

Exercise walk-through

9.6

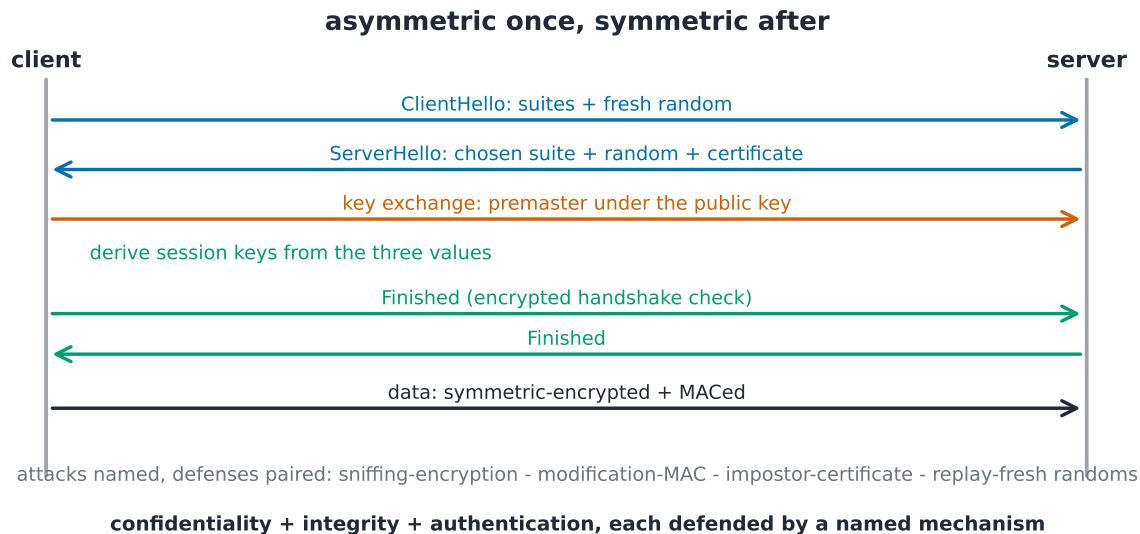
Network security

University Computer Science

Security: three properties, named attacks

- 1 **Handshake** ClientHello and ServerHello with fresh randoms and a certificate; the premaster travels under the public key; both derive session keys; Finished verifies.
- 2 **Pairing** Sniffing defeated by encryption; alteration by the **MAC**; impostors by certificates; replay by the fresh randoms - each attack names its defense.
- 3 **Honest** HTTPS makes the channel private and the server identified - the content can still lie.

TLS flow



ClientHello, certificate, key exchange, both Finished - then **symmetric** data.

Exercises 2.1-2.3

2.1 Which property does a MAC provide? [3]

2.2 Which mechanism defeats an impostor server? [3]

2.3 What do both Hellos contribute against replay? [3]

Exercises 2.1-2.3

2.1 Which property does a MAC provide? [3]

2.1

- Integrity – alteration is detected (with key possession assumed) ✓.
-

2.2 Which mechanism defeats an impostor server? [3]

2.2

- Certificates: the server proves possession of the private key matching the certified public one ✓.
-

2.3 What do both Hellos contribute against replay? [3]

2.3

- Fresh randoms – a replayed handshake derives different keys and fails the Finished check ✓.

Exercise 3.1

3.1 Order these handshake steps and name each: offered suites and a random; chosen suite, a random and a certificate; premaster under the public key; both sides derive keys; both send Finished.

State what each side needs before it can derive the session keys (list the three values).
State what a Finished message proves and what the first data byte uses. [8]

Exercise 3.1

3.1 Order these handshake steps and name each: offered suites and a random; chosen suite, a random and a certificate; premaster under the public key; both sides derive keys; both send Finished.

State what each side needs before it can derive the session keys (list the three values). State what a Finished message proves and what the first data byte uses. [8]

3.1

- Order: ClientHello (suites + random); ServerHello (suite + random – certificate); key exchange (premaster encrypted under the public key); derive session keys; Finished both ways ✓.
- The three values: client random, server random, premaster ✓.
- Finished proves the whole handshake was not tampered with (it is checked under the derived keys) ✓.
- The first data byte uses the symmetric session keys ✓.

Exercise 3.2

3.2 For each attack, name the defense and where it acts: passive sniffing on the wire; in-flight modification of a handshake message; a server impersonating the real one; replay of a captured whole handshake.

State what encrypting without authenticating gives you, in one line. State what HTTPS does and does not make honest. [7]

Exercise 3.2

3.2 For each attack, name the defense and where it acts: passive sniffing on the wire; in-flight modification of a handshake message; a server impersonating the real one; replay of a captured whole handshake.

State what encrypting without authenticating gives you, in one line. State what HTTPS does and does not make honest. [7]

3.2

- Sniffing: encryption (confidentiality) acts on the data stream ✓.
- Handshake modification: the Finished check acts after key derivation – tampering changes the keys, so Finished fails ✓.
- Impostor: the certificate chain to a trusted root ✓.
- Full-handshake replay: the fresh randoms make the derived keys differ, so Finished fails ✓.
- Encrypting without authenticating: a private channel to the wrong machine ✓.
- HTTPS makes the channel private and the server identified – the content can still lie ✓.