CSIA RFI Responses, January 15, 2019

Update to the 2016 Federal Cybersecurity Research and Development Strategic Plan RFI Responses

DISCLAIMER: The RFI public responses received and posted do not represent the views and/or opinions of the U.S. Government, NSTC Subcommittee on Networking and Information Technology Research and Development (NITRD), NITRD National Coordination Office, and/or any other Federal agencies and/or government entities. We bear no responsibility for the accuracy, legality or content of all external links included in this document.

FeedBack to the 2016 Federal Cybersecurity Research and Development Strategic Plan

Von Welch
Director, Indiana University Center for Applied Cybersecurity Research
Director, Trusted CI, the NSF Cybersecurity Center of Excellence
Contact: vwelch@iu.edu, (812) 856-0363

Summary: The Cybersecurity Research and Development Strategic Plan Working Group to continue to maintain research and development to Deter, Protect, Detect, and Adapt to integrity-based attacks a priority.

In response to the following request in the Federal Registry:

> 3. What areas of research or topics of the 2016 Strategic Plan should continue to be a priority for federally funded research and require continued Federal R&D investments?

In Section 2 of the 2016 Federal Cybersecurity Research and Development Strategic Plan, the importance of integrity and availability is recognized: "In many situations, integrity and availability are the dominant properties of interest." While confidentiality is often the critical failure mode of cybersecurity, and indeed breaches of confidentiality continue to make headlines, emphasis on detering, protecting against, detecting, and adapting to integrity availability attacks must continue to be a priority.

Examples of the importance of integrity R&D includes:

- Ransomware continues to be an popular attack on integrity and availability that allows criminals to attack datasets which previously held no financial value.
- Scientific data from a variety of domains often has low confidentiality requirements but strong requirements for integrity and availability to support research. Security controls focused on confidentiality can undermine the Plan's stated goal for research: "...to make cybersecurity less onerous while providing more-effective defenses."
- Trust in scientific research results requires not only integrity protections for its data, but the ability to provide evidence of that data integrity against claims to the contrary.
- Successful integrity attacks are hard to diagnosis well. Modern hash algorithms intentionally do not give information about the nature of change, meaning if two hashes do not match one cannot discern from the difference the extent of damage from an integrity attack.

- Malicious changes to software and hardware designs in the supply chain are a growing threat to weaken operational systems.