Lecture 7

Tuesday, 6 December 2022 15:31

Confidentiality
integrity
authenticity
unforgeability → message must be actually sent (think of (un)deniability)

in the real world, we usually have CIA in a 'private conversation'-setting

but such a conversation is deniable → not always desirable

message authentication code:

both parties have same key

incoming message has valid MAC ⇒ comes from communication partner (since it does not come from myself)

both parties could have generated MACs

ephemeral keys: short-lived keys, for one communication

forward secrecy → secrecy maintained even if keys compromised

OTR: off the record (messaging over XMPP)

have separate keys for encryption & signing ($k_{sign} = hash(k_{enc})$)

delete DH 'keys' when you don't need them anymore

'leak' signing key later on to establish deniability

uses AES in counter mode

forward secrecy | compromise | backward secrecy

pre-compromise secrecy | post-compromise secrecy

identity-misbinding attack

$A \to E: g^x, sign_{skA}(g^x), pk_A$

$E \to B: g^x, sign_{skE}(g^x), pk_E$

$B \to E: g^y, sign_{skB}(g^y), pk_B$

$E \to A: g^y, sign_{skB}(g^y), pk_B$

Alice is talking to 'Bob'
Bob is talking to Eve

breaks authenticity

OTR v_2: ties ephemeral public key to party

users must use an out-of-band channel for authentication

socialist millionaires protocol: check equality of two values without revealing either of those values

multi-party OTR: roughly the same as pairwise OTR

but:

encryption with group key shared in entire group

signing with ephemeral signing keypair

shutdown phase: send hash of all messages to other group members; 'leak' signing key for deniability

Silent Circle instant message protocol (now discontinued, but forms a building block for Signal)

↳ sometimes outputs SAS = short authentication string

which should be compared out of band

anybody can claim to have had a conversation with Bob

Signal:

combine DHE ratchet (OTR) with hash-ratchet (SCIMP)

ratchet = forward secure key update

avoid pre-advertisement of new key shares (first sending a MAC over shares)

authenticate keys by mixing in previous authenticated keys

sending chain

receiving chain

initial root key authenticated with public keys of participants

Signal provides:

- authenticity
- forward secrecy
- deniability
- confidentiality
- integrity