Feedback on OTA IoT Trust Framework – Draft Discussion[1]

Justin C. Klein Keane (Justin.kleinkeane@thingworx.com)
Security Architect
ThingWorx

I think that, to the extent possible, making the framework with the FTC guidelines on IoT security[2] will dramatically increase traction. Many in the IoT community are already looking to see what the FTC will put forth as specific guidelines and enforcement criteria. The IoT Trust Framework could make a great checklist to ensure compliance.

In the framework itself, I foresee some issues with item #3 ("**Manufacturers must conspicuously disclose all personally identifiable data types and attributes collected**.") since "personally identifiable" is a somewhat subjective term. Academic research has shown the trivial ease with which most data becomes personally identifiable when examined in aggregate or combined with other data sets.[3] Furthermore, efforts to de-identify data are nearly universally doomed to fail. I think a more realistic goal might simply be to enumerate the data that is collected via IoT devices. This allows the consumer to choose whether or not they want to participate in information sharing and place their own judgments around the relative value and privacy of certain metrics.

Similarly I think item #4 ("**Any default personal data sharing must be limited to third parties/service providers who agree to confidentiality and to limit usage for specified purposes**.") may be a little tricky to implement requiring legal contractual documents in the same way as HIPAA. Unless there is a data stewardship acknowledgement it is very difficult to define what is a personal data and what purposes are specific. Furthermore, in an era of big data and data mining, companies are seeking new and innovative ways to use data and attempts to restrict the collection of data for future use may be interpreted as obstructionist.

---

1 https://otalliance.org/system/files/files/resource/documents/iot_trust_frameworkv1.pdf

2 https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

3 https://hbr.org/2015/02/theres-no-such-thing-as-anonymous-data

As with #4 above, trying to limit the collection and use of data may be seen as stifling innovation and I would expect a lot of push-back from companies. While I personally am very leery of my personal information being traded around, I think we're at the cusp of realizing true IoT value and much of the value that we have yet to discover is going to be driven by large data sets and retrospective analysis. Denying IoT manufacturers access to this data may retard development and I suspect may be driven more by fears of past generations of marketing concerns rather than necessarily by any demonstrable bad practice in the IoT space. Unless governed by law (again, HIPAA), IoT manufacturers are likely to want to collect as much data from their devices as possible in order to discover how best to deliver value to customers.

I personally believe the transitive nature of IoT devices outlined in #6 ("**Manufacturers must disclose if the user has the ability to remove, have purged or made anonymous personal and sensitive data (other than purchase transaction history) upon discontinuing device use, loss, damage, sale or device end-of-life**.") is one of the biggest challenges of current generation IoT development that has not been sufficiently addressed. When I sell my smart home how do I transfer ownership of my smart devices while retaining my privacy? When a company sells a smart device to a competitor how do they ensure that the device can't be used against them? When IoT devices need to share data to multiple interested parties (especially in the case of medical devices where hospitals, patients, care providers, manufacturers, and maintainers might all need access to device data) how do they protect the various privacy interests of each one?

Encryption solutions in the IoT space are either extremely juvenile or non-existent so the requirements of #7 ("**Personally identifiable data must be encrypted or hashed at rest (storage) and in motion using best practices including connectivity to mobile devices, applications and the cloud utilizing Wi-Fi, Bluetooth and other communications methods**.") make me very nervous. We still can't solve the problems of broadcast encryption, M2M cryptographic trust, or even develop reliable hardware security modules. I believe the wording of #7 needs to be carefully considered and take into account the myriad protocols IoT data traverses, the compute limitations of IoT devices, the need for interoperability, and the complete lack of an IoT industry standard for encryption, lest we encourage WEP style solutions implemented at IoT scale.

#8 ("**Default passwords must be prompted to be reset or changed on first use or uniquely generated**.") is especially perplexing for me because the concept of a password is a very human-centric piece of identification and authentication. In many (most?) IoT deployments there is no human involved, so having a password is a little irrelevant, and the idea of a default takes on a different connotation entirely. Closely connected is the idea of cryptographic identification. IoT devices should strive to implement cryptographic certificates for self identification, enrollment, and authentication if at all possible, and I think this is a much more difficult problem than that of user passwords (which, let's all admit, are going to be crappy if humans have any influence over their choice).

