Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 18, 2020

M. Vucinic
INRIA
G. Selander
J. Mattsson
Ericsson AB
October 16, 2019

Requirements for a Lightweight AKE for OSCORE. draft-selander-lake-reqs-02

Abstract

This document compiles the requirements for a lightweight authenticated key exchange protocol for OSCORE.

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 April 18, 2020.

Table of Contents

1. Introduction

OSCORE [RFC8613] is a lightweight communication security protocol providing end-to-end security on application layer for constrained IoT settings (cf. [RFC7228]). It is expected to be deployed with standards and frameworks using CoAP such as 6TiSCH, LPWAN, OMA Specworks LwM2M, Fairhair Alliance and Open Connectivity Foundation. OSCORE lacks a matching authenticated key exchange protocol (AKE). This document compiles the requirements for such an AKE.

2. Problem description

2.1. Credentials

IoT deployments differ in terms of what credentials can be supported. Currently many systems use pre-shared keys (PSK) provisioned out of band, for various reasons. PSK are often used in a first deployment because of its percieved simplicity. The use of PSK allows for protection of communication without major additional security processing, and also enables the use of symmetric crypto algorithms only, reducing the implementation and computational effort in the endpoints.

However, PSK based provisioning has inherent weaknesses. There has been reports of massive breaches of PSK provisioning systems, and as many systems use PSK without perfect forward secrecy (PFS) they are vulnerable to passive pervasive monitoring. The security of these systems can be improved by adding PFS through an AKE authenticated by the provisioned PSK.

Shared keys can alternatively be established in the endpoints using an AKE protocol authenticated with asymmetric public keys instead of symmetric secret keys. Raw public keys (RPK) can be provisioned with

the same scheme as PSKs, and allows a more relaxed trust model since RPKs need not be secret.

By running the same asymmetric key AKE with public key certificates instead of RPK, key provisioning can be omitted, leading to a more automated bootstrapping procedure.

These steps provide an example of a migration path in limited scoped steps from simple to more robust security bootstrapping and provisioning schemes where each step improves the overall security and/or simplicity of deployment of the IoT system, although not all steps are necessarily feasible for the most constrained settings.

In order to allow for these different schemes, the AKE must support PSK, RPK and certificate based authentication.

Considering the wide variety of deployments it is desirable to support different schemes for transporting and identifying credentials, see Section 2 of [I-D.ietf-cose-x509].

2.2. Crypto Agility

Motivated by long deployment lifetimes, the AKE is required to support crypto agility, including modularity of COSE crypto algorithms and negotiation of preferred crypto algorithms for OSCORE and the AKE. The AKE negotiation must be protected against downgrade attacks.

2.3. AKE for OSCORE

In order to be suitable for OSCORE, at the end of the AKE protocol run the two parties must agree on (see Section 3.2 of [RFC8613]):

- a shared secret (OSCORE Master Secret) with PFS and a good amount of randomness. (The term "good amount of randomness" is borrowed from [HKDF] to signify not necessarily uniformly distributed randomness.)

- identifiers providing a hint to the receiver of what security context to use when decrypting the message (OSCORE Sender IDs of peer endpoints), arbitrarily short

- COSE algorithms to use with OSCORE

Moreover, the AKE must support the same transport as OSCORE, in particular any protocol where CoAP can be transported.

To ensure that the AKE is efficient for the expected applications of OSCORE, we list the relevant public specifications of technologies where OSCORE is included:

- The IETF 6TiSCH WG charter (-02) identifies the need to "secur[e] the join process and mak[e] that fit within the constraints of high latency, low throughput and small frame sizes that characterize IEEE802.15.4 TSCH". OSCORE protects the join protocol as described in 6TiSCH Minimal Security [I-D.ietf-6tisch-minimal-security].

- The IETF LPWAN WG charter (-01) identifies the need to improve the transport capabilities of LPWA networks such as NB-IoT and LoRa whose "common traits include ... frame sizes ... [on] the order of tens of bytes transmitted a few times per day at ultra-low speeds". The application of OSCORE is described in [I-D.ietf-lpwan-coap-static-context-hc].

- OMA Specworks LwM2M version 1.1 [LwM2M] defines bindings to two challenging radio technologies where OSCORE will be deployed: LoRaWAN and NB-IoT.

Other industry fora which plan to use OSCORE:

- Fairhair Alliance has defined an architecture [Fairhair] which adopts OSCORE for multicast, but it is not clear whether the architecture will support unicast OSCORE.

- Open Connectivity Foundation (OCF) has been actively involved in the OSCORE development for the purpose of deploying OSCORE, but no public reference is available since OCF only references RFCs. We believe that these OSCORE consumers reflect similar levels of constraints on the devices and networks in question.

