Scalable Authentication for Smart Objects
Klaas Wierenga <klaas@cisco.com>

Smart Objects come in many form factors. Typically they are constrained, but not all constrained in the same way. Some objects may have constraints on bandwidth use, others on power consumption and again others on processing power. This means that it is highly unlikely that there is a magic bullet for object security. Rather than focusing on such a magic bullet we should aim for a set of principles that allow for maximum flexibility and interoperability:

- multiple authentication mechanisms

It is unlikely that the same form of authentication works in each and every environment, there may be business reasons or privacy constraints that require a certain strength of authentication for some objects whereas for other objects in the same ecosystem the hardware, software or network constraints force to settle for another form of authentication. The chosen solution should therefore support all common authentication means: username/password, certificates, hardware tokens, SIM-card, biometrics etc.

- scalability/federation

It is likely that there are going to be an unprecedented number of objects connected to the (mobile) Internet. It is unlikely that a single authority can manage all of these objects, so multiple authorities are needed that all manage a subset of objects. At the same time it is highly likely that data that is produced by an object that is controlled by one authentication server needs to be consumed by another object or subject that has not under the control of that same operator. Given the potential number of objects it is further desirable that objects can be aggregated and de-aggregated into groups of objects under a common authority. The combination of these two requirements suggests a hierarchical federation concept.

- privacy preserving

Data that is generated by the objects potentially is privacy sensitive. It must be possible to make sure that the content of the messages is integrity and privacy protected. In particular user information is sensitive and it must be possible to prevent third parties from obtaining that information.

- attribute based

Related to the privacy bullet. Often it is not needed to uniquely identify an object, it is often sufficient that an object belongs to a certain class (printer), is in a particular location (room 42) or is controlled by a certain person (sysadmin). Ideally speaking access decisions are therefore not based on the
identity of the object itself but rather based on attributes of that object.

- possible direction

One possible solution can be found in the architecture of eduroam (federated wireless network access in education) that has proven to scale at least to millions of users, and its possible extension in the IETF Abfab working group for using attributes.

Eduroam makes use of the Extensible Authentication Protocol (EAP) for authenticating subjects. EAP allows for the use of multiple authentication methods, including SIM-card based mechanisms like EAP-SIM and EAP-AKA. By using a proper EAP-method privacy preservation can be achieved. Through the use of an hierarchical set of RADIUS servers the span of control of each RADIUS server remains relatively small and manageable. By using a DNS like delegation structure it is easy to route authentication requests coming through a particular RADIUS server to the RADIUS server responsible for authenticating a particular user. Abfab augments eduroam by making the transport of SAML attribute assertions between parties possible and created an API (GSS-API) for applications that want to use the RADIUS-based trust fabric.

It is worth examining whether a similar architecture, using EAP, RADIUS/Diameter, DNS/URNs, SAML/JSON tokens would scale to the size of the projected Internet of Things and is sufficiently lightweight to support the majority of use-cases.