Identification and Authentication of IoT Devices

Alper Yegin, Samsung

Security appears to be one of the most challenging areas about designing the Internet of Things (IoT). On one hand, devices forming the IoT can be extremely constrained (low processing and battery power, low memory, lack of user interface). On the other hand, this is no excuse for them to have less security than any other device on the Internet. IoT devices can be assuming very critical roles, such as monitoring as part of a home security system, or controlling as part of an intelligent transportation system. Compromise of such devices can be more catastrophic than that a typical device on the Internet (e.g., a PC, or a mobile phone).

Security design begins with the selection of credential types. These are the credentials that will be used by the IoT devices for getting authorized for network access followed by application access. Certificates, id/password pairs, and SIMs are the possible choices being considered in the industry. Each one of these credential types has its own pros and cons. Id/password pairs are relatively light-weight, yet managing them in high quantities is not practical. Certificates provide a robust and established solution for large-scale device deployments, but their added cost and dependency on CA vendors are concerning to the service providers. SIMs are attractive but applicable to only a subset of deployments.

The procedure to provision the devices with such credentials depends on the type of the credential. Id/password pairs may be provisioned by the manufacturer and passed on to the service provider who would be managing the devices. Certificates can be provisioned by the manufacturer, and optionally overwritten by the service provider with another certificate. Devices changing service providers may require re-provisioning procedure, which also impacts the choice of credential type. For example, id/password-based credentials cannot be kept the same once the device changes hands.

It appears very difficult for the industry to agree on one type of credential type for all sorts of deployments. It is expected that fragmentation similar to that of general Internet will be seen in the IoT, and application-specific (i.e., vertical) profiling will be needed in order to narrow down the possibilities and achieve interoperability.

Secure service provider discovery and service-specific provisioning is another challenge. Lack of a human user behind the device and difficulty in pre-configuring large number of devices make it difficult for device-initiated discovery and selection mechanisms. On the other hand, network-initiated discovery and selection mechanism leads to device ownership problems (i.e., how would the device know that it shall really be used by that particular service provider contacting it?).

Dealing with one set of credentials is already difficult. Dealing with multiple credentials due to the separation of network access service and application access service is even harder. Therefore, using the same credential for both types of access seems unavoidable. Furthermore, single sign on schemes are being considered as additional optimization tools.

Architecturally, the network access service provider (e.g., 3/4G, fixed broadband operator) and the application service provider who manages the devices for a specific use (e.g., smart grid) don't have to be the same. Nevertheless, former type sees this as an opportunity to expand its business, hence prepares to act as an integrated service provider. That is fine as long as it is considered as a special case. But if the latter type service providers do not emerge to assert their influence, industry designs may get skewed towards one side.

IoT devices are expected to surround our daily lives. Our activities will be closely monitored and reported by them. Unless proper measures are not put in place, our personal privacy will be in a much bigger danger than before. Hiding the device identifiers from neighboring elements and even intermediaries will be essential. Achieving a water-proof solution for the constrained IoT devices presents itself as another challenge.