Secure Systems Group, Aalto University

Mariam Moustafa, Mohit Sethi, Tuomas Aura

Formal models of key exchange with raw public keys

Work in progress

Background

- **TLS with self-signed certificates** and **TLS with raw public keys** [RFC7250] are alternatives to a PKI for smart objects. They require out-of-band public key distribution.
- **Pre-shared public keys** can be manually distributed by the administrator between the TLS client and server.
- **DNS-Based Authentication of Named Entities (DANE)** [RFC7671] distributes raw public keys or self-signed certificates via secure DNS.

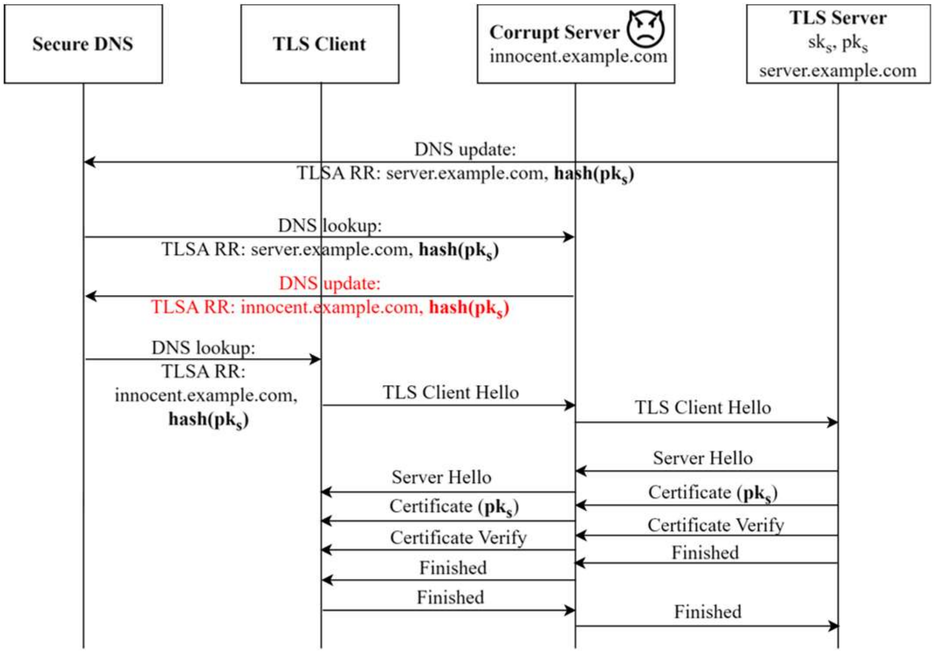
DANE

DANE introduces a new resource record, TLSA RR, which binds the public keys of TLS endpoints to their domains. The RR typically contains a public key hash.

Our work

- Analyze the security of TLS with raw public keys or self-signed certificates, using DANE or pre-shared public keys.
- Model the protocol in applied pi calculus and verify with ProVerif.

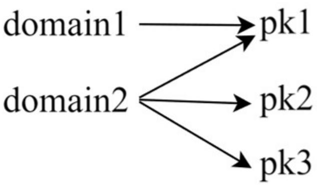
Attack 1



The client is tricked into communicating with an unintended party. This is a misbinding attack.

Attack 2

- Similar attack can happen **without attacker updating DNS** due to the possible many-to-many relation between domains and public keys.



Solutions

1. Client sends **Server Name Indicator (SNI)** in Client Hello and the server checks the value.
2. Server uses **self-signed certificate** and client checks the subject name.

In both solutions, the client and server agree on the server name in the transcript hash of the TLS Finished message. The TLS 1.3 standard should be updated.

Aalto University