Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

In Pursuit of Asymmetric Resilience

Applying Science Practices to Cybersecurity

NICK MULTARI

Pacific Northwest National Laboratory

PNNL-SA-107531

The Cyber Challenge

- Current understanding of cyberspace by practitioners is incomplete
- Defenders rely upon art, practice, and guessing to inform defensive decisions
- The research community lacks a foundational scientific understanding of the cyber domain and security
- Defender costs are grossly disproportional to the cost of an attack

The Science of Cyber Resilience Approach

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by **Battelle** *Since 1965*

- The ability to accomplish mission objectives in the presence of adversaries requires a foundational understanding of cyber systems to
  - Quantify the current state of the system relative to mission
  - Assess the costs and benefits of system changes
  - Choose strategic changes to maintain or enhance functionality

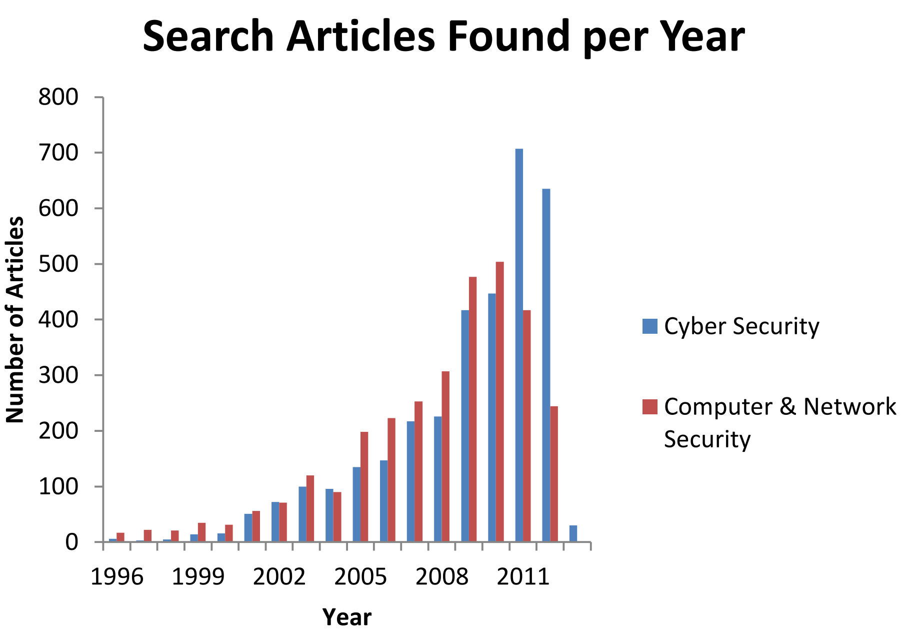
- We believe science-based approaches can transform cyber systems into resilient environments that move the asymmetric advantage to the defender

- We can apply science practices used in other research domains to advance the foundational understanding of cyber systems through
  - Well reasoned research plans
  - Reproducible experiments
  - Verifiable results

Initial Science of Cybersecurity Study

Want to understand why cyber security is not meeting much success?

- Extensive literature survey of the field
  - Search terms (cyber security/cybersecurity, network security, computer security)
  - 17 years (1996 – 2013)
  - Engineering Village Sources (ACM, IEEE, INSPEC)
- 5645 documents collected
- Sorted into 5 categories
  - Proof of concept, study, hypothetico-deductive, modeling and simulation, and theoretical

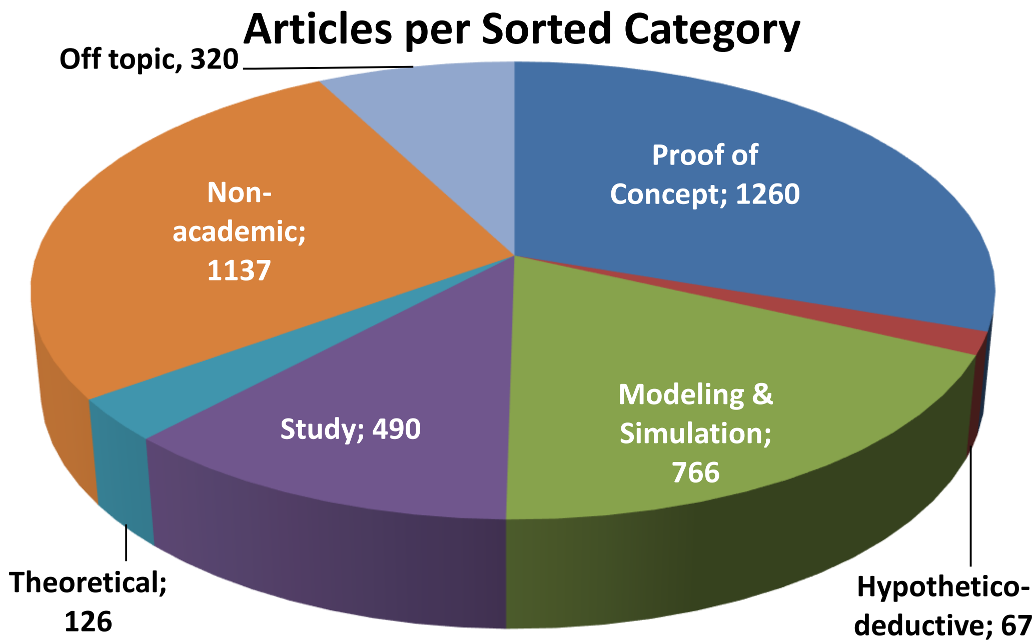


Study Results

- Literature survey findings
  - Small percentage empirically based research
  - Lots of engineering without guiding science principal
  - Poor scientific rigor, limiting conclusions and extensibility
  - Lack of agreed upon protocols

Question: How can we prevent projects from falling into same situation?

