INTERNET-DRAFT
Obsoletes (if approved): RFC 4347
Intended Status: Proposed Standard
Expires: September 14, 2011

E. Rescorla
RTFM, Inc.
N. Modadugu
Stanford University
March 14, 2011

Datagram Transport Layer Security version 1.2
draft-ietf-tls-rfc4347-bis-05.txt

Abstract

This document specifies Version 1.2 of the Datagram Transport Layer Security (DTLS) protocol. The DTLS protocol provides communications privacy for datagram protocols. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. The DTLS protocol is based on the Transport Layer Security (TLS) protocol and provides equivalent security guarantees. Datagram semantics of the underlying transport are preserved by the DTLS protocol. This document updates DTLS 1.0 to work with TLS version 1.2.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 14, 2011.

Table of Contents

1. Introduction

TLS [TLS] is the most widely deployed protocol for securing network traffic. It is widely used for protecting Web traffic and for e-mail protocols such as IMAP [IMAP] and POP [POP]. The primary advantage of TLS is that it provides a transparent connection-oriented channel. Thus, it is easy to secure an application protocol by inserting TLS between the application layer and the transport layer. However, TLS must run over a reliable transport channel -- typically TCP [TCP]. It therefore cannot be used to secure unreliable datagram traffic.

However, an increasing number of application layer protocols have been designed that use UDP transport. In particular protocols such as the Session Initiation Protocol (SIP) [SIP] and electronic gaming protocols are increasingly popular. (Note that SIP can run over both TCP and UDP, but that there are situations in which UDP is preferable). Currently, designers of these applications are faced with a number of unsatisfactory choices. First, they can use IPsec [RFC4301]. However, for a number of reasons detailed in [WHYIPSEC], this is only suitable for some applications. Second, they can design a custom application layer security protocol. Unfortunately, although application layer security protocols generally provide

superior security properties (e.g., end-to-end security in the case of S/MIME), they typically require a large amount of effort to design -- in contrast to the relatively small amount of effort required to run the protocol over TLS.

In many cases, the most desirable way to secure client/server applications would be to use TLS; however, the requirement for datagram semantics automatically prohibits use of TLS. This memo describes a protocol for this purpose: Datagram Transport Layer Security (DTLS). DTLS is deliberately designed to be as similar to TLS as possible, both to minimize new security invention and to maximize the amount of code and infrastructure reuse.

DTLS 1.0 [DTLS1] was originally defined as a delta from [TLS11]. This document introduces a new version of DTLS, DTLS 1.2, which is defined as a series of deltas to TLS 1.2 [TLS12] There is no DTLS 1.1. That version number was skipped in order to harmonize version numbers with TLS. This version also clarifies some confusing points in the DTLS 1.0 specification.

Implementations that speak both DTLS 1.2 and DTLS 1.0 can interoperate with those that speak only DTLS 1.0 (using DTLS 1.0 of course), just as TLS 1.2 implementations can interoperate with previous versions (See Appendix E.1 of [TLS12] for details) with the exception that there is no DTLS version of SSLv2 or SSLv3 so that the backward compatibility issues for those protocols do not apply.

1.1. Requirements Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [REQ].

2. Usage Model

The DTLS protocol is designed to secure data between communicating applications. It is designed to run in application space, without requiring any kernel modifications.

Datagram transport does not require or provide reliable or in-order delivery of data. The DTLS protocol preserves this property for payload data. Applications such as media streaming, Internet telephony, and online gaming use datagram transport for communication due to the delay-sensitive nature of transported data. The behavior of such applications is unchanged when the DTLS protocol is used to secure communication, since the DTLS protocol does not compensate for lost or re-ordered data traffic.

3. Overview of DTLS

The basic design philosophy of DTLS is to construct "TLS over datagram transport." The reason that TLS cannot be used directly in datagram environments is simply that packets may be lost or reordered. TLS has no internal facilities to handle this kind of unreliability, and therefore TLS implementations break when rehosted on datagram transport. The purpose of DTLS is to make only the minimal changes to TLS required to fix this problem. To the greatest extent possible, DTLS is identical to TLS. Whenever we need to invent new mechanisms, we attempt to do so in such a way that preserves the style of TLS.

Unreliability creates problems for TLS at two levels:

1. TLS does not allow independent decryption of individual records. Because the integrity check depends on the sequence number, if record N is not received, then the integrity check on record N+1 will be based on the wrong sequence number and thus will fail. [Note that prior to TLS 1.1, there was no explicit IV and so decryption would also fail.]

2. The TLS handshake layer assumes that handshake messages are delivered reliably and breaks if those messages are lost.

The rest of this section describes the approach that DTLS uses to solve these problems.

3.1. Loss-Insensitive Messaging

In TLS's traffic encryption layer (called the TLS Record Layer), records are not independent. There are two kinds of inter-record dependency:

1. Cryptographic context (stream cipher key stream) is retained between records.

2. Anti-replay and message reordering protection are provided by a MAC that includes a sequence number, but the sequence numbers are implicit in the records.

DTLS solves the first problem by banning stream ciphers. DTLS solves the second problem by adding explicit sequence numbers.

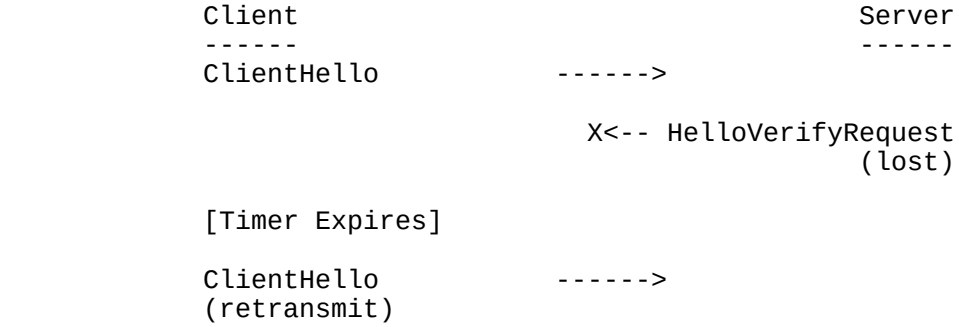
3.2. Providing Reliability for Handshake

The TLS handshake is a lockstep cryptographic handshake. Messages must be transmitted and received in a defined order, and any other

order is an error. Clearly, this is incompatible with reordering and message loss. In addition, TLS handshake messages are potentially larger than any given datagram, thus creating the problem of IP fragmentation. DTLS must provide fixes for both of these problems.

3.2.1. Packet Loss

DTLS uses a simple retransmission timer to handle packet loss. The following figure demonstrates the basic concept, using the first phase of the DTLS handshake:



Once the client has transmitted the ClientHello message, it expects to see a HelloVerifyRequest from the server. However, if the server's message is lost the client knows that either the ClientHello or the HelloVerifyRequest has been lost and retransmits. When the server receives the retransmission, it knows to retransmit. The server also maintains a retransmission timer and retransmits when that timer expires.

Note: timeout and retransmission do not apply to the HelloVerifyRequest, because this requires creating state on the server.

Note: The HelloVerifyRequest is designed to be small enough that it will not itself be fragmented, thus avoiding concerns about interleaving multiple HelloVerifyRequests.

3.2.2. Reordering

In DTLS, each handshake message is assigned a specific sequence number within that handshake. When a peer receives a handshake message, it can quickly determine whether that message is the next message it expects. If it is, then it processes it. If not, it queues it up for future handling once all previous messages have been received.

3.2.3. Message Size

TLS and DTLS handshake messages can be quite large (in theory up to 2^24-1 bytes, in practice many kilobytes). By contrast, UDP datagrams are often limited to <1500 bytes if IP fragmentation is not desired. In order to compensate for this limitation, each DTLS handshake message may be fragmented over several DTLS records, each of which is intended to fit in a single IP datagram. Each DTLS handshake message contains both a fragment offset and a fragment length. Thus, a recipient in possession of all bytes of a handshake message can reassemble the original unfragmented message.

3.3. Replay Detection

DTLS optionally supports record replay detection. The technique used is the same as in IPsec AH/ESP, by maintaining a bitmap window of received records. Records that are too old to fit in the window and records that have previously been received are silently discarded. The replay detection feature is optional, since packet duplication is not always malicious, but can also occur due to routing errors. Applications may conceivably detect duplicate packets and accordingly modify their data transmission strategy.

4. Differences from TLS

As mentioned in Section 3, DTLS is intentionally very similar to TLS. Therefore, instead of presenting DTLS as a new protocol, we present it as a series of deltas from TLS 1.2 [TLS12]. Where we do not explicitly call out differences, DTLS is the same as in [TLS12].

4.1. Record Layer

The DTLS record layer is extremely similar to that of TLS 1.2. The only change is the inclusion of an explicit sequence number in the record. This sequence number allows the recipient to correctly verify the TLS MAC. The DTLS record format is shown below:

```
    struct {
      ContentType type;
      ProtocolVersion version;
      uint16 epoch;                                  // New field
      uint48 sequence_number;                        // New field
      uint16 length;
      opaque fragment[DTLSPlaintext.length];
    } DTLSPlaintext;
```

type
 Equivalent to the type field in a TLS 1.2 record.

version
The version of the protocol being employed. This document describes DTLS Version 1.2, which uses the version { 254, 253 }. The version value of 254.253 is the 1's complement of DTLS Version 1.2. This maximal spacing between TLS and DTLS version numbers ensures that records from the two protocols can be easily distinguished. It should be noted that future on-the-wire version numbers of DTLS are decreasing in value (while the true version number is increasing in value.)

epoch
A counter value that is incremented on every cipher state change.

sequence_number
The sequence number for this record.

length
Identical to the length field in a TLS 1.2 record. As in TLS 1.2, the length should not exceed 2^14.

fragment
Identical to the fragment field of a TLS 1.2 record.

DTLS uses an explicit sequence number, rather than an implicit one, carried in the sequence_number field of the record. Sequence numbers are maintained separately for each epoch, with each sequence_number initially being 0 for each epoch. For instance, if a handshake message from epoch 0 is retransmitted, it might have a sequence number after a message from epoch 1, even if the message from epoch 1 was transmitted first. Note that some care needs to be taken during the handshake to ensure that retransmitted messages use the right epoch and keying material.

