Unknown Key Shares in SDP

draft-thomson-avtcore-sdp-uks-00

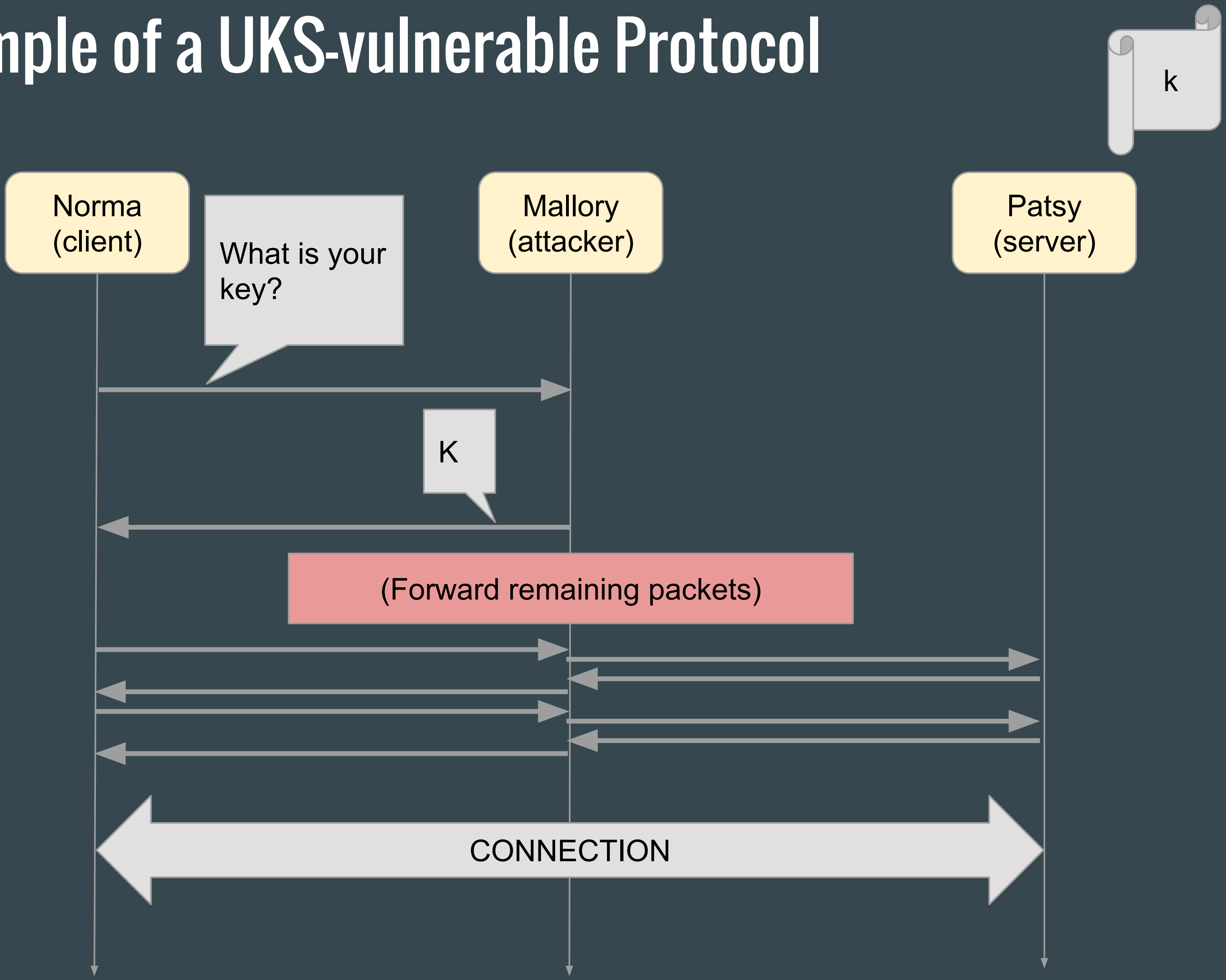
Unknown Key Share

An attack where there is a confusion about the identity of peers

SIGMA paper calls this an “identity-misbinding attack”

Happens when the session keys are bound to different identities by each peer

Example of a UKS-vulnerable Protocol



DANE Example

Mallory (attacker) advertises a TLSA record with public key K

The corresponding private key is owned by Patsy (not Mallory)

