This document was compiled in real time from the multistakeholder discussion at the April 26 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

---

Notes from April 26, 2017, Multistakeholder Meeting on IoT Security Upgradability and Patching

Capabilities Working Group

- Slide presentation
- Question about talking about value in terms of what is being protected – does it consider both direct value and indirect value? Answer: Both
- For example, in the consumer marketplace, for example with lightbulbs. How secure does a lightbulb need to be? If it can act like a controller on the consumer's network, then there's ancillary value like I can now control the lock, access the home, could be a safety issue. Need to look at the other indirect effects because that really is the value that we are protecting.
- The broad issue of IoT security is a massive issue and very important. Focus on applying it back to mapping it to the software update question.
- A lot of concerns that traditional update systems have, wondering if they are not adequately discussed – protecting from different types of attacks that keep clients from obtaining updates. Lots of major tech firms have had people break into different parts of their infrastructure and distribute malicious updates that way, but IoT manufacturers will probably not have as rigorous security as those large firms.
- The complete path needs to be protected; verification is important as well. See steps common for all use cases.
- Fedora was broken into twice and had exactly this design. The organizational provider's operation and maintenance also needs to be part of it. Many organizations have strong policies and procedures in areas where security is important, industry best practices.
- The integrity of the patch is an issue but we also recognize that there is a vast array of companies coming to market with a whole range of maturity in security etc.
- Is the scope of this work to guarantee the integrity of those updates? Or is it to ensure that updates take place?

- This focuses on the manufacturer and his process or the developer, how he updates it. What happens to the govt or developer or whoever in the industry to update the consumers to tell them that there is such a thing as IoT and what they need to do? There are technical issues that many consumers can't deal with.
- Service agreement is key.
- Other working groups are working on the consumer issue.
- Regarding how risk is viewed in this: A discussion about is adding an update going to add risk – anytime you add software you are broadening attack surface. How do we make an updater that minimizes the overall risk to the product?
- Need to do a threat assessment and get to specific level of detail
- The attack issues have been addressed by many standards. We should be able to go through and review these and see if there is a gap.
- Regarding table: It's useful, but some use cases would also be helpful. Use cases will help people understand it. More instruction around here's what this means to this kind of device and the steps that should happen and why it's important.
- Scalability – "transmit the updated code" sounds easy but there may be millions of devices in the field. A scheduling capability is one way to do that. What does this look like on that scale?
- Microsoft published some useful info on how they do updates.
- This seems like something NIST would like to do after the community works on it some more.
- Related CableLabs materials are available on their website.

Existing Standards, Tools, and Initiatives Working Group

- Slide presentation
- Lots of consortium and industry alliance work going on, consensus standards that the org is using, so not typical standards.
- Broadband Forum, new participant, should be included in the research pending column.
- Many things that have been done in the software industry are applicable, lots of best practices can be carried forward.
- These standards are typically a lot more descriptive vs prescriptive.
- Many of these documents aren't focusing on precision. Those that do typically are for a specific case in a specific industry.
- Is there really a difference between the techniques and processes for today in the software industry vs IoT as we move into the future? Maybe we just need to identify what the differences are from traditional software infrastructures.
- Additional help is needed in the WG.
- These may not all be "standards".
- I would segment this out maybe into a grid. Some are very focused on something like technical interoperability, etc. Even though the scope is patching it might be good to have a grid of what these all include.
- There are 3 dimensions to IoT. How to patch device? How to patch mobile app it works with? Plus the cloud.
- We really haven't classified these into SDOs, industry alliance, etc. and we probably do need to do that.

- Often people will intentionally pick and choose what software they update for their Linux systems, for examples, and that is pervasive across the IoT space.
- From a risk standpoint, you can't force every home user to be an informed consumer.
- In some IoT environments there is a master-slave relationship with a very weak device just receiving.
- There is an effort beginning tomorrow led by CDT, beginning to look at some of the same issues and frameworks.
- There is a difference between how to handle a commercial customer update vs a consumer update.
- Some principles are designed to be evergreen deliberately, which is why they don't have a deep level of specificity.
- Add to review: Trusted Computing Group, CableLabs specifications, Europeans' Alliance for Internet of Things, SafeCode, etc
- Mapping it to IoT, looking for gaps, what are the common patterns?

Communicating Upgradability and Improving Transparency Working Group

- Slide presentation
- Consumers have difficulty understanding upgradability
- Group kept militant focus on mandate: ID the critical elements of info that should be communicated to IoT users and consumers
- ID'd 6 elements, 3 that manufacturers should consider communicating to consumers prior to purchase and 3 that can be communicated after purchase.
- Must be careful about conveying false sense of security to consumer.
- The document notes that this is just one narrow slice of issues related to IoT - this is related directly to updatability. It mentions that manufacturers should consider advising consumers on additional issues (such as privacy). This effort has a defined scope deliberately.
- We do not want to tell manufacturers what they can and cannot say.
- Online Trust Alliance outlined 37 principles regarding broader issues.
- Having communications about the expected delivery mechanism and the size of updates and what this means, Microsoft has received complaints from consumers regarding the large update sizes for Win 10 and they are not unique in that regard. Consumers care about size of updates and that would be a nice addition to A2.
- What would the generally accepted size limit be? (Security updates tend to be bundled into a lot of other things.)
- Consumers are not asking these questions now.
- For future discussion? Updates should not override user settings without a flagged exception.
- B3 – Some groups will label and discuss the impacts of different types of compromises in a table
- Level of detail will differ based on product and user type, etc.