If several handshakes are performed in close succession, there might be multiple records on the wire with the same sequence number but from different cipher states. The epoch field allows recipients to distinguish such packets. The epoch number is initially zero and is incremented each time the ChangeCipherSpec messages is sent. In order to ensure that any given sequence/epoch pair is unique, implementations MUST NOT allow the same epoch value to be reused within two times the TCP maximum segment lifetime. In practice, TLS implementations rarely rehandshake and we therefore do not expect this to be a problem.

Note that because DTLS records may be reordered, a record from epoch 1 may be received after epoch 2 has begun. In general, implementations SHOULD discard packets from earlier epochs, but if

packet loss causes noticeable problems MAY choose to retain keying material from previous epochs for up to 120 seconds (the default TCP MSL) to allow for packet reordering. Until the handshake has completed, implementations MUST accept packets from the old epoch.

Conversely, it is possible for records that are protected by the newly negotiated context to be received prior to the completion of a handshake. For instance, the server may send its Finished and then start transmitting data. Implementations MAY either buffer or discard such packets, though when DTLS is used over reliable transports (e.g., SCTP), they SHOULD be buffered and processed once the handshake completes. Note that TLS's restrictions on when packets may be sent still apply, and the receiver treats the packets as if they were sent in the right order. In particular, it is still impermissible to send data prior to completion of the first handshake.

Note that in the special case of a rehandshake on an existing association, it is safe to process a data packet immediately even if the ChangeCipherSpec or Finished has not yet been received provided that either the rehandshake resumes the existing session or that it uses exactly the same security parameters as the existing association. In any other case, the implementation MUST wait for the receipt of the Finished to prevent downgrade attack.

As in TLS, implementations MUST either abandon an association or rehandshake prior to allowing the sequence number to wrap. Similarly, implementations MUST NOT allow the epoch to wrap, but instead MUST establish a new association, terminating the old association as described in Section 4.2.8. In practice, implementations rarely rehandshake repeatedly on the same channel, so this is not likely to be an issue.

4.1.1. Transport Layer Mapping

Each DTLS record MUST fit within a single datagram. In order to avoid IP fragmentation, clients of the DTLS record layer SHOULD attempt to size records so that they fit within any PMTU estimates obtained from the record layer.

Note that unlike IPsec, DTLS records do not contain any association identifiers. Applications must arrange to multiplex between associations. With UDP, this is presumably done with host/port number.

Multiple DTLS records may be placed in a single datagram. They are simply encoded consecutively. The DTLS record framing is sufficient

to determine the boundaries. Note, however, that the first byte of the datagram payload must be the beginning of a record. Records may not span datagrams.

Some transports, such as DCCP [DCCP] provide their own sequence numbers. When carried over those transports, both the DTLS and the transport sequence numbers will be present. Although this introduces a small amount of inefficiency, the transport layer and DTLS sequence numbers serve different purposes, and therefore for conceptual simplicity it is superior to use both sequence numbers. In the future, extensions to DTLS may be specified that allow the use of only one set of sequence numbers for deployment in constrained environments.

Some transports, such as DCCP, provide congestion control for traffic carried over them. If the congestion window is sufficiently narrow, DTLS handshake retransmissions may be held rather than transmitted immediately, potentially leading to timeouts and spurious retransmission. When DTLS is used over such transports, care should be taken not to overrun the likely congestion window. [DCCPDTLS] defines a mapping of DTLS to DCCP that takes these issues into account.

4.1.1.1. PMTU Issues

In general, DTLS's philosophy is to leave PMTU discovery to the application. However, DTLS cannot completely ignore PMTU for three reasons:

- The DTLS record framing expands the datagram size, thus lowering the effective PMTU from the application's perspective.

- In some implementations the application may not directly talk to the network, in which case the DTLS stack may absorb ICMP [RFC1191] Datagram Too Big indications or ICMPv6 [RFC1885] Packet Too Big indications.

- The DTLS handshake messages can exceed the PMTU.

In order to deal with the first two issues, the DTLS record layer SHOULD behave as described below.

If PMTU estimates are available from the underlying transport protocol, they should be made available to upper layer protocols. In particular:

- For DTLS over UDP, the upper layer protocol SHOULD be allowed

to obtain the PMTU estimate maintained in the IP layer.

- For DTLS over DCCP, the upper layer protocol SHOULD be allowed to obtain the current estimate of the PMTU.

- For DTLS over TCP or SCTP, which automatically fragment and reassemble datagrams, there is no PMTU limitation. However, the upper layer protocol MUST NOT write any record that exceeds the maximum record size of 2^14 bytes.

The DTLS record layer SHOULD allow the upper layer protocol to discover the amount of record expansion expected by the DTLS processing. Note that this number is only an estimate because of block padding and the potential use of DTLS compression.

If there is a transport protocol indication (either via ICMP or via a refusal to send the datagram as in DCCP Section 14), then the DTLS record layer MUST inform the upper layer protocol of the error.

The DTLS record layer SHOULD NOT interfere with upper layer protocols performing PMTU discovery, whether via [RFC1191] or [RFC4821] mechanisms. In particular:

- Where allowed by the underlying transport protocol, the upper layer protocol SHOULD be allowed to set the state of the DF bit (in IPv4) or prohibit local fragmentation (in IPv6).

- If the underlying transport protocol allows the application to request PMTU probing (e.g., DCCP), the DTLS record layer should honor this request.

The final issue is the DTLS handshake protocol. From the perspective of the DTLS record layer, this is merely another upper layer protocol. However, DTLS handshakes occur infrequently and involve only a few round trips, and therefore the handshake protocol PMTU handling places a premium on rapid completion over accurate PMTU discovery. In order to allow connections under these circumstances, DTLS implementations SHOULD follow the following rules:

- If the DTLS record layer informs the DTLS handshake layer that a message is too big, it SHOULD immediately attempt to fragment it, using any existing information about the PMTU.

- If repeated retransmissions do not result in a response, and the PMTU is unknown, subsequent retransmissions SHOULD back off to a

smaller record size, fragmenting the handshake message as appropriate. This standard does not specify an exact number of retransmits to attempt before backing off, but 2-3 seems appropriate.

4.1.2. Record Payload Protection

Like TLS, DTLS transmits data as a series of protected records. The rest of this section describes the details of that format.

4.1.2.1. MAC

The DTLS MAC is the same as that of TLS 1.2. However, rather than using TLS's implicit sequence number, the sequence number used to compute the MAC is the 64-bit value formed by concatenating the epoch and the sequence number in the order they appear on the wire. Note that the DTLS epoch + sequence number is the same length as the TLS sequence number.

TLS MAC calculation is parameterized on the protocol version number, which, in the case of DTLS, is the on-the-wire version, i.e., {254, 253} for DTLS 1.2.

Note that one important difference between DTLS and TLS MAC handling is that in TLS MAC errors must result in connection termination. In DTLS, the receiving implementation MAY simply discard the offending record and continue with the connection. This change is possible because DTLS records are not dependent on each other in the way that TLS records are.

In general, DTLS implementations SHOULD silently discard records with bad MACs or that are otherwise invalid. They MAY log an error. If a DTLS implementation chooses to generate an alert when it receives a message with an invalid MAC, it MUST generate a bad_record_mac alert with level fatal and terminate its connection state.

4.1.2.2. Null or Standard Stream Cipher

The DTLS NULL cipher is performed exactly as the TLS 1.2 NULL cipher.

The only stream cipher described in TLS 1.2 is RC4, which cannot be randomly accessed. RC4 MUST NOT be used with DTLS.

4.1.2.3. Block Cipher

DTLS block cipher encryption and decryption are performed exactly as with TLS 1.2.

4.1.2.3. AEAD Ciphers

TLS 1.2 introduced authenticated encryption with additional data (AEAD) cipher suites. The existing AEAD cipher suites, defined in [ECCGCM] and [RSAGCM] can be used with DTLS exactly as with TLS 1.2.

4.1.2.5. New Cipher Suites

Upon registration, new TLS cipher suites MUST indicate whether they are suitable for DTLS usage and what, if any, adaptations must be made (See Section 7 for IANA considerations).

4.1.2.6. Anti-replay

DTLS records contain a sequence number to provide replay protection. Sequence number verification SHOULD be performed using the following sliding window procedure, borrowed from Section 3.4.3 of [ESP].

The receiver packet counter for this session MUST be initialized to zero when the session is established. For each received record, the receiver MUST verify that the record contains a Sequence Number that does not duplicate the Sequence Number of any other record received during the life of this session. This SHOULD be the first check applied to a packet after it has been matched to a session, to speed rejection of duplicate records.

Duplicates are rejected through the use of a sliding receive window. (How the window is implemented is a local matter, but the following text describes the functionality that the implementation must exhibit.) A minimum window size of 32 MUST be supported, but a window size of 64 is preferred and SHOULD be employed as the default. Another window size (larger than the minimum) MAY be chosen by the receiver. (The receiver does not notify the sender of the window size.)

The "right" edge of the window represents the highest validated Sequence Number value received on this session. Records that contain Sequence Numbers lower than the "left" edge of the window are rejected. Packets falling within the window are checked against a list of received packets within the window. An efficient means for performing this check, based on the use of a bit mask, is described in Section 3.4.3 of [ESP].

If the received record falls within the window and is new, or if the packet is to the right of the window, then the receiver proceeds to MAC verification. If the MAC validation fails, the receiver MUST discard the received record as invalid. The receive window is

updated only if the MAC verification succeeds.

4.1.2.7. Handling Invalid Records

Unlike TLS, DTLS is resilient in the face of invalid records (e.g., invalid formatting, length, MAC, etc.) In general, invalid records SHOULD be silently discarded, thus preserving the association, however an error MAY be logged for diagnostic purposes. Implementations which choose to generate an alert instead, MUST generate fatal level alerts to avoid attacks where the attacker repeatedly probes the implementation to see how it responds to various types of error. Note that if DTLS is run over UDP, then any implementation which does this will be extremely susceptible to DoS attacks because UDP forgery is so easy. Thus, this practice is NOT RECOMMENDED for such transports.

If DTLS is being carried over a transport which is resistant to forgery (e.g., SCTP with SCTP-AUTH), then it is safer to send alerts because an attacker will have difficulty forging a datagram which will not be rejected by the transport layer.

4.2. The DTLS Handshake Protocol

DTLS uses all of the same handshake messages and flows as TLS, with three principal changes:

1. A stateless cookie exchange has been added to prevent denial of service attacks.

2. Modifications to the handshake header to handle message loss, reordering, and DTLS message fragmentation (in order to avoid IP fragmentation).

