Network Working Group
Request for Comments: 5430
Category: Informational

M. Salter
National Security Agency
E. Rescorla
Network Resonance
R. Housley
Vigil Security

March 2009

Suite B Profile for Transport Layer Security (TLS)

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

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 defines a profile of Transport Layer Security (TLS) version 1.2 that is fully conformant with Suite B. This document also defines a transitional profile for use with TLS version 1.0 and TLS version 1.1 which employs Suite B algorithms to the greatest extent possible.

Table of Contents

1. Introduction

The United States government has posted the Fact Sheet on National Security Agency (NSA) Suite B Cryptography [NSA], and at the time of writing, it states:

> To complement the existing policy for the use of the Advanced Encryption Standard (AES) to protect national security systems and information as specified in The National Policy on the use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information (CNSSP-15), the National Security Agency (NSA) announced Suite B Cryptography at the 2005 RSA Conference. In addition to the AES, Suite B includes cryptographic algorithms for hashing, digital signatures, and key exchange.
>
> Suite B only specifies the cryptographic algorithms to be used. Many other factors need to be addressed in determining whether a particular device implementing a particular set of

cryptographic algorithms should be used to satisfy a particular requirement.

Among those factors are "requirements for interoperability both domestically and internationally".

This document does not define any new cipher suites; instead, it defines two profiles:

- A Suite B compliant profile for use with TLS version 1.2 [RFC5246] and the cipher suites defined in [RFC5289]. This profile uses only Suite B algorithms.

- A transitional profile for use with TLS version 1.0 [RFC2246] or TLS version 1.1 [RFC4346] and the cipher suites defined in [RFC4492]. This profile uses the Suite B cryptographic algorithms to the greatest extent possible and provides backward compatibility. While the transitional profile is not Suite B compliant, it provides a transition path towards the Suite B compliant profile.

2. 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].

3. Suite B Requirements

The Fact Sheet on Suite B Cryptography requires that key establishment and authentication algorithms be based on Elliptic Curve Cryptography, and that the encryption algorithm be AES [AES]. Suite B defines two security levels, of 128 and 192 bits.

In particular, Suite B includes:

Encryption:	Advanced Encryption Standard (AES) [AES] -- FIPS 197 (with key sizes of 128 and 256 bits)
Digital Signature:	Elliptic Curve Digital Signature Algorithm (ECDSA) [DSS] - FIPS 186-2 (using the curves with 256- and 384-bit prime moduli)
Key Exchange:	Elliptic Curve Diffie-Hellman (ECDH) - NIST Special Publication 800-56A [PWKE] (using the curves with 256- and 384-bit prime moduli)

The 128-bit security level corresponds to an elliptic curve size of 256 bits and AES-128; it also makes use of SHA-256 [SHS]. The 192-bit security level corresponds to an elliptic curve size of 384 bits and AES-256; it also makes use of SHA-384 [SHS].

Note: Some people refer to the two security levels based on the AES key size that is employed instead of the overall security provided by the combination of Suite B algorithms. At the 128-bit security level, an AES key size of 128 bits is used, which does not lead to any confusion. However, at the 192-bit security level, an AES key size of 256 bits is used, which sometimes leads to an expectation of more security than is offered by the combination of Suite B algorithms.

To accommodate backward compatibility, a Suite B compliant client or server can be configured to accept a cipher suite that is not part of Suite B. However, whenever a Suite B compliant client and a Suite B compliant server establish a TLS version 1.2 session, only Suite B algorithms are employed.

4. Suite B Compliance and Interoperability Requirements

TLS version 1.1 [RFC4346] and earlier do not support Galois Counter Mode (GCM) cipher suites [RFC5289]. However, TLS version 1.2 [RFC5246] and later do support GCM. For Suite B TLS compliance, GCM cipher suites are REQUIRED to be used whenever both the client and the server support the necessary cipher suites. Also, for Suite B TLS compliance, Cipher Block Chaining (CBC) cipher suites are employed when GCM cipher suites cannot be employed.