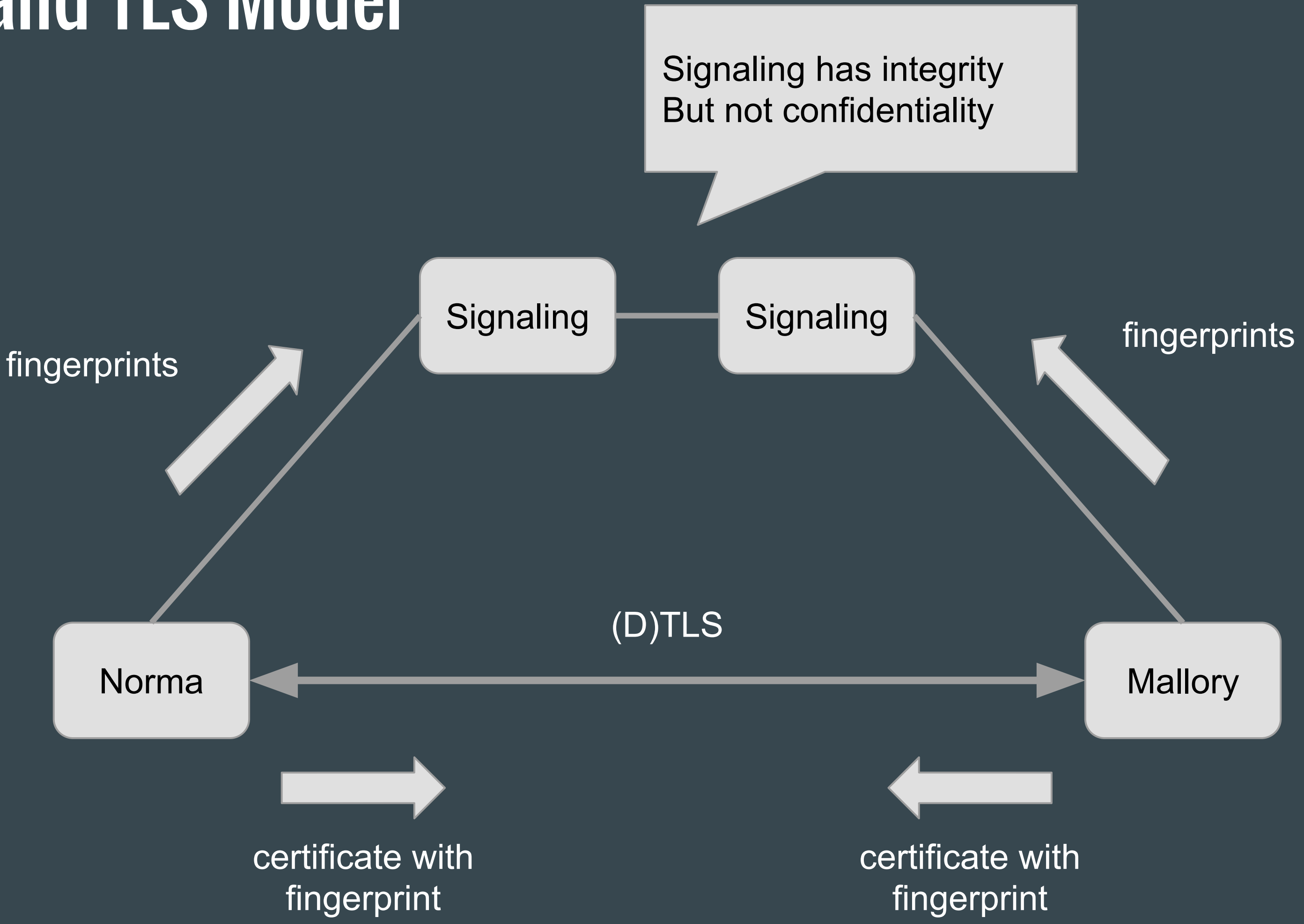
Norma attempts to connect to Mallory

Mallory forwards connection to Patsy

Norma validates the connection using K [RFC 7671, Section 5.1]

