# Standardizing Internet of Things Security

Hannes Tschofenig*

*ARM Limited, Email: Hannes.Tschofenig@arm.com

## I. Extended Abstract

IoT devices are often characterized by their limitations, which include slow processing power, small memory size, no or limited user interface, radio interfaces with small MTU sizes, etc. They are, by their definition, connected to the Internet / Web and used in many different scenarios, as described in RFC 7452. In practice it is hard to draw a line between an IoT and a non-IoT device. For this reason we see IoT is a continuum.

IoT devices need security functionality that takes the Internet threat model into account (see RFC 3552). In addition, IoT devices are increasingly explosed to physical attacks.

Re-using existing Internet security protocols and Internet standards in general that can accommodate the capabilities and constraints of both environments, the IoT and the Web space, has been a goal of many industry players.

It is important to note that standardization only provides a small, although important, part of the overall security story for IoT. Other considerations in the area of secure software implementation and secure deployment practices have to be taken into account as well.

Engineers take various information sources into account when designing a security solution for an IoT product, including lessons learned from attacks, best current practices, the classical threat analysis, design patterns. Real-world attacks reflect current problems in the industry and allow to demonstrate the consequences of failures to offer selected security mechanisms. The subsequent table lists common attacks and example security protocols that mitigate these attacks.

Extended abstract for the 'Workshop on Cryptography and Hardware Security for the Internet of Things', Oct. 8 - 9, 2015 organized by the University of Maryland/US. This paper represents the views of the author.

| | |
|---|---|
| Missing or limited software / firmware update mechanism | OMA LWM2M, TR-69 |
| Missing key management | Several key management protocols standardized in the IETF, OMA LWM2M, Alljoyn, OIC, oneM2M, Thread, Zigbee IP, Bluetooth, |
| Inappropriate access control | Protocols often bundled with key management protocols (e.g., IETF ACE, OAuth) |
| Missing communication security | TLS/DTLS (TLS 1.3, DTLS/TLS IoT profile, application layer security based on JSON (IETF JOSE), CBOR (IETF COSE) |
| Physical attacks | Introduction of trusted execution environments, secure elements, Trusted Computing Modules. (Global Platform, ISO/IEC 7816, TCG). |

Several of the standardization activites are still ongoing and also the business models for IoT are still evolving. It is therefore premature to predict the market acceptance of certain IoT deployment ideas. For example, it is still unclear to what extend companies will prefer the use of application layer gateways for IoT deployments or instead utilize an end-to-end IP communication model. Even the market success of certain radio technologies purposely built for the IoT market is still uncertain.

Better cooperation between the research and the standardization communities is needed! Support for the ongoing standardization development activities from the research community is highly appreciated since many of the standardization groups are quite small and would benefit from reviews of additional stakeholders. Performance measurements of state-of-the-art cryptographic algorithms and protocols are often unavailable and we expect that those measurements will help to determine whether there are indeed problems with running certain classes of security protocols on todays IoT device platforms. Some of the newly standardized security protocols have not been analysed by the larger research community either.

Finally, an important contribution from the research community is to analyse deployed IoT products and services and to point to security and privacy problems. Industry players often lack incentives to make such investigations.