***This document was compiled in real time from the multistakeholder discussion at the October 19 multistakeholder meeting on IoT Security upgradability and patching. The notes were recorded live in front of participants. No further attempt to edit or organize the raw notes has been made.***

***For more information, please go to:*** [***https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security***](https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security)

Notes from October 19 Multistakeholder meeting on IoT Security Upgradability and Patching

**Outcomes and Goals**

* Scalable approach – heterogeneity of technology
* What about private (not Internet) networks as solution channels
* Framework for solution, adoption? OTA framework used as checklist
* Leverage IAC security framework (focused on industrial
)
* End of life/patchability transparency for consumers
* Definition of scope of framework (argument for broad)
* Scope include different application layers, specificity around layers
* Minimal security on devices
* Durable vs. non-durable goods
* Vocabularies and communications patterns for the public
	+ Internet of ransomware things - bitcoin
* Security before release, development lifecycle
* What are the goals- what are levels of patchability?
* How to make markets more transparent
* Leverage government acquisition processes
* Make people more aware when things are not patched
* Scope: patching which layer, can be used to educate consumers
* Horizontal vs vertical, consistent methodology
* Identify quick wins
* Certification- level by level
* Good practice: Encryption, notification of patches, checked regularly for firmware
* Think about reducing complexity, necessity of connectivity during manufacturing process
* +1 Orphan devices
* 3-part framework: Devices, applications, network
* Non-critical sector as a focus
* What are the desired outcomes?
* Tag devices?
* Signaling to consumer, or differentiation?
* Build market to enable differentiation based on security practices of companies
* Functioning of current market is not necessarily market failure
* Education/awareness long road, but needed
* Don’t accidentally create DRM enforcement mechanism
* Quick win: get companies to follow as code of conduct; difficult to do
* Benchmark of state of the market so as to measure project
* Possible outcomes:
	+ Clear public commitments
	+ Easily measurable if commitments are hit
	+ Look more broadly than consumer, include industrial and regulated industries- just consumer is too specific, not enough on objectives/goals
	+ General buckets/categories of patching
		- +1 Who/what/when/how/why
* Take a global view
* Diversity of stakeholders (children, etc)
* Where are the gaps? Don’t duplicate efforts/fragment guidance
* Dependency is a problem
* User driven market/government procurement
* IETF Code/AES encryption standard
* Leverage other efforts, philosophies are the same
* Why: Important to protect global public good; inventory of benefits, “whys”- low hanging fruit
* Why: why is this update being sent? Notification
* Working group: look at other standards/frameworks, create superset, include in output of process
* Why: reverse engineering of patches
* Unintended consequences: upgrades that break something that works
* Responsible disclosure practice
* Educate on reasonable security practices
* Highlight the barriers to security ecosystem- potential of litigation, how are incentives created for addressing vulnerabilities
* Scope: broad or narrow?
* Success if breaks in other areas?
* Narrow that can be modified, grow into larger solution
* Thermostat- other things that can cross industries
* How to get to win with global, regulatory challenges
* Narrow will allow companies to define themselves out of participation
* Kickstarter companies
* Test case
* Different visions:
	+ standards [not a standards making process]
	+ No enforcement mechanisms [completely voluntary]
* Look at thresholds, mechanics
	+ Public attestation of how long a device will be updated
	+ Each industry would define own thresholds
	+ Types of things that could be committed to (superset)
* Minimum thresholds vs. categories of things that should be considered with updatability
* Products on the market, what to be done, big picture would be naïve
* Desired end states regardless of industry
* Focus of NIST was process-oriented, develop broad process-based recommendations
* Get security to be a priority
* Not methods, companies incentivized to adopt procedures
* Recommendations not achievable
* Broad can be too general, not have impact
* Easy wins: transparency reporting, how long device patches, 5 questions consumers could know/understand
* DHS ICE-CERT reporting is happening
* Could be recommendation from group, monitoring agency could take this up
* 4 stage ecosystem – 0 thing, 1 sensor, 2 data aggregator, 3 computing, 4 data center/cloud, adapt patching across different levels
* +1 Actionable:
	+ List of barriers to upgrading devices, recommendations of how to remove them
	+ Identify was that industry could fix problem faster
		- Consumer education
		- Installer education
	+ Identify consortia that could be needed
	+ Experts to bring into process
	+ Who is likely party that would coordinate with other entities around the globe
	+ Metrics and tracking
* Updating device before it is compromised, after?
* Explicit naming of dependencies
* Sometimes there are vulnerabilities that are not patchable
* Updating a device- what does it mean; within ecosystem?
* All different parts of ecosystem could need updates
* What is trusted computing base
* Class A device (full stack) vs. Class M devices (constrained)
* Four layer classification scheme, pyramid with minimal memory devices on bottom (16 kbs), small, medium, large (laptops, desktops) [IETF]
* Need downloadable code for stovepipe, focus on small devices
* Work on problem, come up with solution, make available to producers
* Otherwise free thing will be used with vulnerability
* Free and open: have global effect
* Other governments will pay attention to what we are doing; already happening
* Is a market for more expensive secure devices
* Requirement: resiliency, what does the system depend on for updating
* Technology neutral
* Working group: What existing efforts are out there
	+ Outcome: what are general requirements from any vendor at any level, look at other efforts and what they have already done (superset)
* OMA owns this issue for mobile platforms
* Working group: Look at incentives, what are barriers
* Automotive engineers
* When have different groups made different decisions
* +1 Role for shared infrastructure (resiliency)
* How to get adoption of labeling
	+ No practical software liability
	+ Labeling may stave of liability
* +1 Working group: Pros and cons of labeling
	+ Hardware, network, application
* First principles sourced off of existing work
* Process oriented, high level categories and subcategories
	+ Standards as informative references
* Working group: stewardship of data that is collected
* Labeling consumer education?
	+ Labels not perfect, go through pros and cons
	+ How to couple this to consumer education campaign
	+ Similar to Truste?
* Consumers will never be as security conscious as a security professional
* Make label, language applicable to consumer need
	+ Device out of service time during upgrading
	+ Good to know how long a device is supported
	+ Being able to make informed choice will be of use to consumers, even if not all consumers
* Working group for each class of device
	+ Maximum capability and minimum requirements
* Consider the demographics of device users
* How can you convey to users when a device needs to be replaced?
* What would a work product look like? Security checklists (consumer-facing separate from supply chain).
* Principles, standards already exist, do not need to be duplicated or made more complicated