3. Retransmission timers to handle message loss.

With these exceptions, the DTLS message formats, flows, and logic are the same as those of TLS 1.2.

4.2.1. Denial of Service Countermeasures

Datagram security protocols are extremely susceptible to a variety of denial of service (DoS) attacks. Two attacks are of particular concern:

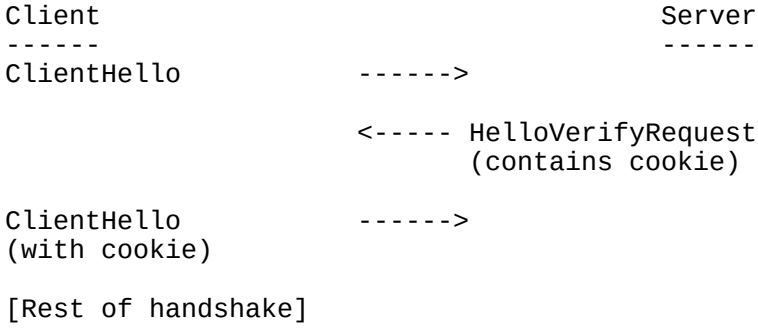
1. An attacker can consume excessive resources on the server by transmitting a series of handshake initiation requests, causing the server to allocate state and potentially to perform expensive

cryptographic operations.

2. An attacker can use the server as an amplifier by sending connection initiation messages with a forged source of the victim. The server then sends its next message (in DTLS, a Certificate message, which can be quite large) to the victim machine, thus flooding it.

In order to counter both of these attacks, DTLS borrows the stateless cookie technique used by Photuris [PHOTURIS] and IKE [IKEv2]. When the client sends its ClientHello message to the server, the server MAY respond with a HelloVerifyRequest message. This message contains a stateless cookie generated using the technique of [PHOTURIS]. The client MUST retransmit the ClientHello with the cookie added. The server then verifies the cookie and proceeds with the handshake only if it is valid. This mechanism forces the attacker/client to be able to receive the cookie, which makes DoS attacks with spoofed IP addresses difficult. This mechanism does not provide any defense against DoS attacks mounted from valid IP addresses.

The exchange is shown below:



DTLS therefore modifies the ClientHello message to add the cookie value.

```
struct {
  ProtocolVersion client_version;
  Random random;
  SessionID session_id;
  opaque cookie<0..2^8-1>;                          // New field
  CipherSuite cipher_suites<2..2^16-1>;
  CompressionMethod compression_methods<1..2^8-1>;
} ClientHello;
```

When sending the first ClientHello, the client does not have a cookie

yet; in this case, the Cookie field is left empty (zero length).

The definition of HelloVerifyRequest is as follows:

```
struct {
  ProtocolVersion server_version;
  opaque cookie<0..2^8-1>;
} HelloVerifyRequest;
```

The HelloVerifyRequest message type is hello_verify_request(3).

The server_version field is defined as in TLS.

When responding to a HelloVerifyRequest the client MUST use the same parameter values (version, random, session_id, cipher_suites, compression_method) as it did in the original ClientHello. The server SHOULD use those values to generate its cookie and verify that they are correct upon cookie receipt. The server MUST use the same version number in the HelloVerifyRequest that it would use when sending a ServerHello. Upon receipt of the ServerHello, the client MUST verify that the server version values match.

Note: this specification increases the cookie size limit to 255 bytes for greater future flexibility. The limit remains 32 for previous versions of DTLS.

The DTLS server SHOULD generate cookies in such a way that they can be verified without retaining any per-client state on the server. One technique is to have a randomly generated secret and generate cookies as: Cookie = HMAC(Secret, Client-IP, Client-Parameters)

When the second ClientHello is received, the server can verify that the Cookie is valid and that the client can receive packets at the given IP address.

One potential attack on this scheme is for the attacker to collect a number of cookies from different addresses and then reuse them to attack the server. The server can defend against this attack by changing the Secret value frequently, thus invalidating those cookies. If the server wishes that legitimate clients be able to handshake through the transition (e.g., they received a cookie with Secret 1 and then sent the second ClientHello after the server has changed to Secret 2), the server can have a limited window during which it accepts both secrets. [IKEv2] suggests adding a version number to cookies to detect this case. An alternative approach is simply to try verifying with both secrets.

DTLS servers SHOULD perform a cookie exchange whenever a new

handshake is being performed. If the server is being operated in an environment where amplification is not a problem, the server MAY be configured not to perform a cookie exchange. The default SHOULD be that the exchange is performed, however. In addition, the server MAY choose not to do a cookie exchange when a session is resumed. Clients MUST be prepared to do a cookie exchange with every handshake.

If HelloVerifyRequest is used, the initial ClientHello and HelloVerifyRequest are not included in the calculation of the handshake_messages (for the CertificateVerify message) and verify_data (for the Finished message).

If a server receives a ClientHello with an invalid cookie, it SHOULD treat it the same as a ClientHello with no cookie. This avoids race/deadlock conditions if the client somehow gets a bad cookie (e.g., because the server changes its cookie signing key).

Note to implementors: this may results in clients receiving multiple HelloVerifyRequest messages with different cookies. Clients SHOULD handle this by sending a new ClientHello with a cookie in response to the new HelloVerifyRequest. Note that this message should have the same handshake sequence number (0) and record sequence number (0), thus avoiding the need to create state on the server. This also implies that the client MUST NOT do replay suppression during the initial handshake (this is safe as handshake messages have their own sequence numbers). [OPEN ISSUE: It's not clear that this is the best choice. Michael Tuexen suggested mimicing the client's record sequence number instead.]

4.2.2. Handshake Message Format

In order to support message loss, reordering, and message fragmentation, DTLS modifies the TLS 1.2 handshake header:

```
   struct {
     HandshakeType msg_type;
     uint24 length;
     uint16 message_seq;                                // New field
     uint24 fragment_offset;                            // New field
     uint24 fragment_length;                            // New field
     select (HandshakeType) {
       case hello_request: HelloRequest;
       case client_hello:  ClientHello;
       case hello_verify_request: HelloVerifyRequest;   // New type
       case server_hello:  ServerHello;
       case certificate:Certificate;
```

```
          case server_key_exchange: ServerKeyExchange;
          case certificate_request: CertificateRequest;
          case server_hello_done:ServerHelloDone;
          case certificate_verify:  CertificateVerify;
          case client_key_exchange: ClientKeyExchange;
          case finished: Finished;
        } body;
      } Handshake;
```

The first message each side transmits in each handshake always has message_seq = 0. Whenever each new message is generated, the message_seq value is incremented by one. When a message is retransmitted, the same message_seq value is used. For example:

```
   Client                              Server
   ------                              ------
   ClientHello (seq=0)  ------>

                           X<-- HelloVerifyRequest (seq=0)
                                          (lost)

   [Timer Expires]

   ClientHello (seq=0)  ------>
   (retransmit)

                        <------ HelloVerifyRequest (seq=0)

   ClientHello (seq=1)  ------>
   (with cookie)

                        <------        ServerHello (seq=1)
                        <------        Certificate (seq=2)
                        <------    ServerHelloDone (seq=3)

   [Rest of handshake]
```

Note, however, that from the perspective of the DTLS record layer, the retransmission is a new record. This record will have a new DTLSPlaintext.sequence_number value.

DTLS implementations maintain (at least notionally) a next_receive_seq counter. This counter is initially set to zero. When a message is received, if its sequence number matches next_receive_seq, next_receive_seq is incremented and the message is processed. If the sequence number is less than next_receive_seq, the message MUST be discarded. If the sequence number is greater than next_receive_seq, the implementation SHOULD queue the message but MAY

discard it. (This is a simple space/bandwidth tradeoff).

4.2.3. Handshake Message Fragmentation and Reassembly

As noted in Section 4.1.1, each DTLS message MUST fit within a single transport layer datagram. However, handshake messages are potentially bigger than the maximum record size. Therefore, DTLS provides a mechanism for fragmenting a handshake message over a number of records, each of which can be transmitted separately, thus avoiding IP fragmentation.

When transmitting the handshake message, the sender divides the message into a series of N contiguous data ranges. These ranges MUST NOT be larger than the maximum handshake fragment size and MUST jointly contain the entire handshake message. The ranges SHOULD NOT overlap. The sender then creates N handshake messages, all with the same message_seq value as the original handshake message. Each new message is labelled with the fragment_offset (the number of bytes contained in previous fragments) and the fragment_length (the length of this fragment). The length field in all messages is the same as the length field of the original message. An unfragmented message is a degenerate case with fragment_offset=0 and fragment_length=length.

When a DTLS implementation receives a handshake message fragment, it MUST buffer it until it has the entire handshake message. DTLS implementations MUST be able to handle overlapping fragment ranges. This allows senders to retransmit handshake messages with smaller fragment sizes if the PMTU estimate changes.

Note that as with TLS, multiple handshake messages may be placed in the same DTLS record, provided that there is room and that they are part of the same flight. Thus, there are two acceptable ways to pack two DTLS messages into the same datagram: in the same record or in separate records.

4.2.4. Timeout and Retransmission

DTLS messages are grouped into a series of message flights, according to the diagrams below. Although each flight of messages may consist of a number of messages, they should be viewed as monolithic for the purpose of timeout and retransmission.

