Tussles in IoT Space: Crucial Considerations for Consumer Devices

Susan Landau[1]
The Fletcher School and School of Engineering
Tufts University
susan.landau@tufts.edu
August 8, 2021

Given the billions of IoT devices that will be in consumers' homes, vehicles, and on their persons, there's a clear need to enable consumers to make informed choices about the security of these devices. And the initial issues on which labeling might be based—no universal default passwords in IoT devices; having a vulnerability disclosure policy; providing a "defined support period" during which time security updates would be issued—are ones for which there is little disagreement. But getting past that initial step will be significantly harder. That's not only because the next set of security improvements will be more complex for manufacturers to implement; it is because security is only one aspect in a set of fundamental IoT requirements. Others include controllability (who is able to control the device), data portability (will data on the device be portable to another), efficiency, interoperability, privacy, safety, and usability. In tradeoffs between these aspects, manufacturers' and users' interests may not be aligned. And in some cases there may be third parties, such as a utility company, that, through law or regulation, are also involved.

Such situations are not new. Years ago, the Trusted Computing Group (TCG) produced Best Practice Principles to govern tradeoffs between security, privacy, interoperality, data portability, controllability, and ease-of-use in TCG technology [2]. One situation concerned controllability of an enterprise laptop: should it be the company, which owned it, or the employee, who used it? The Controllability Principle determined that, "Each owner should have effective choice and control over the use and operation of the TCG-enabled capabilities that belong to them; their participation must be opt-in. Subsequently any user can reliably disable the TCG functionality in a way that does not violate the owner's [security] policy." [2, p. 10]. Thus if a user opts for greater privacy while using the laptop, they will be limited in the capabilities they have on the device. This careful slicing between interests enables both user privacy protection **and** enterprise security.

This is a classic tussle between competing requirements [1]. While initial

[1]This work was partially supported by NSF grant CNS-1955805.

efforts on security labeling will not involve such tussles, once labeling gets past the easy problems, many will arise: between security and controllability, security and interoperability, security and usability, privacy and usability, etc. Developing appropriate security protections requires resolving these clashes, but unless there is a clear and overriding way to handle the conflict, each resolution will be a one-off decision, one without clarity as to basic ways that consumer IoT devices should function. That is a lose/lose situation.

With a tight time frame for responding to Executive Order 14028, it is impossible to develop a set of best practice principles to govern the initial security labeling. That doesn't obviate the need for such a set of principles to guide inevitable clashes between competing goals. Hammering out where tradeoffs need to be made (e.g., between security and safety) and where core requirements need to be balanced, would be extremely useful for developing sound security practices. As part of the effort in responding to the executive order, NIST should provide a convening function to develop best practice principles for consumers of IoT devices. Developing a set of principles would require participation of IoT industry, consumer groups, and researchers from both technical and policy communities. The following are key goals:

1. Determine "core" needs for consumer IoT devices. Is data portability, efficiency, interoperability, privacy, and security the right list? Are other fundamental characteristics currently missing?

2. Determine a set of Best Practice Principles to govern conflicts between competing needs.

Labeling of IoT devices that focuses on the single attribute of security is likely to be too narrow to actually fit consumer needs. By developing informed decisions *now* about tradeoffs between the various aspects affecting quality of function of IoT devices, the security labeling effort has a much greater likelihood of long-term success. That would be a major win. It is a strong argument for NIST to broaden its IoT security labeling project to begin efforts developing IoT Best Practice Principles.

References

[1] Clark, David D., John Wroclawski, Karen Sollins, and Robert Braden, "Tussle in Cyberspace: Defining Tomorrow's Internet," SIGCOMM, 2003.

[2] Best Practices Committee, Trusted Computing Group, "Design, Implementation, and Usage Principles, Version 3.0," February 2011.