The solution will presumably be useful in other scenarios as well since a low security overhead improves the overall performance, but we do not require the solution to necessarily be applicable anywhere else.

2.4. Lightweight

As motivated in Section 2.3 we target an AKE which is efficiently deployable in 6TiSCH multi-hop networks, LoRaWAN networks and NB-IoT networks. The desire is to optimize the AKE to be 'as lightweight as reasonably achievable' in these environments, where 'lightweight' refers to:

- resource consumption, measured by bytes on the wire, wall-clock time and number of round trips to complete, or power consumption

- the amount of new code required on end systems which already have an OSCORE stack

These properties need to be considered in the context of the use of an existing CoAP/OSCORE stack in the targeted networks. However, some properties may be difficult to evaluate for a given protocol, for example, because they depend on the radio conditions or other simultaneous network traffic. Therefore these properties should be taken as input for identifying plausible protocol metrics that can be more easily measured and compared between protocols.

Per 'bytes on the wire', it is desirable for these AKE messages to fit into the MTU size of these protocols; and if not possible, within as few frames as possible, since using multiple MTUs can have significant costs in terms of time and power.

Per 'time', it is desirable for the AKE message exchange(s) to complete in a reasonable amount of time, both for a single uncongested exchange and when multiple exchanges are running in an interleaved fashion, like e.g. in a "network formation" setting when multiple devices connect for the first time. This latency may not be a linear function depending on congestion and the specific radio technology used. As these are relatively low data rate networks, the latency contribution due to computation is in general not expected to be dominant.

Per 'round-trips', it is desirable that the number of completed request/response message exchanges required before the initiating endpoint can start sending protected traffic data is as small as possible, since this reduces completion time. See Section 2.4.4 for a discussion about the tradeoff between message size and number of messages.

Per 'power', it is desirable for the transmission of AKE messages and crypto to draw as little power as possible. The best mechanism for doing so differs across radio technologies. For example, NB-IoT uses licensed spectrum and thus can transmit at higher power to improve coverage, making the transmitted byte count relatively more important than for other radio technologies. In other cases, the radio transmitter will be active for a full MTU frame regardless of how much of the frame is occupied by message content, which makes the byte count less sensitive for the power consumption. Increased power consumption is unavoidable in poor network conditions, such as most wide-area settings including LoRaWAN.

Per 'new code', it is desirable to introduce as little new code as possible onto OSCORE-enabled devices to support this new AKE. These devices have on the order of 10s of kB of memory and 100 kB of storage on which an embedded OS; a COAP stack; CORE and AKE libraries; and target applications would run. It is expected that the majority of this space is available for actual application logic, as opposed to the support libraries. In a typical OSCORE implementation COSE encrypt and signature structures will be available, as will support for COSE algorithms relevant for IoT enabling the same algorithms as is used for OSCORE (e.g. COSE algorithm no. 10 = CCM* used by 6TiSCH). The use of those, or CBOR or CoAP, would not add to the footprint.

While the large variety of settings and capabilities of the devices and networks makes it challenging to produce exact values of some these dimensions, there are some key benchmarks that are tractable for security protocol engineering and which have a significant impact.

2.4.1. LoRaWAN

LoRaWAN employs unlicensed radio frequency bands in the 868MHz ISM band, in Europe regulated by ETSI EN 300 220. For LoRaWAN the most relevant metric is the Time-on-Air, which determines the back-off times and can be used an indicator to calculate energy consumption. LoRaWAN is legally required to use a 1% (or smaller) duty cycle, a payload split into two fragments instead of one increases the time to complete the sending of this payload by at least 10,000%. The use of an AKE for providing end-to-end security on application layer need to comply with the duty cycle. One relevant benchmark is performance in low coverage with Data Rates 0-2 corresponding to a packet size of 51 bytes [LoRaWAN]. While larger frame sizes are also defined, their use depend on good radio conditions. Some libraries/providers only support 51 bytes packet size.

2.4.2. 6TiSCH

For 6TiSCH specifically, as a time-sliced network, bytes of the wire (or rather, the quantization into frame count) is particularly noteworthy, since more frames contribute to congestion for spectrum (and concomitant error rates) in a non-linear way, especially in scenarios when large numbers of independent nodes are attempting to execute an AKE to join a network.

The available size for key exchange messages depends the topology of the network and other parameters. One benchmark which is relevant for studying AKE is the network formation setting. For a 6TiSCH production network 5 hops deep in a network formation setting, the

available CoAP overhead to avoid fragmentation is 47/45 bytes (uplink/downlink) [AKE-for-6TiSCH].