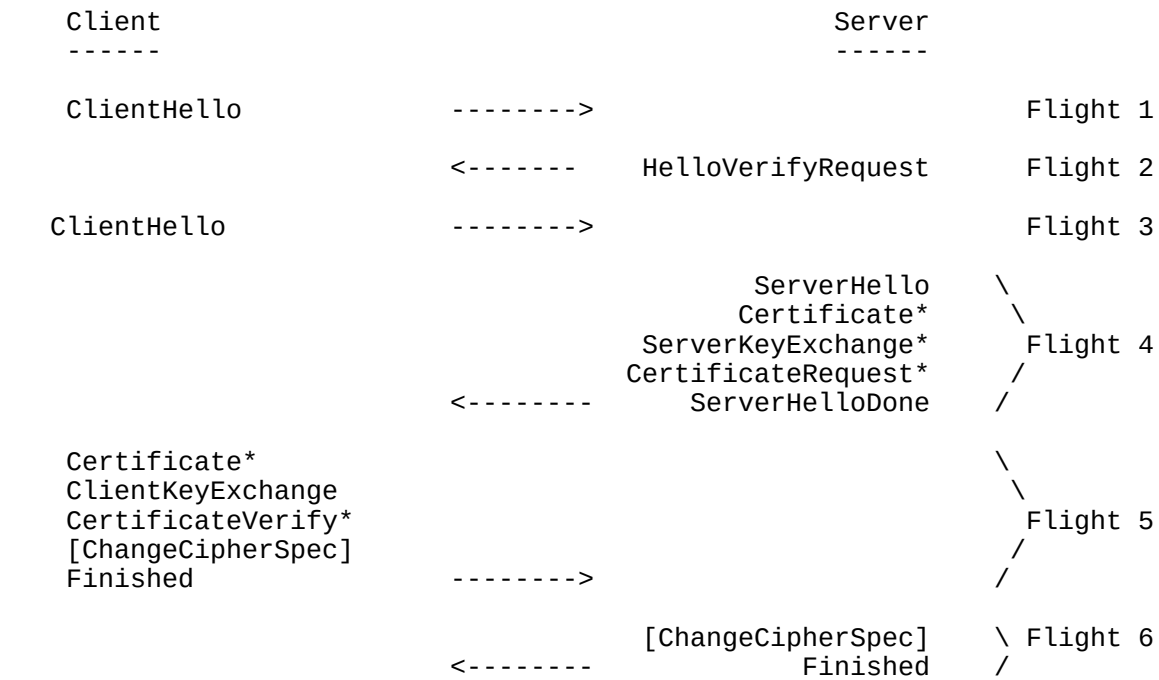


Figure 1. Message flights for full handshake

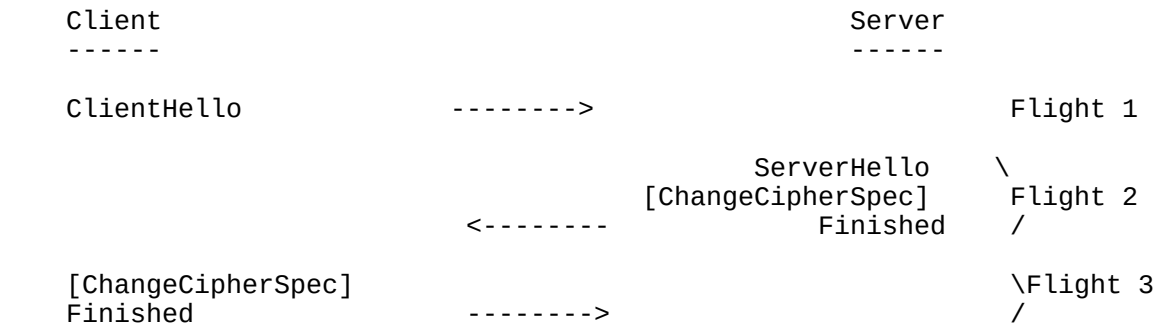


Figure 2. Message flights for session-resuming handshake
(no cookie exchange)

DTLS uses a simple timeout and retransmission scheme with the following state machine. Because DTLS clients send the first message (ClientHello), they start in the PREPARING state. DTLS servers start in the WAITING state, but with empty buffers and no retransmit timer.

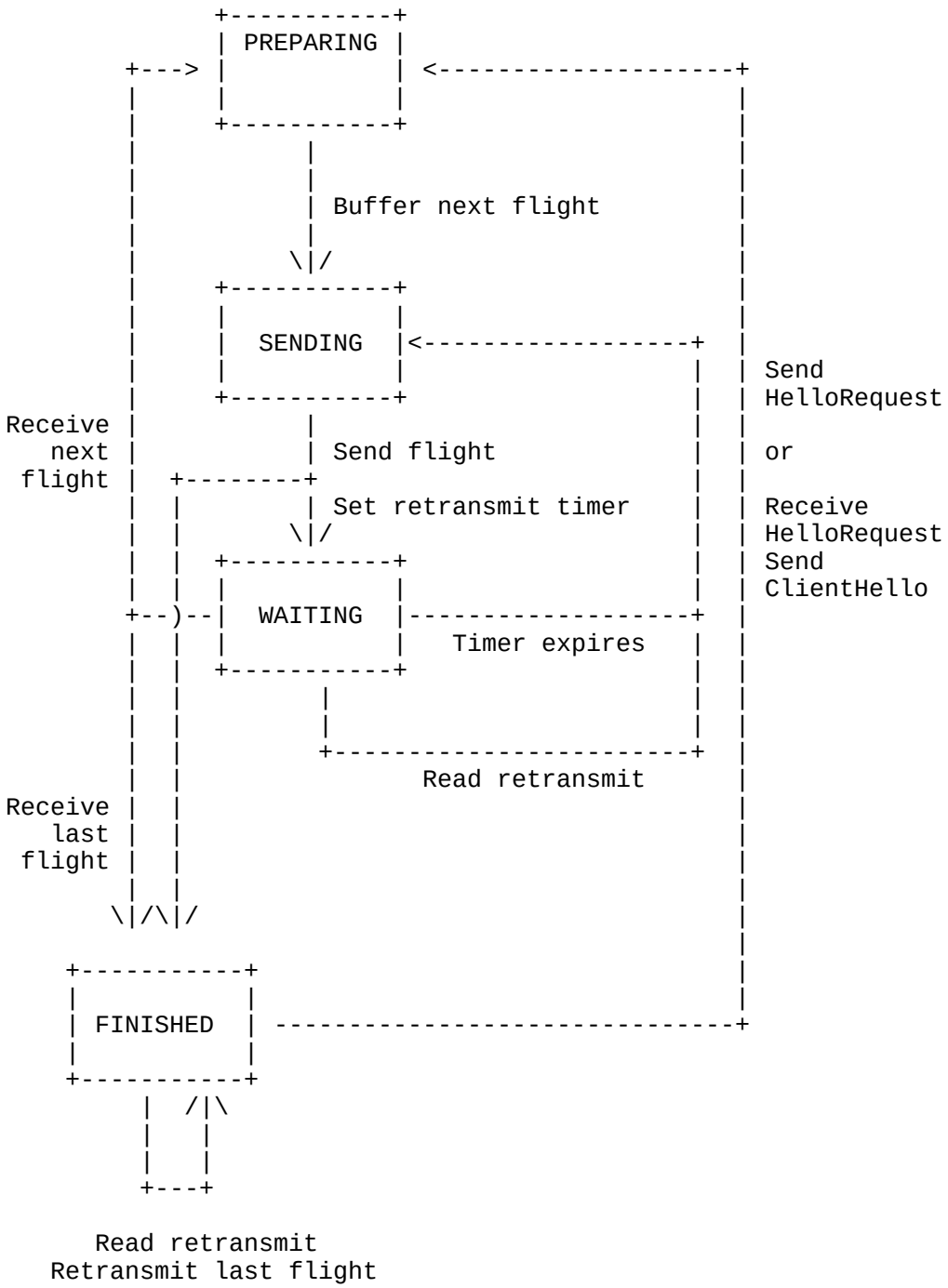

PREPARING
Buffer next flight
SENDING
Send flight
Set retransmit timer
WAITING
Timer expires
Read retransmit
Send HelloRequest or Receive HelloRequest Send ClientHello
Receive next flight
Receive last flight
FINISHED
Read retransmit
Retransmit last flight

Figure 3. DTLS timeout and retransmission state machine

The state machine has three basic states.

In the PREPARING state the implementation does whatever computations are necessary to prepare the next flight of messages. It then buffers them up for transmission (emptying the buffer first) and enters the SENDING state.

In the SENDING state, the implementation transmits the buffered flight of messages. Once the messages have been sent, the implementation then enters the FINISHED state if this is the last flight in the handshake. Or, if the implementation expects to receive more messages, it sets a retransmit timer and then enters the WAITING state.

There are three ways to exit the WAITING state:

1. The retransmit timer expires: the implementation transitions to the SENDING state, where it retransmits the flight, resets the retransmit timer, and returns to the WAITING state.

2. The implementation reads a retransmitted flight from the peer: the implementation transitions to the SENDING state, where it retransmits the flight, resets the retransmit timer, and returns to the WAITING state. The rationale here is that the receipt of a duplicate message is the likely result of timer expiry on the peer and therefore suggests that part of one’s previous flight was lost.

3. The implementation receives the next flight of messages: if this is the final flight of messages, the implementation transitions to FINISHED. If the implementation needs to send a new flight, it transitions to the PREPARING state. Partial reads (whether partial messages or only some of the messages in the flight) do not cause state transitions or timer resets.

Because DTLS clients send the first message (ClientHello), they start in the PREPARING state. DTLS servers start in the WAITING state, but with empty buffers and no retransmit timer.

When the server desires a rehandshake, it transitions from the FINISHED state to the PREPARING state to transmit the HelloRequest. When the client receives a HelloRequest it transitions from FINISHED to PREPARING to transmit the ClientHello.

In addition, for at least 2MSL, when in the FINISHED state, the node which transmits the last flight (the server in an ordinary handshake

or the client in a resumed handshake) MUST respond to a retransmit of the peer's last flight with a retransmit of the last flight. This avoids deadlock conditions if the last flight gets lost. This requirement applies to DTLS 1.0 as well, and though not explicit in [DTLS1] but was always required for the state machine to function correctly. To see why this is necessary, consider what happens in an ordinary handshake if the server's Finished is lost: the server believes the handshake is complete but it actually is not. As the client is waiting for the Finished, the client's retransmit timer will fire and it will retransmit the client Finished, causing the server to respond with its own Finished, completing the handshake. The same logic applies on the server side for the resumed handshake.

Note that because of packet loss it is possible for one side to be sending application data even though the other side has not received the first side's Finished. Implementations MUST either discard or buffer all application data packets for the new epoch until they have received the Finished for that epoch. Implementations MAY treat receipt of application data with a new epoch prior to receipt of the corresponding Finished as evidence of reordering or packet loss and retransmit their final flight immediately, shortcutting the retransmission timer.