For a client to implement the Suite B compliant profile, it MUST implement TLS version 1.2 or later, and the following cipher suite rules apply:

- A Suite B compliant TLS version 1.2 or later client MUST offer at least two cipher suites for each supported security level. For the 128-bit security level, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 MUST be offered in this order in the ClientHello message. For the 192-bit security level, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 and TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 MUST be offered in this order in the ClientHello message. One of these cipher suites MUST be the first (most preferred) cipher suite in the ClientHello message.

- A Suite B compliant TLS version 1.2 or later client that offers backward compatibility with TLS version 1.1 or earlier servers MAY offer an additional cipher suite for each supported security level. If these cipher suites are offered, they MUST appear after the ones discussed above. For the 128-bit security level, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA MAY be offered in the ClientHello message. For the 192-bit security level, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA MAY be offered in the ClientHello message.

- A Suite B compliant TLS version 1.2 or later client that offers interoperability with non-Suite B compliant servers MAY offer additional cipher suites. If any additional cipher suites are offered, they MUST appear after the ones discussed above in the ClientHello message.

For a client to implement the Suite B transitional profile, it MUST implement TLS version 1.1 or earlier and the following cipher suite rules apply:

- A Suite B transitional TLS version 1.1 or earlier client MUST offer the cipher suite for the 128-bit security level, the cipher suite for the 192-bit security level, or both. For the 128-bit security level, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA MUST be offered in the ClientHello message. For the 192-bit security level, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA MUST be offered in the ClientHello message. One of these cipher suites MUST be the first (most preferred) cipher suite in the ClientHello message.

- A Suite B transitional TLS version 1.1 or earlier client that offers interoperability with non-Suite B compliant servers MAY offer additional cipher suites. If any additional cipher suites are offered, they MUST appear after the ones discussed above in the ClientHello message.

A Suite B compliant TLS server MUST be configured to support the 128-bit security level, the 192-bit security level, or both security levels. The cipher suite rules for each of these security levels is described below. If a Suite B compliant TLS server is configured to support both security levels, then the configuration MUST prefer one security level over the other. In practice, this means that the cipher suite rules associated with the cipher suites listed in Section 4.1 for the preferred security level are processed before the cipher suite rules for the less preferred security level.

For a server to implement the Suite B conformant profile at the 128-bit security level, the following cipher suite rules apply:

- A Suite B compliant TLS version 1.2 or later server MUST accept the TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 cipher suite if it is offered.

- If the preceding cipher suite is not offered, then a Suite B compliant TLS version 1.2 or later server MUST accept the TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 cipher suite if it is offered.

- If neither of the preceding two cipher suites is offered, then a Suite B compliant TLS version 1.2 or later server that offers backward compatibility with TLS version 1.1 or earlier clients MAY accept the TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA cipher suite if it is offered.

- If the server is not offered any of the preceding three cipher suites and interoperability with clients that are not compliant or interoperable with Suite B is desired, then the server MAY accept another offered cipher suite that is considered acceptable by the server administrator.

For a server to implement the Suite B transitional profile at the 128-bit security level, the following cipher suite rules apply:

- A Suite B transitional TLS version 1.1 or earlier server MUST accept the TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA cipher suite if it is offered.

- If the server is not offered the preceding cipher suite and interoperability with clients that are not Suite B transitional is desired, then the server MAY accept another offered cipher suite that is considered acceptable by the server administrator.

For a server to implement the Suite B conformant profile at the 192-bit security level, the following cipher suite rules apply:

- A Suite B compliant TLS version 1.2 or later server MUST accept the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher suite if it is offered.

- If the preceding cipher suite is not offered, then a Suite B compliant TLS version 1.2 or later server MUST accept the TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 cipher suite if it is offered.

- If neither of the preceding two cipher suites is offered, then a Suite B compliant TLS version 1.2 or later server that offers backward compatibility with TLS version 1.1 or earlier clients MAY accept the TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA cipher suite if it is offered.