Incentives, Barriers, and Adoption Working Group

- Slide presentation
- Might mean norm/authority instead of standard in slide

- Suggestion re user group: Run this for residential consumer, industrial consumer, high end consumer, etc.
- Group was not going to be able to tackle the risk management exercise. There is an infinite number of scenarios, had to scope it.
- White paper, need to identify target audience.
- Is this a useful direction?
- Producers decide if it's upgradeable, but consumers can influence it.
- Integrators might be another category – they have challenges trying to bridge the gap between a producer and user.
- Companies that want to bring products and services to market are hungry for direction.
- Tiering – The users can be put into tiers to define whether security updates should be available.
- But then the horizon starts going further and further out. There are immediate concerns.
- Stakeholder that is missing: "everybody else" – stakeholders that are potentially affected are not the actual user of the device. Impact to others who are affected by what is done by the device (DDoS attacks). IoT security as a tragedy of the commons.
- IoT Analytics segments the IoT marketplace into IoTtoC and IoTtoB. Incentives within each category are fairly similar.
- Voluntary vs regulatory – that kind of material can come down from on high, but for manufacturers or developers who are building it, what is the lowest threshold?
- In the taxonomy, we try and fit it into a lowered barrier or stronger incentives.
- Re NIST WG on Cyber Physical Systems document, it is inaccessible because it does not have use cases. There is a huge market for use cases with an appropriate identification of what features need to be in products.
- There will be enough diversity of use cases among producers alone, and that gives you the most bang for your buck. It will be harder to nail down cases for regulators – politics alone is a huge barrier or incentive. Users come from a huge array of backgrounds. In the end, we are talking more about the upgradability of IoT devices and the only people who can really do that are the producers.
- Why don't producers currently include upgradability in their products? Is it a technical issue? Profit margin? Just didn't think of it before?
- Or if something is upgradable, is it easy/intuitive to make the upgrades or is it prohibitively complex?
- Barriers: Cost, control (manufacturers want to maintain control of the devices they produced), business model (sell the product and I'm done with it).
- Can the elements of the updates be quantified? Most common cost raised from the start is that it costs $ to put security in. Then my competitor can undercut my price.
- Once there is a major adopter, then everyone else wants to follow.
- Make it something people can use out of the box, then we can invent.
- The market is a barrier – getting the device to market.
- The various IoT domains are different enough that you can't have the same ideas for each one.
- Need to convince the manufacturers that there is value in going through this process.
- Requested assistance from producers, helping to frame group in real terms. Need more concrete and informative use cases.

Stakeholder Discussion

- What does success look like?
    - NTIA is the facilitator. We do not build metrics around success. We want to demonstrate the value of this sort of initiative.
    - Some bodies have recurring publications – triennials national standards policy doc (DOC and vol standards community), TOC of standards catalog has 15-20 standards bodies who might want to be polled for their collective consensus view for how things might roll out, and then OSTP will produce a national technology plan that should include IoT and could reflect the consensus from these working groups.
- What form might this work finally take?
    - Work of each group is valuable as a stand-alone document, but could also be integrated into a whole.
    - Target audience for each output may be different. Mature each output individually first. Then potentially could create a larger combined document. Final product might look like the four groups' document and then perhaps something that synthesizes them all, but that may not be necessary.
    - Metrics for each output will be different. Metrics for the valuable compendium of standards might be downloads, but for consumer group the metrics would relate to adoption.
    - Eventual synthesis document would help us understand what we're missing.
    - Take advantage of multisector nature of this and find a way to do multisector communication. Need events, NOT a cybersecurity conference, with a variety of panelists (not just security experts).
    - Single document would need simple messages without too much granularity.
    - Could number each of the four working group's documents in a complementary manner.
    - Additional stakeholder suggestion: state attorneys general's DC offices
    - NIST might be a good place to try to get work out.
    - Stakeholders want NTIA to champion this issue.
    - Discuss venues for promotion. Second IOT National Institute, Open Connectivity Foundation, User Service Platform forum, OMG IIoT, panels at cybersecurity events, RSA 2018, where do the device manufacturers go? CES, should think outside the box, National Retail Federation, Society of Maintenance and Reliability Professions (SMRP)
    - Develop core deck that people could use in briefing after documents were done
- Virtual meeting in 3-4th week of June
- Next in-person meeting early fall (associate with timing for non-cybersecurity target, get more people who could use the information into the room).