Sécurité des Applications

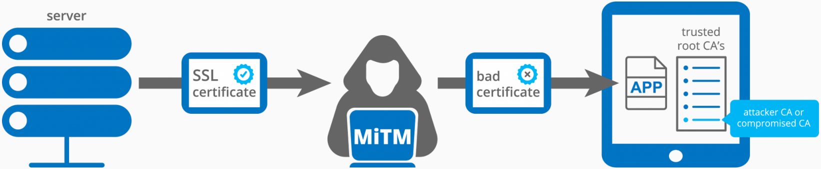
Certificate Pinning

Stéphane Küng

December 1, 2020

Certificate Pinning

Normal TLS Connexion



mailapurvpandey

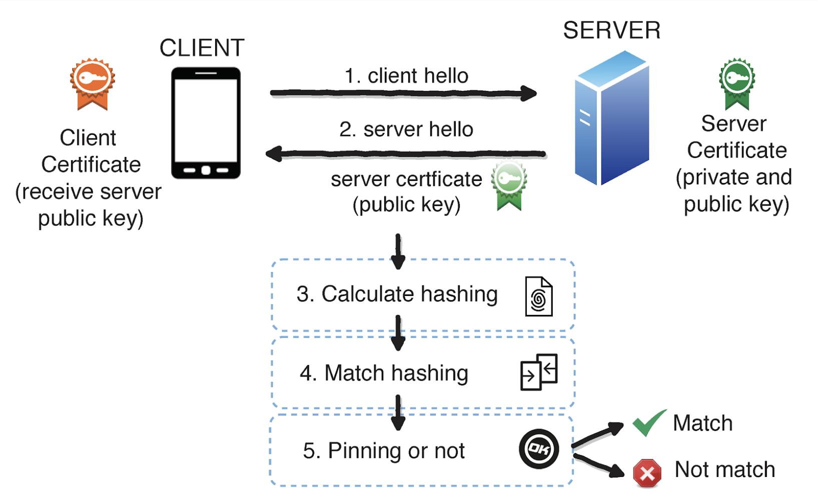
Where an attacker

- On the same network (Spoofing)
- Proxy Server
- Router

What an attacker can do

- Inspect data
- Modify Data
- . . .

What is Certificate Pinning ?


CLIENT
SERVER
Client Certificate (receive server public key)
1. client hello
2. server hello
server certficate (public key)
Server Certificate (private and public key)
3. Calculate hashing
4. Match hashing
5. Pinning or not
OK
Match
Not match

What can we pin

- Full Certificate (Cert or Hash)
- Public Key Information (subjectPublicKeyInfo)
- Public Key

OWASP

What Certificate

- **Default**: Any from local trusted CA
- Leaf Certificate
- Intermediate Certificate
- Root CA

How to

- **Adnroid** : TrustManager, OkHttp and CertificatePinner, TrustKit Android library
- **iOS** : TrustKit
- **.Net** : `ServicePointManager`

What can go wrong

- Blocking all access
    - Key compromise
    - Renewal
    - Revocation