- If the server is not offered any of the preceding three cipher suites and interoperability with clients that are not compliant or interoperable with Suite B is desired, then the server MAY accept another offered cipher suite that is considered acceptable by the server administrator.

For a server to implement the Suite B transitional profile at the 192-bit security level, the following cipher suite rules apply:

- A Suite B transitional TLS version 1.1 or earlier server MUST accept the TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA cipher suite if it is offered.

- If the server is not offered the preceding cipher suite and interoperability with clients that are not Suite B transitional is desired, then the server MAY accept another offered cipher suite that is considered acceptable by the server administrator.

Note that these rules explicitly permit the use of CBC cipher suites in TLS version 1.2 connections in order to permit operation between Suite B compliant and non-Suite B compliant implementations. For instance, a Suite B compliant TLS version 1.2 client might offer TLS version 1.2 with both GCM and CBC cipher suites when communicating with a non-Suite B TLS version 1.2 server, which then selected the CBC cipher suites. This connection would nevertheless meet the requirements of this specification. However, any two Suite B compliant implementations will negotiate a GCM cipher suite when doing TLS version 1.2.

4.1. Security Levels

As described in Section 1, Suite B specifies two security levels: 128-bit and 192-bit. The following table lists the cipher suites for each security level. Within each security level, the cipher suites are listed in their preferred order for selection by a TLS version 1.2 implementation.

Cipher Suite	Security Level
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	128
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	128
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	192
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	192
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	192

4.2. Acceptable Curves

RFC 4492 defines a variety of elliptic curves. For cipher suites defined in this specification, only secp256r1(23) or secp384r1(24) may be used. These are the same curves that appear in FIPS 186-2 [DSS] as P-256 and P-384, respectively. For cipher suites at the 128-bit security level, secp256r1 MUST be used. For cipher suites at the 192-bit security level, secp384r1 MUST be used. RFC 4492 requires that the uncompressed(0) form be supported. The ansiX962_compressed_prime(1) point formats MAY also be supported.

Clients desiring to negotiate only a Suite B compliant connection MUST generate a "Supported Elliptic Curves Extension" containing only the allowed curves. These curves MUST match the cipher suite security levels being offered. Clients that are willing to do both Suite B compliant and non-Suite B compliant connections MAY omit the extension or send the extension but offer other curves as well as the appropriate Suite B ones.

Servers desiring to negotiate a Suite B compliant connection SHOULD check for the presence of the extension, but MUST NOT negotiate inappropriate curves even if they are offered by the client. This allows a client that is willing to do either Suite B compliant or non-Suite B compliant modes to interoperate with a server that will only do Suite B compliant modes. If the client does not advertise an acceptable curve, the server MUST generate a fatal "handshake_failure" alert and terminate the connection. Clients MUST check the chosen curve to make sure it is acceptable.

4.3. Certificates

Server and client certificates used to establish a Suite B compliant connection MUST be signed with ECDSA. Digital signatures MUST be calculated using either the P-256 curve along with the SHA-256 hash algorithm or calculated using the P-384 curve along with the SHA-384 hash algorithm. For certificates used at the 128-bit security level, the subject public key MUST use the P-256 curve and be signed with either the P-384 curve or the P-256 curve. For certificates used at the 192-bit security level, the subject public key MUST use the P-384 curve and be signed with the P-384 curve.

In TLS version 1.0 and TLS version 1.1, the key exchange algorithm used in the TLS_ECDHE_ECDSA-collection of cipher suites requires the server's certificate to be signed with a particular signature scheme. TLS version 1.2 offers more flexibility. This specification does not impose any additional restrictions on the server certificate signature or the signature schemes used elsewhere in the certification path. (Often such restrictions will be useful, and it is expected that this will be taken into account in practices of certification authorities. However, such restrictions are not strictly required, even if it is beyond the capabilities of a client to completely validate a given certification path, the client may be able to validate the server's certificate by relying on a trusted certification authority whose certificate appears as one of the intermediate certificates in the certification path.)

Likewise, this specification does not impose restrictions on signature schemes used in the certification path for the client's certificate when mutual authentication is employed.