Norma is talking to Patsy, but thinks they are talking to Mallory

SDP and TLS Model



Signaling has integrity
But not confidentiality

Attack on SDP

>= 2 concurrent sessions

... from the same (honest) endpoint

... at the same time

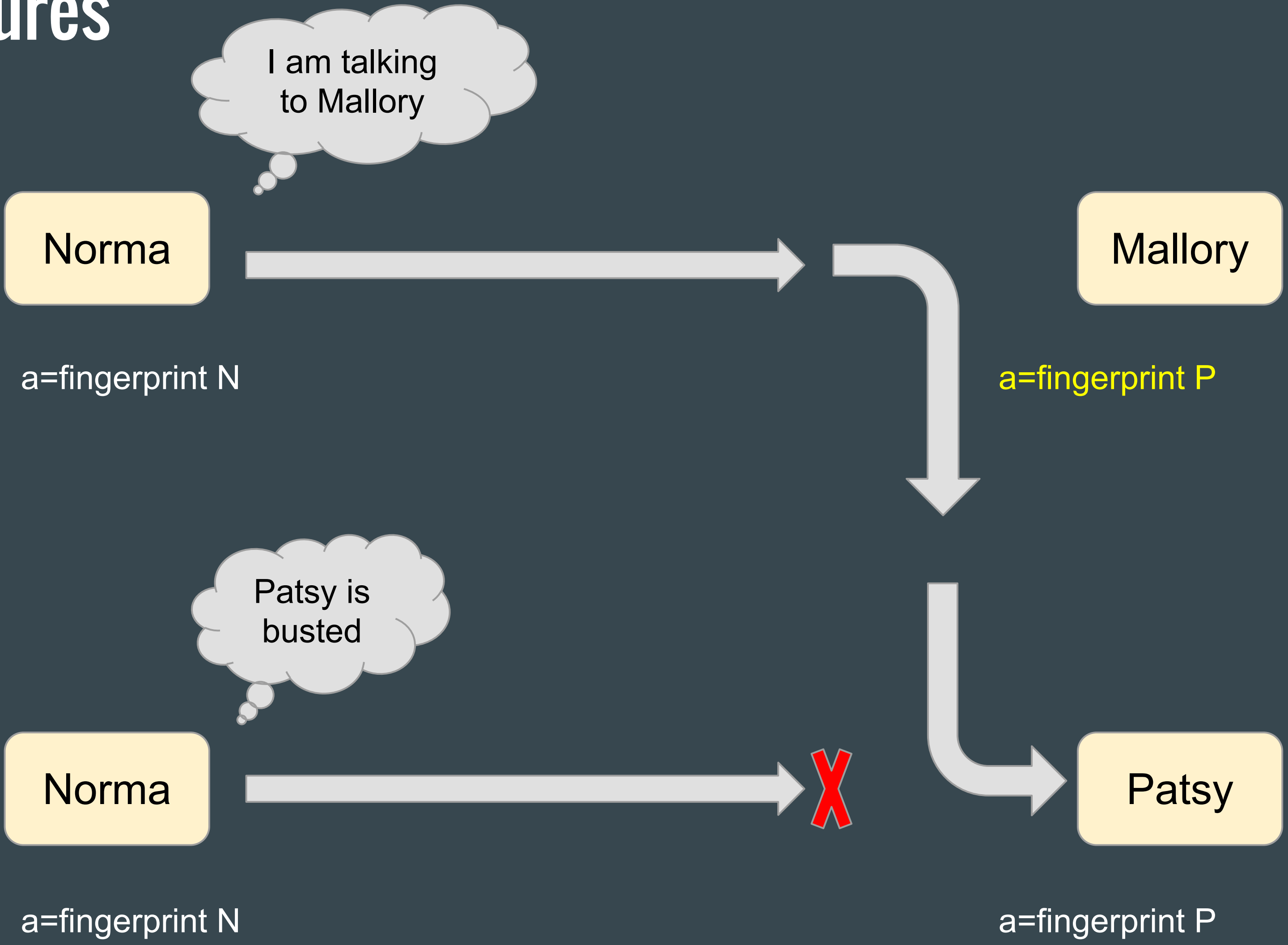
... with the same key.

An attacker can switch a session toward them

... with any other active session toward the same peer.

Produces a session where the victim thinks they are talking to the attacker, but they are talking to someone else.

