Server ID Checking (draft-saintandre-tls-server-id-check)

Apps Area, IETF 76

I-D by P. Saint-Andre, K. Zeilenga, J. Hodges, R. Morgan
Presentation by Peter Saint-Andre

Context

- Many application protocols use TLS with X.509 certs (HTTP, IMAP, LDAP, XMPP, etc.)
- Each protocol defines its own rules for checking the ID of the application server
- Much commonality across protocols, but also subtle differences
- Goal: abstract a set of common rules

Scope

- Talking about application servers that function as TLS servers
- How an application client checks the identity of an application server
- Out of scope:
  - Mutual auth (server checks client)
  - End-to-end (client checks client)

What is Identity?

- Domain name
- Machine name? (cf. RFC 4985)
- IP address
- URL/URI?
- MAC?
- Other?

Basic Process

- Presented identity = an identity presented by the server to the client in a certificate
- Reference identity = the expected identity of the server as provided by a user
- During TLS negotiation, check reference identity against each presented identity
- Success on any match

Rules (1)

- Rules vary by identity type (domain name, IP address, etc.)
- E.g., to check IP address type, convert the reference identity and presented identity to network byte order octet strings (4 octets for IPv4, 16 octets for IPv6) and verify that the strings are identical

Rules (2)

- Traditional domain name: compare the set of domain components using a case-insensitive ASCII comparison
- Internationalized domain name: more complex (see I-D)
- Fallback to Common Name if preferred subjectAltName extensions (dNSName and SRVName) are not presented

Open Issues

- Include client checking in this I-D?
- Include fingerprint matching?
- Include non-X.509 certs, keys, etc.?
- Expand beyond TLS? (IPsec, DTLS, etc.)
- Allow wildcard "*" in reference identity?
- Other?