IoT AB Cybersecurity Subteam

1. Section Content
    1. National Cybersecurity Label for Consumer Connected Devices (White House Initiative) – foundational element for IoT and can be extended beyond consumer.
    2. More emphasis on the linkage between security and privacy; how do we address the privacy concerns around the data collected by the devices, especially consumer privacy in confined spaces - e.g., home, car – device is in close proximity to the user; SPLICE initiative from NSF – focus on security and privacy of consumer IoT devices; address disconnect between hardware and privacy – unclear who is responsible for addressing privacy concerns (e.g., device, application); have to deal with privacy across the ecosystem but the concern starts at the edge as the data is collected by the IoT device; policy issues but also design concerns to make devices more privacy aware
    3. Can distinguish among major sectors of IoT, industrial control systems/operational technology has unique concerns for security which are different from consumer devices; some sectors (e.g., health care/medical) are heavily regulated
    4. Security should be from the chip inside; microcontrollers are making progress but not the same across the board; associated standards for security at the chip level; need to distinguish use cases / market segments but microcontrollers are at the root; have to look at the uniform chip layer; horizontal issue around implementation of security at the chip level; sensor level currently has no security – currently presumed to be a cost issue; traceability needed; different level of security depending on power, performance, market sector etc.; need for a security framework for types of devices; how do you address the risks associated with devices and incorporate into your ecosystem (distinguish between microcontroller versus microprocessor- different security aspects, need to monitor this space as there is some crossover, closed infrastructure some of the ICs act as gateways to the cloud)
    5. Legacy IOT devices have to be addressed (e.g., unpatched camera) ,
    6. In the OT space, smart buildings, manufacturing, are systems that are open systems with no security.
    7. TPM and secure device architectures, esp. for critical infrastructure, secure elements as well that can enter at the low end.
    8. Defining the attack vector, including some of the newer attacks, e.g. battery attacks (Battery draining attacks against edge computing nodes in IoT networks | DeepAI)
    9. Interconnection between security and traceability- addressed in supply chain-linkage paragraph.

2. Policy Topics:
    1. Clarity on the distinction between major IoT sectors: IIoT, IoMT, consumer, etc.
    2. Liability issues – can be a reason to hold back (barrier) on security.
    3. Cyber incident reporting for critical infrastructure

3. Issues:
    1. Security vs privacy, at the hardware level
        1. The group discussed the role of the Cybersecurity Subgroup vs. the Privacy Subgroup with regard to “privacy”, and tentatively decided our role may land on devices collecting and storing data locally. Once the data is exposed beyond the device, it is more clearly a topic for the Privacy subgroup.
    2. Legacy IoT devices (installed base issue in cybersecurity) – (e.g. SCADA systems that interface with process sensors
    3. Global ecosystem and fragmentation (complying with multiple regulatory regimes)
    4. Transparency
    5. Traceability
        1. Trusted devices v. secure devices
    6. Evolving attacks
        1. Battery draining attacks
4. (Potential) Solutions and Activities and Opportunities
    1. Consumer IoT (national consumer cybersecurity label effort)
    2. e-Labeling
    3. Security by Design (Secure Development Life Cycle)
    4. Built-in security in products and systems (co-design: HW/FW hardware and firmware, and SW/OS software operating system/apps)
    5. Harmonization to address global fragmentation.
    6. Market incentives for implementing cybersecurity
    7. Other technologies being deployed in industry (TPM, e.g.)
    8. Training and workforce development- things that are specific to cybersecurity with a linkage back to the workforce subgroup.
5. Recommendations should flow from the above – (items 3 to 6 are some suggestions)
6. Issues which have international implications- need input from the international sub team.
7. References: Section 3.2 of the WH National Cybersecurity Strategy, others TBD
8. Speakers: forthcoming once topics are finalized. US Policy director from Intel one suggestion (US perspective can address workforce development), possibly a European perspective as well.