I like the idea of encouraging transport layer security (#9 "**All user sites must adhere to SSL best practices using industry standard testing mechanisms.**"), but it may be wise to stay away from any specifics. Encryption ages like fish, not wine, so any specification will need to evolve. Another problem is that device lifetime in IoT is typically much longer than other software systems. Not only does a device need to be manufactured to adhere to best cryptographic practices, it needs to be engineered to be able to evolve over time. This ties in to #10 ("**All device sites and cloud services must utilize HTTPS encryption by default**") as well although I think it might be better to specify "encrypted protocols" by default since many IoT solutions use various protocols and may involve HTTP but only as one piece of the communications fabric.

Pen testing is a perfect recommendation (#11 "**Manufacturers must conduct penetration testing for devices, applications and services**."); bearing in mind that pen testing isn't always the most scientific (repeatable) form of testing. Software and architectural security review would probably go a lot further than penetration testing in many cases (but as a security architect I'm biased ;).

The ability to perform remote updates (#12 "**Manufacturers must have capabilities to remediate vulnerabilities in a prompt and reliable manner either through remote updates and/or through consumer notifications and instructions**.") is critical for IoT - not just for vulnerability remediation but also for evolving security considerations (such as cryptographic improvements). It might be worth mentioning that (cryptographic) verification of updates is a necessary component as well in #12 although it is called out specifically in #16.

#14 ("**Manufacturers must provide secure recovery mechanisms for passwords**.") is especially tricky when there is no human involved and I think that deserves calling out. IoT systems need to implement systems for re-credentialing of participants, especially in cases where those participants aren't humans that can recall answers to security questions or be reached on the phone. Devices need to have the capability to accept and act on re-credentialing messages to protect ecosystems without human intervention (this lack of human intervention is, I believe, a key component of the IoT security challenge). If a system is unable to handle a re-credential event then it is will fail at the first compromise.

I believe #15 ("**Device must provide a visible indicator or require user confirmation when pairing or connecting with other devices**.") simply won't work with M2M and defeats much of the functionality of M2M ecosystems. IoT operates at a scale that necessitates that human intervention need not be required. This might make perfect sense when your phone wants to pair with your watch, but many devices will need to pair with other devices that have no visible interface or otherwise preclude any human involvement. It could make sense that in such cases a clear, user accessible audit log of pairing and trust relationships be available, but we can't expect human intervention.

I believe #17 ("**For products and services which are designed to be used by multiple family members and collect PII, manufacturers need to incorporate the capability for creating individual profiles and/or have parental or administrative level controls and passwords.**") is actually much broader than just a family. Again, medical devices come to mind. Many IoT devices collect data or offer functionality that is of use to more than one ecosystem, owner, or operator. Accurate and timely tools for controlling, auditing, and verifying access, trust, and delegation are essential for the success of next generation IoT products.

#18and #19 spot on.

I have reservations about #20 ("**The device must have controls and/or documentation enabling the consumer to set, revise and manage privacy and security preferences including what information is transmitted via the device.**"), especially in cases where devices don't have interfaces or where owner reconfiguration could have a deleterious effect on a device. Toggling data fields might be unreasonable. I think as long as users are aware of the data types

and can opt out that may be sufficient. It might also be worth recognizing that many device settings can be updated by the manufacturer, and the effect this might have on user choices (are those choices adapted, reset, or ignored, and is the user advised of these changes?).

#23 ("**Configure all security and privacy related email communications to adopt email authentication protocols.**") is a little confusing to me - is this intended to combat spam coming from devices or just as a general best practice? I might opt to strike that recommendation altogether since it doesn't seem very IoT specific.

Concerns Not Addressed in the Proposal

One area of concern that I think needs to be specifically called out is the fact that IoT devices, by nature of their placement and interaction in the physical world, may collect data about minors or about people other than owners or operators. Special consideration should be taken when data might be collected about humans who might not want to, or be able to, consent to such monitoring or data collection.

Closely related, especially for consumer IoT, is that many IoT devices will operate in extremely sensitive and private arenas of human life, such as the operating room, the nursery, or the bedroom. Due care and consideration should be given to the potential impact of data collection in such situations as well as the stewardship responsibility that comes with such data. Privacy concerns extend to criminal liability, government or law enforcement surveillance, malfeasance, or simple wishes to keep certain aspects of personal life private and confidential. In some situations it is conceivable that lifestyle choices could have profound social, moral, or legal ramifications and IoT devices may be introduced into a position to observe and record data about these lifestyle choices.