CoRE Working Group
Internet-Draft
Intended status: Informational
Expires: March 20, 2014

L. Seitz
SICS Swedish ICT AB
S. Gerdes
Universitaet Bremen TZI
G. Selander
Ericsson

September 16, 2013

Use cases for CoRE security
draft-seitz-core-sec-usecases-00

Abstract

This document presents use cases for security measures in scenarios involving constrained RESTful devices. Special focus is placed on access control and authentication. Where specific details are relevant, it is assumed that the devices use CoAP as communication protocol, however most conclusions apply generally.

A number of security requirements are derived from the use cases, which are intended as a guideline for developing a comprehensive authentication and authorization approach for this class of scenarios.

Status of this Memo

This Internet-Draft will expire on March 20, 2014.

Copyright Notice

Table of Contents

1. Introduction

This document presents use cases in an attempt to analyze the security requirements especially on authentication and access control in an Internet of Things setting. This setting features constrained devices [I-D.ietf-lwig-terminology] communicating over the Internet. Some of these devices may have very low capacity in terms of memory and processing power, and may additionally be limited by the fact that they run on battery power.

These devices offer resources such as sensor data and actuators, which are accessed by clients, that may be users or other devices.

Where specific detail is necessary it is assumed that the devices communicate using the CoAP protocol [I-D.ietf-core-coap], although most conclusions are generic. Currently CoAP proposes to use DTLS [RFC6347] for authentication, and access control lists on the devices, that specify which clients may initiate a DTLS connection. One goal of this document is to point out use cases where this approach is not satisfactory.

1.1. Terminology

Resource Server (RS): The constrained device which hosts resources the Client wants to access.

Client (C): A device which wants to access a resource on the Resource Server. This could also be a constrained device.

Resource Owner (RO): The subject who owns the resource and controls its access permissions.

2. Use Cases

This section lists use cases involving constrained devices with security requirements. Each use case first presents a general description of the application area, then one or more specific use cases, and finally the resulting security requirements.

2.1. Container monitoring

The ability of sensors to communicate environmental data wirelessly opens up new application areas. The use of such sensor systems makes it possible to transmit specific characteristics such as temperature, humidity and gas content during transportation and storage of goods.

The proper handling of the sensors in this scenario is not easy to accomplish. They have to be associated to the appropriate pallet of the respective container. Moreover, the goods and the corresponding sensors belong to specific customers.

During the shipment to their destination the goods often pass stops where they are transloaded to other means of transportation, e.g. from ship transport to road transport.

2.1.1. Bananas for Munich

A Munich supermarket chain buys bananas from a Costa Rican fruit vendor. It instructs a transport company to deliver the goods via ship to Rotterdam where they are picked up by their own company trucks.

The supermarket’s quality management wants to assure the quality of their products and thus uses the fruit vendor’s service of equipping the bananas with sensors. The state of the goods is monitored consistently during the shipment and abnormal sensor values are recorded. Additionally, the sensor values are used to control the climate within the cargo containers.

The personnel of the transport company and the supermarket’s delivery service has to be able to locate the proper goods and match them to the corresponding customer. The state of the cargo must not be disclosed to them, however.

When the goods arrive at the supermarket in Munich, their state is checked.
If no anomalies occurred during the transport, the bananas are admitted for sale.

2.1.2. Requirements

- U1.1 The supermarket chain must be able to allow the transport company and the delivery service to access the position data on the monitoring devices. Other state information must not be accessible.

- U1.2 The climate regulation system in the containers must be able to access the monitoring devices' state information to regulate the climate accordingly.

- U1.3 The integrity and availability of the sensor data must be assured for proper operation of climate control.

- U1.4 The supermarket chain must be able to allow the supermarket's quality management to access the recorded state information on the monitoring devices.

- U1.5 The supermarket chain will not want other companies to be able to read sensor information so the confidentiality of the monitoring devices' state information must be assured.

2.2. Home Automation

Automation of the home, housework or household activity is propagated as a future market for the Internet of Things. A home automation system integrates electrical devices in a house with each other, such as heating, ventilation, lighting, home entertainment and home security.

Such a system needs to accommodate a number of regular users (inhabitants, close friends, cleaning personnel) as well as a heterogeneous group of dynamically varying users (visitors, repairmen, delivery men).

The security required by the systems integrated in a automated home varies, however it is clear that the security system controlling e.g. the doors, alarms, and other critical systems needs to be at least as secure as for a comparable unautomated home.

As the users are not typically trained in security (or even computer use), the configuration must use secure default settings, and the interface must be well adapted to novice users.

2.2.1. Remotely letting in a visitor

Jane is the owner of an automated home, that allows her to remotely control all electrical devices through a web interface or mobile application.

