TLS Extension for out-of-band public key validation
draft-wouters-tls-dane-pubkey

Paul Wouters paul@xelerance.com
John Gilmore gnu@toad.com
Sam Weiler weiler@tislabs.com

July 28, 2011 - IETF81, Quebec City

Goal of the TLS extension

Goal of the TLS extension

- Allow alternative methods alongside [PKIX] for authenticating TLS server public keys.
- Avoid contradicting data with unused [PKIX] information (Expiry vs RRSIG/TTL, RRLabel vs CN=)
- Reduce TLS server key/certificate management for large scale vhost deployments
- Reduce size and latency of TLS handshake (Do not send unneeded [PKIX] blobs)
- Allow re-use of cached TLS credentials

Examples of out-of-band methods

Examples of out-of-band methods

- TLS public key authentication via DNSSEC with [DANE] (See draft-ietf-dane-protocol-08 Section 2.1.1. type 3)
- TLS public key via firmware/OS provisioning (signed updates)
- TLS public key authentication via [LDAP] with [Kerberos]
- TLS public key cached from previous traditional exchange
- TLS public key via DNSSEC chains without Internet connectivity (See draft-agl-dane-serializechain-01)

Current specification

Current specification

```
enum {
    oob_pubkey_list([TBD]) (65535)
  } ExtensionType;
```

```
struct {
        IdentifierType identifier_type;
        select (identifier_type) {
            case key_raw_pubkey: subjectPublicKeyInfo;
            case key_sha256_hash: SHA256Hash;
        } identifier;
    } PublicKey;

    enum {
        key_raw_pubkey(0), key_sha1_hash(1) (255)
    } IdentifierType;

    opaque subjectPublicKeyInfo<1..2^16-1>;

    opaque SHA256Hash<32>;

     struct {
        PublicKey public_key_list<1..2^16-1>
     } PublicKeyList;
```

Questions for TLS WG

TLS WG item?

Is this something the TLS WG is willing to take on as item?

Discussions for TLS ML

- How to handle error conditions (Always abort?)
- Should this document include a client name identification extension, similar to SNI to allow out-of-band pubkey authentication of the TLS client?
- Should the server ACK with its pubkey or an empty list?
- Current draft uses raw *subjectPublicKeyInfo* or *SHA256 hashes*. Do we need others?
- Did we miss any Oracle attacks or privacy leaks if there is a MITM attack?