From: Hastings, Nelson (Fed)
To: Regenscheid, Andrew R. (Fed)
Subject: FW: NoaC security consideration - PML/ITL brainstorming workshop
Date: Wednesday, April 17, 2019 2:52:14 PM

FYI - Nelson

From: "Martin, Natalia G. (Fed)" <natalia.martin@nist.gov>
Date: Wednesday, April 17, 2019 at 12:20 PM
To: "Goldstein, Barbara L. (Fed)" <barbara.goldstein@nist.gov>, Murugiah Souppaya <murugiah.souppaya@nist.gov>, "Klimov, Nikolai (Fed)" <nikolai.klimov@nist.gov>, "Westly, Daron A. (Fed)" <daron.westly@nist.gov>, "Scherschligt, Julia (Fed)" <julia.scherschligt@nist.gov>, "Fagan, Michael J. (Fed)" <michael.fagan@nist.gov>, Matthew Scholl <matthew.scholl@nist.gov>, Andrew Regenscheid <andrew.regenscheid@nist.gov>, Kevin Stine <kevin.stine@nist.gov>, Nelson Hastings <nelson.hastings@nist.gov>, "Badger, Mark Lee (Fed)" <mark.badger@nist.gov>, "Brown, Hannah (Fed)" <hannah.brown@nist.gov>
Cc: "Strouse, Gregory F. Mr. (Fed)" <gregory.strouse@nist.gov>, Donna Dodson <donna.dodson@nist.gov>
Subject: RE: NoaC security consideration - PML/ITL brainstorming workshop

Dear Colleagues,

Thanks for your interest and participation in the NoaC security brainstorming session yesterday. Our next step is to do a deep dive into a specific use case for Standard Photonic Thermometer. Below please find a summary of our discussion.

Discussion Points:

- Barbara Goldstein provided an overview of the NoaC program and talked about technology transfer roadmap.
- Discussed the goals of this PML/ITL collaboration:
  - Identify and implement security considerations during design of NoaC devices
  - Provide further recommendations to NoaC manufactures on a set of cybersecurity capabilities and security profile
- Why it's important - NoaC devices will be associated with NIST brand and reputation for high quality, precision measurement, integrity, and security.
- Automation is another driver for looking at security questions, and a big part of it is an ability to demonstrate SI tradability. Julia Scherschligt explained that the biggest add-on value of Quantum SI is that NIST doesn't have to be "traceability police". We would want to realize traceability through SI observed in the nature by measuring material properties.
- Discussed use of NoaC as IoT devices and related methods for surveillance. One chip can have several types of measurement capabilities (temperature, moisture, humidity for example), or several chips can be deployed together on one platform.
- Matt Scholl suggested that we should look at security from the outcome perspective and

focus on the device itself rather than where it's going. He also suggested to involve Lisa Carnahan from the Standards Coordination Office into further discussions. Lisa has an extensive experience in the area of standards, inseparability and risk management.

- Discussed the need for simplification to understand a common platform components, modules, and composition of the channels. This would allow us to consider necessary security controls and perhaps "wrapping" technologies. To do so, we will start by considering 1 device example with use cases.
- Agreed that Standard Photonic Thermometer would be a good test bed for the effort. Standard Photonic Thermometer (SPoT) is a nano-scale device that uses fiber coupling for connection interface. The data from the sensor can be read remotely. Envisioned application - high accuracy and precision measurements with an ability to be IoT imbedded device.
- Path forward: consider use cases for SPoT to understand design, assumptions, technology composition, communication channels and perform thread modeling. This will be achieved via slide presentation, lab visit and brainstorming discussion in about 2 hours block of time.

Action items:

- Set up SPoT security brainstorming session – organizers: Natalia Martin/Nikolai Klimov

Please let me know if I've missed anything important.

Looking forward to working together on this exciting initiative.

Natalia Martin
Business Operations Office | External Partnerships
National Institute of Standards and Technology
(301) 975-8688

-----Original Message-----
From: Souppaya, Murugiah (Fed)
Sent: Tuesday, April 16, 2019 2:43 PM
To: Martin, Natalia G. (Fed) <natalia.martin@nist.gov>; Klimov, Nikolai (Fed) <nikolai.klimov@nist.gov>; Goldstein, Barbara L. (Fed) <barbara.goldstein@nist.gov>; Westly, Daron A. (Fed) <daron.westly@nist.gov>; Scherschligt, Julia (Fed) <julia.scherschligt@nist.gov>
Cc: Fagan, Michael J. (Fed) <michael.fagan@nist.gov>; Scholl, Matthew (Fed) <matthew.scholl@nist.gov>; Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>; Stine, Kevin (Fed) <kevin.stine@nist.gov>; Hastings, Nelson (Fed) <nelson.hastings@nist.gov>; Badger, Mark Lee (Fed) <mark.badger@nist.gov>
Subject: Re: NoaC security consideration - PML/ITL brainstorming workshop

A reference to the threat modeling draft.

https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800_154_draft.pdf

Murugiah

_____

From: Martin, Natalia G. (Fed)
Sent: Thursday, February 28, 2019 3:40 PM
To: Martin, Natalia G. (Fed); Strouse, Gregory F. Mr. (Fed); Scherschligt, Julia (Fed); Klimov, Nikolai (Fed); Dodson, Donna F. (Fed); Regenscheid, Andrew (Fed); Stine, Kevin (Fed); Scholl, Matthew (Fed); Souppaya, Murugiah (Fed); Hastings, Nelson (Fed); Megas, Katerina N. (Fed); Srinivasan, Kartik (Fed); Goldstein, Barbara L. (Fed); Ahmed, Zeeshan (Fed)
Cc: Fagan, Michael J. (Fed); Westly, Daron A. (Fed); Brown, Hannah (Fed)
Subject: NoaC security consideration - PML/ITL brainstorming workshop
When: Tuesday, April 16, 2019 1:00 PM-4:00 PM.
Where: 222/B341

Colleagues,

This workshop is to discuss security profiles for NoaC device development and manufacturing. Please see background information attached.

Goal: joint paper (ITL, PML, MR) that could be used for manufacturing recommendations, licensing agreements on what manufacturers need to do for security assurance of the NoaC devices.

Path forward to achieve the goal: ITL and PML scientists to whiteboard several use cases for NoaC sensors within systems. We will start with something simple and create at least 3 examples of manufacturing security control profiles.