4.2.4.1. Timer Values

Though timer values are the choice of the implementation, mishandling of the timer can lead to serious congestion problems; for example, if many instances of a DTLS time out early and retransmit too quickly on a congested link. Implementations SHOULD use an initial timer value of 1 second (the minimum defined in RFC 2988 [RFC2988]) and double the value at each retransmission, up to no less than the RFC 2988 maximum of 60 seconds. Note that we recommend a 1-second timer rather than the 3-second RFC 2988 default in order to improve latency for time-sensitive applications. Because DTLS only uses retransmission for handshake and not dataflow, the effect on congestion should be minimal.

Implementations SHOULD retain the current timer value until a transmission without loss occurs, at which time the value may be reset to the initial value. After a long period of idleness, no less than 10 times the current timer value, implementations may reset the timer to the initial value. One situation where this might occur is when a rehandshake is used after substantial data transfer.

4.2.5. ChangeCipherSpec

As with TLS, the ChangeCipherSpec message is not technically a handshake message but MUST be treated as part of the same flight as

the associated Finished message for the purposes of timeout and retransmission.

4.2.6. CertificateVerify and Finished Messages

CertificateVerify and Finished messages have the same format as in TLS. Hash calculations include entire handshake messages, including DTLS specific fields: message_seq, fragment_offset and fragment_length. However, in order to remove sensitivity to handshake message fragmentation, the Finished MAC MUST be computed as if each handshake message had been sent as a single fragment. Note that in cases where the cookie exchange is used, the initial ClientHello and HelloVerifyRequest MUST NOT be included in the CertificateVerify or Finished MAC computations.

4.2.7. Alert Messages

Note that Alert messages are not retransmitted at all, even when they occur in the context of a handshake. However, a DTLS implementation SHOULD generate a new alert message if the offending record is received again (e.g., as a retransmitted handshake message). Implementations SHOULD detect when a peer is persistently sending bad messages and terminate the local connection state after such misbehavior is detected.

4.2.8. Establishing New Associations With Existing Parameters

If a DTLS client-server pair are configured in such a way that repeated connections happen on the same host/port quartet, then it is possible that a client will silently abandon one connection and then initiate another with the same parameters (e.g., after a reboot). This will appear to the server as a new handshake with epoch=0. In cases where a server believes it has an existing association on a given host/port quartet and it receives an epoch=0 ClientHello, it SHOULD proceed with a new handshake but MUST NOT destroy the existing association until the client has demonstrated reachability either by completing a cookie exchange or by completing a complete handshake including delivering a verifiable Finished message. After a correct Finished is received, the server MUST abandon the previous association to avoid confusion between two valid associations with overlapping epochs. The reachability requirement prevents off-path/blind attackers from destroying associations merely by sending forged ClientHellos.

4.3. Summary of new syntax

This section includes specifications for the data structures that

have changed between TLS 1.2 and DTLS 1.2. See [TLS12] for the definition of this syntax.

4.3.1. Record Layer

```
      struct {
        ContentType type;
        ProtocolVersion version;
        uint16 epoch;                                  // New field
        uint48 sequence_number;                        // New field
        uint16 length;
        opaque fragment[DTLSPlaintext.length];
      } DTLSPlaintext;

      struct {
        ContentType type;
        ProtocolVersion version;
        uint16 epoch;                                  // New field
        uint48 sequence_number;                        // New field
        uint16 length;
        opaque fragment[DTLSCompressed.length];
      } DTLSCompressed;

      struct {
        ContentType type;
        ProtocolVersion version;
        uint16 epoch;                                  // New field
        uint48 sequence_number;                        // New field
        uint16 length;
        select (CipherSpec.cipher_type) {
          case block:  GenericBlockCipher;
          case aead:   GenericAEADCipher;              // New field
        } fragment;
      } DTLSCiphertext;
```

4.3.2. Handshake Protocol

```
      enum {
        hello_request(0), client_hello(1), server_hello(2),
        hello_verify_request(3),                       // New field
        certificate(11), server_key_exchange (12),
        certificate_request(13), server_hello_done(14),
        certificate_verify(15), client_key_exchange(16),
        finished(20), (255)
      } HandshakeType;

      struct {
        HandshakeType msg_type;
        uint24 length;
        uint16 message_seq;                            // New field
        uint24 fragment_offset;                        // New field
```

```
        uint24 fragment_length;                          // New field
        select (HandshakeType) {
          case hello_request: HelloRequest;
          case client_hello:  ClientHello;
          case server_hello:  ServerHello;
          case hello_verify_request: HelloVerifyRequest;  // New field
          case certificate:Certificate;
          case server_key_exchange: ServerKeyExchange;
          case certificate_request: CertificateRequest;
          case server_hello_done:ServerHelloDone;
          case certificate_verify:  CertificateVerify;
          case client_key_exchange: ClientKeyExchange;
          case finished: Finished;
        } body;
      } Handshake;

      struct {
        ProtocolVersion client_version;
        Random random;
        SessionID session_id;
        opaque cookie<0..2^8-1>;                            // New field
        CipherSuite cipher_suites<2..2^16-1>;
        CompressionMethod compression_methods<1..2^8-1>;
      } ClientHello;

      struct {
        ProtocolVersion server_version;
        opaque cookie<0..2^8-1>;
      } HelloVerifyRequest;
```

5. Security Considerations

This document describes a variant of TLS 1.2 and therefore most of the security considerations are the same as those of TLS 1.2 [TLS12], described in Appendices D, E, and F.

The primary additional security consideration raised by DTLS is that of denial of service. DTLS includes a cookie exchange designed to protect against denial of service. However, implementations which do not use this cookie exchange are still vulnerable to DoS. In particular, DTLS servers which do not use the cookie exchange may be used as attack amplifiers even if they themselves are not experiencing DoS. Therefore, DTLS servers SHOULD use the cookie exchange unless there is good reason to believe that amplification is not a threat in their environment. Clients MUST be prepared to do a cookie exchange with every handshake.

Unlike TLS implementations DTLS implementations SHOULD NOT respond to

invalid records by terminating the connection. See Section 4.1.2.7 for details on this.

6. Acknowledgements

The authors would like to thank Dan Boneh, Eu-Jin Goh, Russ Housley, Constantine Sapuntzakis, and Hovav Shacham for discussions and comments on the design of DTLS. Thanks to the anonymous NDSS reviewers of our original NDSS paper on DTLS [DTLS] for their comments. Also, thanks to Steve Kent for feedback that helped clarify many points. The section on PMTU was cribbed from the DCCP specification [DCCP]. Pasi Eronen provided a detailed review of this specification. Peter Saint-Andre provided the changes list in Section 8. elpful comments on the document were also received from Mark Allman, Jari Arkko, Mohamed Badra, Michael D'Errico, Adrian Farrell, Joel Halpern, Ted Hardie, Charlia Kaufman, Pekka Savola, Allison Mankin, Nikos Mavrogiannopoulos, Alexey Melnikov, Robin Seggelman, Michael Tuexen, Juho Vaha-Herttua, and Florian Weimer.

7. IANA Considerations

This document uses the same identifier space as TLS [TLS12], so no new IANA registries are required. When new identifiers are assigned for TLS, authors MUST specify whether they are suitable for DTLS. IANA [should modify/has modified] all TLS parameter registries to add a DTLS-OK flag, indicating whether the specification may be used with DTLS.

This document defines a new handshake message, hello_verify_request, whose value has been allocated from the TLS HandshakeType registry defined in [TLS12]. The value "3" has been assigned by the IANA.

8. Changes Since DTLS 1.0

This document reflects the following changes since DTLS 1.0 [DTLS1].

- Updated to match TLS 1.2 [TLS12].

- Addition of AEAD Ciphers in Section 4.1.2.3 (tracking changes in TLS 1.2.

- Clarifications regarding sequence numbers and epochs in Section 4.1 and a clear procedure for dealing with state loss in Section 4.2.8.

- Clarifications and more detailed rules regarding Path MTU issues in Section 4.1.1.1. Clarification of the fragmentation text throughout.

- Clarifications regarding handling of invalid records in Section 4.1.2.7.

- A new paragraph describing handling of invalid cookies at the end of

Section 4.2.1.

- Some new text describing how to avoid handshake deadlock conditions at the end of Section 4.2.4.

- Some new text about CertificateVerify messages in Section 4.2.6.

- A prohibition on epoch wrapping in Section 4.1.

- Clarification of the IANA requirements and the explicit requirement for a new IANA registration flag for each parameter.

- Numerous editorial changes.

9. References

9.1. Normative References

[RFC1191] Mogul, J. and S. Deering, "Path MTU discovery", RFC 1191, November 1990.

[RFC1885] Conta, A., and S. Deering, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 1885, December 1995.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC2988] Paxson, V. and M. Allman, "Computing TCP's Retransmission Timer", RFC 2988, November 2000.

[RFC4821] Mathis, M., and J. Heffner, "Packetization Layer Path MTU Discovery", RFC 4821, March 2007.

[RSAGCM] Salowey, J., Choudhury, A., and D. McGrew, "AES-GCM Cipher Suites for TLS", RFC 5288, August 2008.

[TCP] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, September 1981.

[TLS12] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, May 2008.

9.2. Informative References

[DCCP] Kohler, E., Handley, M., Floyd, S., Padhye, J., "Datagram Congestion Control Protocol", Work in Progress, 10 March 2005.

[DCCPDTLS] T. Phelan, "Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP)", RFC 5238, May 2008.

[DTLS] Modadugu, N., Rescorla, E., "The Design and Implementation of Datagram TLS", Proceedings of ISOC NDSS 2004, February 2004.

[DTLS1] Rescorla, E., and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.

[ECCGCM] E. Rescorla, "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode", RFC 5289, August 2008.

[ESP] S. Kent "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[IKEv2] C. Kaufman (ed), "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[IMAP] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, March 2003.

[PHOTURIS] Karn, P. and W. Simpson, "Photuris: Session-Key Management Protocol", RFC 2522, March 1999.

[POP] Myers, J. and M. Rose, "Post Office Protocol - Version 3", STD 53, RFC 1939, May 1996.

[REQ] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[SIP] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[TLS] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[TLS11] Dierks, T. and E. Rescorla, "The Transport Layer Security

(TLS) Protocol Version 1.1", RFC 4346, April 2006.

[WHYIPSEC] Bellovin, S., "Guidelines for Mandating the Use of IPsec", RFC 5406, October 2003.

