CoRE
Internet-Draft
Intended status: Informational
Expires: March 10, 2014

B. Greevenbosch
Huawei Technologies

September 06, 2013

Use cases and requirements for authentication and authorisation in CoAP
draft-greevenbosch-core-authreq-00

Abstract

This draft describes use cases and requirements for authenticated and authorised CoAP. The draft especially focuses on threats and their prevention.

Note

Discussion and suggestions for improvement are requested, and should be sent to core@ietf.org.

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 http://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 March 10, 2014.

Copyright Notice

Table of Contents

1. Requirements notation

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].

2. Introduction

This draft describes use cases and requirements for secure authentication and authorisation, as well as their expiry and revocation, in CoAP.

The draft consists of the following parts:

- The draft starts with several use cases.

- o A section with requirements related to the use cases follows.
- o Discussion of the various security trade-offs that need to be made can be found in Section 5.

The goal of the draft is to provide background material for usage when defining a solution for authorised CoAP.

3. Use cases

3.1. Authorised and unauthorised devices

Company A produces sensor devices. These devices are of high quality, and no vulnerabilities have been detected. As such, they have been certified to be used in a wide area of applications.

Company B produces also sensor devices. However, these devices are of low quality, and have known security issues. They failed the certification requirements.

Company C is oblivious of this fact, and since it needs this kind of sensors to monitor its industrial process, it buys some to test.

During installation of the sensors into Company C's monitoring network, the credentials of the sensors are verified by the system. The sensors from Company A install without problem. However, for the sensors from Company B the authentication fails, and the installation of the sensors is refused. The system informs the installation engineers about the reason of failure.

Fortunately the authentication mechanism revealed that the sensors from Company B are not to be used. This avoided a lot of trouble and potential security issues.

3.2. Home security

Henry has an advanced home security system. The security system provides protection against burglary, as well as against fire. It has sensors on doors, motion sensors, smoke detectors, cameras etc. It also has actuators for the electronic locks, a sprinkler system and actuators that can close the gas tap and cut the electricity.

The system comes with tokens. These tokens are used to turn on or off part of the system, and allow certain actions that need human interaction. One of these actions is to open or close the front door lock. Henry has provided a token to each of his family members.

The system has a solid authorisation and authentication model, ensuring that only Henry and his family's tokens can drive the system. Even though the tokens can be bought in a regular store, only tokens that Henry has approved can be used in the system.

Certain peripherals allow different access rights to different entities. For example, the electricity closure can only be set by Henry and the master system, whereas its on/off status can be read by all family members.

All peripherals are certified by an impartial certification body, which has specified minimum security requirements. In this way, Henry is assured that when he adds a new peripheral and it is accepted by the system, it can be deemed reliable.

3.3. Illegal smart-meters

An electricity company depends on smart-meters to measure energy usage of the households it servers. The gathered information is used for several purposes, billing being one of them.

On the black market, there appear illegal smart-meters that only report 75% of the actual electricity usage. These smart-meters are based on a clone of a valid public key.

Once the electricity company discovers this, it revokes the associated public key, thereby ensuring that the illegal meters cannot be installed anymore.

3.4. Maintaining and extending a network of sensors and actuators

An agricultural company uses an IP network to ensure an optimal climate for the vegetables they grow in their green houses. Sensors do measurements about e.g. humidity and sunlight, whereas actuators can drive artificial rain and supporting light. A central controller is responsible for processing the sensor readings and driving the actuators accordingly.

Sometimes, a sensor or actuator needs replacement as part of the normal maintenance cycle. This is a routine task for the associated engineer, and involves simply disconnecting the old apparatus and connecting a new one. The rest of the installation to the network happens automatically.

As the agricultural company is doing good business, it decides to expand. It buys another piece of land, and modernises the green house that was already built on the land. The modernisation includes installing new sensors and actuators, which are seamlessly integrated

into the already existent network, such that they can work with the central controller too.

The use case illustrates the need to be able to automatically install and update network nodes in an existing network. It is also important to note, that installation of the network nodes includes proper authentication and authorisation. After all, the agricultural company does not want outsiders to be able to influence the climate in the green houses, for example by driving the actuators or modifying the sensor readings.

3.5. Discovered compromised device

Company A has a certain type of actuators installed throughout its building. On a certain time, some of these actuators start behaving funny. It turns out that some hackers have been able to access the sensors, and drive them as they wish.

Company A can’t de-install the actuators immediately, after all, they are installed everywhere in the building. Instead Company A has the actuators revoked, and then can replace them on a less hasty schedule.

3.6. Vulnerability discovery in actuators in a chemical plant

A chemical plant deploys sensors for the several properties of the substance being produced, and actuators that start certain processes when the substance is ready for the next step.

A vulnerability in certain of the actuators is discovered; it would allow unauthorised third parties to take over the actuators and start processes at their will.

After the discovery of the vulnerability, the chemical plant pro-actively de-activates the actuators and revokes their keys. It then makes sure the vulnerability is resolved as quickly as possible, such that normal production can resume.

3.7. Revocation of a non-compromised device

Jack worked at the IT department of company E.

However, due to a conflict with the company, Jack has been fired. When leaving, he smuggled out some tokens used to control several of the company’s peripherals.

