ACE Working Group
Internet-Draft
Intended status: Informational
Expires: January 3, 2015

L. Seitz, Ed.
SICS Swedish ICT AB
S. Gerdes, Ed.
Universitaet Bremen TZI
G. Selander
Ericsson
M. Mani
Itron
S. Kumar
Philips Research
July 02, 2014

ACE use cases
draft-seitz-ace-usecases-01

Abstract

This document presents use cases for authentication and access control in scenarios involving constrained RESTful devices. 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 access control approach for this class of scenarios.

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 January 3, 2015.

Copyright Notice

Table of Contents

1. Introduction

This document presents use cases in an attempt to analyze the authentication and access control requirements in an Internet of Things setting. This setting features constrained devices [RFC7228] 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, sometimes without human intervention (M2M). In some situations the communication will happen through intermediaries (e.g. gateways, proxies).

Where specific detail is necessary it is assumed that the devices communicate using the CoAP protocol [RFC7252], although most conclusions are generic.

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 requirements. We assume that basic communication security requirements apply for all of these scenarios.

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 continuously track and transmit specific characteristics such as temperature, humidity and gas content during the 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.

The transportation and storage of perishable goods is especially challenging since they have to be stored at a constant temperature and with proper ventilation. Additionally, it is very important for the vendors to be informed about irregularities in the temperature and ventilation of fruits to avoid the delivery of decomposed fruits to their customers. The need for a constant monitoring of perishable goods has led to projects such as The Intelligent Container (http://www.intelligentcontainer.com).

2.1.1. Bananas for Munich

A fruit vendor grows bananas in Costa Rica for the German market. It instructs a transport company to deliver the goods via ship to Rotterdam where they are picked up by trucks and transported to a ripening facility. A Munich supermarket chain buys ripened bananas from the fruit vendor and transports them with their own company trucks.

The fruit vendor’s quality management wants to assure the quality of their products and thus equips the banana boxes with sensors. The state of the goods is monitored consistently during shipment and ripening and abnormal sensor values are recorded. Additionally, the sensor values are used to control the climate within the cargo

containers.

The personnel that transloades the goods must be able to locate the goods meant for a specific customer. However the fruit vendor does not want to disclose sensor information pertaining to the condition of the goods to other companies.

When the goods arrive at the supermarket in Munich, the supermarket conducts its own quality check. If no anomalies occurred during the transport, the bananas are admitted for sale.

2.1.2. Requirements

- U1.1 The fruit vendor 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, without manual intervention of the resource owner.

- U1.3 The fruit vendor must be able to allow the fruit vendor's quality management to access the recorded state information on the monitoring devices.

- U1.4 Since the fruit vendor does not want other companies to be able to read sensor information, there should be some access control for the monitoring devices' state information.

2.2. Home Automation

Automation of the home has the potential to become a big future market for the Internet of Things. A home automation system connects electrical devices in a house to the Internet and thus makes them accessible and manageable remotely. Such devices might control for example heating, ventilation, lighting, home entertainment or 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 in a automated home varies, however it is clear that the security system controlling e.g. the door-locks and alarms 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 a flat with automated connected door-locks and alarm system, that allow her to remotely control them through a web interface or mobile application. To allow for centralized management of both locks and the alarm system, they need to be able to communicate with both the web interface and the mobile application using a standardized, secure protocol.

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

Jeffrey downloads an application that lets him communicate with Jane’s door-lock and alarm system. Then Jane sets permissions for Jeffery that allow him to open the door, and shut down the alarm when he arrives.

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 users.
- U2.4 Jane must be able to apply context-based conditions (presence, time) to authorizations, and the devices (door-lock or alarm) need to be able to verify these conditions.
- U2.5 The security mechanisms of the door-lock and the alarm in Jane’s home need to be able to communicate with different control devices (e.g. Jeffrey’s mobile phone).
- U2.6 The access control configuration of Jane’s home needs to be secure by default.

- o U2.7 It must be easy for Jane to edit the access control policies for her home, even remotely and easy for Jeffrey to get access with correct authorization.

