Public Comments OTA IoT Trust Framework

Submitted September 18, 2015

UL welcomes the activities of OTA, the ITWG, and member companies, developing the trust framework for IoT. We respectfully submit these comments in an effort to engage in dialogue also based on UL's activities linked to IoT. We look forward to further engagement with OTA and ITWG.

UL is an independent testing and certification organization dedicated to public safety. UL is in the process of developing a Cybersecurity Assurance Program that includes the development of a voluntary Cybersecurity standard for product testing and bears relevance for IoT as well.

1. Who would be subject to the requirements in the framework: device manufacturers, or also service, connectivity and platform providers, looking at the entire IoT ecosystem?
2. For example as well, in talking about storage of personal and sensitive data in a few requirements, are there any requirements for (the protection of data at rest in) the cloud?
3. Not all devices, applications and services, depending on the type of data, require the same level of privacy obviously. Would requirements allow for differentiation in privacy/security levels?
4. Do you consider any requirement for data/network isolation for devices with (access to) multiple components, (sub-)systems and networks?
5. The introduction reads that the ITWG supports the investigation and development of a certification program. Has any work in that direction been performed, based on the requirements in the Framework?
6. Requirement 3, and elsewhere, refers to personally identifiable data. Suggestion to extend to all sensitive data (which is not always personally identifiable). Requirement 6 defines: personal and sensitive data, which in our view is the better definition.
7. Requirement 5 refers to data retention policy. Considering that the number and variety of IoT devices increases, how should regulation/policies related to retention of metadata be applied to IoT? Do you consider any particular policy for metadata?
8. Requirement 7 refers to end-to-end encryption of all personal data as the best approach. But what about devices with limited processing power, which is quite common for IoT devices?
9. Requirement 9 refers to SSL best practices using industry standard tooling. Any particular tooling and testing that you have in mind here? We note the reference to Qualys on your website.
10. Requirement 11 refers to penetration testing. Idem: any testing practices that you have in mind here?
11. Requirement 12 refers to patch management/remediation of vulnerabilities. Idem: any practices that you have in mind here, also noting the complexity of patching a large variety of IoT devices in the field (deployed under different circumstances as well)?
12. Linked to recommendation 7 (and 10), but also as a general question, do you plan on (cross-) referencing any (other) IoT protocols/standards that exist today?

Contact information:

Gonda Lamberink
Business Development Manager

Underwriters Laboratories (UL LLC)
Software & Security division
47173 Benicia Street
Fremont, CA 94538
E: gonda.lamberink@ul.com