TLS – Cached Information

Stefan Santesson

AAA-sec.com

Approach

- To allow cached information to be replaced with its hash in the handshake protocol
- Client provides hashes over cached data in Client Hello
- Server acknowledge in Server Hello
- Finished message calculated over actual exchanged data

Syntax

```
enum {
     certificate_chain(1), trusted_cas(2), (255)
} CachedInformationType;

struct {
     HashAlgorithm hash;
     opaque hash_value<1..255>;
} CachedInformationHash;

struct {
     CachedInformationType type;
     CachedInformationHash hashes<1..2^16-1>;
} CachedObject;

struct {
     CachedObject cached_info<1..2^24-1>;;
} CachedInformation;
```

Conventions

- Only hashes over one object in each CachedObject
- Server responds with a cached_information extension with empty extension_data
- Server replaces accepted cached data with one of the hashes provided by the client

Design goals

- Allow the server to decide whether to replace cached data or not when the data is about to be exchanged (not when sending the Server Hello)
- Provide unambiguous information to the client whether information has been replaced or not

Issues to resolve

- Proposals to add conventions that reduce the risk of a client mistaking a hash for real data or vice versa
- It remains to be demonstrated that current draft does not provide adequate functionality

Way forward

- Are we done?