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. The need for open industry standards to ensure interoperability between products has lead to initiatives such as Continua Alliance (continuaalliance.org) and Personal Connected Health Alliance (pchalliance.org). Personal health 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 through an intermediary base-station, 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. Parts of the system must operate with minimal maintenance. Especially 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 HeartGuard also broadcasts emergency information in the neighborhood to notify doctors or people with certain skills who have been enrolled in an emergency program, e.g. people who got training in heart and lung rescue. For doctors, medical information or diagnosis can be provided with the notification to improve immediate treatment.

The device includes some smart logic, with which it identifies its owner John and allows him to configure the device’s settings, including access control.

This prevents situation where someone else wearing that device can act as the owner and mess up the access control and security settings.

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, or even to the fact that he is wearing a HeartGuard, since they might refuse to renew his insurance if they decided he was too big a risk for them.

NOTE: Monitoring of some state parameter (e.g. an alarm button) and the position of a person also fits well into an elderly care service. This is particularly useful for people suffering from dementia, where the relatives or caregivers need to be notified of the whereabouts of the person under certain conditions. In this case it is not the patient that decides about access.

2.3.2. Requirements

- U3.1 John must be able to pre-configure access rights to the position data for persons or groups, in the context of 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 in an otherwise allowed group (e.g. doctors in an emergency), if he mistrusts them.
- U3.4 The security measures must consider the battery lifetime of the devices and should consume as little energy as possible.
- U3.5 The device must have secure access control settings by default.
- U3.6 The device's access control settings must be easy to configure for an authorized, non-technical user.
- U3.7 Security mechanisms on medical devices must not provide opportunities for denial of service attacks on the device.

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 to save energy where possible. This includes for example heating, ventilation and air condition (HVAC) as well as illumination and security systems such as fire alarms.

Different areas of these buildings are often exclusively leased to different companies. However they also share some of the common areas of the building.
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 control 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.

2.4.1. Device Lifecycle

2.4.1.1. Installation and Commissioning

A building is hired out to different companies for office space. This building features various automated systems, such as a fire alarm system, which is triggered by several smoke detectors which are spread out across the building. It also has automated HVAC, lighting and physical access control systems.

A vacant area of the building has been recently leased to company A. Before moving into its new office, Company A wishes to replace the lighting with a more energy efficient and a better light quality luminaries. They hire an installation and commissioning company C to redo the illumination. Company C is instructed to integrate the new lighting devices, which may be from multiple manufacturers, into the existing lighting infrastructure of the building which includes presence sensors, switches, controllers etc.

Company C gets the necessary authorization from the service company to interact with the existing Building and Lighting Management System (BLMS).
To prevent disturbance to other occupants of the building, Company C is provided authorization to perform the commissioning only during non-office hours and only to modify configuration on devices belonging to the domain of Company A’s space. After installation (wiring) of the new lighting devices, the commissioner adds the devices into the company A’s lighting domain.

Once the devices are in the correct domain, the commissioner authorizes the interaction rules between the new lighting devices and existing devices like presence sensors. For this, the commissioner creates the authorization rules on the BLMS which define which lights form a group and which sensors /switches/controllers are allowed to control which groups. These authorization rules may be context based like time of the day (office or non-office hours) or location of the handheld lighting controller etc.

2.4.1.2. Operational

Company A's staff move into the newly furnished office space. Most lighting is controlled by presence sensors which control the lighting of specific group of lights based on the authorization rules in the BLMS. Additionally employees are allowed to manually override the lighting brightness and color in their office by using the switches or handheld controllers. Such changes are allowed only if the authorization rules exist in the BLMS. For example lighting in the corridors may not be manually adjustable.

At the end of the day, lighting is dimmed down or switched off if no occupancy is detected even if manually overridden during the day.

On a later date company B also moves into the same building, and shares some of the common spaces with company A. On a really hot day 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.

2.4.1.3. Maintenance

Company A's staff are annoyed that the lights switch off too often in their rooms if they work silently in front of their computer. Company A notifies the commissioning Company C about the issue and asks them to increase the delay before lights switch off.

