
    - ❏ The person can’t decrypt FB’s on wire communication, because he doesn’t have g^(ab)
    - ❏ The person can only pose as Facebook for future communications.