Work streams:

* 1. **Standards and initiatives review** applying to security patching and upgradability. Summary of the existing standards-related efforts, produce report for industry documenting existing practices.
		1. Kent to lead, Deral Heiland (potential co-chair)
	2. **Incentives and elimination of barriers**. How do we foster greater adoption?
		1. Vic to co-chair
		2. Potential to combine with c.?
	3. **Communication of elements**. Review existing labels and communications, understand pros and cons of this approach.
		1. Harley, Beau, Aaron to co-chair
		2. Keep separate from defining standards for the elements
		3. Define what we mean by “consumer” – direct vs. indirect stakeholders (buyer of device vs. those who could be affected by the device)
		4. Make sure to keep things process oriented, and stay away from too much specificity, which might harm flexibility
		5. Potential UL participation
		6. Broad, shared set of definitions
	4. **Maximum capability, minimum expectations** for each class of device (4 stage description).
		1. Aalap and Shukri co-chair
		2. Not prescriptive
	5. **Shared, open upgrade framework** for IoT lifecycle
		1. Todd to co-chair, Tadayoshi Kohno (tentative)
		2. Identifying requirements
		3. Find out who could benefit
		4. Identifying points of failure/weakness
		5. There may be examples of this already, could be applied in a different way. Review existing vendors
* Continue to think about unexpected consequences
	+ Acknowledge the role that testing plays
* How will the group deal with definitional differences? Potential area of ambiguity
* This process has a unique ability to address patchability, whereas there are already efforts underway addressing device security
	+ Working groups could define “problem statement” that would include focus of security upgradability and patchability

Next meeting

* + Location, Date
		- IIC meeting in San Diego first week of December
		- IEEE World Forum on IoT in mid-December (Reston, Va.)