Authors' Addresses

Eric Rescorla
RTFM, Inc.
2064 Edgewood Drive
Palo Alto, CA 94303

EMail: ekr@rtfm.com

Nagendra Modadugu
Computer Science Department
Stanford University
353 Serra Mall
Stanford, CA 94305

EMail: nagendra@cs.stanford.edu

TLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 15, 2011

D. McGrew
Cisco Systems, Inc.
D. Bailey
RSA, the Security Division of EMC

March 14, 2011

AES-CCM Cipher Suites for TLS
draft-mcgrew-tls-aes-ccm-01

Abstract

This memo describes the use of the Advanced Encryption Standard (AES) in the Counter and CBC-MAC Mode (CCM) of operation within Transport Layer Security (TLS) to provide confidentiality and data origin authentication. The AES-CCM algorithm is amenable to compact implementations, making it suitable for constrained environments.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 15, 2011.

Copyright Notice

described in the Simplified BSD License.

Table of Contents

1. Introduction

This document describes the use of Advanced Encryption Standard (AES) [AES] in Counter with CBC-MAC Mode (CCM) [CCM] in several TLS ciphersuites. AES-CCM provides both authentication and confidentiality and uses as its only primitive the AES encrypt operation (the AES decrypt operation is not needed). This makes it amenable to compact implementations, which is advantageous in constrained environments. The use of AES-CCM has been specified for IPsec ESP [RFC4309] and 802.15.4 wireless networks [IEEE802154].

Authenticated encryption, in addition to providing confidentiality for the plaintext that is encrypted, provides a way to check its integrity and authenticity. Authenticated Encryption with Associated Data, or AEAD [RFC5116], adds the ability to check the integrity and authenticity of some associated data that is not encrypted. This note utilizes the AEAD facility within TLS 1.2 [RFC5246] and the AES-CCM-based AEAD algorithms defined in [RFC5116]. Additional AEAD algorithms are defined, which use AES-CCM but which have shorter authentication tags, and therefore are more suitable for use across networks in which bandwidth is constrained and message sizes may be small.

The ciphersuites defined in this document use RSA or Pre-Shared Key (PSK) as their key establishment mechanism; these ciphersuites can be used with DTLS [RFC4347].

2. Conventions Used In This Document

he key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]

3. RSA Based AES-CCM Cipher Suites

The ciphersuites defined in this document are based on the the AES-CCM authenticated encryption with associated data (AEAD) algorithms AEAD_AES_128_CCM and AEAD_AES_256_CCM described in [RFC5116]. The following RSA-based ciphersuites are defined:

```
CipherSuite TLS_RSA_WITH_AES_128_CCM = {TBD1,TBD1}
CipherSuite TLS_RSA_WITH_AES_256_CCM = {TBD2,TBD2)
CipherSuite TLS_RSA_DHE_WITH_AES_128_CCM = {TBD3,TBD3}
CipherSuite TLS_RSA_DHE_WITH_AES_256_CCM = {TBD4,TBD4}
CipherSuite TLS_RSA_WITH_AES_128_CCM_8 = {TBD5,TBD5}
CipherSuite TLS_RSA_WITH_AES_256_CCM_8 = {TBD6,TBD6)
```

```
   CipherSuite TLS_RSA_DHE_WITH_AES_128_CCM_8 = {TBD7,TBD7}
   CipherSuite TLS_RSA_DHE_WITH_AES_256_CCM_8 = {TBD8,TBD8}
```

These ciphersuites make use of the AEAD capability in TLS 1.2 [RFC5246]. Note that each of these AEAD algorithms uses a 128-bit authentication tag with CCM.

The HMAC truncation option described in Section 3.5 of [RFC4366] (which negotiates the "truncated_hmac" TLS extension) does not have an effect on cipher suites that do not use HMAC.

The "nonce" input to the AEAD algorithm is exactly that of [RFC5288]: the "nonce" SHALL be 12 bytes long and is constructed as follows:

```
      struct {
         case client:
            uint32 client_write_IV;  // low order 32-bits
         case server:
            uint32 server_write_IV;  // low order 32-bits
         uint64 seq_num;
      } CCMNonce.
```

In DTLS, the 64-bit seq_num is the 16-bit epoch concatenated with the 48-bit seq_num.

These ciphersuites make use of the default TLS 1.2 Pseudorandom Function (PRF), which uses HMAC with the SHA-256 hash function. The RSA and RSA-DHE key exchange is performed as defined in [RFC5288].

4. PSK Based AES-CCM Cipher Suites

As in Section Section 3, these ciphersuites follow [RFC5116]. The following ciphersuites are defined:

```
   CipherSuite TLS_PSK_WITH_AES_128_CCM = {TBD9,TBD9}
   CipherSuite TLS_PSK_WITH_AES_256_CCM = {TBD10,TBD10)
   CipherSuite TLS_PSK_DHE_WITH_AES_128_CCM = {TBD11,TBD11}
   CipherSuite TLS_PSK_DHE_WITH_AES_256_CCM = {TBD12,TBD12}
   CipherSuite TLS_PSK_WITH_AES_128_CCM_8 = {TBD13,TBD13}
   CipherSuite TLS_PSK_WITH_AES_256_CCM_8 = {TBD14,TBD14)
   CipherSuite TLS_PSK_DHE_WITH_AES_128_CCM_8 = {TBD15,TBD15}
   CipherSuite TLS_PSK_DHE_WITH_AES_256_CCM_8 = {TBD16,TBD16}
```

The "nonce" input to the AEAD algorithm is defined as in Section Section 3.

These ciphersuites make use of the default TLS 1.2 Pseudorandom

Function (PRF), which uses HMAC with the SHA-256 hash function. The PSK and PSK-DHE key exchange is performed as defined in [RFC5487].

5. TLS Versions

These ciphersuites make use of the authenticated encryption with additional data defined in TLS 1.2 [RFC5288]. They MUST NOT be negotiated in older versions of TLS. Clients MUST NOT offer these cipher suites if they do not offer TLS 1.2 or later. Servers which select an earlier version of TLS MUST NOT select one of these cipher suites. Because TLS has no way for the client to indicate that it supports TLS 1.2 but not earlier, a non-compliant server might potentially negotiate TLS 1.1 or earlier and select one of the cipher suites in this document. Clients MUST check the TLS version and generate a fatal "illegal_parameter" alert if they detect an incorrect version.

6. New AEAD algorithms

The following AEAD algorithms are defined:

```
AEAD_AES_128_CCM_8 = TBD17
AEAD_AES_256_CCM_8 = TBD18
AEAD_AES_128_CCM_12 = TBD19
AEAD_AES_256_CCM_12 = TBD20
```

6.1. AES-128-CCM with an 8-octet Integrity Check Value (ICV)

The AEAD_AES_128_CCM_8 authenticated encryption algorithm is identical to the AEAD_AES_128_CCM algorithm (see Section 5.3 of [RFC5116]), except that it uses eight octets for authentication, instead of the full sixteen octets used by AEAD_AES_128_CCM. The AEAD_AES_128_CCM_8 ciphertext consists of the ciphertext output of the CCM encryption operation concatenated with the 8-octet authentication tag output of the CCM encryption operation. Test cases are provided in [CCM]. The input and output lengths are as for AEAD_AES_128_CCM. An AEAD_AES_128_CCM_8 ciphertext is exactly 8 octets longer than its corresponding plaintext.

6.2. AES-256-CCM with a 8-octet Integrity Check Value (ICV)

The AEAD_AES_256_CCM_8 authenticated encryption algorithm is identical to the AEAD_AES_256_CCM algorithm (see Section 5.4 of [RFC5116]), except that it uses eight octets for authentication, instead of the full sixteen octets used by AEAD_AES_256_CCM. The AEAD_AES_256_CCM_8 ciphertext consists of the ciphertext output of the CCM encryption operation concatenated with the 8-octet

authentication tag output of the CCM encryption operation. Test cases are provided in [CCM]. The input and output lengths are as as for AEAD_AES_128_CCM. An AEAD_AES_128_CCM_8 ciphertext is exactly 8 octets longer than its corresponding plaintext.

7. IANA Considerations

IANA has assigned the values for the ciphersuites defined in Section 3 and Section 4 and the values of the AEAD algorithms defined in Section 6.

8. Security Considerations

8.1. Perfect Forward Secrecy

The perfect forward secrecy properties of RSA based TLS ciphersuites are discussed in the security analysis of [RFC4346]. It should be noted that only the ephemeral Diffie-Hellman based ciphersuites are capable of providing perfect forward secrecy.

8.2. Counter Reuse

AES-CCM security requires that the counter is never reused. The IV construction in Section 3 is designed to prevent counter reuse.

9. Acknowledgements

This draft borrows heavily from [RFC5288].

10. References

10.1. Normative References

[AES] National Institute of Standards and Technology, "Specification for the Advanced Encryption Standard (AES)", FIPS 197, November 2001.

[CCM] National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", SP 800-38C, May 2004.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[RFC4347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security", RFC 4347, April 2006.

[RFC4366] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 4366, April 2006.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, January 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5288] Salowey, J., Choudhury, A., and D. McGrew, "AES Galois Counter Mode (GCM) Cipher Suites for TLS", RFC 5288, August 2008.

[RFC5487] Badra, M., "Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode", RFC 5487, March 2009.

10.2. Informative References

[IEEE802154] Institute of Electrical and Electronics Engineers, "Wireless Personal Area Networks", IEEE Standard 802.15.4-2006, 2006.

[RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, December 2005.

Authors' Addresses

David McGrew
Cisco Systems, Inc.
170 W Tasman Drive
San Jose, CA 95134
USA

Email: mcgrew@cisco.com

Daniel V. Bailey
RSA, the Security Division of EMC
174 Middlesex Tpke.
Bedford, MA 01463
USA

Email: dbailey@rsa.com

TLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: July 23, 2011

D. McGrew
Cisco Systems, Inc.
D. Bailey
RSA/EMC
M. Campagna
R. Dugal
Certicom Corp.

January 19, 2011

AES-CCM ECC Cipher Suites for TLS
draft-mcgrew-tls-aes-ccm-ecc-01

Abstract

This memo describes the use of the Advanced Encryption Standard (AES) in the Counter and CBC-MAC Mode (CCM) of operation within Transport Layer Security (TLS) to provide confidentiality and data origin authentication. The AES-CCM algorithm is amenable to compact implementations, making it suitable for constrained environments. The ciphersuites defined in this document use Elliptic Curve Cryptography (ECC), and are intended for use in networks with limited bandwidth.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 23, 2011.

