Computing Community Consortium (CCC) Response to Establishing Confidence in IoT Device Security: How do we get there?

June 2021

Nadya T. Bliss (Arizona State University), Kathleen Fisher (Tufts University), and Daniel Lopresti (Lehigh University/CCC Vice Chair)

Response to NIST Cybersecurity White Paper (DRAFT):
https://csrc.nist.gov/publications/detail/white-paper/2021/05/14/establishing-confidence-in-iot-device-security/draft

Thank you to the authors for this insightful white paper on the important issue of establishing confidence in IoT device security.

In the short time since the draft was released, a number of current events have occurred that we believe should be mentioned in the final white paper. In particular, we point to the topic of ransomware and its paralyzing effects on critical infrastructure, as was made clear by the Colonial Pipeline hack which broke on May 10, 2021 and the later JBS meat processing attack on June 2, 2021. Ransomware is a growing threat vector that increases the importance of confidence measures for IoT devices, in particular those that are embedded in critical industrial settings (IIoT).

We also believe the report should put more emphasis on the security ecosystem, and how the security of IoT devices should be evaluated for whether they could compromise other, larger parts of a system. The report says some IoT devices might be very cheap and short lived and as such not worth extensive protections (which is of course true). It also says that a consideration is whether the IoT device might compromise a local area network (which is also true). But the draft doesn't clearly bring together the issue of the cheap, short-lived IoT device being used to compromise a local network that can then compromise a much bigger system. The pieces are there, but the white paper should draw the conclusion for the reader, so that the problem can be fully understood.

While we think it is useful that different risks are highlighted, there is more to be done on quantifying those risks. It is difficult to establish confidence without explicit cost metrics.There is discussion in Theme 2 in Section 6.1 about various kinds of risk, but not how to actually quantify it. If it is just called out but not properly priced, it is not clear that it can contribute to an effective confidence mechanism. Calling it out is a good first step, but not sufficient. There is some discussion of policy and regulations, but this does not really address the fact that there also needs to be a connection to market incentives.

In National Efforts, Section 5.1, a number of examples are highlighted. Another example to consider including is the new U.S. Food and Drug Administration position, held by University of Michigan computer science researcher and former Computing Community Consortium (CCC)[1] Council member Kevin Fu. Fu has been named acting director of medical device cybersecurity in the FDA's Center for Devices and Radiological Health[2]. The current draft briefly mentions smart medical and health devices, but clearly this is an area where establishing appropriate levels of confidence will be critical.

We note that NIST has covered some of these important missing points in other recent whitepapers[3] [4]. While we understand the "divide and conquer" approach to tackling complex issues such as this, it has become apparent that taking a fully comprehensive view will be critical in addressing the security challenges and the resulting confidence issues when it comes to IoT and other advanced computing technologies. We know that adversaries are always searching for the weakest link in a chain, and all-to-often they are successful in finding one.

CCC is happy to have follow up conversations as needed. We have Task Force focused on Cybersecurity and Cybertrust [5] which is actively working in the areas of ransomware, incentives for hardware security, cyber insurance, and the research ecosystem for security. Please feel free to reach out to us with any questions (cybersecurity-taskforce@cra.org).

[1] https://cra.org/ccc/
[2] https://news.umich.edu/u-m-professor-appointed-to-fda-medical-device-security-post/
[3] https://www.nccoe.nist.gov/projects/use-cases/energy-sector/iiot
[4] https://csrc.nist.gov/CSRC/media/Publications/nistir/draft/documents/NIST.IR.8374-preliminary-draft.pdf
[5] https://cra.org/ccc/task-forces/cybersecurity-and-cybertrust/