TLS
Internet-Draft
Intended status: Informational
Expires: June 22, 2019

N. Cam-Winget
Cisco Systems
J. Visoky
ODVA

December 19, 2018

TLS 1.3 Authentication and Integrity only Ciphersuites
draft-camwinget-tls-ts13-macciphersuites-02

Abstract

There are use cases, specifically in Internet of Things (IoT) and constrained environments that do not require confidentiality, though mutual authentication during tunnel establishment and message integrity is still mandated. This document defines the use of HMAC only as ciphersuites in TLS 1.3.

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 https://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 June 22, 2019.

Table of Contents

1. Introduction

There are several use cases in which communications privacy is not strictly needed, although authenticity of the communications transport is still very important. For example, within the Industrial Automation space there could be TCP or UDP communications which command a robotic arm to move a certain distance at a certain speed. Without authenticity guarantees an attacker could modify the packets to change the movement of the robotic arm, potentially causing physical damage. However, the motion control commands are not considered to be sensitive information and thus there is no requirement to provide confidentiality. Another IoT example with no strong requirement for confidentiality is the reporting of weather information; however, message authenticity is required to ensure integrity of the message..

Besides having a strong need for authenticity and a weak need for confidentiality, many of these systems also have serious latency requirements. Furthermore, several IoT devices (industrial or otherwise) have limited processing capability. However, these IoT systems still gain great benefit from leveraging TLS 1.3 for secure communications. Given the reduced need for confidentiality TLS 1.3 [RFC8446] cipher suites that maintain data integrity without confidentiality are described in this document.

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. Applicability Statement

The ciphersuites defined in this document are intended for a small limited set of applications where confidentiality requirements are relaxed and the need to minimize the cryptographic algorithms are prioritized. This section describes some of those applicable use cases.

Use cases in the industrial automation industry, while requiring data integrity, relax the confidential communications requirement. Mainly, information communicated to unmanned machines to execute repetitive tasks do not convey private information. For example, there could be a system with a robotic arm that is doing high speed pick-and-place of materials. The position synchronization data and motion commands are required to have very low latency, as the process needs to be done at high speed on a compute and memory constrained device. However, information such as the position, speed, acceleration of the robotic arm or other material in the system is not confidential. That is, while an attacker can determine the behavioral aspects and task of the device; no intellectual property concerns or data privacy concerns exist for these communications. However, data integrity is required as being able to modify this data would be a threat that an attacker might seek to exploit with serious consequences; the attacker could modify the motion information in order to cause physical damage to the equipment.

Another use case which is closely related is that of fine grained time updates. Motion systems often rely on time synchronization to ensure proper execution. Time updates are essentially public, there is no threat from an attacker knowing the time update information. This should make intuitive sense to those not familiar with these applications; rarely if ever does time information present a serious attack surface dealing with privacy. However the authenticity is still quite important. Modification of the data can at best lead to a denial-of-service attack, although a more intelligent threat actor might be able to cause actual physical damage. As these time synchronization updates are very fine-grained, it is again important for latency to be very low.

A third use case deals with Alarming data. Industrial control sensing equipment can be configured to send alarm information when it meets certain conditions. Often times this data is used to detect

certain out-of-tolerance conditions, allowing an operator or automated system to take corrective action. Once again, in many systems the reading of this data doesn't grant the attacker information that can be exploited, it is generally just information regarding the physical state of the system. At the same time, being able to modify this data would allow an attacker to either trigger alarms falsely or to cover up evidence of an attack that might allow for detection of their malicious activity. Furthermore, sensors are often low powered devices that might struggle to process encrypted and authenticated data. Sending data that is just authenticated significantly eases the burden placed on these devices, yet still allows the data to be protected against any tampering threats.

The above use cases describe the relaxed requirements to provide confidentiality, and as these devices come with a small runtime memory footprint and reduced processing power, the need to minimize the number of cryptographic algorithms used is prioritized.

4. Using Integrity only Cipher Suites

This document defines the following cipher suites for use in TLS 1.3:

TLS_SHA256_SHA256 {0xC0, 0xB4}

TLS_SHA384_SHA384 {0xC0, 0xB5}

These cipher suites allow the use of SHA-256 or SHA-384 as the HMACs for data integrity protection as well as its use for HKDF. The authentication mechanisms remain unchanged with the intent to only update the cipher suites to relax the need for confidentiality.

5. Record Payload Protection for Integrity only Cipher Suites

The record payload protection as defined in [RFC8446] can be retained when integrity only cipher suites are used. This section describes the mapping of record payload structures when integrity only cipher suites are employed.

As integrity is provided with protection over the full record, the encrypted_record in the TLSCiphertext along with the additional_data input to AEADEncrypted as defined in Section 5.2 [RFC8446] remains the same. The TLSCiphertext.length for the integrity cipher suites will be:

TLS_SHA256_SHA256: TLSPlaintext.length + 32

TLS_SHA384_SHA384: TLSPlaintext.length + 64

The resulting encrypted_record is the concatenation of the TLSPlaintext with the resulting HMAC. With this mapping, the decrypt order as defined in Section 5.2 of [RFC8446] remains the same. The encrypt and decrypt operations provide the integrity protection using HMAC SHA-256 or SHA-384 as described in [RFC4634].

6. Key Schedule when using Integrity only Cipher Suites

The key derivation process for Integrity only Cipher Suites remains the same as defined in [RFC8446]. The only difference is that the keys used to protect the tunnel applies to the negotiated HMAC SHA-256 or HMAC SHA-384 ciphers.

7. IANA Considerations

IANA has granted registration the following specifically for this document:

TLS_SHA256_SHA256 {0xC0, 0xB4} cipher suite and TLS_SHA384_SHA384 {0xC0, 0xB5} cipher suite.

8. Security and Privacy Considerations

In general, with the exception of confidentiality and privacy, the security considerations detailed in [RFC8446] and in [RFC5246] apply to this document. Furthermore, as the cipher suites described in this document do not provide any confidentiality, it is important that they only be used in cases where there are no confidentiality or privacy requirements and concerns; and the runtime memory requirements can accommodate support for more cryptographic constructs.

With the lack of data encryption specified in this draft, no confidentiality or privacy is provided for the data transported in the the TLS tunnel. To highlight the loss of privacy, the information carried in both the Server and Client certificates, while integrity protected, will be sent unencrypted. Similarly, other TLS extensions that may be carried in the Server's EncryptedExtensions message will only be integrity protected without provisions for confidentiality.

9. Acknowledgements

The authors would like to acknowledge the work done by Industrial Communications Standards Groups (such as ODVA) as the motivation for this document. In addition, we are grateful for the advice and feedback from Joe Salowey, Blake Anderson and David McGrew.

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4634] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and HMAC-SHA)", RFC 4634, DOI 10.17487/RFC4634, July 2006, <https://www.rfc-editor.org/info/rfc4634>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

10.2. Informative Reference

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

Authors' Addresses

Nancy Cam-Winget
Cisco Systems
3550 Cisco Way
San Jose, CA 95134
USA

Email: ncamwing@cisco.com

Jack Visoky
ODVA
1 Allen Bradley Dr
Mayfield Heights, OH 44124
USA

Email: jmvisoky@ra.rockwell.com