Checking Certs in XMPP

Matt Miller

IETF 87 - Berlin

XMPP in a Nutshell

- Application-level asynchronous XML router
- Client-server architecture
- Distributed servers
- Discovery via DNS SRV
  - IN SRV _xmpp-client._tcp.shire.example 0 0 5222 hosting.example.net
- Addressing similar to email
  - bilbo.baggins@shire.example

XMPP Deployment

- Lots and lots of client implementations
- Lots of server implementations
- Lots of individually hosted services
- Several multi-tenant services

What is Multi-Tenant?

- One service → hosting.example.net
- Multiple domains
  - shire.example
  - rivendell.example
  - mordor.example
- Domains owned by **different organizations**

TLS in XMPP

- STARTTLS
  - Start connection unencrypted, upgrade to TLS
  - Addressing in plain hints at requested domain
- Verification process
  - PKIX end entity certificate
  - Signed by CA
  - Chains to established trust anchors
  - Contains proper identifier

TLS Identifier

- Clients/Servers talk to *domains*, **not** *services*
  - ✓ shire.example
  - ✗ hosting.example.net
- RFC 6125
  - Service names (_xmpp-client._tcp.shire.example) [srvName]
  - Domain names (shire.example) [dnsName]
  - Wildcards (*.shire.example) [dnsName]
  - XMPP addresses (shire.example) [id-on-xmppAdr]

How Multi-Tenant Falls Down

Trusted Issuance

✓ PKIX end entity certificate

✓ Signed by CA

✓ Chains to established trust anchors

✗ Contains service identifier

Proper Name

✓ PKIX end entity certificate

✗ Not signed by CA

✗ No chain to established trust anchors

✓ Contains domain identifier

Why Multi-tenant Falls Down

- Liability
  - CAs won't issue cross-organization certs (e.g., "shire.example" to "hosting.example.net")
- Liability
  - Customers reluctant to provide private key to Hosts
- Liability
  - Hosts reluctant to retain customer private keys

Multi-Tenant Realities

- Service to Client – Just Trust Us
  - Most users manually accept cert (forever)
  - Some clients auto-accept cert!
- Service to Service – TLS optional
  - And often ***not*** negotiated
- No longer acceptable
  - Users starting to care
  - Operators starting to care

More Generalized

- Looking at other technologies …
  - SIP
  - IMAP
  - IdP (e.g., Persona, OpenID Connect)
- … a pattern seems to arise

Alternative #1
DNSSEC + DANE

- Secure delegation (SRV + DNSSEC)
  - Service name can be automatically accepted
- Trustworthy verification (DANE)
  - Certificate can be automatically accepted
- Requires infrastructure changes
  - Nameservers, resolvers, providers, libraries, operating systems, clients, servers, etc

Alternative #2
POSH?

- Secure delegation (HTTPS redirects)
  - Service name can be automatically accepted
- Trustworthy verification (HTTPS content)
  - Certificate can be automatically accepted
- Re-use existing infrastructure
  - HTTPS servers, static files
  - Clients and servers still need upgrading

DANKE!

References

- RFC 6120: XMPP – Core
  - < http://tools.ietf.org/html/rfc6120 >
- RFC 6121: XMPP – IM
  - < http://tools.ietf.org/html/rfc6121 >
- RFC 6122: XMPP – Address Format
  - < http://tools.ietf.org/html/rfc6121 >
- RFC 6125: Service Identity
  - < http://tools.ietf.org/html/rfc6125 >

References

- DNSSEC
  - < http://tools.ietf.org/html/rfc4033 >
  - < http://tools.ietf.org/html/rfc4034 >
  - < http://tools.ietf.org/html/rfc4035 >
- DANE
  - < http://tools.ietf.org/html/rfc6698 >
- POSH (WIP)
  - < http://tools.ietf.org/html/draft-miller-posh-00 >