Copyright Notice

Table of Contents

1. Introduction

This document describes the use of Advanced Encryption Standard (AES) [AES] in Counter with CBC-MAC Mode (CCM) [CCM] in several TLS ciphersuites. AES-CCM provides both authentication and confidentiality and uses as its only primitive the AES encrypt operation (the AES decrypt operation is not needed). This makes it amenable to compact implementations, which is advantageous in constrained environments. The use of AES-CCM has been specified for IPsec ESP [RFC4309] and 802.15.4 wireless networks [IEEE802154].

Authenticated encryption, in addition to providing confidentiality for the plaintext that is encrypted, provides a way to check its integrity and authenticity. Authenticated Encryption with Associated Data, or AEAD [RFC5116], adds the ability to check the integrity and authenticity of some associated data that is not encrypted. This note utilizes the AEAD facility within TLS 1.2 [RFC5246] and the AES-CCM-based AEAD algorithms defined in [RFC5116]. Additional AEAD algorithms are defined in this note; these use AES-CCM but have shorter authentication tags, and therefore are more suitable for use across networks in which bandwidth is constrained and message sizes may be small.

The ciphersuites defined in this document use Ephemeral Elliptic Curve Diffie-Hellman (ECDHE) as their key establishment mechanism; these ciphersuites can be used with DTLS [I-D.ietf-tls-rfc4347-bis].

1.1. Conventions Used In This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]

2. ECC based AES-CCM Cipher Suites

The ciphersuites defined in this document are based on the AES-CCM authenticated encryption with associated data (AEAD) algorithms AEAD_AES_128_CCM and AEAD_AES_256_CCM described in [RFC5116]. The following ciphersuites are defined:

```
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_CCM = {TBD1,TBD1}
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_CCM = {TBD2,TBD2)
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 = {TBD3,TBD3}
CipherSuite TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 = {TBD4,TBD4)
```

These ciphersuites make use of the AEAD capability in TLS 1.2 [RFC5246]. Note that each of these AEAD algorithms uses AES-CCM. Ciphersuites ending with "8" use eight-octet authentication tags; the other ciphersuites have 16 octet authentication tags.

The HMAC truncation option described in Section 3.5 of [RFC4366] (which negotiates the "truncated_hmac" TLS extension) does not have an effect on the cipher suites defined in this note, because they do not use HMAC to protect TLS records.

The "nonce" input to the AEAD algorithm is defined as in [RFC5288]. The "nonce" SHALL be 12 bytes long and constructed as follows:

```
struct {
   case client:
      uint32 client_write_IV;  // low order 32-bits
   case server:
      uint32 server_write_IV;  // low order 32-bits
   uint64 seq_num;
} CCMNonce.
```

In DTLS, the 64-bit seq_num field is the 16-bit DTLS epoch field concatenated with the 48-bit sequence_number field. The epoch and sequence_number appear in the DTLS record layer.

This construction allows the internal counter to be 32-bits long, which is a convenient size for use with CCM.

These ciphersuites make use of the default TLS 1.2 Pseudorandom Function (PRF), which uses HMAC with the SHA-256 hash function.

The ECDHE_ECDSA key exchange is performed as defined in [RFC4492], with the following additional stipulations:

The curves secp256r1 and secp384r1 MUST be supported, and the curve secp521r1 MAY be supported; these curves are equivalent to

the NIST P-256, P-384, and P-521 curves. Note that all of these curves have cofactor equal to one, which simplifies their use.

The server's certificate MUST contain an ECDSA-capable public key, it MUST be signed with ECDSA, and it MUST use SHA-256, SHA-384, or SHA-512. The Signature Algorithms extension (Section 7.4.1.4.1 of [RFC5246]) MUST be used to indicate support of those signature and hash algorithms. If a client certificate is used, the same conditions apply to it. The acceptable choices of hashes and curves that can be used with each ciphersuite are detailed in Section 2.1.

The uncompressed point format MUST be supported. Other point formats MAY be used.

The client MUST offer the elliptic_curves extension and the server MUST expect to receive it.

The client MAY offer the ec_point_formats extension, but the server need not expect to receive it.

[I-D.mcgrew-fundamental-ecc] MAY be used as an implementation method.

Implementations of these ciphersuites will interoperate with [RFC4492], but can be more compact than a full implementation of that RFC.

2.1. Required Algorithms for each CipherSuite

The curves and hash algorithms that can be used with each ciphersuite are described in the following table.

CipherSuite	Algorithms
TLS_ECDHE_ECDSA_WITH_AES_128_CCM TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8	MUST support secp256r1, SHA-256 MAY support secp384r1, SHA-384 MAY support secp521r1, SHA-512
TLS_ECDHE_ECDSA_WITH_AES_256_CCM TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8	MUST support secp384r1, SHA-384

	MAY support secp521r1, SHA-512

3. TLS Versions

These ciphersuites make use of the authenticated encryption with additional data defined in TLS 1.2 [RFC5288]. They MUST NOT be negotiated in older versions of TLS. Clients MUST NOT offer these cipher suites if they do not offer TLS 1.2 or later. Servers which select an earlier version of TLS MUST NOT select one of these cipher suites. Because TLS has no way for the client to indicate that it supports TLS 1.2 but not earlier, a non-compliant server might potentially negotiate TLS 1.1 or earlier and select one of the cipher suites in this document. Clients MUST check the TLS version and generate a fatal "illegal_parameter" alert if they detect an incorrect version.

4. New AEAD algorithms

The following AEAD algorithms are defined:

```
AEAD_AES_128_CCM_8 = TBD9
AEAD_AES_256_CCM_8 = TBD10
AEAD_AES_128_CCM_12 = TBD11
AEAD_AES_256_CCM_12 = TBD12
```

4.1. AES-128-CCM with an 8-octet ICV

The AEAD_AES_128_CCM_8 authenticated encryption algorithm is identical to the AEAD_AES_128_CCM algorithm (see Section 5.3 of [RFC5116]), except that it uses eight octets for authentication, instead of the full sixteen octets used by AEAD_AES_128_CCM. The AEAD_AES_128_CCM_8 ciphertext consists of the ciphertext output of the CCM encryption operation concatenated with the 8-octet authentication tag output of the CCM encryption operation. Test cases are provided in [CCM]. The input and output lengths are as for AEAD_AES_128_CCM. An AEAD_AES_128_CCM_8 ciphertext is exactly 8 octets longer than its corresponding plaintext.

4.2. AES-256-CCM with an 8-octet ICV

The AEAD_AES_256_CCM_8 authenticated encryption algorithm is identical to the AEAD_AES_256_CCM algorithm (see Section 5.4 of [RFC5116]), except that it uses eight octets for authentication, instead of the full sixteen octets used by AEAD_AES_256_CCM. The AEAD_AES_256_CCM_8 ciphertext consists of the ciphertext output of the CCM encryption operation concatenated with the 8-octet authentication tag output of the CCM encryption operation. Test cases are provided in [CCM]. The input and output lengths are as for AEAD_AES_128_CCM. An AEAD_AES_128_CCM_8 ciphertext is exactly 8 octets longer than its corresponding plaintext.

5. IANA Considerations

IANA has assigned values for the Ciphersuites defined in Section 2 and the AEAD algorithms defined in Section 4 of this note.

6. Security Considerations

6.1. Perfect Forward Secrecy

The perfect forward secrecy properties of ephemeral Diffie-Hellman ciphersuites are discussed in the security analysis of [RFC4346]. This analysis applies to the ECDHE ciphersuites.

6.2. Counter Reuse

AES-CCM security requires that the counter is never reused. The IV construction in Section 2 is designed to prevent counter reuse.

7. Acknowledgements

This draft borrows heavily from [RFC5288].

This draft is motivated by the considerations raised in the Zigbee Smart Energy 2.0 working group.

8. References

8.1. Normative References

[AES] National Institute of Standards and Technology, "Specification for the Advanced Encryption Standard (AES)", FIPS 197, November 2001.

[CCM] National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", SP 800-38C, May 2004.

[I-D.ietf-tls-rfc4347-bis] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security version 1.2", draft-ietf-tls-rfc4347-bis-03 (work in progress), October 2009.

[I-D.mcgrew-fundamental-ecc] McGrew, D., Igoe, K., and M. Salter, "Fundamental Elliptic Curve Cryptography Algorithms", draft-mcgrew-fundamental-ecc-04 (work in progress), December 2010.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[RFC4366] Blake-Wilson, S., Nystrom, M., Hopwood, D., Mikkelsen, J., and T. Wright, "Transport Layer Security (TLS) Extensions", RFC 4366, April 2006.

[RFC4492] Blake-Wilson, S., Bolyard, N., Gupta, V., Hawk, C., and B. Moeller, "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)", RFC 4492, May 2006.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, January 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5288] Salowey, J., Choudhury, A., and D. McGrew, "AES Galois Counter Mode (GCM) Cipher Suites for TLS", RFC 5288, August 2008.

8.2. Informative References

[IEEE802154]
Institute of Electrical and Electronics Engineers, "Wireless Personal Area Networks", IEEE Standard 802.15.4-2006, 2006.

[RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, December 2005.

Authors' Addresses

David McGrew
Cisco Systems, Inc.
170 W Tasman Drive
San Jose, CA 95134
USA

Email: mcgrew@cisco.com

Daniel V. Bailey
RSA/EMC
174 Middlesex Tpke.
Bedford, MA 01463
USA

Email: dbailey@rsa.com

Matthew Campagna
Certicom Corp.
5520 Explorer Drive #400
Mississauga, Ontario L4W 5L1
Canada

Email: mcampagna@certicom.com

Robert Dugal
Certicom Corp.
5520 Explorer Drive #400
Mississauga, Ontario L4W 5L1
Canada

Email: rdugal@certicom.com

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: September 15, 2011

Y. Pettersen
Opera Software ASA

March 14, 2011

Adding Multiple TLS Certificate Status Extension requests draft-pettersen-tls-ext-multiple-ocsp-02

Abstract

This document introduces a replacement of the TLS Certificate Status Extension to allow clients to specify and support multiple certificate status methods. Also being introduced is a new OCSP-based method that servers can use to provide status information not just about the server's own certificate, but also the status of intermediate certificates in the chain.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 15, 2011.

