TLS in XMPP

Peter Saint-Andre
APPS AREA / XMPP WG
IETF 88, Vancouver

XMPP Past

- 1999 (jabberd): SSL on separate port (5223), but no SSL port for server-to-server
- 2000: dialback for server-to-server verification, but unencrypted
- 2004 (RFC 3920): STARTTLS on port 5222, support required in clients and servers, TLS_RSA_WITH_3DES_EDE_CBC_SHA
- 2011 (RFC 6120): cipher MTI upgraded to TLS_RSA_WITH_AES_128_CBC_SHA

XMPP Present

- Most client-to-server connections TLS-protected (perhaps 90% or more)
- Many server-to-server connections TLS-protected but few authenticated (TLS+Dialback, not PKIX)
- Lack of knowledge about current state, how to configure servers correctly, etc.
- New "IM Observatory" at https://xmpp.net/ is helping to increase awareness

XMPP Future

- Updated guidelines and recommendations now published in draft-saintandre-xmpp-tls (covered in the following slides)
- Open "manifesto" to encrypt the public XMPP network, see https://github.com/stpeter/manifesto
- Test dates in early 2014, switchover to always-on channel encryption on May 19, 2014
- Also working on DANE/DNSSEC, POSH, key pinning, certificate transparency, etc.

SSL/TLS Versions

- SSLv2 = must not
- SSLv3 = must not
- TLS 1.0 = should not
- TLS 1.1 = may
- TLS 1.2 = preferred

Cipher Suites (1)

- Forbidden:
  - NULL
  - RC4
  - anything with less than 128 bits of security
- Preferred:
  - Cipher suites with forward secrecy, authentication, and 256+ bits of security

Cipher Suites (2)

- Currently recommended...
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- Note: these cipher suites are TLS 1.2 only (might also address TLS 1.1)

Open Issues / Next Steps

- Is opportunistic encryption truly OK as a fallback?
- Need to specify how TLS + Server Dialback works (Philipp Hancke volunteered to write XEP)
- What about multi-tenanted environments? (DNA/DANE/POSH)
- Cite general TLS guidelines where possible (i.e., draft-sheffer-tls-bcp) or make all-in-one document?
- Gain experience with TLS-only network in 2014

Software Configuration & Interfaces

- Servers and clients must provide options to require channel encryption, set acceptable TLS versions and cipher suites, etc.

- Show admin or end user the encryption and authentication status of a connection, the TLS version and cipher suite in use, details about the server certificate, etc.

- Warn about changes to server certificates

TLS Usage

- Unauthenticated connections are acceptable (i.e., "opportunistic encryption" = TLS+Dialback), but strong domain name associations connections are preferred (PKIX, DANE, POSH)
- TLS session resumption: use Session IDs (RFC 5246), not Session Tickets (RFC 5077)
- Compression optional (since XMPP is not subject to the CRIME attack), can use application-layer compression (XEP-0138 @ xmpp.org)