TLS – Cached Information

Stefan Santesson
3xA Security

(http://AAA-sec.com)
Status

• Summary past discussions
  – Problems related to use of hash algorithms
    • Agility complexity
    • Need to specify a must implement hash for interoperability
    • No strong security requirements
  – Problems related to use of FNV
    • Does not preserve security properties of Finished calculations
  – Problems related to use of Finished message hash function
    • TLS 1.0 and TLS 1.1 use a combination of MD5 and SHA-1.
    • No hash identifier for TLS prf.
Major changes in draft 09

- All use of FNV-1 digest replaced with hash used in Finished calculation of cached handshake
  - Problem: This does only work for TLS 1.2
- Reconnaissance updated
  - Client may check server capability before caching
- Updated substitution syntax for each cached information type
  - Preserving original handshake message syntax
OLD:

Replacing cached objects in the handshake protocol

NEW:

Replacing cached objects in the handshake protocol
Extension syntax

Old

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

struct {
    CachedInformationType type;
    opaque digest_value<0..8>;
} CachedObject;

struct {
    CachedObject cached_info<1..2^16-1>;
} CachedInformation;

New

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

struct {
    CachedInformationType type;
    HashAlgorithm hash;
    opaque hash_value<1..255>;
} CachedObject;

struct {
    CachedObject cached_info<1..2^16-1>;
} CachedInformation;
Message flow

Client

Client Hello with Cached Information Extension

Server Hello with Cached Information Extension

Example substitution

Certificate Message


Cached Object
Substitution Syntax – certificate_chain

Original handshake message syntax defined in RFC 5246 [RFC5246]:

    opaque ASN.1Cert<1..2^24-1>;

Substitution syntax is defined by expanding the definition of the opaque ASN.1Cert structure:

    CachedObject ASN.1Cert<1..2^24-1>;}
Substitution Syntax – trusted_cas

Original handshake message syntax defined in RFC 5246 [RFC5246]:

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

The substitution syntax is defined by expanding the definition of the opaque DistinguishedName structure:

    CachedObject DistinguishedName<1..2^16-1>;}
Using PRF

• Syntax
  - \texttt{PRF(secret, label, seed) = P\_MD5(S1, label + seed) \texttt{XOR} P\_SHA-1(S2, label + seed)};

• Proposal (by Marsh Ray)
  - \texttt{PRF("cached info", "cached info", MD5(cached\_info\_object) + SHA-1(cached\_info\_object)) [0..11]}
Possible approach

Current

```c
struct {
    CachedInformationType type;
    HashAlgorithm hash;
    opaque hash_value<1..255>;
} CachedObject;
```

PRF

```c
enum {
    prf(1), hash(2),
    (255)
} CacheHashMethod;

struct {
    CachedInformationType type;
    select (CacheHashMethod){
        case prf: cached_info_prf<1..255>;
        case hash: HashValue;
    }
} CachedObject;

Struct {
    HashAlgorithm hash;
    opaque hash_value<1..255>;
} HashValue;

cached_info_prf carry the value of:
PRF("cached info", "cached info",
    MD5(cached_info_object) +
    SHA-1(cached_info_object)) [0..11])
Remaining issues and way forward

- Define algorithm for generating cached info hash for < TLS 1.2
- If PRF, then how do we indentify PRF in the protocol?
- WGLC?
Questions / Comments