Certificate Transparency for Signed Executable Software

Dacheng Zhang

IETF 90

Use Case 1

- Digital signatures are commonly used for software distribution
- A valid digital signature gives a user reason to believe that the software was created by a known vendor
- If the verification of signature relies on PKI, then it suffers from the same issues mentioned in Certificate Transparency
- CT can help detect the adversaries impersonating a legal company to distribute software

Use Case 2 (1)

- It is hard for a vendor to prove there are no backdoors in their devices.
- By publishing the signature of firmware, it is possible to convince a customer that:
  - There is no backdoor particularly make for the customer, the firmware it uses is identical to other customer used all over the world
  - If there are drawbacks or backdoors in the firmware, it might have been detected by other customers which are good at security

Use Case 2 (2)

- It is possible for a customer to verify the integrity of software after the deployment

Operations

- The owner of software (or a trust third party) generates a certificate with its private key. The certificate should include:
  - Binary of the software/ hash of the Binary (Optional)
  - Information identifying the software (should include version information and appended patches)
  - Owner's name
  - Issuer's name
  - Signature
  - ……

End