Jane has invited over her acquaintance Jeffrey for dinner, but is stuck in traffic and can not arrive in time, while Jeffrey who uses the subway arrives punctually. Jane calls Jeffrey and offers him to let him in remotely, so he can make himself comfortable and use Jane’s home entertainment system.

Jeffrey downloads an application that lets him communicate with Jane’s home, and Jane remotely instructs the door to open for him, and the alarm to shut down. She gives Jeffrey access to lighting and HVAC and also limited access to the home entertainment system, allowing Jeffrey to all services except those that are pay-per-use or those that Jane has marked as private.

2.2.2. Requirements

- U2.1 Jane needs to be able to spontaneously provision authentication means to Jeffrey

- U2.2 Jane must be able to spontaneously change the access control policies

- U2.3 Jane needs to be able to apply different rights for different devices and users

- U2.4 Jane must be able to apply local conditions (presence, time) to authorizations, and the device (e.g. the door) needs to be able to verify these conditions

- U2.5 The different devices in Jane’s home need to be able to communicate with each other and with different control devices

- U2.6 The configuration of Jane’s home needs to be secure by default

- U2.7 It must be easy for Jane to edit the access control policies for her home

2.3. Personal Health Monitoring

The use of wearable health monitoring technology is expected to grow strongly, as a multitude of novel devices are developed and marketed. These devices are typically battery driven, and located physically on the user. They monitor some bodily function, such as e.g. temperature, blood pressure, or pulse. They are connected to the Internet, either through an intermediary base-station or directly, using wireless technologies. Through this connection they report the monitored data to some entity, which may either be the user herself, or some medical personnel in charge of the user.

Medical data has always been considered as very sensitive, and therefore requires good protection against unauthorized disclosure. A frequent, conflicting requirement is the capability for medical personnel to gain emergency access, even if no specific access rights exist. As a result, the importance of secure audit logs increases in such scenarios.

Since the users are not typically trained in security (or even computer use), the configuration must use secure default settings, and the interface must be well adapted to novice users. Also the system must require very little maintenance, so e.g. frequent changes of battery are unacceptable.

2.3.1. John and the heart rate monitor

John has a heart condition, that can result in sudden cardiac arrests. He therefore uses a device called HeartGuard that monitors his heart rate and his position. In case of a cardiac arrest it automatically sends an alarm to an emergency service, transmitting John’s current location. The device also functions as a implanted cardioverter defibrilator, i.e. it can deliver a shock in order to try and normalize Johns heart rate.

John can configure additional persons that get notified in an emergency, for example his daughter Jill. Furthermore the device stores data on John’s heart rate, which can later be accessed by a physician to assess the condition of John’s heart.

However John is a rather private person, and is worried that Jill might use HeartGuard to monitor his location while there is no emergency. Furthermore he doesn’t want his health insurance to get access to the HeartGuard data, since they might refuse to renew his insurance if they decided he was too big a risk for them.

2.3.2. Requirements

- U3.1 John must be able to selectively allow different persons or groups to access the position data on condition that there is an emergency.

- U3.2 John must be able to selectively allow different persons or groups to access the heart rate data.

- U3.3 John must be able to block access to specific persons or groups, if he mistrusts them.

- U3.4 The device must operate in a way that does not require frequent battery changes

- U3.5 The device must ensure that both incoming and outgoing communication is confidentiality and integrity protected

- U3.6 The device must have secure settings by default

- U3.7 The device’s security settings must be easy to configure

2.4. Building Automation

Buildings for commercial use such as shopping malls or office buildings nowadays are equipped increasingly with semi-automatic components to enhance the overall living quality and save energy where possible. This includes for example heating, ventilation and air condition (HVAC) as well as illumination and fire alarm systems.

These buildings are often used by more than one company who share some parts of the building while other areas are used by each of them exclusively. Accordingly, a company must be able to control the light and HVAC system of its own part of the building and must not have access to rooms that belong to other companies.

Some parts of the building automation system such as entrance illumination and fire alarm systems are controlled either by all parties together or by a service company.

The building automation system has to provide for a security mechanism which allows for authentication and fine-grained authorization.

2.4.1. Fire Alarm

The Companies A and B share an office building which is equipped with a fire alarm system. It is triggered by several smoke detectors which are spread out across the building.

It is a really hot day and James who works for company A turns on the air condition in his office. Lucy who works for company B wants to make tea using an electric kettle. After she turned it on she goes outside to talk to a colleague until the water is boiling. Unfortunately, her kettle has a malfunction which causes overheating and results in a smoldering fire of the kettle’s plastic case.

