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.

SANDIA REPORT
SAND2019-0196
Printed January 2019

Sandia National Laboratories

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

Submitted by:
Thomas D. Tarman
Sandia National Laboratories
tdtarma@sandia.gov

January 15, 2019

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

This report contains a response from Sandia National Laboratories for the 2019 update to the 2016 Federal Cybersecurity Research and Development Strategic Plan.

ACKNOWLEDGEMENTS

The following staff contributed to the contents of this response:

- Susan Adams
- Karin Butler
- Stacey Hendrickson
- S. Todd Jones
- Michelle Leger
- Kimberly Montoya
- Nicole Murchison
- Ali Pinar
- Paul Schutte
- Thomas Tarman

1. INTRODUCTION

Sandia National Laboratories is pleased at the opportunity to respond to this request for information for the 2019 update to the 2016 Federal Cybersecurity Research and Development Strategic Plan. As a national laboratory, cybersecurity is paramount as we execute our national security mission. However, as software and the distributed infrastructure on which it runs becomes increasingly complex, our ability to assess the trust we keep in these systems must keep pace with the changing cyber landscape. A Federal Cybersecurity Strategic Plan that evolves with technology is necessary in this dynamic environment.

This response describes research topics and technologies for understanding complex software and distributed systems, and the human factors associated with this understanding and with cyber security more generally. This response addresses the following questions contained in the RFI:

> 1. What innovative, transformational technologies have the potential to greatly enhance the security, reliability, resiliency, and trustworthiness of the digital infrastructure, and to protect consumer privacy?
>
> 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?
>
> 4. What challenges or objectives not included in the 2016 Strategic Plan should be strategic priorities for federally funded R&D in cybersecurity? Discuss what new capabilities would be desired, what objectives should guide such research, and why those capabilities and objectives should be strategic priorities.

2. SOFTWARE AND DISTRIBUTED SYSTEM ANALYSIS FOR ASSESSING TRUST

The 2016 Federal Cybersecurity Research and Development Strategic Plan correctly identifies the challenges relating to the asymmetric advantage that adversaries enjoy when exploiting vulnerabilities in cyber systems. Rapid software release/update cycles hinder the defender's ability to analyze software in timely fashion to assess trustworthiness and mitigations prior to deployment into production systems. This challenge extends beyond standalone software – modern information technology (IT) services are deployed in a distributed fashion using cloud computing and storage infrastructure running on hardware that is globally distributed, and uses software from a variety of sources to implement the service and the cloud infrastructure on which it depends. Assessing IT trustworthiness in these environments requires new technology and tools that are capable of instrumenting distributed applications and "microservices", and integrating large volumes of data in order to allow a human analyst to understand (and, eventually, gain trust in) these services at timescales that are commensurate with software release/update cycles.

A number of emerging technologies that were identified in the 2016 Strategic Plan challenge an analyst's ability to understand an IT system and establish trust in it:

- **Cloud systems (cloud computing, cloud storage, and software defined networking)**. Cloud computing allows distributed IT systems to respond to changing conditions such as user demand, network load, and availability of compute and network resources by replicating and migrating virtual machines and containers in response. Similarly, cloud storage and software defined networking provide robust, dynamic access to available data storage and networking bandwidth. The infrastructure that implements cloud systems is itself a complex software system, which provides a substrate to applications that must be considered when assessing the trustworthiness of a cloud-enabled IT system.
- **Mobile devices, embedded devices, and Internet of things**. Mobile, embedded, and IoT devices increase the "attack surface" for distributed IT systems. They are ubiquitous and often managed by users who do not possess the technical sophistication or time to properly secure them. Because IoT devices rely on other Internet services, they represent a potential vector of attack into larger infrastructure.
- **Autonomy**. As computing platforms become more powerful and distributed, new applications for autonomy will be developed and deployed in situations where security and trust are highly relevant. Understanding the trustworthiness of autonomous cyber elements will become more important as the technology is inserted into high consequence cyber applications.

We have identified the following research thrusts that can lead to technical innovations that address the problem of assessing trust in modern distributed systems and software:

- **Tools and processes for rigorous cyber experimentation**. We consider the process of discerning trust in distributed systems as analogous to scientific inquiry. Hypotheses regarding the cybersecurity posture of a system are guided by theory (e.g. using static analysis and formal methods) and tested in a (predictive) cyber experimentation environment. Experimental results are then used to confirm or modify the hypothesis and/or theory. To be useful in establishing trust for potentially high-consequence IT systems, one must have

confidence in the predictive capability of the experimentation environment used to test cyber hypotheses. Therefore, techniques for quantifying trust/predictiveness in cyber experimentation environments are needed. These techniques include metrics and testing techniques for assessing experimental model validity, and uncertainty quantification techniques that propagate uncertainty in model inputs (e.g., topology, threat, users, and current conditions at the time of interest) to uncertainty in results.

