TLS Server Identity Pinning

draft-Sheffer-identity-pinning

Yaron Sheffer – Daniel Migault

Problem Statement

With miss-issued or fake certificates, a TLS client may establish a secure TLS session with attacker rather than the TLS Legitimate Server.

Both Client and Server are victims of impersonating attacks.

- TLS Client believes it is connected to the TLS Legitimate Server
- TLS Legitimate Server cannot detect it is being impersonated
- TLS Client cannot detect it has been a victim.

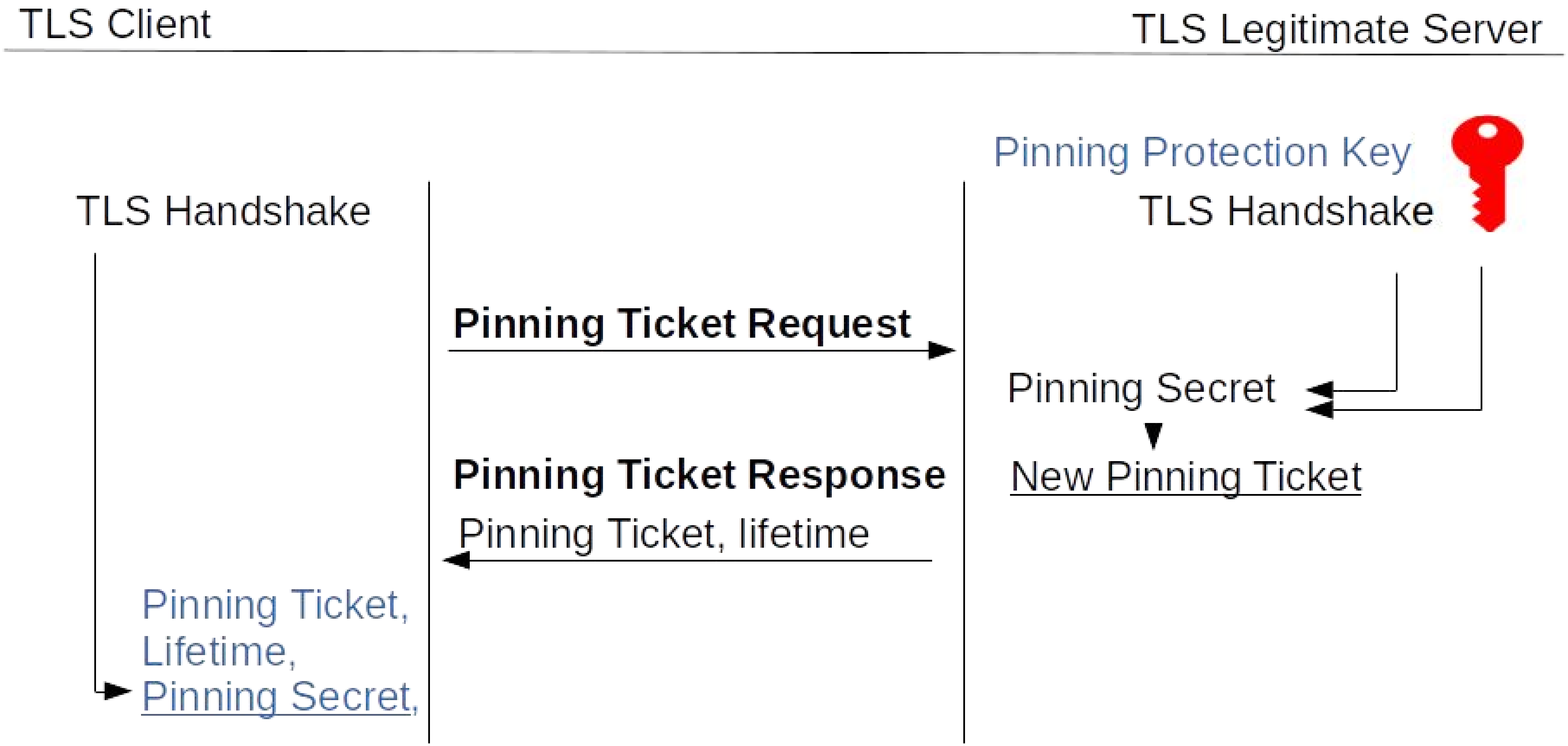
TLS Server Identity Pinning

TLS Server Identity Pinning is a TLS1.3 extension that performs a second

factor authentication and ensures:

- TLS Client establish TLS sessions with the same TLS Server Identity
- TLS Legitimate Server serves TLS Client whose previous session has not been impersonated.
- It is a Trust On First Use (TOFU) mechanism

