ASYMMETRIC RESILIENT CYBERSECURITY

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

ARC Science Council

CHALLENGE

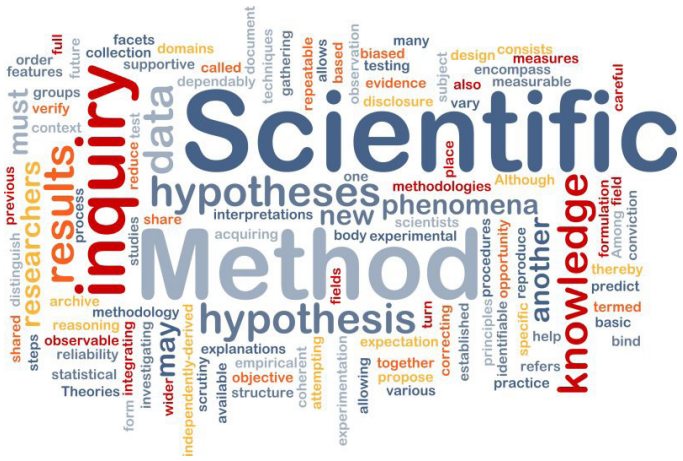
The history of responses to cyber attacks has been heavily skewed to tactical responses with a very strong emphasis on rapid recovery. All cyber systems, including government and corporate entities with top of the line security systems, are vulnerable to attacks. It has become an expected part of life that cyber incidents will occur. While threat mitigation is important and can be time critical, a knowledge gap exists with respect to developing the science of cybersecurity. The benefit to having such a science is the development and testing of strategies and theories that lead to understanding the broad sweep of cyber threats and the ability to assess trade-offs in sustaining network missions while mitigating attacks.

There is increasing attention to applying a formal scientific approach to cybersecurity. The JASONs published a report on applying the scientific method to cybersecurity, Cornell University has a science of cybersecurity blueprint, and the National Security Administration launched its 'Science of Security' Lablets program to engage universities. All of this is to say that there is substantial agreement that a more formal approach to cybersecurity is necessary and the conversation on how to do so is becoming pervasive.

CURRENT PRACTICE

Cybersecurity research emerged as a discipline in response to adversarial attacks interfering with or preventing normal cyber activities. As the cyber

Advancing the science of cybersecurity through well designed questions and repeatable experiments



environment has expanded and become more complex, so have the nature of adversaries and styles of attacks.

The current practice of cybersecurity has two main attributes. The first attribute is that a cyber system has a boundary that can be defended against attackers. This boundary may be associated with a single machine or with an enterprise network. The second attribute is that cyber defense is threat focused. Cyber defenses are currently heavily invested in making rapid tactical moves to thwart attacks irrespective of their origin or impact to

U.S. DEPARTMENT OF
ENERGY

the system being defended. This philosophy of cyber defense arose as the cyber environment rapidly evolved from a curiosity to a critical element in many aspects of the contemporary world including commerce, law enforcement, national defense, medicine, and the conduct of our personal and professional lives.

The current practice of cybersecurity is largely a trade craft with talented practitioners making tactical responses to threats in order to sustain their cyber systems. This approach lacks unifying objectives that can lead to strategies for cyber defense that focus primarily on sustaining the mission of the organization as opposed to sustaining the cyber resources.

APPROACH

The Science Council consists of seven active researchers in the fields of ecology, economics, statistics, physics, computational chemistry, microbiology and genetics, and geochemistry. The makeup of the council is intended to access the experiences across many empirical domains to inform a robust science approach for cybersecurity. The council also includes two members who are active cybersecurity researchers to keep the council grounded in the realities of the cyber domain.

The first key hypothesis for the Science Council is that science practices developed for other disciplines can be applied to research in cybersecurity in order to generate meaningful research outcomes that are the products of experiments that can be repeated by others. Fundamental to science is the idea that experimental results can be repeated and refuted or confirmed.

The second key hypothesis for the Science Council is that large complex problems are intractable because it's impossible to conduct controlled experiments directly on them. They can be addressed by identifying and investigating smaller sub-problems. The results from multiple sub-problem experiments can be integrated to gain insights and develop a generalized understanding and theories about the large problem.

The Science Council has identified seven practices that can be applied to cybersecurity research to improve the quality of experiments and generate outcomes that can be repeated. The practices are:

- Define a tractable problem
- Develop falsifiable research questions
- Identify ground truth
- Document assumptions
- Test tools and assumptions
- Start with simple experiments
- Assess progress towards the larger problem

IMPACT

Implementing science practices in cybersecurity research from other empirical domains will help to shift cybersecurity research from anecdotal accounts to defensible research results that can be repeated by others in the pursuit of developing the theory of cybersecurity. The impact on cyber enterprises will be strategic approaches to security investments that acknowledge the reality of continual attacks and the preservation of mission outcomes.

Contact

Mark Tardiff
Principal Investigator
(509) 375-2530
mark.tardiff@pnnl.gov

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*