DICE Working Group
Internet Draft
Intended status: Standards Track
Expires: September 23, 2015

Jaeduck Choi
Gunhee Lee
NSRI
Namhi Kang
Duksung Women's University
Seungwook Jung
Souhwan Jung
Soongsil University

March 24, 2015

Fine-grained Support of Security Services for Constrained Devices using DTLS
draft-choi-dice-finegrained-dtls-security-01.txt

Abstract

This document proposes a method that can selectively apply application data encryption to the DTLS record layer. The CoAP used for resource-constrained devices defines the use of DTLS as a basic security mechanism, and CoAP standard specifies the use of AES_CCM that provides data integrity and confidentiality as a cipher suite for DTLS. However, not all CoAP messages require both data integrity and confidentiality. For example, in case of CoAP messages that include information for turning a light off at home or in a building, or simple ACK information, encryption might not be necessary because such information might not be useful to attackers. Furthermore, from the perspective of effective resource use of resource-constrained devices, reducing the computation load required to perform data encryption every time is necessary. This document describes the methods for CoAP nodes to establish DTLS security channels using the AES_CCM cipher suite, and to selectively apply the encryption function in the DTLS record layer by considering sensitivity to application data leakage.

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), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

This Internet-Draft will expire on September 23, 2015.

Copyright Notice

Table of Contents

1. Introduction

IETF CoRE WG has standardized Constrained Application Protocol (CoAP), which can be used for resource-constrained devices [RFC7252]. CoAP defines the use of Datagram Transport Layer Security (DTLS) for device authentication and communication data security, and DTLS specifies TLS_PSK_WITH_AES_128_CCM_8 as a mandatory cipher suite. For a public key-based DTLS cipher suite, CoAP recommends TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8. The DTLS cipher suite is negotiated between the CoAP client and server in the process of performing the DTLS handshake protocol. For CoAP application data, data integrity and confidentiality are provided in the DTLS record layer protocol by AES_CCM after completing the DTLS handshake protocol.

However, examining whether data integrity and confidentiality should be provided always for CoAP messages in resource-constrained devices is necessary. For example, the necessity of a data confidentiality function to send a CoAP message for turning a light switch off in a building or house is questionable. In the case of simultaneously turning on or off all lights in a building or house, such a function can provide clues for identifying whether residents are present in the building or house to malicious attackers intent on illegal entry. However, eavesdropping on CoAP messages for turning off or on some of the lights might not be significant to malicious attackers. In addition, simple ACK messages received from many devices in a CoAP group communication might not be useful to attackers. Furthermore, from the perspective of effective resource use of resource-constrained devices, reducing the computation load required to execute data encryption every time is necessary. Therefore, to minimize resource consumption of IoT devices, selectively applying the data confidentiality function by considering the sensitivity to leakage of application data is necessary.

The strain on memory capacity for loading an encryption module on IoT devices should also be considered. TLS defines the cipher suites that provide data integrity only using hash functions such as TLS_PSK_WITH_NULL_SHA256 [RFC5487]. Only integrity function can be provided to CoAP messages in the DTLS record layer after completing the DTLS handshake protocol with TLS_PSK_WITH_NULL_SHA256. However, if TLS_PSK_WITH_AES_128_CCM_8 and TLS_PSK_WITH_NULL_SHA256 are implemented on resource-constrained devices, burden on memory capacity can occur compared to devices that have only implemented TLS_PSK_WITH_AES_128_CCM_8 because the SHA256 module also has to be loaded.

In selectively applying the confidentiality function of CoAP messages, DTLS sessions would be re-established frequently. For example, to send a CoAP message that needs encryption, CoAP nodes will establish the DTLS session to the TLS_PSK_WITH_AES_128_CCM_8 or TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 cipher suits. While the DTLS session is maintained during the effective period, if a CoAP message that does not require encryption has to be sent, the CoAP nodes will terminate the current DTLS session and resume the DTLS session with the TLS_PSK_WITH_NULL_SHA256 cipher suite. In other words, because of unpredictable IoT service scenario characteristics (the characteristics where sensitivities to data leakage are different), situations can occur often whereby CoAP nodes have to re-establish DTLS sessions for different cipher suites that provide functions for both data integrity and confidentiality, and functions for data integrity only. This becomes a major cause for wasting resources when applying DTLS to CoAP nodes.

This document describes a method for selectively applying encryption functions in the DTLS record layer by considering the sensitivity to leakage of application data without changing the DTLS cipher suite, which is defined as the default in the CoAP protocol.

2. 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].

