Network Working Group
Internet Draft
Intended Status: Informational
Expires: June 29, 2014

M. Peck
The MITRE Corporation
K. Igoe
National Security Agency
December 26, 2013

Suite B Profile for Datagram Transport Layer Security / Secure Real-time Transport Protocol (DTLS-SRTP) draft-peck-suiteb-dtls-srtp-04

Status of this Memo

Copyright Notice

Abstract

The United States government has published guidelines for "NSA Suite B Cryptography", which defines cryptographic algorithm policy for national security applications. This document describes the use of Suite B cryptography with the Datagram Transport Layer Security (DTLS) protocol, the Secure Real-Time Transport Protocol (SRTP), and the Secure Real-Time Transport Control Protocol (SRTCP) to provide a robust architecture for securing real-time data.

Table of Contents

1. Introduction

This document specifies the conventions for using NSA Suite B Cryptography [SuiteB] with the Datagram Transport Layer Security (DTLS) protocol, the Secure Real-time Transport Protocol (SRTP), and the Secure Real-time Transport Control Protocol (SRTCP) to provide a robust architecture for securing real-time data.

The Secure Real-time Transport Protocol (SRTP) provides confidentiality and message authentication to RTP traffic. The Secure Real-time Transport Control Protocol (SRTCP) provides message authentication and optional confidentiality to the Real-time Transport Control Protocol (RTCP) [RFC3711]. SRTP and SRTCP depend upon external key management to provide secret master keys from which to form encryption and authentication keys. RTP and RTCP are usually run over the User Datagram Protocol, UDP.

Datagram Transport Layer Security (DTLS), based upon the Transport Layer Security protocol (TLS), provides communication security for datagram protocols such as UDP [RFC6347]. DTLS-SRTP is an extension for DTLS that provides key management to SRTP and SRTCP as well as a choice of algorithms and parameters for the SRTP and SRTCP sessions [RFC5764].

[RFC6460] describes a Suite B profile for TLS and DTLS. This document builds upon RFC 6460, adding additional components to provide a Suite B profile for DTLS-SRTP.

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 [RFC2119].

2. Suite B Requirements

Suite B requires that key establishment and signature algorithms be based upon Elliptic Curve Cryptography and that the encryption algorithm be AES [FIPS197]. Suite B algorithms are defined to support two minimum levels of security: 128 and 192 bits. Suite B includes [SuiteB]:

Encryption	Advanced Encryption Standard (AES) (key sizes of 128 and 256 bits)
Digital Signature	Elliptic Curve Digital Signature Algorithm (ECDSA) [FIPS186-4] (using the curves with 256-

	and 384-bit prime moduli as specified in FIPS PUB 186-4)
Key Agreement	Elliptic Curve Diffie-Hellman (ECDH) [SP800-56A] (using the curves with 256- and 384-bit prime moduli as specified in FIPS PUB 186-4)
Secure Hash	SHA-256 and SHA-384 [FIPS180-4]

The curves with 256- and 384-bit prime moduli are described in NIST FIPS 186-4 [FIPS186-4]. They are referred to as P-256 and P-384, respectively. These elliptic curves appear in the literature under two different names. For sake of clarity, we list both names below:

Curve	NIST name	SECG name
P-256	nistp256	secp256r1
P-384	nistp384	secp384r1

3. Minimum Security Levels for Suite B Compliant Implementations

Suite B provides for two levels of cryptographic security, namely a 128-bit minimum level of security (minLOS_128) and a 192-bit minimum level of security (minLOS_192). Each level defines a minimum strength that all cryptographic algorithms must provide. We divide the Suite B non-signature primitives into two columns as shown in Table 1.

	Column 1	Column 2
Encryption	AES-128	AES-256
Key Agreement	ECDH on P-256	ECDH on P-384
Hash for PRF/MAC	SHA-256	SHA-384

Table 1: Suite B Cryptographic Non-Signature Primitives

At the 128-bit minimum level of security the non-signature primitives MUST either come exclusively from Column 1 or exclusively from Column 2.

