Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Cybersecurity is a large hairball problem. There are many different layers, characteristics, and variables that play into a cyber environment. Performing research to secure across all layers and variables at once is an intractable problem.

A solution is to divide the hairball problem into sub-problems or phenomena that can be constrained and investigated. The goal is to investigate the phenomenology and develop mechanistic models of how things work. This is often challenging because it's not obvious how to cleave the large problem into sub-problems that are useful to understanding the whole.

Science Council

Objective

There have been many attempts to articulate the fundamental steps of the scientific method. The difficulty lies in the differences between how science is described and how it is conducted. Science, as practiced, is often roiled with false starts, miscommunications, hidden assumptions, disciplinary dogmas, and occasional insights.

Developing a Research Plan

- Assert falsifiability
- Define ground truth
- Document assumptions
- Test the tools and assumptions
- Start with simple experiments
- Assess progress

Research Steps

From Crawford and Stucki (1990):

1. Define a question
2. Gather information and resources (observe)
3. Form an explanatory hypothesis
4. Test the hypothesis by performing an experiment and collecting data in a reproducible manner
5. Analyze the data
6. Interpret the data and draw conclusions that serve as a starting point for new hypothesis
7. Publish results
8. Retest (frequently done by other scientists)

Achievements

- Finalized two papers (*Science Council: Cybersecurity Publications Review* and *Science Council: Influencing Cybersecurity Research with Science Practices*)
- Applied research steps to two ARC projects, and helped the PIs to refine their research plans based on Science Council members' feedback
- Interpret the data and draw conclusions that serve as a starting point for new hypothesis

Impact

A fundamental assumption of the ARC Initiative is that significant improvements in sustaining functionality of cyber systems in the face of ongoing attacks requires thinking strategically about the problem and conducting research that is defensible, repeatable, and has enduring impact. The initiative has engaged scientists from other research domains to develop science practices that are relevant to cybersecurity research with the intent of enhancing the quality and impact of the initiative's research results.

For more information on the science you see here, please contact:

Mark Tardiff
Pacific Northwest National Laboratory
P.O. Box 999, MSIN: K8-15
Richland, WA 99352
(509) 375-2530
mark.tardiff@pnnl.gov