Aalto University

Network Security: TLS 1.3 security properties

Tuomas Aura, Aalto University

CS-E4300 Network security

TLS 1.3 full handshake

1. C → S: N_C , supported_versions, supported_groups, signature_algorithms, cipher_suites, server_name, certificate_authorities, g^x
2. S → C: N_S , version, cipher_suite, g^y
   EncryptedExtensions
   $Cert_S$, $Sign_S(TH)$
   $HMAC_{Kfks}(TH)$
   } encrypted with K_{shts}
3. C → S: $Cert_C$, $Sign_C(TH)$
   $HMAC_{Kfkc}(TH)$
   } encrypted with K_{chts}

Which security properties?

- Secret, fresh session key
- Mutual or one-way authentication
- Entity authentication, key confirmation
- Perfect forward secrecy (PFS)
- Contributory key exchange
- Downgrading protection
- Identity protection
- Non-repudiation
- Plausible deniability
- DoS resistance

$Cert_C$, $Cert_S$ = certificate chain

TH = transcript hash i.e. hash of all previous messagas

Exchange keys K_{chts}, K_{shts}, K_{fkc}, K_{fks} session keys K_{cats}, K_{sats} derived from g^{xy} and TH

Identity protection?

- Client sends server name indication (SNI) and CAs in plaintext
  - SNI needed to have multiple server names at one IP address
- Server certificates are encrypted against passive sniffing
  - However, anyone can get them from server by connecting to it and sending the right SNI
- Client certificates (if used) are encrypted
  - Protected also against server impersonation

Summary: server identity leaked; client identity well protected