At the 192-bit minimum level of security the non-signature primitives MUST come exclusively from Column 2.

3.1. DTLS Cryptographic Suites for minLOS_128 and minLOS_192

Each system MUST specify a security level of a minimum of 128 bits or 192 bits. The security level determines which suites from the Suite B compliant profile of [RFC6460] are allowed.

The two Suite B combinations, "SuiteB_Combination_1" or "SuiteB_Combination_2" from section 3.1 of [RFC6460], satisfy the requirements of section 3 of this document for the DTLS connection.

For a system to implement the Suite B compliant DLTS-SRTP profile, it MUST follow the requirements of [RFC6460] for the DTLS connection. The cipher suite rules from section 4 of [RFC6460] are summarized here:

- A Suite B compliant DTLS MUST use version 1.2 or higher.
- A system configured at a minimum level of security of 128 bits MUST use either TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, with TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 being the preferred choice.
- If configured at a minimum level of security of 192 bits, the system MUST use TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.
- The choice of curve used in the ECDH key exchange MUST agree with the requirements listed in Table 1 of section 3.

3.2. Suite B DTLS Authentication

Digital signatures using ECDSA MUST be used for authentication by Suite B compliant implementations. Using the notation of [RFC6460], "ECDSA-256" represents an instantiation of the ECDSA algorithm using the P-256 curve and the SHA-256 hash function. "ECDSA-384" represents an instantiation of the ECDSA algorithm using the P-384 curve and the SHA-384 hash function.

When running in Suite B compliant mode, a system configured at a minimum level of security of 128 bits MUST use either ECDSA-256 or ECDSA-384 for client and server authentication. It is allowable for one party to authenticate with ECDSA-256 and the other party to authenticate with ECDSA-384. This flexibility will allow

interoperability between a client and a server that have different sizes of ECDSA authentication keys.

In Suite B compliant mode, clients and servers in a system configured at a minimum level of security of 128 bits MUST be able to verify ECDSA-256 signatures and SHOULD be able to verify ECDSA-384 signatures unless it is absolutely certain that the implementation will never need to verify certificates from an authority which uses an ECDSA-384 signing key.

A system compliant with the Suite B profile and configured at a minimum level of security of 192 bits MUST use ECDSA-384 for both client and server DTLS authentication.

Clients and servers in a system configured at a minimum level of security of 192 bits MUST be able to verify ECDSA-384 signatures.

When in Suite B compliant mode, authentication methods other than ECDSA-256 and ECDSA-384 MUST NOT be used for DTLS authentication. If a relying party receives a message signed with any other authentication method, it MUST return a DTLS error and stop the DTLS handshake.

Mutual authentication MUST be performed by client and server [RFC5764].

3.3. Digital Signatures and Certificates

The initiator and responder, at both minimum levels of security, MUST each have an X.509 certificate that complies with the end entity signature certificate format defined in section 4.5.3 of "Suite B Certificate and Certificate Revocation List (CRL) Profile" [RFC5759].

4. Client and Server Handshake to Create DTLS Premaster Secret

DTLS-SRTP is defined for point-to-point media sessions, in which there are exactly two participants [RFC5764]. Two DTLS peers MUST follow the guidelines in [RFC6460] in order to be Suite B compliant. Two peers who wish to implement the Suite B DTLS-SRTP profile MUST implement DTLS 1.2 or later.

The peers MUST each generate an ephemeral elliptic curve key pair for key agreement using either the P-256 or P-384 curve. The curve chosen will depend upon the selected cipher suite, following the requirements of section 3. The peers will then execute the elliptic curve Diffie-Hellman (ECDH) key agreement to obtain a DTLS premaster

secret [SP800-56A, section 6.1.2.2]).

The DTLS premaster secret will be 32 bytes in length when using the P-256 curve and 48 bytes in length when using the P-384 curve.

