Network Working Group P. Porambage
Internet-Draft University of Oulou
Intended status: Standards Track C. Schmitt
Expires: August 18, 2014 University of Zurich
A. Gurtov
Aalto University
S. Gerdes
Universitaet Bremen TZI
February 14, 2014

X.509 Public Key Infrastructure Certificates for the Constrained Application Protocol (CoAP)

<draft-porambage-core-ace-x509-00>

Abstract

The Constrained Application Protocol (CoAP) is a web transfer protocol designed for resource limited nodes in constrained networks. For securing the protocol, CoAP defines a binding to Datagram Transport Layer Security (DTLS) with four security modes. One of them is the Certificate mode where the device has an asymmetric key pair with an X.509 certificate. However, the intrinsic properties of x.509 certificates impede the application on the resource constrained nodes. This draft describes the necessary adjustments and derives a modified profile for X.509 certificates to cope with the resource limitations of low-power low-performing devices

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

The Constrained Application Protocol (CoAP) [I-D.ietf-core-coap] is proposed as a lightweight alternative for HTTP protocol, in order to support web services while realizing the REST architecture on top of the most constrained nodes and networks. CoAP is designed for the special requirements of this constrained environments, especially considering energy, building automation and other machine-to-machine (M2M) applications.

CoAP defines a binding to Datagram Transport Layer Security (DTLS) [RFC6347] and specifies four security modes: NoSec, PreSharedKey, RawPublicKey and Certificate. In the Certificate Mode, the device has an X.509 certificate [RFC5280], which binds the public key of the device to its Authority name and is signed by a common trust root.

Complex asymmetric algorithms like RSA use a lot of resources such as processing power and memory. Devices may have to dedicate the major portion of these resources on security algorithms instead of spending them on the application they are intended for. Therefore, it is necessary to adapt a low cost solution for the DTLS Certificate mode in CoAP.

Mismatches of X.509 certificates in their original formats; According to [RFC5280] the content of X.509 certificates is mainly composed of three parts: TBSCertificate, Signature Algorithm and Signature Value. We would like to focus on the internal configurations and attributes of TBSCertificate component. The standard X.509 certificates use RSA public key algorithm and keys as the public key infrastructure. According to the definitions of Classes of devices as given in [I-D.ietf-lwig-terms] class 0 and 1 are the most constrained devices. These low performing devices are not capable of handling RSA PKI algorithms due to their limited memory capacities and processing capabilities.

1.1. Document Structure

Section 2 mentions conventions used in this draft. Afterwards the assumed design requirements are briefly mentioned in Section 3. Section 4 describes the proposed approach using X.509 public key infrastructure (PKI) certificates for CoAP,followed by security considerations.

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. Design Requirements

The key design goal is to profile the content and operations of X.509 certificates in such a way to balance the resource constraints of the devices along with the security requirements. Therefore, we emphasize the following design requirements: Low memory consumption; Less complexity of mathematical operations for authentication and authorization processes; Support interoperability among different vendor devices. Alternatively, we focus on profiling X.509 certificates according to the specifications of CoAP enabled devices.

4. Overview of the approach

It is obvious that the utilization of X.509 certificates with RSA public key algorithm would not be a lightweight solution. We can adjust the size and the complexity of the certificate by changing the attributes in TBSCertificate part in the original certificates. Elliptic Curve Cryptography (ECC) algorithms would be suitable candidate for PKI replacement in X.509 certificates. Alternatively this could be reusable for digital signature in the certificates too. For instance the algorithm in Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV) would be a feasible solution for this[1].

5. Security Considerations

The following security goals are addressed by the key idea presented in this draft similar to proposed considerations in [I-D.draft-schmitt-two-way-authentication-for-iot]:

Authenticity

Recipients of a message can identify their communication partners and can detect if the sender information has been forged.

Integrity

Communication partners can detect changes to a message during transmission.

Confidentiality

Attackers cannot gain knowledge about the content of a secured message.

6. Acknowledgement

This work has been supported by Tekes under Massive Scale Machine-to-Machine Service (MAMMotH) project and Academy of Finland project SEMOHealth.

The ongoing work is supported partially by the SmartenIT [2] and the FLAMINGO [3] projects, funded by the EU FP7 Program under Contract No. FP7-2012-ICT-317846 and No. FP7-2012-ICT-318488, respectively.

7. Formal Syntax

CoAP - Constrained Application Protocol

DTLS - Datagram Transport Layer Security

ECC - Elliptic Curve Cryptography

ECQV - Elliptic Curve Qu-Vanstone Implicit Certificate Scheme

IETF - Internet Engineering Task Force

M2M - Machine-to-Machine

PKI - Public Key Infrastructure

8. References

8.1. Norminative References

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

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

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List

(CRL) Profile", RFC 5280, May 2008.

[I-D.ietf-core-coap]
Shelby, Z., Hartke, K., and C. Bormann, "Constrained Application Protocol (CoAP), http://www.ietf.org/internet-drafts/draft-ietf-core-coap-18.txt", draft-ietf-core-coap-18 (work in progress), March 2013.

[I-D.ietf-lwig-terms]
Bormann, C. and M. Ersue, "Terminology for Constrained Node Networks, http://www.ietf.org/internet-drafts/draft-ietf-lwig-terms-00.txt", draft-bormann-lwig-terms-00 (work in progress), November 2012.

[I-D.draft-schmitt-two-way-authentication-for-iot]
Schmitt, C. and B. Stiller, "DTLS-based Security with two-way Authentication for IoT, http://www.ietf.org/id/draft-schmitt-two-way-authentication-for-iot-02.txt", draft-schmitt-two-way-authentication-for-iot-02 (work in progress), February 2014.

8.2. Informative References

[1] "Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV), v0.97, http://www.secg.org/download/aid-785/sec4-0.97.pdf", SEC 4, March 2011.

[2] SmartenIT Consortium, "Socially-aware Management of New Overlay Application Traffic combined with Energy Efficiency in the Internet (SmartenIT), http://www.smartenit.eu/", 20103.

[3] Flamingo Consortium, "FLAMINGO - Management of the Future Internet, http://www.fp7-flamingo.eu/", 2013.

Authors' Addresses

Pawani Porambage
University of Oulou
P.O. Box 4500
Oulu 90014
Finland

Email: pporamba@ee.oulu.fi

Corinna Schmitt
Univerity of Zurich
Department for Informatics
Communication Systems Group
Binzmuehlestrasse 14
Zurich 8050
Switzerland

Email: schmitt@ifi.uzh.ch

Andrei Gurtov
Aalto University
Otakaari 1
Espoo 02150
Finland

Email: gurtov@hiit.fi

Stefanie Gerdes
Universitaet Bremen TZI
Postfach 330440
Bremen 28359
Germany

Email: gerdes@tzi.org