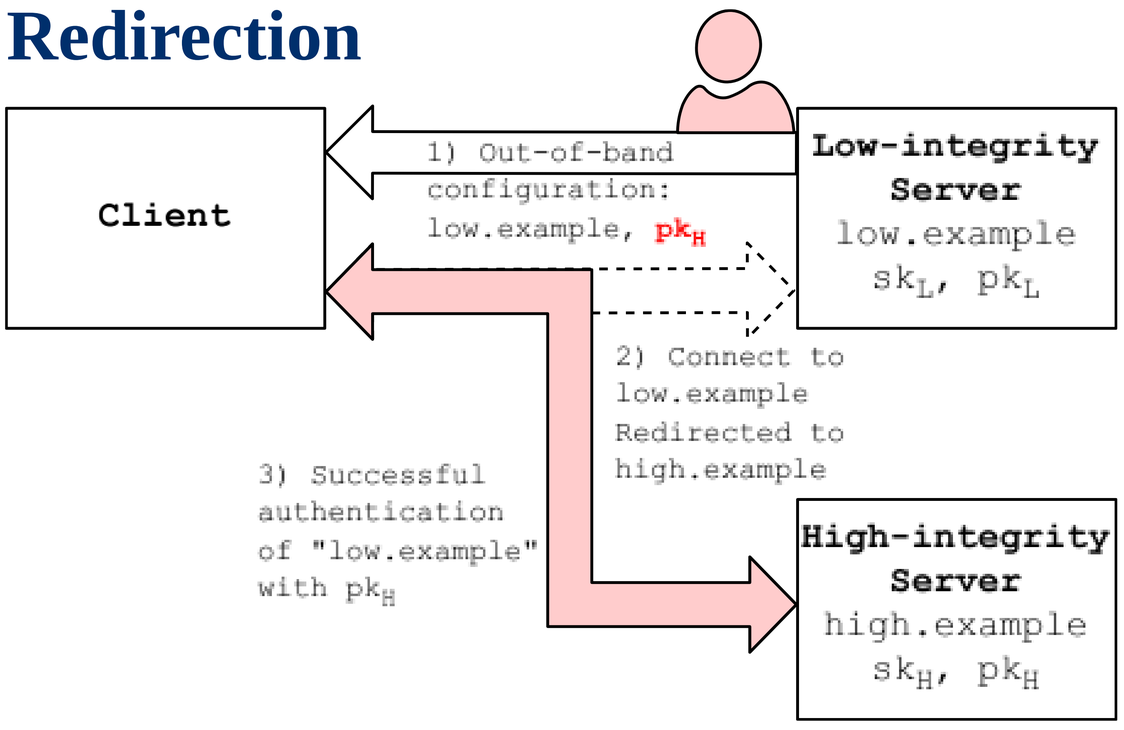
Secure Systems Group, Aalto University

Mariam Moustafa, Mohit Sethi, Tuomas Aura

Attacks on Key Ownership in Common Security Protocols

Work in progress

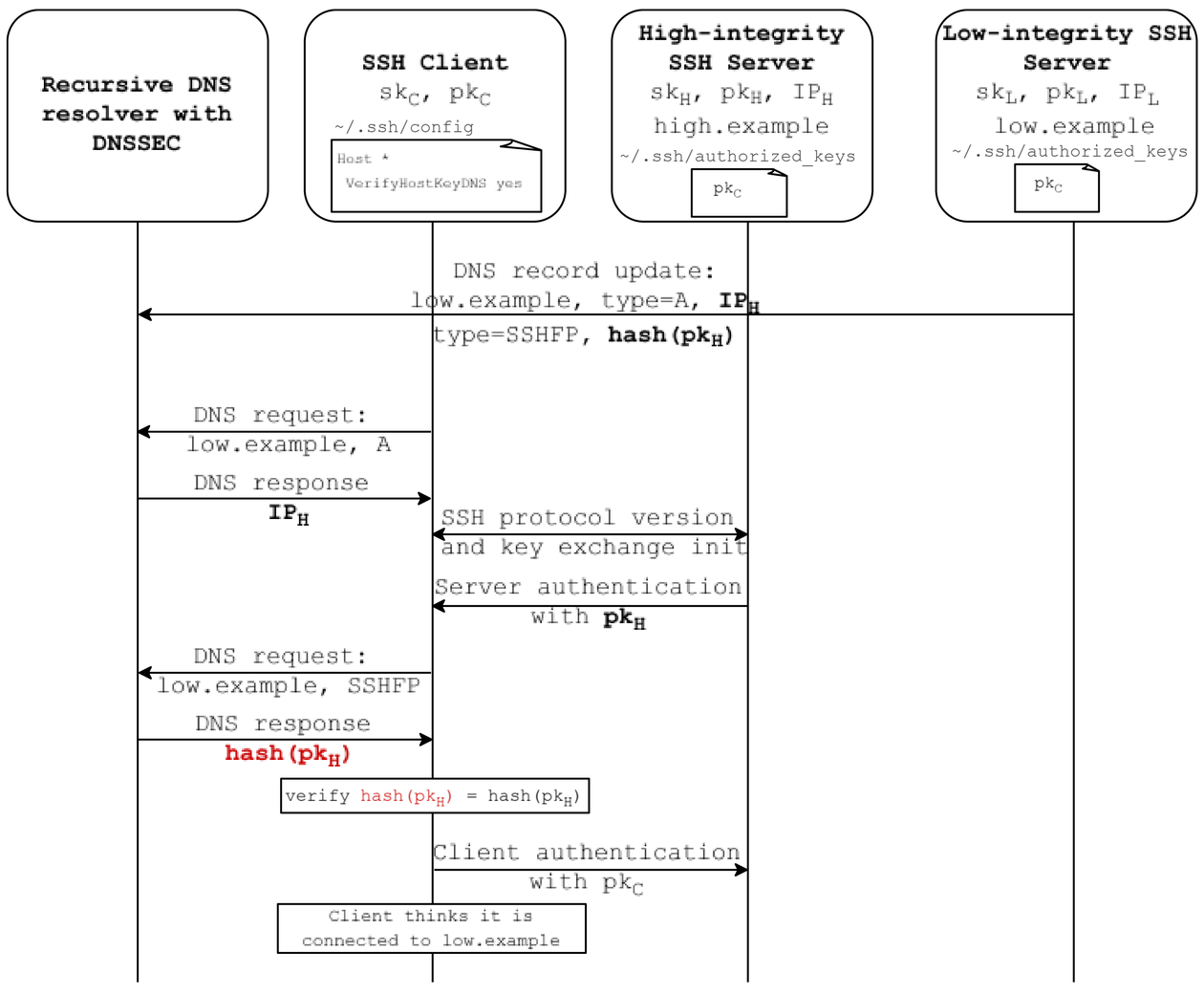
Redirection



DNSSEC-based authentication

- Out-of-band distribution of public keys via secure DNS
- SSHFP Resource Record (RR) binds public key fingerprint of SSH server to its domain
- IPSECKEY RR binds the raw public key of the IPsec endpoint to its domain
- TLSA RR binds the public keys of endpoints to their domains. The RR typically contains a public key hash.