Two Suite B DTLS-SRTP compliant peers MUST each have an X.509 certificate that complies with the Suite B end entity digital signature certificate profile [RFC5759]. The peer acting as the DTLS server will use his key and the ECDSA algorithm to sign the DTLS server key exchange message. For DTLS-SRTP implementations [RFC5764], the peer acting as server will send the CertificateRequest message. The peer acting as the client MUST then use his key and the ECDSA algorithm to sign the CertificateVerify message.

Peers compliant with Suite B for DTLS-SRTP MUST follow the certificate guidance in section 4.3 of [RFC6460].

5. DTLS Master Secret

For Suite B applications using DTLS 1.2 or later versions, the PRF used to compute the DTLS master secret will be:

When selecting the TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 cipher suite, the TLS PRF with SHA-256 as the hash function MUST be used as in [RFC5246].

When selecting the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher suite, the TLS PRF with SHA-384 as the hash function MUST be used as in [RFC5246].

The master secret will be 48 bytes in length for both PRFs.

6. SRTP Master Key and Master Salt

The DTLS master key is used in DTLS-SRTP to create SRTP master key and salt pairs for the two peers acting as client and server via the TLS exporter [RFC5764]. In particular, the PRF used to compute each SRTP master key and salt is the following:

- When the TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 cipher suite is chosen, the TLS PRF with SHA-256 as the hash function MUST be used. The SRTP master keys exported for the client and server MUST be 128 bits in size. The SRTP master salt values for the client and server MUST be 112 bits.

- When the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher suite is

chosen, the TLS PRF with SHA-384 as the hash function MUST be used. The SRTP master keys exported for the client and server MUST be 256 bits in size. The SRTP master salt values for the client and server MUST be 112 bits.

7. Suite B SRTP Protection Profiles

For Suite B applications, AES in Galois Counter Mode, AES-GCM, MUST be used to protect SRTP and SRTCP packets. Note that encryption is OPTIONAL but message authentication is MANDATORY for SRTCP packets [RFC3711]. Section 14.2 of [srtp-gcm] defines the DTLS-SRTP "SRTP Protection Profiles" used for Suite B.

The following AES_128 based SRTP protection profiles are applicable when using the TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 cipher suite for DTLS:

AEAD_AES_128_GCM_8
AEAD_AES_128_GCM_12

The following AES_256 based SRTP protection profiles are applicable when using the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher suite for DTLS:

AEAD_AES_256_GCM_8
AEAD_AES_256_GCM_12

Any Suite B compliant DTLS-SRTP application MUST use one of the above, no other encryption or integrity algorithms are allowed. In addition, the following constraints are imposed upon on any Suite B compliant DTLS-SRTP applications:

- Any application running at the 192-bit minimum level of security MUST support AEAD_AES_256_GCM_8 and SHOULD support AEAD_AES_256_GCM_12. The AES_128 based profiles MUST NOT be used.

- For applications running at the 128-bit minimum level of security, there are three options:

  - Option 1 (AES_128 based): The application MUST support AEAD_AES_128_GCM_8 and and SHOULD support AEAD_AES_128_GCM_12.

  - Option 2 (AES_256 based): The application MUST support AEAD_AES_256_GCM_8 and and SHOULD support AEAD_AES_256_GCM_12.

- Option 3 (both AES_128 and AES_256): The application MUST support both AEAD_AES_128_GCM_8 and AEAD_AES_256_GCM_8 and SHOULD support AEAD_AES_128_GCM_12 and AEAD_AES_256_GCM_12.

- Since the AES_128 based profiles are the preferred choice at the 128-bit minimum level of security, if Option 3 is used the AES_128 based profiles MUST be offered before the AES_256 based profiles.

8. DTLS Cipher Suite and SRTP Protection Profile Negotiation

As described in [RFC5764], the DTLS-SRTP peer acting as the client signals its acceptable SRTP protection profiles to the DTLS-SRTP peer acting as the server with the "use_srtp" DTLS extension. For Suite B, the client determines its acceptable SRTP protection profiles based on its offered TLS cipher suites.