Company C again gets the necessary authorization from the service company to interact with the BLMS. The commissioner's tool gets the necessary authorization from BMLS to send a configuration change to all lighting devices in Company A's offices to increase their delay before they switch off.

2.4.1.4. Decommissioning

Company A has noticed that the handheld controllers are often misplaced and hard to find when needed. So most of the time staff use the existing wall switches for manual control. Company A decides it would be better to completely remove handheld controllers and asks Company C to decommission them from the lighting system.

Company C again gets the necessary authorization from the service company to interact with the BLMS. The commissioner now deletes any rules that allowed handheld controllers authorization to control the lighting. Additionally the commissioner instructs the BLMS to push these new rules to prevent cached rules at the end devices from being used.

2.4.2. Requirements

- U4.1. A user with sufficient authorization to a device should be able to transfer the device to a different authorization server.
- U4.2. Authorization rules may be context-based.
- U4.3. Devices can access resources on other devices only if a rule exists in the authorization server (default deny).
- U4.4 Devices can be authorized to control individual devices using unicast or multiple devices using multicast.
- U4.5. Devices may cache authorization rules locally.
- U4.6. Subsystems under different operational domains must be able to interoperate with each other if the domain owners agree.
- U4.7. A user with sufficient authorization to a device should be able to remove the device from an authorization server.

- o U4.8. Authorization server may have a mechanism to override locally cached rules at devices.

- o U4.9. Revocation of security credentials should be possible.

2.5. Smart Metering

Automated measuring of customer consumption is an established technology for electricity, water, and gas providers. Increasingly these systems also feature networking capability to allow for remote management. Such systems are in use for commercial, industrial and residential customers and require a certain level of security, in order to avoid economic loss to the providers, vulnerability of the distribution system, as well as disruption of services for the customers.

The smart metering equipment for gas and water solutions is battery driven and communication should be used sparingly due to battery consumption. Therefore the types of meters sleep most of the time, and only wake up every minute/hour to check for incoming instructions. Furthermore they wake up a few times a day (based on their configuration) to upload their measured metering data.

Different networking topologies exist for smart metering solutions. Based on environment, regulatory rules and expected cost, one or a mixture of these topologies may be deployed to collect the metering information. Drive-By metering is one of the most current solutions deployed for collection of gas and water meters.

2.5.1. Drive-by metering

A company offers smart metering infrastructures and related services to various providers. Among these is a water provider, who in turn supplies several residential complexes in a city. The smart meters are installed in the end customer’s homes to measure water consumption and thus generate billing data for the provider. The meters do so by sending data to a base station. Several base stations are installed around the city to collect the metering data. However in the denser urban areas, the base stations would have to be installed very close to the meters. This would require a high number of base stations and expose this more expensive equipment to manipulation or sabotage. The company has therefore chosen another approach, which is to drive around with a mobile base-station and let the meters connect to that in regular intervals in order to gather metering data.

2.5.2. Meshed Topology

In another deployment, the water meters are installed in a building that already has power meters installed, the latter are mains powered, and are therefore not subject to the same power saving restrictions. The water meters can therefore use the power meters as proxies, in order to achieve better connectivity. This requires the security measures on the water meters to work through intermediaries.

2.5.3. Customer Direct Access to the metering Data

The provider also wishes to offer its customer limited access to some of the data on the metering devices, in order to allow them to check and optimize their consumption. However the provider expects the company to implement measures to prevent tampering with the data relevant for billing.

2.5.4. Requirements

- U5.1 If security information can be recovered by a physical attack on a meter, this information must not be usable in an attack on other parts of the metering infrastructure.

- U5.2 The meters must be able to perform fine-grained access control on the metering data and on the configuration while being offline.

- U5.3 Authentication and access control must function without online connection to a back-end server.

- U5.4 Since there are many smart meters deployed and reaching them is difficult, authentication and access control policy updates must not depend on directly (or worse manually) provisioning these updates to individual meters.

- U5.5 The authentication and access control measures must cope with the presence of intermediary proxies between the Resource Servers and the Client.