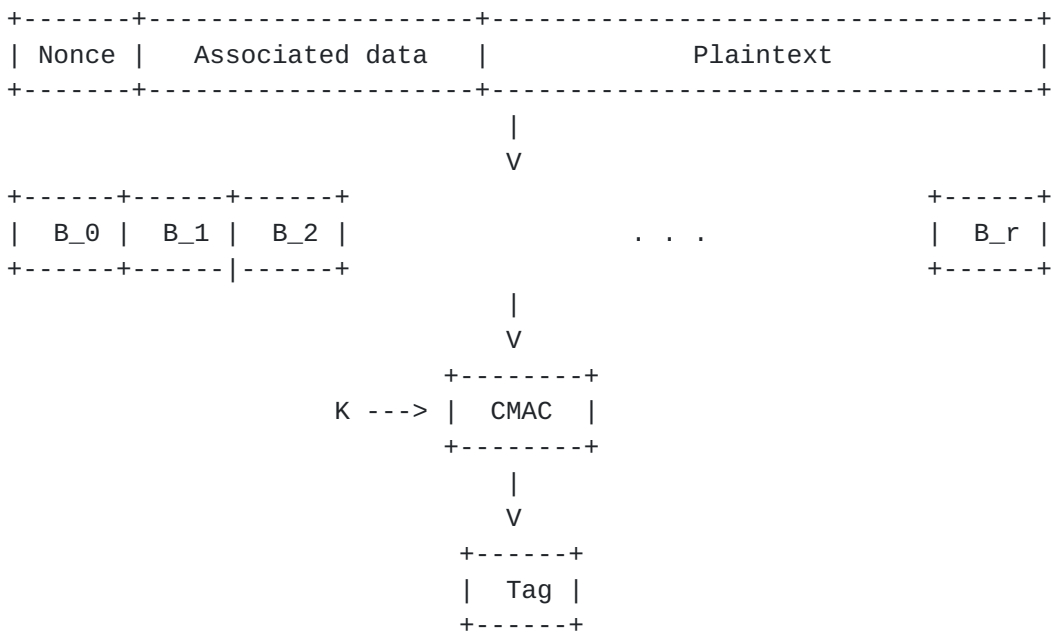
3. Overview

This section describes a basic concept of the proposed method.

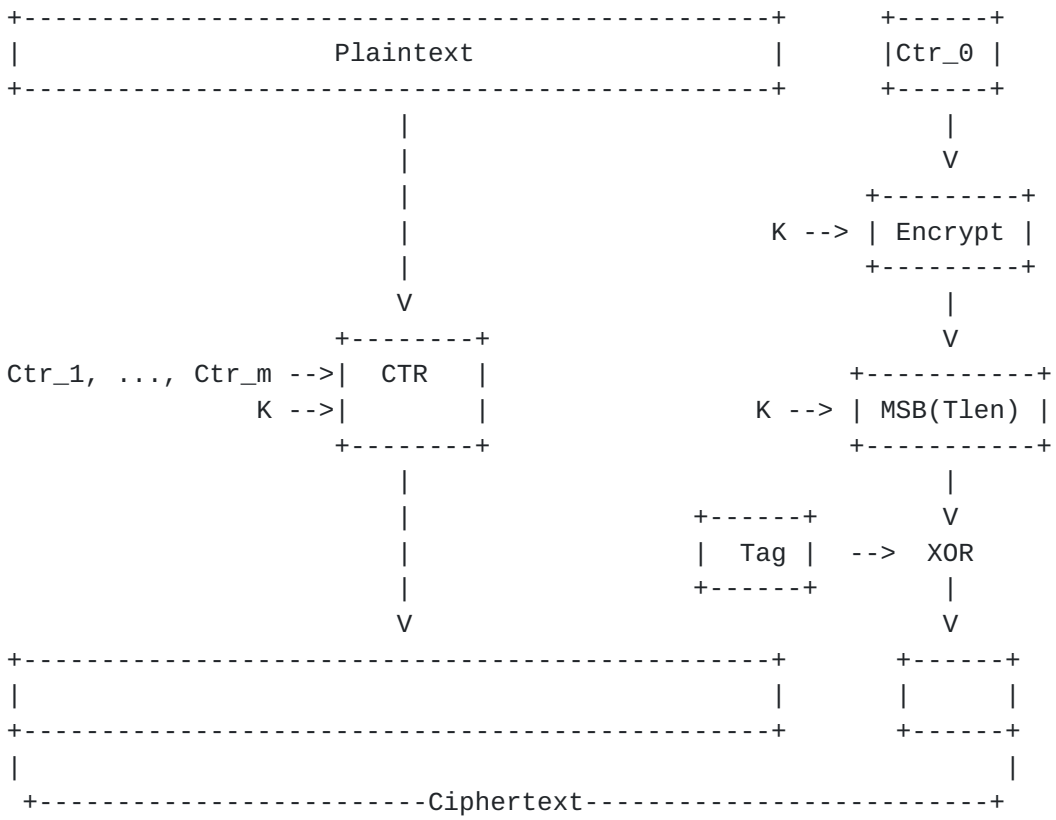
When security negotiation is performed with the default cipher suite during the DTLS handshake protocol between a CoAP client and server, the two nodes complete the preparation for providing the CoAP message data integrity in the DTLS record layer, or for providing both data integrity and confidentiality. Here, how should the CoAP message that needs to provide the data integrity function only in the DTLS record be defined? This question is not covered in the scope of this standard. An example of the solution of the question is the CoAP message that has to provide the integrity function only, and which can be set in advance in the IoT service definition and development stages. Furthermore, such CoAP messages can be