Due to the smoke coming from the kettle the fire alarm is triggered. Alarm sirens throughout the building are notified and alert the staff of both companies. Additionally, the ventilation system of the whole building is closed off to prevent the smoke from spreading and to withdraw oxygen from the fire. The smoke cannot get into James' office although he turned on his air condition because the fire alarm overrides the manual setting.

The fire department is notified of the fire automatically and arrives within a short time. After inspecting the damage and extinguishing the smoldering fire a fire fighter resets the fire alarm because only the fire department is authorized to do that.

2.4.2. Requirements

- U4.1 The building control devices of company A must be able to interoperate with those of company B. The devices might be produced by different vendors and might be operated by different service providers.

- U4.2 Only the smoke detectors must be able to trigger an alarm.

- U4.3 The availability and integrity of the smoke detector's alarm messages have to be assured.

- U4.4 Only the fire department must be able to reset the fire alarm.

- U4.5 James must be able to control the air conditioning in his office.

- U4.6 The emergency system must be able to automatically close off the ventilation system.

- U4.7 During fire alarm, the personnel must not be allowed to regulate the climate control.

- U4.8 No unauthorized device must be able to access building control devices.

- U4.9 Since replacing devices in the building is very work intensive and thus expensive (there are many devices, and some are in places that are hard to access), the devices and their batteries should function for a very long time without maintenance.

2.5. Industrial Control Systems

Industrial control systems (ICS) and especially supervisory control and data acquisition systems (SCADA) use a multitude of sensors and actuators in order to monitor and control industrial processes in the physical world. Example processes include manufacturing, power generation, and refining of raw materials.

Since the advent of the Stuxnet worm it has become obvious to the general public how vulnerable this kind of systems are, especially when connected to the Internet. These severity of these vulnerabilities are exacerbated by the fact that many ICS are used to control critical public infrastructure, such as power, water treatment of traffic control. Nevertheless the economical advantages of connecting such systems to the Internet can be significant if appropriate security measures are put in place.

2.5.1. Water treatment plant

The communal water treatment plant of a mid-sized city is controlled by a networked ICS. Spread across the city are numerous nodes, sensors (e.g. pollution meters, pressure indicators) and actuators (e.g. valves, pumps) communicating via a wireless network. Since the range of the network is limited, many nodes communicate through intermediary proxies that relay communications to the administration clients of the ICS.

Jenny is a technician whose job it is to monitor the plant and take appropriate measure, if abnormal conditions are detected (e.g. if water pollution is detected, or the pressure in a pump reaches critical levels).

When Jenny is on holiday or sick-leave, the service company sends a replacement worker from a pool of available, qualified persons.

Joshuah is a young, computer savvy kid with too much time at his hands. He spends time wardriving and stumbles upon the wireless network, used by the plant’s sensors and actuators. Joshuah tries to interact with the devices on this network and manages to stall a valve controlling water flow to a part of the city. Jenny quickly discovers the intrusion and is able to take appropriate measures to prevent damage to the value and quickly restore normal service conditions.

2.5.2. Requirements

- U5.1 The Integrity of the messages sent between the nodes in the ICS must be protected.

- U5.2 The nodes must be resilient to denial of service attacks.

- U5.3 The security measures must cope with the presence of intermediary proxies between the Resource Server and the Client.

- U5.4 Since most of the processing capacity of the nodes and the network load capacity must go towards production tasks, the security measures must use minimal resources, both on the network and on the nodes.

- U5.5 Since replacement workers can spontaneously jump in for Jenny, the system needs to be able to handle authorization updates without re-provisioning each node individually.

- U5.6 After a replacement worker has finished taking care of the system, the corresponding authorization and authentication means need to be revoked remotely.

3. Requirements From The Use Cases

This section lists requirements derived from the use cases above. Note that not every single requirement applies to every Resource Server, however protocols should allow for all of these requirements to be fulfilled.

3.1. General Security Requirements

The following requirements refer to general security measures, not directly linked to authentication and authorization which are listed in detail in the next sections.

- Integrity, confidentiality and replay protection of the message exchanges between the Resource Server, the Client and other involved parties (U1.3, U1.5, U3.5, U4.3, U5.1).

  This may be achieved by either establishing a secure channel (such as e.g. DTLS [RFC6347]) or object security applied to the payloads (e.g. JWS/JWE [I-D.ietf-jose-json-web-signature], [I-D.ietf-jose-json-web-encryption]).

- Protect the Resource Server against denial of service (U3.4, U4.3, U5.2) - Minimize the number of protocol steps that an attacker can induce a Resource Server to perform without proper authentication and authorization.

  - Note well that for constrained devices this includes attacks that aim to drain the battery of the target.

- Security measures must work when traffic from the Client to the Resource Server goes through intermediary nodes (U5.3).