Copyright Notice

Table of Contents

1. Introduction

The Transport Layer Security Extension [RFC6066] framework defines, among other extensions, the Certificate Status Extension that clients can use to request the server's copy of the current status of its certificate. The benefits of this extension include a reduced number of roundtrips and network delays for the client to verify the status of the server's certificate using other retrieval methods and a reduced load on the certificate issuer's status response servers, thus solving a problem that can become significant when the issued certificate is presented by a frequently visited server.

There are two problems with the existing Certificate Status extension as it is currently defined. First, it does not provide functionality to request the status information about intermediate CA certificates, which means the client has to request this through other retrieval methods, such as CRLs, which can cause significant delays when the revocation list has to be refreshed. Second, the current format of the extension and requirements in the TLS protocol prevents a client from offering the server multiple status methods.

Many Certificate Authorities are now issuing intermediate CA certificates that not only specify a CRL Distribution Point[RFC5280], but also a URL for OCSP [RFC2560] Certificate Status requests. Given that CRLs, particularly those cached by the client, are frequently less up to date than is possible for an OCSP responder, using OCSP to access up-to-date status information about intermediate CA certificates will be of great benefit to clients. The benefit to the issuing CA is less clear, as providing the bandwidth for the OCSP responder can be costly, especially for CAs with many subscriber sites. The author is aware that the cost of providing this bandwidth just for site certificates has been a concern to some CAs, particularly the smaller ones, and it follows naturally that doubling or tripling this cost could be problematic for the CAs. The author is also aware of at least one case when OCSP requests for a high traffic site caused significant network problems for the issuing CA.

For these reasons, it will be beneficial to use the TLS server to provide the certificate status information not just for the server certificate, but also for the intermediate CA certificates. This will reduce the roundtrips needed to complete the handshake by the client to just those needed for negotiating the TLS connection. Also, for the Certificate Authorities, the load on their servers will depend on the number of certificates they have issued, not on the number of visitors to those sites.

For such a new system to be introduced seamlessly, it must be possible for clients to indicate support for the existing OCSP

Certificate Status method, and a new multiple, OCSP mode.

Unfortunately, the definition of the Certificate Status extension only allows a single Certificate Status extension to be defined in a single extension record in the handshake, and the TLS Protocol only allows a single record in the extension list for any given extension. This means that it is not possible for clients to indicate support for new methods while still supporting older methods, which would cause problems for interoperability between newer clients and older servers. This will not just be an issue for the multiple status request mode proposed above, but also for any other future status methods that might be introduced. This will be true not just for the current PKIX infrastructure, but also for alternative PKI structures.

The solution to this problem is to define a new extension, status_request_v2, with an extended format that allows the client to indicate support for multiple status request methods. This is implemented by using a list of CertificateStatusRequest records in the extension record. As the server will select the single status method based on the selected cipher suite and the certificate presented, no significant changes are needed in the server's extension format.

2. Multiple Certificate Status Extension

2.1. New extension

The extension added by this document is indicated by the "status_request_v2" in the ExtensionType enum, which is updated with this value:

```
enum {
    status_request_v2(XX) (65535)
} ExtensionType;
```

[[EDITOR: The value used for status_request_v2 has been left as XX. This value will be assigned when this draft progresses to RFC.]]

2.2. Multiple Certificate Status Request record

Clients that support a certificate status protocol like OCSP may send the status_request_v2 extension to the server in order to use the TLS handshake to transfer such data instead of downloading it through separate connections. When using this extension, the "extension_data" field of the extension SHALL contain a CertificateStatusRequestList where:

```
struct {
  CertificateStatusType status_type;
  select (status_type) {
    case ocsp: OCSPStatusRequest;
    case ocsp_multi: OCSPStatusRequest;
  } request;
} CertificateStatusRequest;

enum { ocsp(1), ocsp_multi(YY), (255) } CertificateStatusType;

struct {
  ResponderID responder_id_list<0..2^16-1>;
  Extensions request_extensions;
} OCSPStatusRequest;

opaque ResponderID<1..2^16-1>;
opaque Extensions<0..2^16-1>;

struct {
  CertificateStatusRequest certificate_status_req_list<1..2^16-1>
} CertificateStatusRequestList
```

[[EDITOR: The value used for ocsp_multi has been left as YY. This value will be assigned when this draft progresses to RFC.]]

In the OCSPStatusRequest, the "ResponderIDs" provides a list of OCSP responders that the client trusts. A zero-length "responder_id_list" sequence has the special meaning that the responders are implicitly known to the server, e.g., by prior arrangement, or are identfied by the certificates used by the server. "Extensions" is a DER encoding of OCSP request extensions.

Both "ResponderID" and "Extensions" are DER-encoded ASN.1 types as defined in [RFC2560]. "Extensions" is imported from [RFC5280]. A zero-length "request_extensions" value means that there are no extensions (as opposed to a zero-length ASN.1 SEQUENCE, which is not valid for the "Extensions" type).

In the case of the "id-pkix-ocsp-nonce" OCSP extension, [RFC2560] is unclear about its encoding; for clarification, the nonce MUST be a DER-encoded OCTET STRING, which is encapsulated as another OCTET STRING (note that implementations based on an existing OCSP client will need to be checked for conformance to this requirement).

The list of CertificateStatusRequest entries MUST be in order of preference.

Servers that receive a client hello containing the "status_request" extension MAY return a suitable certificate status response to the client along with their certificate. If OCSP is requested, they SHOULD use the information contained in the extension when selecting an OCSP responder and SHOULD include request_extensions in the OCSP request.

Servers return a certificate status response along with their certificate by sending a "CertificateStatus" message immediately after the "Certificate" message (and before any "ServerKeyExchange" or "CertificateRequest" messages). If a server returns a "CertificateStatus" message in response to a status_request_v2 request, then the server MUST have included an extension of type "status_request_v2" with empty "extension_data" in the extended server hello. The "CertificateStatus" message is conveyed using the handshake message type "certificate_status" as follows (see also [RFC6066]):

```
struct {
  CertificateStatusType status_type;
  select (status_type) {
    case ocsp: OCSPResponse;
    case ocsp_multi: OCSPResponseList;
  } response;
} CertificateStatus;

opaque OCSPResponse<0..2^24-1>;

struct {
  OCSPResponse ocsp_response_list<1..2^24-1>
} OCSPResponseList
```

An "OCSPResponse" element contains a complete, DER-encoded OCSP response (using the ASN.1 type OCSPResponse defined in [RFC2560]) . Only one OCSP response, with a length of at least one byte, may be sent for status_type "ocsp".

An "ocsp_response_list" contains a list of "OCSPResponse" elements, as specified above, each containing the OCSP response for the matching corresponding certificate in the server's Certificate TLS handshake message. that is, the first entry is the OCSP response for the first certificate in the Certificate list, the second entry is the response for the second certificate, and so on. The list MAY contain fewer OCSP responses than there were certificates in the Certificate handshake message, but there MUST NOT be more responses than there were certificates in the list. Individual elements of the list MAY have a length of 0 (zero) bytes, if the server does not have

the OCSP response for that particular certificate stored, in which case, the client MUST act as if a response was not received for that particular certificate. If the client receives a "ocsp_response_list" that does not contain a response for one or more of the certificates in the completed certificate chain, the client SHOULD attempt to validate the certificate using an alternative retrieval method, such as downloading the relevant CRL; OCSP SHOULD in this situation only be used for the end entity certificate, not intermediate CA certificates, for reasons stated above.

Note that a server MAY also choose not to send a "CertificateStatus" message, even if it has received a "status_request_v2" extension in the client hello message and has sent a "status_request_v2" extension in the server hello message. Additionally, note that that a server MUST NOT send the "CertificateStatus" message unless it received either a "status_request" or "status_request_v2" extension in the client hello message and sent a corresponding "status_request" or "status_request_v2" extension in the server hello message.

Clients requesting an OCSP response and receiving one or more OCSP responses in a "CertificateStatus" message MUST check the OCSP response(s) and abort the handshake, if the response is a revoked status or is otherwise not satisfactory with a bad_certificate_status_response(113) alert. This alert is always fatal.

[[Open issue: At least one reviewer has suggested that the client should treat an unsatisfactory (non-revoked) response as an empty response for that particular response and fall back to the alternative method described above]]

3. IANA Considerations

Section 2.1 defines the new TLS Extension status_request_v2 enum, which should be added to the ExtensionType Values list in the IANA TLS category after IETF Concensus has decided to add the value.

Section 2.2 describes a TLS CertificateStatusType Registry to be maintained by the IANA. CertificateStatusType values are to be assigned via IETF Review as defined in [RFC5226]. The initial registry corresponds to the definition of "ExtensionType" in Section 2.2.

4. Security Considerations

General Security Considerations for TLS Extensions are covered in

[RFC5246]. Security Considerations for the particular extension specified in this document are given below. In general, implementers should continue to monitor the state of the art and address any weaknesses identified.

4.1. Security Considerations for status_request

If a client requests an OCSP response, it must take into account that an attacker's server using a compromised key could (and probably would) pretend not to support the extension. In this case, a client that requires OCSP validation of certificates SHOULD either contact the OCSP server directly or abort the handshake.

Use of the OCSP nonce request extension (id-pkix-ocsp-nonce) may improve security against attacks that attempt to replay OCSP responses; see Section 4.4.1 of [RFC2560] for further details.

5. Alternative methods for similar functionality

There may be alternative methods to accomplish the same objective as this proposal, but without defining a new TLS Extension.

One possible method is that each OCSP response includes, recursively or separately, the OCSP response for its own signer as a responseExtensions. The problem with this method is that either the responder has to send this to all requestors, leading to increased bandwidth usage, or a special request extension or URL have to be sent by the TLS server requesting the OCSP response, and it would also lead to unnecessary bandwidth usage for the TLS server, if the connecting client cannot use the extra OCSP responses. It is the author's opinion that this approach would require the same level of complexity as the proposed extension in the webservers, in order to reduce bandwidth consumption, at least while phasing in the technology, and the OCSP responders would require similar level of complexity to produce the variant responses.

6. Acknowledgements

This document is based on [RFC6066] authored by Donald Eastlake 3rd.

7. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", RFC 2560, June 1999.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

[RFC6066] Eastlake, D., "Transport Layer Security (TLS) Extensions: Extension Definitions", RFC 6066, January 2011.

Author’s Address

Yngve N. Pettersen
Opera Software ASA

Email: yngve@opera.com