Pictures



I am talking to Mallory

Norma

Mallory

a=fingerprint N

a=fingerprint P

Patsy is busted

Norma

Patsy

a=fingerprint N

a=fingerprint P

Conditions

Victim needs two concurrent sessions with the same key

Attacker copies a=fingerprint from other session into their SDP

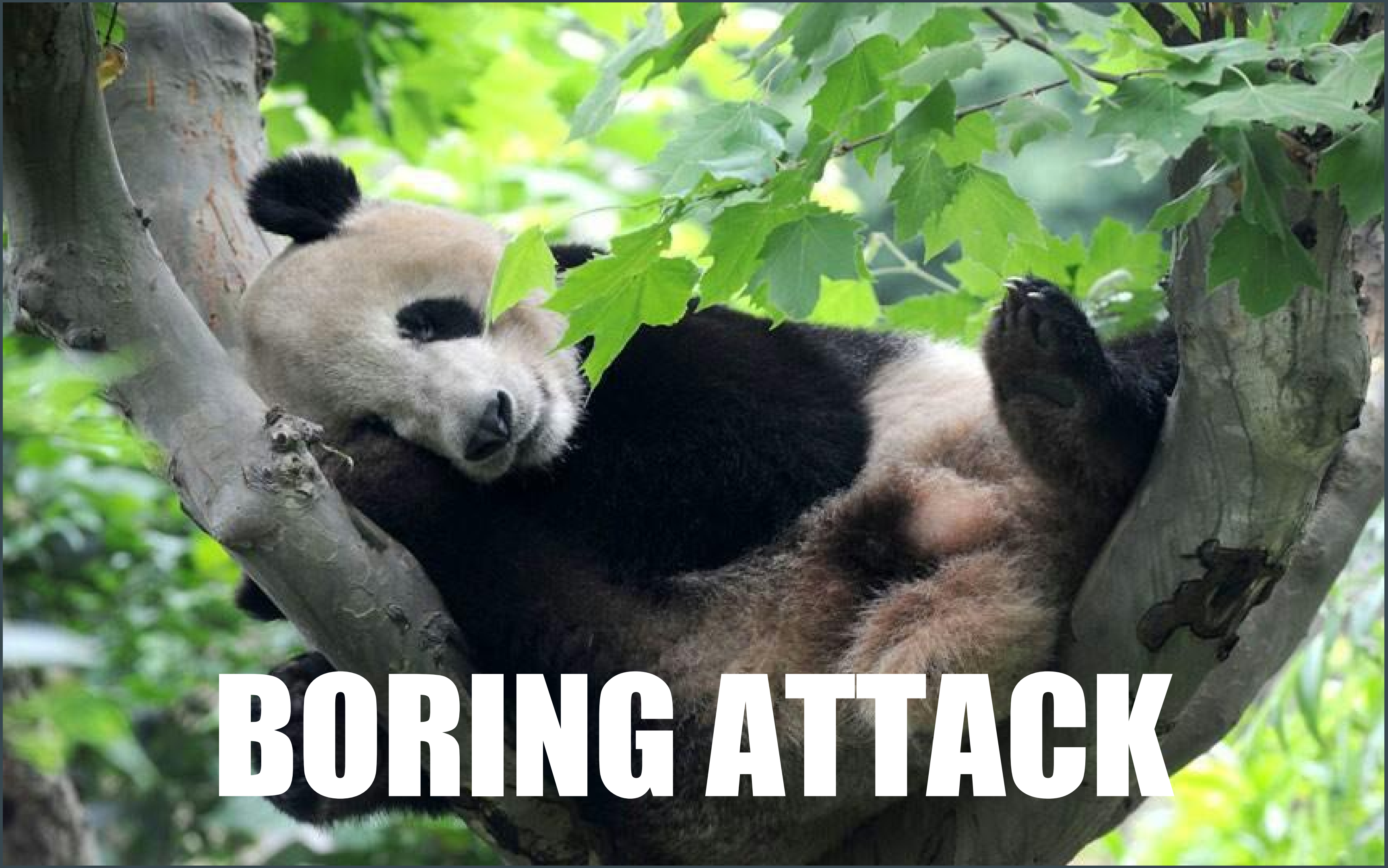
Needs to know *of* victim

Needs to knows a=fingerprint from victim

Attacker needs to forward (D)TLS to the (other) victim

Needs to know transport parameters for victim

Attacker maybe needs to block session between the two victims


BORING ATTACK