identified in the DTLS record layer using a bit flag value or optional field that is defined separately in the existing CoAP header.

In the case of CoAP messages that do not require encryption, the CoAP node generates an authentication tag value of the CoAP message in the DTLS record layer, and sends the CoAP message to the corresponding CoAP node without performing encryption (only the process shown in Fig. 1(a) is performed). For CoAP messages that require encryption, an authentication tag value is generated in the DTLS record layer, and both the CoAP message and authentication tag value are encrypted (the processes shown in Figs. 1(a) and 1(b) are performed) and sent. Here, the sender node of the CoAP message sets the encryption flag value of the DTLS record protocol header to "0" (integrity is provided) or "1" (integrity and confidentiality are provided); depending on the flag value, the receiver node of the CoAP message performs the process of integrity verification only or the processes of decryption and integrity verification. Fig. 2 shows the overall flow of the proposed method.



(a) Authentication



(b) Encryption

Figure 1: AES_CCM Block Diagram

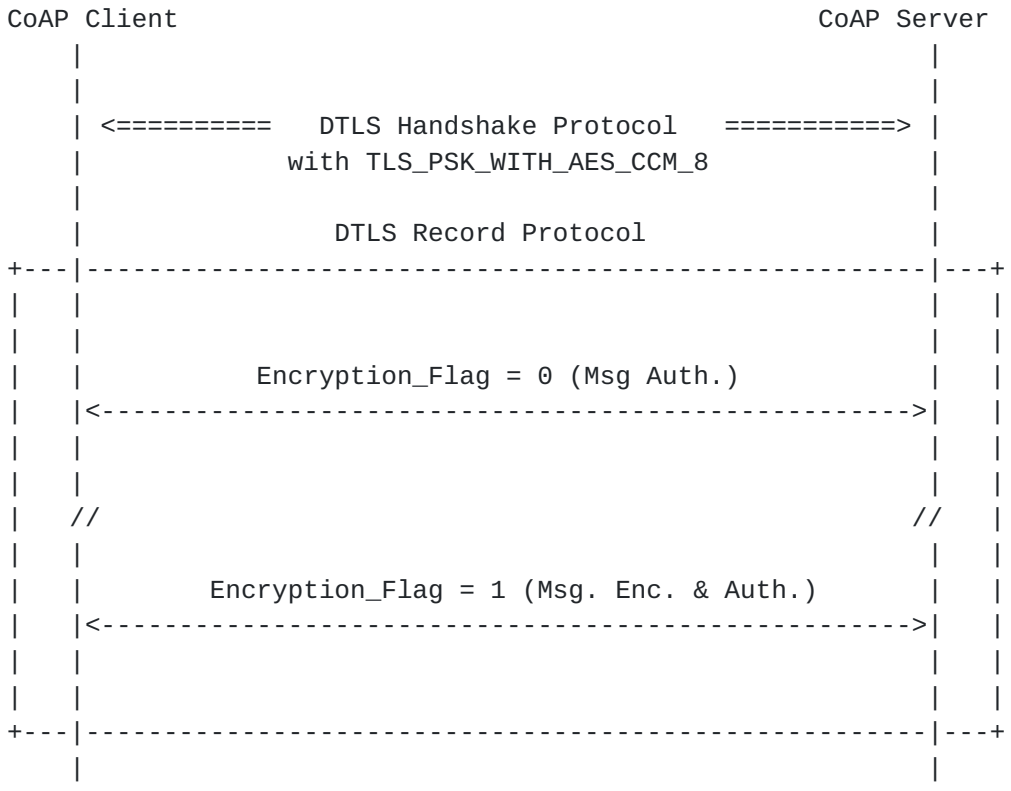


Figure 2: Protocol Flow

4. Protocol Operations

4.1. DTLS Record Layer Header

This document defines the encryption flag (F) in the DTLS record layer header to identify whether integrity only or both integrity and confidentiality functions are supported for the messages exchanged between the CoAP nodes through the DTLS security channel. In this document, the top level one bit of the "epoch" field in the DTLS record header is used as a bit to identify whether to apply the encryption. Figure 3 shows the DTLS record layer header format defined in this document, and Table 1 lists the definition of the encryption flag.