When the company realises it misses the tokens, it revokes them to ensure they cannot be used to control the peripherals anymore.

Jack fails to wreak havoc as his revenge, and neither can he sell the tokens to other adversaries.

3.8. Mixing nodes from different vendors

A weather analysis and forecast agency needs global coverage for collection of temperature and air-pressure data. It has contracts with several local authorities and companies for the placement of their sensors.

For both logistic and economic reasons, the weather agency does not want to rely on one particular type of sensor from a single vendor. Instead, it wants to allow different sensors from different vendors, as long as these sensors meet certain criteria concerning precision, response time and reliability.

To ensure the criteria are met, the weather agency performs several tests with new candidate sensors. When the sensors pass the tests, the agency allows their usage in its network. When the sensors fail the tests, the agency is ensured that they cannot be used for collecting data, lest the quality of the agency's analysis and forecast suffer from data of bad quality.

In this use case, the vendor pro-actively controls which sensor types can be used in their network. It uses an authentication and authorisation mechanism to automatically ensure that only those types it has approved can be installed. The use case illustrates the need for interoperability in authentication between nodes manifactured by different vendors, as well as the need to exclude nodes that are not authorised to join the network.

3.9. Privacy of medical communications

Mr P has developed a heart problem. To diagnose and monitor the condition of Mr P's heart, his cardiologist has requested Mr P to wear a sensor during the day. The sensor measures the heartbeat and other vital functions. The sensor transmits this information to the hospital, generally once every day. When needed, e.g. when a situation occurs that requires extra attention, the sensor can also send information ad-hoc.

Protecting the integrity of the sensor readings is important, even when it is unlikely that an adversary will tamper with the sensor readings. After all, doing so would constitute a serious crime. Protecting Mr P's privacy adds significantly to the value of a solid security model in this use case. In any case eavesdropping needs to be prevented, and that includes man-in-the-middle attacks.

4. Requirements

This section lists requirements associated with authentication and authorisation in CoAP:

1. It SHALL be possible to verify the binding between the key and the entity associated with it.

2. It SHALL be possible to verify whether an entity is authorised to establish the connection.

3. It SHALL be possible to specify authorisation for a specific resource.

4. It SHOULD be possible to specify authorisation based on the message type.

5. It SHALL NOT be possible for an unauthorised third party to establish a cryptographic relationship.

6. There SHALL be a mechanism that allows revocation of previously granted authorisation.

7. It SHALL be possible for a receiver to determine whether a key has been revoked.

8. It SHALL be possible to perform authentication, authorisation and revocation verification fully automatically.

9. The verification technology MUST NOT require much complexity on constrained entities.

10. The verification mechanism SHALL be scalable, allowing potentially millions of entities to verify authentication and authorisation.

11. It SHOULD be possible to specify an expiry date for keys and/or authorisation.

12. It SHALL be possible to revoke compromised keys.

13. Revocation SHALL NOT require physically unplugging the device.

14. There SHALL be protection against an unauthorised third party spoofing authorisation and/or revocation of keys and entities.

15. There SHOULD be protection against denial of service (DoS) attacks, as far as it is feasible.

5. Discussion

In this section, we discuss the various trade-offs that need to be made, and implications they may have.

5.1. Certificate authority

Much of a traditional Public Key Infrastructure depends on a certificate authority. The certificate authority (CA) signs the certificate of the device, or an intermediate certificate that signs the certificate of the device.

This creates islands of trust, in which the CA has the power to revoke any key on its island. Interoperability between devices of different CAs may still be possible, depending on which CAs the entities trust apart from their own CA.

5.2. Expiry

X.509 certificates [X.509] contain an expiry date. This means that the certificates automatically become invalid after a time has passed. Should the device's lifetime be longer than the validity period of the certificate, then the certificate has to be updated.

The expiry date has the advantage that there is no need to keep track of revoked certificates infinitely. After the certificate's expiration, the revocation status can be forgotten.

However a major draw-back is that a mechanism is needed to update expired certificates, provided that the entities holding them should continue to be used.

5.3. Time of revocation

Authentication and revocation are normally checked when two entities meet each other for the first time. But how about entities that are to be revoked later?

The dealings with this highly depends on the security requirements of the employed system. For example, home light-switches may have less stringent security requirements than actuators in a chemical plant. In the former, a revocation mechanism for deployed devices may not be needed, whereas in the latter it is essential.

6. Security considerations

This whole draft concerns security considerations. It indicates use cases and requirements for authentication, authorisation and

associated expiry and revocation. In addition it discusses several of the associated details and trade-offs.

We refer to the rest of the draft for the complete picture.

7. IANA considerations

No IANA requests are required for this document.

8. Acknowledgements

Thanks to Rene Struik and Kepeng Li for their valuable feedback.

9. References

9.1. Normative References

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

9.2. Informative References

[X.509] , "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks. ", ITU-T Recommendation X.509, ISO/IEC 9594-8:2005, 2005.

Author’s Address

Bert Greevenbosch
Huawei Technologies Co., Ltd.
Huawei Industrial Base
Bantian, Longgang District
Shenzhen 518129
P.R. China

Phone: +86-755-28978088
Email: bert.greevenbosch@huawei.com