3. Consolidated Requirements From The Use Cases

This section consolidates the 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 that are affected by the design of authentication and access control protocols.

- Protect the Resource Server against denial of service (U3.7)
  - Minimize the number of protocol steps that an attacker can induce a Resource Server to perform without proper authentication and access control.
  - Note well that for constrained devices this includes attacks that aim to drain the battery of the target.
- Authentication and access control measures must work when traffic from the Client to the Resource Server goes through intermediary nodes. (U5.5)

  Rationale: In many deployments, there will be gateways, proxies, firewalls etc. between a Client and a Resource Server. This means that e.g. DTLS [RFC6347] client authentication can not be used to authenticate the Client.
- Minimize resource usage for authentication and access control on the constrained device(s) (U3.4)
  - Minimize battery usage
    - Minimize message exchanges required by security measures
    - Minimize the size of authentication and access control data that is transmitted
    - Minimize the size of code required and reuse existing code libraries
    - Minimize memory and stack usage on the devices

- Require secure default settings (U1.4, U2.6, U3.5, U4.3)

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

- Interoperability (U1.1, U2.5, U4.6)

  Rationale: Resource Owners may interact with Clients from various manufacturers and vice-versa. For the overall system to function correctly the authentication and access control mechanisms need to work consistently. This is best achieved by standardization.

- Usability (U2.7, U3.6)

  * Keep response times reasonable

  * Make authentication and access control transparent for human users where possible

  * Make the administration of authentication and access control as simple as possible

3.2. Authentication Requirements

- Standardized provisioning of authentication means to Clients and Resource Servers (U2.1, U4.1, U4.7)

  * Allow for remote provisioning as an option

- Enable remote revocation of authentication means (U4.9, U5.4)

3.3. Access Control Requirements

- Enforce the access control policies of the Resource Owner (all use cases)

  * Provision of access control policies set by the Resource Owner to the Policy Decision Point [RFC2904] (which may be on the Resource Server or on another trusted entity).

  * Apply the access control policies to incoming requests (this may be done by the Resource Server or by another trusted entity).

- Allow for different rights to the same resource for different requesting entities (U1.1, U1.2, U2.3, U3.1, U3.2, U3.3, U5.2)

  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, U3.1, U3.2, U5.2) 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.

- Support access control on multicast requests to several Resource Servers (U4.4)

- Access control must work when the Resource Server has intermittent connectivity (U4.5)

- The Resource Server should be able to evaluate context-based permissions (U2.4, U3.1, U4.2)

  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 individual devices (U2.2, U4.7, U4.8, U5.4)

  Rationale: Clients can change rapidly and re-provisioning might be prohibitively expensive.

- Do not require manual intervention of the Resource Owner in the access control process (U1.2, U3.1, U5.4).

  Rationale: Manually approving access requests, while being a common solution in web access control, does not scale well in an M2M scenario.

- Enable revocation of authorizations, also considering locally cached authorization information (U4.9)

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, Sumit Singhal, John Mattson, Mohit Sethi, Carsten Bormann, Corinna Schmitt, Hannes Tschofenig, and Erik Wahlstroem for reviewing and/or contributing to the document. Also, thanks to Markus Becker, Thomas Poetsch and Koojana Kuladinithi for their input on the container monitoring use case."

6. IANA Considerations

This document has no IANA actions.

7. Informative References

[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.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, May 2014.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, June 2014.

Authors' Addresses

Ludwig Seitz (editor)
SICS Swedish ICT AB
Scheelevaegen 17
Lund 223 70
Sweden

Email: ludwig@sics.se

Stefanie Gerdes (editor)
Universitaet Bremen TZI
Postfach 330440
Bremen 28359
Germany

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

Goeran Selander
Ericsson
Faroegatan 6
Kista 164 80
Sweden

Email: goran.selander@ericsson.com

Mehdi Mani
Itron
52, rue Camille Desmoulins
Issy-les-Moulineaux 92130
France

Email: Mehdi.Mani@itron.com

Sandeep S. Kumar
Philips Research
High Tech Campus
Eindhoven 5656 AA
The Netherlands

Email: sandeep.kumar@philips.com