- If the client offers TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, then the client MUST offer AEAD_AES_128_GCM_8 and MAY offer AEAD_AES_128_GCM_12.

- If the client offers TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, then the client MUST offer AEAD_AES_256_GCM_8 and MAY offer AEAD_AES_256_GCM_12.

The client MAY offer other cipher suites or protection profiles, but if used, the connection will not be Suite B compliant.

For Suite B, the DTLS-SRTP peer acting as the server chooses the DTLS cipher suite from the client's offerings and also chooses the SRTP protection profile from the client's offerings.

- If the server chooses TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, then it MUST choose AEAD_AES_128_GCM_8 or AEAD_AES_128_GCM_12.

- If the server chooses TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, then it MUST choose AEAD_AES_256_GCM_8 or AEAD_AES_256_GCM_12.

The server MAY choose other cipher suites or protection profiles, but if used, the connection will not be Suite B compliant. The client and server each have the option to terminate the connection if the chosen cipher suite and protection profile are not acceptable.

9. SRTP/SRTCP Key Derivation

The AES Counter Mode based key derivation function is used to derive

session keys and salts for SRTP/SRTCP [RFC3711]. The session keys and salts MUST have the following bit sizes:

When using the AEAD_AES_128_GCM_8 or AEAD_AES_128_GCM_12 protection profile:

```
SRTP master key (generated from DTLS):  128 bits
SRTP master salt (generated from DTLS): 112 bits
SRTP session encryption key:            128 bits
SRTP session authentication key:        not used for GCM
SRTP session salting key:               96 bits
```

When using the AEAD_AES_256_GCM_8 or AEAD_AES_256_GCM_12 protection profile:

```
SRTP master key (generated from DTLS):  256 bits
SRTP master salt (generated from DTLS): 112 bits
SRTP session encryption key:            256 bits
SRTP session authentication key:        not used for GCM
SRTP session salting key:               96 bits
```

10. Security Considerations

The security considerations of this document follow those in [srtp-gcm], [RFC3711], [RFC5759], [RFC5764], [RFC6347], and [RFC6460].

11. IANA Considerations

This document has no actions for IANA.

12. References

12.1. Normative References

[FIPS180-4] National Institute of Standards and Technology, FIPS Publication 180-4: "Secure Hash Standard", March 2012.

[FIPS186-4] National Institute of Standards and Technology, FIPS Publication 186-4: "Digital Signature Standard (DSS)", July 2013.

[FIPS197] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", FIPS Publication 197, November 2001.

[srtp-gcm] McGrew, D., and K. Igoe, "AES-GCM and AES-CCM

Authenticated Encryption in Secure RTP (SRTP)", draft-ietf-avtcore-srtp-aes-gcm-10, Work in Progress, September 2013.

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

[RFC3711] Baugher, M. McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

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

[RFC5759] Solinas, J. and L. Zieglar, "Suite B Certificate and Certificate Revocation List (CRL) Profile", RFC 5759, January 2010.

[RFC5764] McGrew, D. and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for Secure Real-time Transport Protocol (SRTP)", RFC 5764, May 2010.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[RFC6460] Salter, M. and R. Housley, "Suite B Profile for Transport Layer Security (TLS)", RFC 6460, January 2012.

12.2. Informative References

[SuiteB] U.S. National Security Agency, "NSA Suite B Cryptography", January 2009, <http://www.nsa.gov/ia/programs/suiteb_cryptography/>.

[SP800-56A] National Institute of Standards and Technology, Special Publication 800-56A: "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)", March 2007.

Authors' Addresses

Michael A. Peck
The MITRE Corporation
Email: mpeck@mitre.org

Kevin M. Igoe
NSA/CSS Commercial Solutions Center
National Security Agency
Email: kmigoe@nsa.gov

Acknowledgement

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).