- **Integrated, automated software and system analysis tools that effectively interface with human analysts who guide the tools**. Static analysis tools and formal methods can make more generalized claims about the security posture of the software under study, and they can guide experimentation toward "regions of interest" to test hypotheses and claims. However, given the increasing pace of software updates, techniques that require human interaction do not scale. New methods to integrate, automate, and scale software and system analysis tools are needed. Ideally, these tools would work closely with a human analyst who guides the analysis activity (e.g., by providing hypotheses) while the tools increasingly relieve the analyst from burdensome analysis tasks. Related to this research thrust is the problem of establishing trust in (potentially) autonomous systems for software analysis.

To pursue these research thrusts, a plan for transitioning this Strategic Plan into R&D is critically needed (much as "transition [R&D] to practice" was identified in the 2016 Strategic Plan as a critical dependency). Steps toward this goal include communicating this Strategic Plan to all Federal agencies that fund cyber security research, developing incentives that encourage funding agencies toward supporting more *strategic* cybersecurity needs, and promoting techniques for measuring and rewarding progress.

3. HUMAN FACTORS IN CYBER DEFENSE

In response to the in-progress update to the Federal cybersecurity research and development (R&D) strategic plan, experts in the field of Human Factors (HF) at Sandia National Laboratories identified research thrusts which should be considered as part of the 2016 Strategic Plan, to identify gaps in research areas considering a 10-year research plan. The intent was to identify fundamental, evidence-based research and transformative new approaches from a HF perspective. Specifically, the following relates to those areas that consider the human aspects and human dimension of cybersecurity R&D.

The 2016 Strategic Plan identified many areas of research that are critical for cybersecurity, including but not limited to (1) the anticipated evolution from current to future risk landscape in cyber domains, including detection of previously unidentified or new cyber threats; (2) facilitating teaming across entities involved in cybersecurity R&D efforts; (3) identifying different roles humans play in cybersecurity including defenders, users, developers, etc., and enabling improved (more effective) performance for each; (4) understanding, improving and enabling knowledge sharing, handoffs, and feedback loops across various cybersecurity roles; (5) addressing an asymmetric advantage enjoyed by adversaries employing exploitative techniques when compared to protection and defense; and (6) integrating human actors in automated systems from a systems of systems approach.

We have identified three categories of research on how the human is interacting with the cyber environment which should be considered in the latest revision of the Federal Cybersecurity Research and Development Strategic Plan. More specific research activities are provided.

1. Understanding decision making and analysis processes of cyber defenders

- Understand the decision-making needs of threat detection in both immediate-threat environments and for proactive threat detection (including decisions around scoping the problem space); when something is anomalous, what anomalies should cyber defenders look at (understanding what is going on as a way of assessing risk – enabling triage to escalate to further assessment). Research can include development of risk-based assessment approaches and application of naturalistic decision-making methods.
- Enable pattern detection and recognition of previously unknown/new types of threats for both "big data" environments and sparse data environments. Research should include human pattern recognition, automation, and human-autonomy teaming.
- Develop HF methods for understanding analysis environments, building on work domain analysis and other methods. As new analysis tools are developed, they need to be integrated into the existing work flow and analysis environment; a process that is a current hurdle. Better understanding of these environments can enable tool developers to create tools that are more readily and effectively adopted by analysts and will help analysts to understand which tools will be effective for different problems or mission questions.
- Study ways in which teams of people and teams of software and humans can work to get the best out of whatever software is available, even if not optimal, to enable cyber defenders to leverage a suite of tools more efficiently for threat detection. Research should include studies of case-based reasoning, naturalistic decision making, as well as human intuition.

2. Understanding cyber attackers

- Facilitate partnerships with other groups such as modeling of social interactions and economics modeling.
- Research on how cultural differences may impact cyber attacker behaviors or how we may thwart attacks.

3. Understanding how vulnerabilities are unintentionally introduced

- Assessment of the variables that influence the likelihood of vulnerabilities being introduced into code unintentionally, including the behaviors of code developers and their work environments. Implement techniques to reduce bugs in code in a proactive manner by understanding what conditions can lead to vulnerabilities/what cues relate to vulnerabilities and mitigating against those.

This page left blank

DISTRIBUTION

Email—External

Name	Company Email Address	Company Name
Tomas Vagoun	cybersecurity@nitrd.gov	NCO/NITRD

Email—Internal

Name	Org.	Sandia Email Address
Thomas D. Tarman	5824	tdtarma@sandia.gov
Technical Library	9536	libref@sandia.gov

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.