CableLabs®

Response to OTA Draft Trust Framework

IoT Trust Framework – Discussion Draft Comments
Reviewed by Brian Scriber, Security Architect, CableLabs (b.scriber@cablelabs.com)
Review date: Aug 17, 2015
Based on the Aug 11, 2015 release of the OTA Draft (updated August 13)

Overall, this list presents responsibilities that fall to the manufacturer, but the users and network operators need to be able to trust the certification process and also the de-certification (revocation) process. Listed in the proposed minimum requirements, a clear requirement for the regulatory/certification body to revoke manufacturers who deviate from trust framework requirements.

1. On issue #7, the wording of "best practices" for data in motion (transit) is weak, if this proposal requires HTTPS for device sites and cloud services, it's not asking too much to explicitly require TLS or DTLS for encryption of data in transit. Listing specifics, hash algorithms, encryption algorithms, acceptable curves (as well as unacceptable curves/algorithms) would be beneficial.
2. On Issue #8, when using passwords, should there be minimum complexity/length requirements?
3. On Issue #9, this should not require "SSL best practices." SSL is effectively past its end-of-life. Please require the use of TLS instead.
4. On Issue #11, what is the minimum level of penetration testing for devices, applications and services?
5. On Issue #12, for vulnerability remediation, devices should only accept (and verify) code signed by a trusted source, perhaps reference or combine with Issue #16.
6. Aside from an indicator during pairing, device to device communication was not listed here.
    a. What information is discoverable during pairing?
    b. How can the user prevent all/some of this?
    c. How is on-boarding to a home network handled?
    d. Will the device store the WIFI password?
    e. What level of encryption for storing external credentials will be required?
7. Remote access to in-home devices was not listed.
    a. What kind of fire-walling will be required?
    b. How will bandwidth usage be able to be throttled by the user (or network operator)?
    c. Will additional security measures be required for devices with direct remote access?
8. Trusted Roots and Device Certificates: network operators and users need to be able to uniquely identify devices (particularly when devices are acting erratically, exhibiting malicious network behavior, or when compromised), quarantine them, and potentially revoke permissions on the network. Requiring signed code is one step, but providing each device a unique X509v3 certificate, private key and public key help with all of the 23 issues currently listed in the framework.