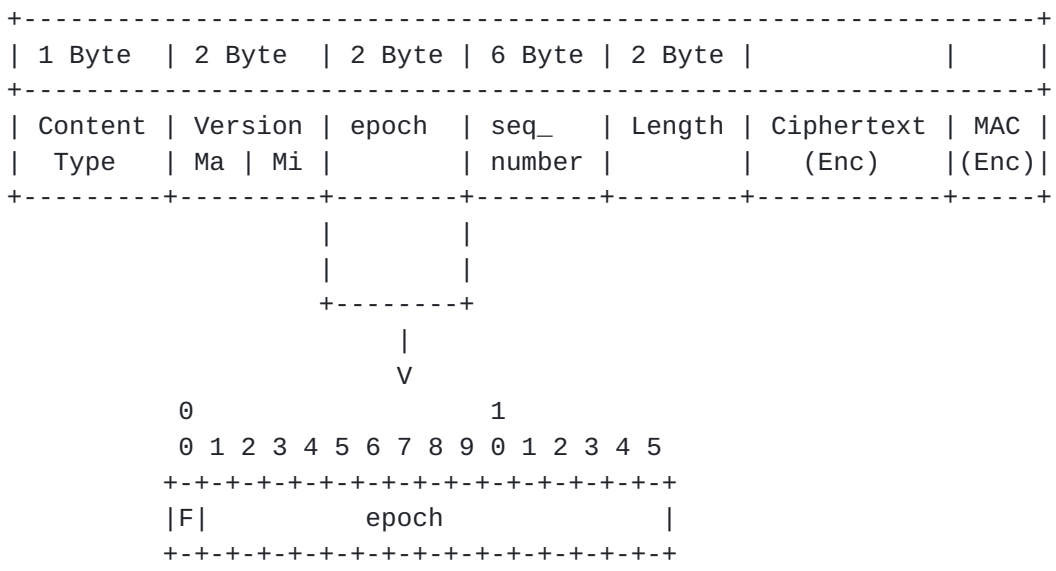


Figure 3: The encryption flag (F) in the DTLS record layer header

F	Description
0	integrity support
1	both integrity & encryption support

Table 1: Encryption flag (F) description

4.2. Node Behaviors

4.2.1. Sender

A sender that sends a CoAP message MUST check whether the confidentiality function of the CoAP message is to be provided (not in the scope of this standard document).

When only the integrity function has to be provided for the CoAP message, the process of generating an authentication tag value of the CoAP message MUST be performed using the traditional AES_CCM procedure in the DTLS record layer, and the encryption function MUST NOT be performed. The sender MUST set the flag "F" of the DTLS

record layer header to "0." Then, the sender MUST send the CoAP message and authentication tag value to the CoAP receiver.

When both the integrity and confidentiality functions have to be provided for the CoAP message, according to the AES_CCM procedure, the CoAP message authentication tag value MUST be generated and the message MUST be encrypted in the DTLS record layer. Prior to sending the encrypted message, CoAP MUST set the flag "F" of the DTLS record layer header to "1." The sender then MUST send the encrypted CoAP message to the CoAP receiver.

The other processes managed in the DTLS record layer MUST follow the DTLS 1.2 [RFC6347] standard.

4.2.2. Receiver

The receiver node that receives the CoAP message through the DTLS security channel MUST check the value of the flag "F" in the DTLS record layer header. If the flag value is "0," only the authentication tag value of the CoAP message MUST be verified; if the flag value is "1," the processes to decrypt the CoAP message and verify the authentication tag value MUST be performed.

The other processes managed in the DTLS record layer MUST follow the DTLS 1.2 [RFC6347] standard.

5. Security Considerations

(TBD)

6. IANA Considerations

This memo includes no request to IANA.

7. References

7.1. Normative References

[RFC7252] Shelby, Z., Hartke, K., and Bormann, C., "The Constrained Application Protocol (CoAP)", RFC 7252, June 2014.

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

7.2. Informative References

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

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

8. Acknowledgments

(TBD)

Authors' Addresses

Jaeduck Choi
National Security Research Institute
Daejeon, Korea
Email: cjduck@ensec.re.kr

Gunhee Lee
National Security Research Institute
Daejeon, Korea
Email: icezzoco@ensec.re.kr

Namhi Kang
Duksung Women's University
Seoul, Korea
Email: kang@duksung.ac.kr

Seungwook Jung
Sonngsil University
Seoul, Korea
Email: seungwookj@ssu.ac.kr

Souhwan Jung
Soongsil University
Seoul, Korea
Email: souhwanj@ssu.ac.kr