  Rationale: In many deployments, there will be gateways, proxies, firewalls etc. between a Client and a Resource Server. Security measures should therefore not require the Client to be directly connected to the Resource Server.

- Use minimal resources for security measures (U3.4, U4.9, U5.4)

  - Minimize battery usage

    - Minimize message exchanges only for security

    - Minimize the size of authorization and authentication data that is transmitted

    + Minimize the size of required software libraries

    + Minimize memory and stack usage on the devices

- Enable security by default (U2.6, U3.6)

  Rationale: Many attacks exploit insecure default settings, and experience shows that default settings are rarely changed by the end users. Therefore the protocols for constrained devices should require secure modes of use by default.

- Interoperability (U1.1, U1.2, U2.5, U4.1)

  Rationale: Resource Owners may interact with Clients from various manufacturers and vice-versa. In order to function correctly the security mechanisms need to work together. This is best achieved by standardization

- Usability (U2.7, U3.7)

  * Keep response times reasonable

  * Make the security measures transparent for human users where possible

  * Make the administration of security as simple as possible

3.2. Authentication Requirements

- Enable mutual authentication between the Client and the Resource Server (U1.1, U1.2, U2.1, U4.4, U4.5, U4.6)

- Provision authentication means to Clients and Resource Servers (U1.1, U1.2, U2.1, U4.4, U4.5, U4.6, U5.5)

  * Optionally allow for remote provisioning.

- Enable remote revocation of authentication means (U3.3, U4.9, U5.6)

3.3. Access Control Requirements

- Enforce the access control policies of the Resource Owner (U1.1, U1.2, U1.4, U3.1, U3.2, U4.2, U4.4, U4.5, U4.6, U4.8) - Provision access control policies set by the Resource Owner to the Policy Decision Point (which may be on the Resource Server or on another trusted entity) [RFC2904]. - Apply the access control policies to incoming requests (this may be done by the Resource Server or by another trusted entity).

- Do not send additional messages just for access control (U3.4, U5.4) Rationale: Sending and receiving is a much bigger battery drainer, compared to processing on the device.

- Apply different rights for different requesting entities (U1.1, U1.2, U2.3, U4.2, U4.4, U4.5, U4.6) Rationale: In some cases different types of users require different access rights, as opposed to all-or-nothing access control.

- Allow for fine-grained access control (U1.1, U1.2, U4.2, U4.4, U4.5, U4.6) Resource Servers can host several resources, and a resource (e.g. an actuator) can have different settings. In some cases access rights need to be different at this level of granularity.

- Apply local conditions (U2.4, U3.1, U4.7) Access may depend on local conditions e.g. access to health data in an emergency. The Policy Decision Point must be able to take such conditions into account.

- Enable policy updates without re-provisioning the device (U2.2, U4.9, U5.5, U5.6) Rationale: Clients can change rapidly and re-provisioning might be prohibitively expensive.

4. Security Considerations

This document lists security requirements for constrained devices, motivated by specific use cases. Therefore the whole document deals with security considerations.

5. Acknowledgments

The authors would like to thank Olaf Bergmann, and Mohit Sethi for contributing to the discussion and giving helpful comments. Also, thanks to Markus Becker for his input on the container monitoring use case.

6. IANA Considerations

This document has no IANA actions.

7. Informative References

[I-D.ietf-core-coap]
Shelby, Z., Hartke, K., and C. Bormann, "Constrained Application Protocol (CoAP)", draft-ietf-core-coap-18 (work in progress), June 2013.

[I-D.ietf-jose-json-web-encryption]
Jones, M., Rescorla, E., and J. Hildebrand, "JSON Web Encryption (JWE)", draft-ietf-jose-json-web-encryption-16 (work in progress), September 2013.

[I-D.ietf-jose-json-web-signature]
Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", draft-ietf-jose-json-web-signature-16 (work in progress), September 2013.

[I-D.ietf-lwig-terminology]
Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained Node Networks", draft-ietf-lwig-terminology-05 (work in progress), July 2013.

[RFC2904] Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruijn, B., de Laat, C., Holdrege, M., and D. Spence, "AAA Authorization Framework", RFC 2904, August 2000.

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

Authors' Addresses

Ludwig Seitz
SICS Swedish ICT AB
Scheelevaegen 17
Lund 22370
Sweden

Email: ludwig@sics.se

Stefanie Gerdes
Universitaet Bremen TZI
Postfach 330440
Bremen D-28359
Germany

Phone: +49-421-218-63906
Email: gerdes@tzi.org

Goeran Selander
Ericsson
Faroegatan 6
Kista 16480
Sweden

Email: goran.selander@ericsson.com