4.4. signature_algorithms Extension

The signature_algorithms extension is defined in Section 7.4.1.4.1 of TLS version 1.2 [RFC5246]. A Suite B compliant TLS version 1.2 or later client MUST include the signature_algorithms extension. For the 128-bit security level, SHA-256 with ECDSA MUST be offered in the signature_algorithms extension. For the 192-bit security level, SHA-384 with ECDSA MUST be offered in the signature_algorithms extension. Other offerings MAY be included to indicate the signature algorithms that are acceptable in cipher suites that are offered for interoperability with servers that are not compliant with Suite B and to indicate the signature algorithms that are acceptable for certification path validation.

4.5. CertificateRequest Message

A Suite B compliant TLS version 1.2 or later server MUST include SHA-256 with ECDSA and/or SHA-384 with ECDSA in the supported_signature_algorithms field of the CertificateRequest message. For the 128-bit security level, SHA-256 with ECDSA MUST appear in the supported_signature_algorithms field. For the 192-bit security level, SHA-384 with ECDSA MUST appear in the supported_signature_algorithms field.

4.6. CertificateVerify Message

A Suite B compliant TLS version 1.2 or later client MUST use SHA-256 with ECDSA or SHA-384 with ECDSA for the signature in the CertificateVerify message. For the 128-bit security level, SHA-256 with ECDSA MUST be used. For the 192-bit security level, SHA-384 with ECDSA MUST be used.

4.7. ServerKeyExchange Message Signature

In the TLS_ECDHE_ECDSA-collection of cipher suites, the server sends its ephemeral ECDH public key and a specification of the corresponding curve in the ServerKeyExchange message. These parameters MUST be signed with ECDSA using the private key corresponding to the public key in the server’s certificate.

A TLS version 1.1 or earlier server MUST sign the ServerKeyExchange message using SHA-1 with ECDSA.

A Suite B compliant TLS version 1.2 or later server MUST sign the ServerKeyExchange message using either SHA-256 with ECDSA or SHA-384 with ECDSA. For the 128-bit security level, SHA-256 with ECDSA MUST be used. For the 192-bit security level, SHA-384 with ECDSA MUST be used.

5. Security Considerations

Most of the security considerations for this document are described in "The Transport Layer Security (TLS) Protocol Version 1.2" [RFC5246], "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)" [RFC4492], "AES Galois Counter Mode (GCM) Cipher Suites for TLS" [RFC5288], and "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)" [RFC5289]. Readers should consult those documents.

In order to meet the goal of a consistent security level for the entire cipher suite, in Suite B mode TLS implementations MUST ONLY use the curves defined in Section 4.2. Otherwise, it is possible to have a set of symmetric algorithms with much weaker or stronger security properties than the asymmetric (ECC) algorithms.

6. Acknowledgements

Thanks to Pasi Eronen, Steve Hanna, and Paul Hoffman for their review, comments, and insightful suggestions.

This work was supported by the US Department of Defense.

7. References

7.1. Normative References

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

[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.

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

[RFC5289] Rescorla, E., "TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)", RFC 5289, August 2008.

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

[DSS] National Institute of Standards and Technology, "Digital Signature Standard", FIPS 186-2, January 2000.

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

[SHS] National Institute of Standards and Technology, "Secure Hash Standard", FIPS 180-2, August 2002.

7.2. Informative References

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

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

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

[NSA] National Security Agency, "Fact Sheet NSA Suite B Cryptography", <http://www.nsa.gov/ia/Industry/crypto_suite_b.cfm>.

Authors' Addresses

Margaret Salter
National Security Agency
9800 Savage Rd.
Fort Meade 20755-6709
USA

EMail: msalter@restarea.ncsc.mil

Eric Rescorla
Network Resonance
2064 Edgewood Drive
Palo Alto 94303
USA

EMail: ekr@rtfm.com

Russ Housley
Vigil Security
918 Spring Knoll Drive
Herndon 21070
USA

EMail: housley@vigilsec.com