Transport Layer Security (TLS)

Dr Rosanne English

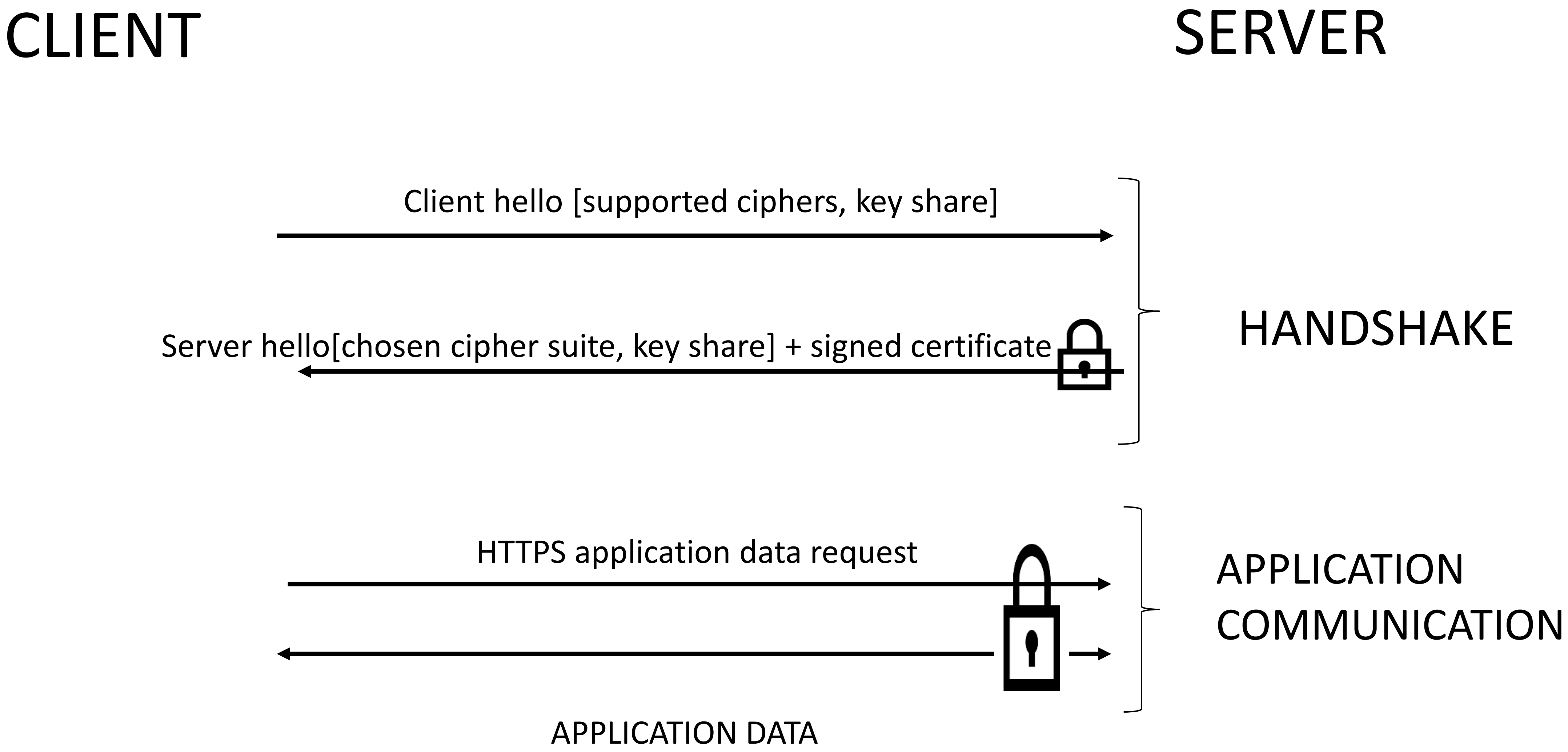
Trust

- Client has to trust CA
- CA digitally signs certificate to confirm ownership of a public key
- Client uses pre-installed CA certificate to get CA public key
- Client can now verify digital signature

Public Key Infrastructure (PKI)

- The set of hardware, software, people, policies, and procedures that are needed to create, manage, distribute, use, store, and revoke digital certificates

Transport Layer Security (V 1.3)



CLIENT

SERVER

Client hello [supported ciphers, key share]

Server hello[chosen cipher suite, key share] + signed certificate

HANDSHAKE

HTTPS application data request

APPLICATION COMMUNICATION

APPLICATION DATA

🔒 This padlock symbol indicates messages are encrypted

(Perfect) Forward Secrecy

Keys to encrypt and decrypt are ethereal such that they are only used within that communication session

This means, even if a key is broken the past and future communications remain confidential