2.4.3. NB-IoT

For NB-IoT, in contrast to the other two technologies below, the radio bearers are not characterized by a fixed sized PDU. Concatenation, segmentation and reassembly are part of the service provided by the radio layer. Furthermore, since NB-IoT is operating in licensed spectrum, the packets on the radio interface can be transmitted back-to-back, so the time before sending OSCORE protected data is dependent on the number of round trips/messages of the AKE. An AKE providing challenge-response based mutual authentication requires at least three messages/one round trip before it is possible to encrypt traffic data between peers meeting for the first time. NB-IoT has a high per byte energy consumption component for uplink transfers, implying that those messages should be as small as possible.

2.4.4. Discussion

While "as small protocol messages as possible" does not lend itself to a sharp boundary threshold, "as few protocol messages as possible" does and is relevant in all settings above.

The penalty is high for not fitting into the frame sizes of 6TiSCH and LoRaWAN networks. Fragmentation is not defined within these technologies so requires fragmentation scheme on a higher layer in the stack. With fragmentation increases the number of frames per message, each with its associated overhead in terms of power consumption and latency. Additionally the probability for errors increases, which leads to retransmissions of frames or entire messages that in turn increases the power consumption and latency.

There are trade-offs between "few messages" and "few frames"; if overhead is spread out over more messages such that each message fits into a particular frame this may reduce the overall power consumption. While it may be possible to engineer such a solution for a particular radio technology and signature algorithm, the benefits in terms of fewer messages/round trips in general and for NB-IoT in particular (see Section 2.4.3) are considered more important than optimizing for a specific scenario. Hence an optimal AKE protocol has 3 messages and each message fits into as few frames as possible, ideally 1 frame per message.

3. Requirements Summary

- The AKE must support PSK, RPK and certificate based authentication and crypto agility, be 3-pass and support the same transport as OSCORE. It is desirable to support different schemes for transporting and identifying credentials.

- After the AKE run, the peers must agree on a shared secret with PFS and good amount of randomness, peer identifiers (potentially short), and COSE algorithms to use.

- The AKE must reuse CBOR, CoAP and COSE primitives and algorithms for low code complexity of a combined OSCORE and AKE implementation.

- The messages must be as small as reasonably achievable and fit into as few LoRaWAN packets and 6TiSCH frames as possible, optimally 1 for each message.

4. Security Considerations

This document compiles the requirements for an AKE and provides some related security considerations.

The AKE must provide the security properties expected of IETF protocols, e.g., providing confidentiality protection, integrity protection, and authentication with strong work factor.

5. IANA Considerations

None.

6. Informative References

[AKE-for-6TiSCH]
"AKE for 6TiSCH", March 2019, <https://docs.google.com/document/d/1wLoIexMLG3U9iYO5hzGzKjkvi-VDndQBbYRNsMUlh-k>.

[Fairhair]
"Security Architecture for the Internet of Things (IoT) in Commercial Buildings, Fairhair Alliance white paper", March 2018, <https://www.fairhair-alliance.org/data/downloadables/1/9/fairhair_security_wp_march-2018.pdf>.

[HKDF] Krawczyk, H., "Cryptographic Extraction and Key Derivation: The HKDF Scheme", May 2010, <https://eprint.iacr.org/2010/264.pdf>.

[I-D.ietf-6tisch-minimal-security] Vucinic, M., Simon, J., Pister, K., and M. Richardson, "Minimal Security Framework for 6TiSCH", draft-ietf-6tisch-minimal-security-12 (work in progress), July 2019.

[I-D.ietf-cose-x509] Schaad, J., "CBOR Object Signing and Encryption (COSE): Headers for carrying and referencing X.509 certificates", draft-ietf-cose-x509-04 (work in progress), September 2019.

[I-D.ietf-lpwan-coap-static-context-hc] Minaburo, A., Toutain, L., and R. Andreasen, "LPWAN Static Context Header Compression (SCHC) for CoAP", draft-ietf-lpwan-coap-static-context-hc-11 (work in progress), October 2019.

[LoRaWAN] "LoRaWAN Regional Parameters v1.0.2rB", February 2017, <https://lora-alliance.org/resource-hub/lorawantm-regional-parameters-v102rb>.

[LwM2M] "OMA SpecWorks LwM2M", August 2018, <http://www.openmobilealliance.org/release/LightweightM2M/V1_1-20180710-A/OMA-TS-LightweightM2M_Transport-V1_1-20180710-A.pdf>.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <https://www.rfc-editor.org/info/rfc7228>.

[RFC8613] Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", RFC 8613, DOI 10.17487/RFC8613, July 2019, <https://www.rfc-editor.org/info/rfc8613>.

Authors' Addresses

Malisa Vucinic
INRIA

Email: malisa.vucinic@inria.fr

Goeran Selander
Ericsson AB

Email: goran.selander@ericsson.com

John Mattsson
Ericsson AB

Email: john.mattsson@ericsson.com