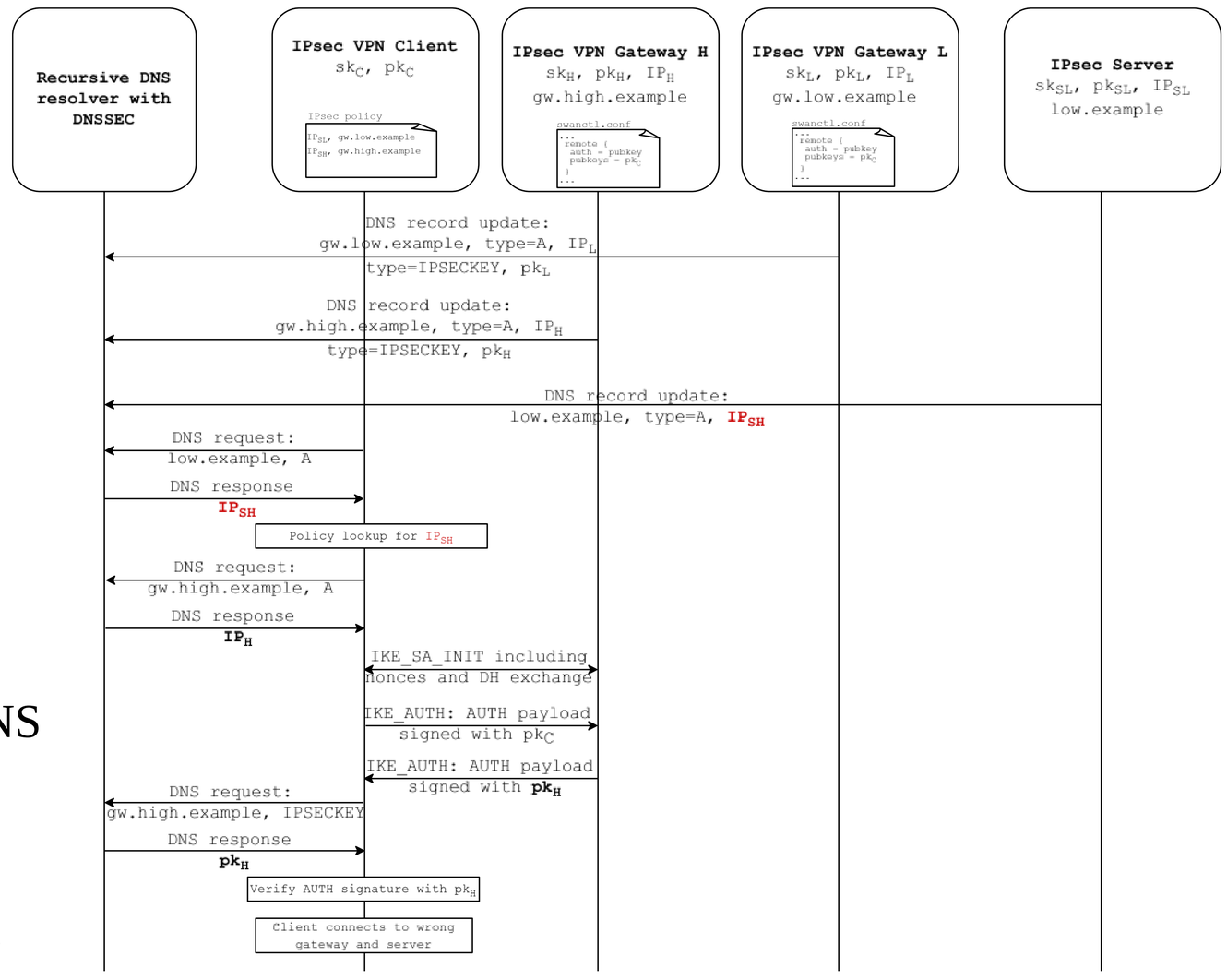
Redirection vulnerability in SSH



Client is tricked into communicating with a different server

Tested the attack with SSH, Git, and SFTP

Redirection vulnerability in IPsec



Tested the attack with strongSwan IPsec-based VPN

Redirection vulnerability in TLS RPK

- **TLS with raw public keys** [RFC7250] is a possible alternative to a PKI for smart objects.
- The Certificate message in TLS contains only the public key object as opposed to the full X.509 certificate
- **low.example** adds the public key hash of **high.example** as its own
- **Tested the attack with CoAP and SMTP**

Solutions

The endpoints should know and check each other's identities.

1. Proof of key ownership at registration
2. Identity validation during protocol handshake
3. Self-signed certificate for client to validate
4. Application-layer identity validation
5. Unique client credentials for every server

Some of the protocol standards being updated are addressing our findings.

Aalto University

Contact: {firstname.lastname}@aalto.fi