TLS Server Identity Pinning – Initial Exchange



TLS Client

TLS Legitimate Server

Pinning Protection Key

TLS Handshake

TLS Handshake

Pinning Ticket Request

Pinning Secret

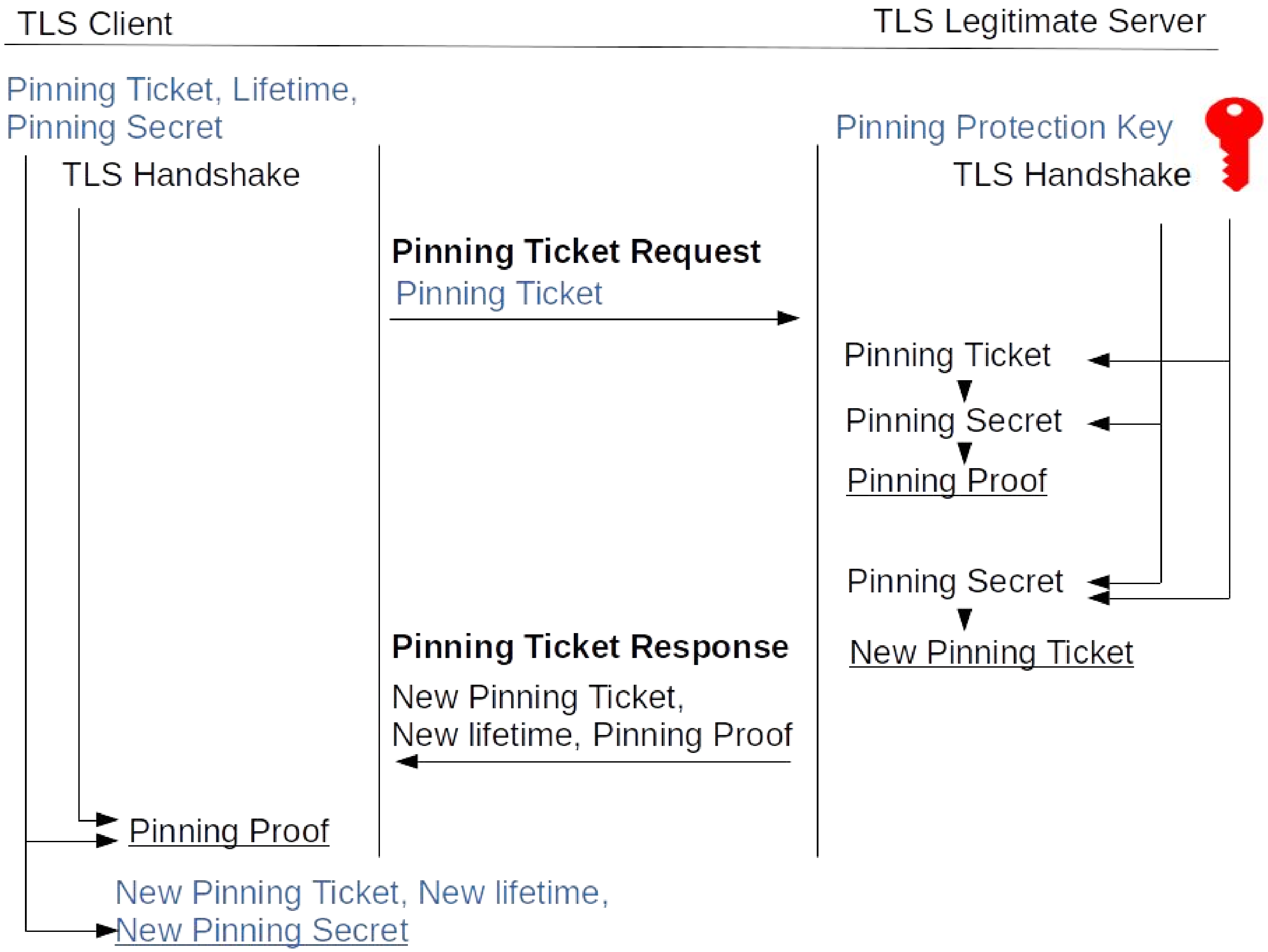
New Pinning Ticket

Pinning Ticket Response

Pinning Ticket, lifetime

Pinning Ticket,
Lifetime,
Pinning Secret,

TLS Server Identity Pinning – Further Exchange



Thanks!

(Backup)

Comparison with HPKP - Similarities

Pinning Identity and HPKP are TOFU mechanisms addressing the same problem in very different ways and can be seen as complementary:

- Pinning Identity is a second factor authentication
  - HPKP uses HTTP to configure or activate policies of the TLS primary authentication
- Pinning Identity can be enabled for any application layer
  - HPKP is focused on HTTP

Pinning Identity and HPKP are a hard fail mechanism

- … but with considerably lower risks

Comparison with HPKP - Advantages

While HPKP seems to be progressively abandoned because of operational and hard failure, Pinning Identity provides the following operational advantage:

- Pinning Identity is independent from key roll over, CA changes
- Pinning Identity requires less constraints for the Pinning Protection Key
    - Pinning Protection Keys are ephemeral vs long term backup keys.
        - backup has less constraints in term of isolation
        - frequent rotation involve frequent storage procedure
        - … but backup procedure needs also be tested
- Pinning Identity has a in-band monitoring and error reporting:
    - Verification is performed by the server and errors quickly detected.
    - Note -- there is still room for client reporting fake proof returned by a attacker
- Pinning Identity can be completely automated and does not require manual operations.
-

Comparison with HPKP - Attacks

HPKP Footgun: The key used for the primary authentication is rolled over

- Pinning Identity is not impact par any certificate operation.
- Pinning Protection Key may also be rolled-over:
  - Roll-over is independent with very limited side effect
  - Continuous monitoring makes error to be detected in real time
  - Roll over is completely automated

HPKP Suicide attack: All Keys are wiped from the server

- The use of ephemeral key makes backup procedure easier to test.

HPKP Ransom: A rogue servers rotates the key while keeping the ransom key remotely

- TLS processes are expected to have attack surface that http with more user interactions.
- Pinning Identity has no backup key, it cannot be used for ransom.
- Damages would be similar but with less reward