From: Jonathan Lampe <jlampe@filetransferconsulting.com>
Date: September 7, 2015 at 9:59:48 PM PDT
To: admin@otalliance.org
Subject: IoT Trust Framework

This is a great initiative and parallels a lot of discussions I've been having with IoT vendors locally! I'll be chiming in from @iot_security on Twitter from time to time on this too. Here are my comments on the August 11, 2015 (updated August 13) draft (https://otalliance.org/system/files/files/resource/documents/iot_trust_frameworkv1.pdf)

=-=-=-=-=-=-=-=-=-=-=-=-=

With regard to "privacy policy" I'd like to see more guidance steering people away from xeroxing their existing web privacy policy and developing something new for IoT. (See http://iotsecuritylab.com/category/lowes/ for a bad example of xeroxing.)

You're giving vendors a LOT of wiggle room - specifically, enough wiggle room to push privacy notices to post-purchase - with this language *(emphasis mine)*:

- review prior to product purchase, download or activation *(post-purchase)*
- notices may be provided on first use or when activating a new feature or within the welcome information packet included with physical product *(all post-purchase)*

Note that item 4 seems to conflict with current privacy guidance from the FTC, which seems to only require vendors to ask for permission to consume or transmit data if it's beyond that which is reasonably expected. See https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf , especially page 40

In item 5, the wording makes it sound like the CONSUMER must delete their own data: " data will be retained as long as a customer uses the product or service and must be deleted upon expiration or account termination. " (Change "must" to "will automatically" if you mean the vendor will automatically delete this data.)

In item 6, anonymization and data export appear to be comingled in a strange way. Most companies anonymize data regularly (particularly so they can share it), but data export is usually an end-of-life (of account) event.

Awkward phrasing in 7: "This requirement requires the use of current encryption technologies solutions currently being deployed by industry." It's also quite vague; if any item should refer to future guidance (e.g., standards per protocol) it should be this one.

Item 8 would benefit from best password practices from infosec. For example, "Ideally passwords should be randomly generated." is not necessarily true from a "don't make all users write all passwords down" POV. Length and complexity are also best practices to incorporate here.

Item 9 should include an "if applicable" phrase. It should also comingle "SSL" and "TLS" (e.g., "SSL/TLS") so that both newbies (who only know SSL) and security experts (who currently demand TLS) can agree.

Item 11: Please consider also naming "gateways" - these devices are often afterthoughts (since they often act as protocol converters or proxies to cloud services) but are also a frequent target.

Item 12: Please consider adding the terms "firmware" and "software" in the list of possible remediations - manufacturers would be right to get freaked out if they faced the prospect of replacing physical devices several times over their lifetime.

Item 13: "Semi-annually" seems a bit frequent; I'd be OK if it was just annually as long as it was actually done!

Item 17: Are you sure you want to tackle something this big with a "v1" release? Cleaning up security basics like upgrading firmware with trusted patches and privacy basics like retention policy and controls seem like better goals to me.

Item 21: "life of device" is not a reasonable time period. Something in the range of 2-5 years would be. Type of support (the "service level") should also be defined, as in "security and privacy patches")

Item 23: Suddenly the guidance is quite specific and technical; I think this should probably be pushed into a companion document (or reference to a third party) about email best practices.

Additional Recommendations Item 12: It's a nice goal, but I don't understand why this is on a list of "Privacy" or "Security" items.

=-=-=-=-=-=-=-=-=-=-=-=-=-=

Regards,

Jonathan Lampe, CFTP, CISSP
File Transfer Consulting, LLC
920-248-0656 - jlampe@filetransferconsulting.com - @ftexperts