TLS Identity Pinning

ICANN 71 DNSSEC workshop

Yaron Sheffer, Daniel Migault

What do we use TLS for ?

TLS is used to establish a **confidential** channel with an **authenticated peer**.

- The TLS client must make sure the other end point is the **expected** TLS server.
- The TLS client may be authenticated which does not improve TLS server authentication
- Once authenticated the TLS client can start communicating with the TLS server:
  - login / passwords
  - EPP

Making sure the other peer is THE server ?

Current solution is based on Certificate.

- The TLS server provides a X509 certificate that binds www.example to the key K.
- The TLS client trusts the binding if it is signed by:
  - a trusted CA
  - an entity trusted by the trusted CA

How trusted can be the CA?

- web browser have ≈ 75 CAs (Chrome, Firefox).
- Certificate issuance is based on domain names ownership 2019-02 DNSpionage...
- CA get breached, Certificate Authorities - The Weak Link of Internet Security...

"Server-side 2FA" complements certificate authentication

Certificate pinning ensures future TLS sessions happen with the **same** certificate

- What if my certificate is re-issued ?
  - OK, so let's just pin the CA so future TLS session happen with the **same** CA
    - What if I am changing CA ?
      - OK, operationaly too complex!

We need so pin to the **server's identity**, independent of any certificate

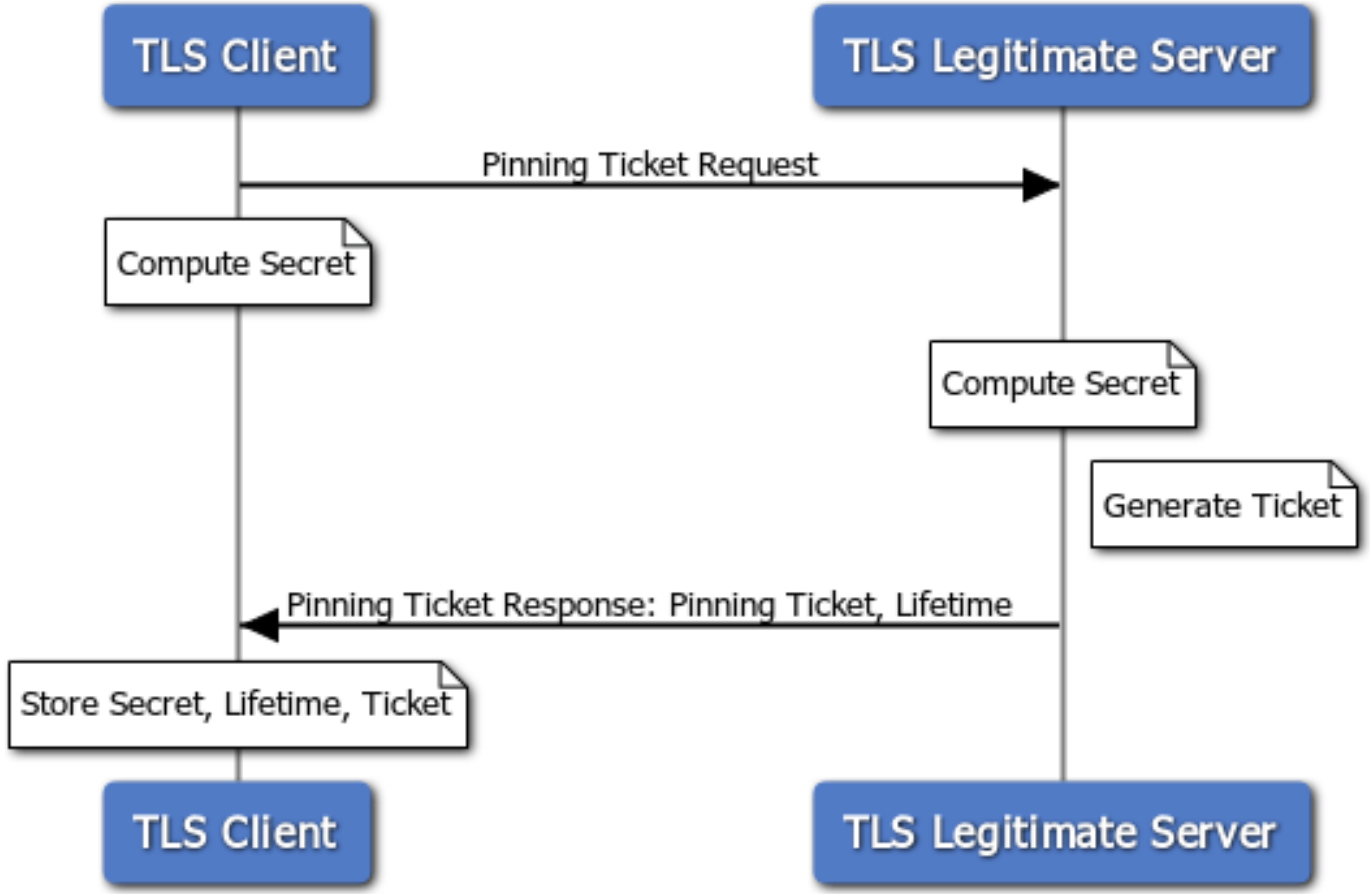
Identity

Principle:

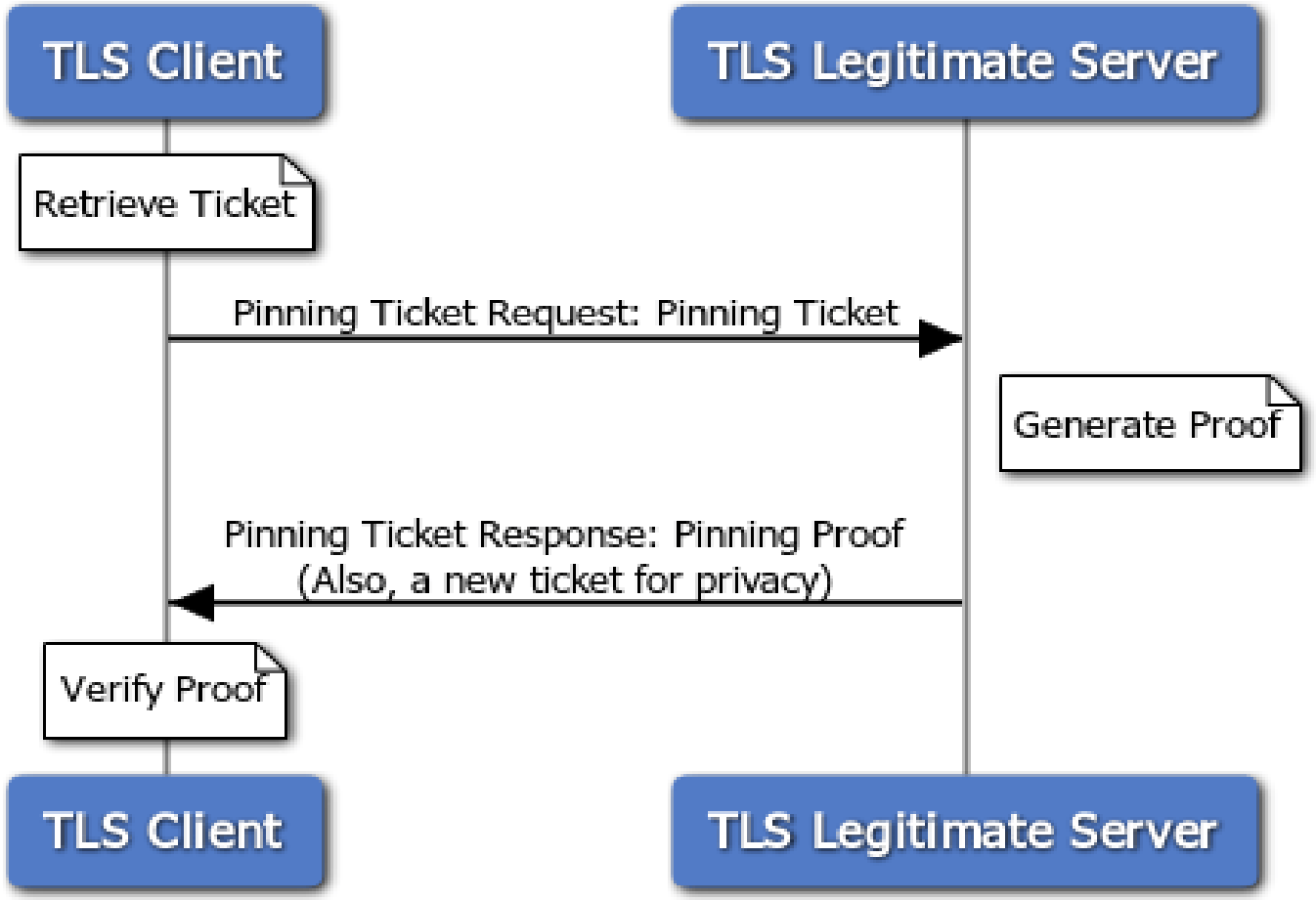
- Establish a First TLS session with a TLS server
- Ensure the next session is established with the same TLS server
  - **same** : proving the knowledge of a secret associated to the previous TLS session

A good fit for enterprise-internal deployments, where Certificate Transparency is not used

Initial Exchange



Subsequent Exchange



Advantages:

TLS-only and works with any protocol on top of TLS

Zero management on the TLS client side

Orthogonal to TLS certificates (not a replacement!)

Very good fit for B2B secure communications

Resources

Blog: Identity Pinning: A New Approach to Certificate Validation, October 2019

- URL: https://yaronf.svbtle.com/identity-pinning

RFC 8672: TLS Server Identity Pinning with Tickets, October 2019

- URL: https://www.rfc-editor.org/rfc/rfc8672.pdf

PoC: mint - A Minimal TLS 1.3 stack

- URL: https://github.com/yaronf/mint