IETF 105 TLSWG

Delegated Credentials

R. Barnes, S. Iyengar, N. Sullivan, E. Rescorla

draft-ietf-tls-subcerts-04

Changes in -04

Add proposed TLS extension text for IANA #23

Using delegated credentials with client certificates #13

Running Code Update

Running on kc2kdm.com with 7-day Delegated Credential and Digicert Certificate

Patch for server-side landed in BoringSSL

Patch for client-side landed in NSS

Can be enabled with a preference flag in Firefox nightly

Open Issues

Time to cut ties with LURK? #30

PSS #28

Point to Formal Analysis #31

Consider changing name from "Delegated Credentials" to "Delegated Signing Keys"

Cut ties with LURK

Proposal:

Replace text referencing LURK I-D with generic remote signing mechanism

PSS

Proposal:

Explicitly prohibit PKCS#1 v1.5 signatures in DelegatedCredential.algorithm

Formal Analysis Outline

We want to prove:

1. That DCs do not weaken the current PKI
2. That they strengthen the current PKI

Cheval et al. define a formal set of requirements for a PKI to be secure.

Proof methodology: by-hand proof.

Secure Composition of PKIs with Public Key Protocols, Cheval et al. [1]

Cheval et al. define a set of requirements on PKIs and Public Key Protocols that when used together are secure (i.e. meet the security requirements they set out).

Proof Sketch:

1. Assume that the current PKI is secure*
2. Prove that DC meet the requirements of a secure Public Key Protocol
3. Prove that PKI+DC meets the requirements of a secure PKI
4. Stretch Goal: Prove that any flaw that exists in PKI+DC also exists in the underlying PKI

[1] Vincent Cheval, Véronique Cortier, and Bogdan Warinschi. "Secure composition of PKIs with public key protocols." *2017 IEEE 30th Computer Security Foundations Symposium (CSF)*. IEEE, 2017.

Consider changing name from "Delegated Credentials" to "Delegated Signing Keys"

Motivation:

Delegated credentials do not have the ability to modify anything about the properties of the certificate’s credentials other than:

- Signing key
- Narrowing validity period

Getting to Last Call

Two options

- Begin last call process alongside formal analysis
- Wait for formal analysis to be complete

Questions?

IETF 105 TLSWG

Delegated Credentials

R. Barnes, S. Iyengar, N. Sullivan, E. Rescorla

draft-ietf-tls-subcerts-04