Representation and Verification of Application Server Identity (draft-saintandre-tls-server-id-check-03)

IETF 77

Peter Saint-Andre

Problem Statement

- Many client-server technologies use TLS (HTTP, IMAP, LDAP, SIP, SMTP, XMPP, etc.)
- Client needs to verify identity of the server to which it connects
- Each application protocol defines slightly different rules for identity verification
- No guidance regarding certificate issuance

Goals

- Define secure practices for authentication of a server in client-server applications
- Provide guidance to:
  - Certificate issuers
  - Application client developers
- Might also be helpful to server developers, operators, etc.

What is a "Server"?

- This concept is still imprecise in the I-D
- Rough idea: the application or service that a client or user expects to interact with, e.g., "the IMAP server at example.com"
- Typically this is, or is based on, a domain name – can be represented in various ways (dNSName, SRVName, URI, CN, etc.)

Scope

- Define rules for representation (certificate issuance) and verification (client handling)
- Application servers only (not clients, not specific machines or IP addresses)
- TLS only (not IPsec, DTLS, etc.)
- PKIX only (not OpenPGP etc.)

Issuance Rules (1)

- Wildcard character "*"
  - Never allowed as fragment (e.g., foo*.example.com)
  - Can be allowed as the entire left-most label (e.g., *.example.com)
  - Application protocol must specify whether wildcard is allowed

Issuance Rules (2)

- If application technology uses DNS SRV records, cert should include SRVName
- Cert MAY include identity type of URI
- Cert MAY include other identity types (e.g., XmppAddr)
- If no SRVName, URI, or other identity type, must include dNSName

Issuance Rules (3)

- Use of Common Name (CN) discouraged
- Include only in leaf (left-most) position within the Relative Distinguished Name
  - Issue: is this too restrictive?
- Must not represent identity as a series of Domain Component (DC) attributes

Verification Rules (1)

- Gather reference identity from user or configuration (not automated resolution)
- OK to derive "securely" (e.g., DNSSEC)
- Iterate through all identities presented in server certificate
- If one presented identity matches reference identity, accept the cert

Verification Rules (2)

- Traditional domain name: case-insensitive ASCII comparison
- Internationalized domain name: follow rules in IDNA2003 or IDNA2008
- Check wildcard "*" only as left-most label
- Application protocol can disallow wildcards

Verification Rules (3)

- Check CN only if certificate does not contain dNSName, SRVName, URI, or other application-specific identity
- Ignore CN if not leaf RDN
- Ignore RDNs other than CN
- Are the foregoing rules necessary and sufficient?

Open Issues

- IDNA2003 vs. IDNA2008 – specify handling of both, or only IDNA2008?
- Allow CN as other than leaf RDN?
- Restore text about secure derivation of identity via DNSSEC, host table, etc.
- Add text about using dNSName only if server will never be manually configured

Next Steps

- Submit -04 ASAP
- Solicit feedback from certification authorities, application developers, operators, security experts
- Discussion venue: certid@ietf.org