Approach: Formalize the scientific process with broad perspective



Science Council Formation

- Assemble a team of empirical scientists from multiple domains and include members that represent the operations and research aspects of cybersecurity to assure relevance to the cyber domain
- Approach
  - Develop a cybersecurity relevant methodology
  - Apply the methodology, iterate, and improve
  - Strategize participation in conferences presentations/publications on applying science practices to cybersecurity

Science Council Membership Domains

- Microbiology and genetics
- Geochemistry and subsurface ecology
- Computational chemistry
- Ecology and systems science
- Physics and x-ray spectroscopy
- Statistics and social behavioral modeling
- Cybersecurity research
- Cybersecurity services manager

Over 175 years of combined experience

Scientific Method

- Define a question
- Gather information and resources (observe)
- Form an explanatory hypothesis
- Test the hypothesis by performing an experiment and collecting data in a reproducible manner
- Analyze the data
- Interpret the data and draw conclusions that serve as a starting point for new hypotheses
- Publish results
- Retest (frequently done by others)

Operation: some action done to the system being investigated

Observation: what happens when the operation is done to the system

Model: a fact, hypothesis, theory, or the phenomenon itself at a certain moment

Utility function: a measure of the usefulness of the model to explain, predict, and control the cost of using of it

Research Context Along the Science Continuum

Early	Mid-point	Mature
Problem is poorly understood and in observational stage	Developing general models using specific examples to be tested	Models validated for operational use

Explore: Describe the Phenomenon	Make Predictions: Challenge the Conceptual Model	Implement: Signatures Monitoring
Develop a Conceptual Model	Falsifiable Questions Conduct Experiments	Support Assessments Decisions

Our Implementation of the Scientific Process

- Seven Practices
  - Define a tractable problem
  - Ensure falsifiability
  - Obtain ground truth
  - Document assumptions
  - Test assumptions and methods
  - Start with simple experiments
  - Assess progress to the larger problem

Define a Tractable Problem

- Challenge
  - Cybersecurity is a large complex problem
  - Research across all layers and variables at once is an intractable problem

- Simplify the problem
  - Extract a sub-problem that can be constrained and investigated
  - Iterate to refine the problem definition
  - Explicate coherence between the research problem and the larger complex problem

Initial Project Problem Statement

Initial problem: Develop an operational metric tool to identify more resilient and secure architectures (CIA)

Revised problem: Verify a metric can be developed that correlates with improved availability

Ensure Falsifiability

- A useful hypothesis is one that can be proven wrong
- Logical underpinning is that it's impossible to prove a hypothesis is always true
- Requires moving from inductive to deductive reasoning
  - Inductive: individual observations leading to a general conclusion
    - We see 1000 white swans, but have no basis to claim all swans are white – there are always more swans we haven't seen
  - Deductive: State a general model and challenge it with specific observations
    - State a hypothesis that all swans are white
    - Collect data and If one swan is not white, we reject the hypothesis

Initial Project

Initial hypothesis: Operations will be more resilient with our tool than without

Revised hypothesis: An availability metric corresponds with resiliency measures in a simulated environment

Obtain Ground Truth

- Observations where the state for particular variables is known with certainty
- Can be challenging to generate but without it, experimental results are only anecdotal
- Network resilience: Instances of networks that have no attacks (benign) and networks with known attacks (compromised) to determine whether we can sense a change in resilience

Initial Project Ground Truth Methodology

1. Developed four network configurations
2. Each run in normal and stressed simulation environments using known traffic
3. Ranked the configurations in order of resiliency according to simulation results

Document Assumptions

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

- It's very unlikely that experiments can be conducted without assumptions
- Example assumptions
  - How the experimental environment is defined
  - variables and parameters of interest
  - measurement methods
  - data analysis methods

Initial Project Assumptions

1. CORE simulation environment reflects reality
2. Can realistically simulate network traffic
3. DOS attacks provide sufficient stress to disprove hypothesis
4. Same results are achieved whether using uniform or informed attack probabilities

Test Assumptions and Methods

- Assumptions are often sacred cows
  - Be alert to evidence that an assumption is incorrect
  - Conduct a simple proof of principle to validate all important assumptions
- Investigation requires ways to sense the experimental environment: instruments, measurements and/or algorithms
- Calibrate - Critical first step is to test tools against simple problems with known outcomes to confirm they work as expected

Initial Project Testing of Assumptions

1. Validated realism of configurations with operational security and networking personnel
2. Validating assumptions on traffic and simulation environments

Start with Simple Experiments

- Rationale: If we can't perform well on a simplified problem its very unlikely that performance will improve with complexity
- Process: Add complexity as results indicate
  - confidence that the experimental design represents the phenomena of interest
  - outcomes are useful to the research question
- Maintain healthy skepticism
  - Is there a flaw in our thinking, experimental design, or execution that leads to desirable results for unexpected or wrong reasons?

Initial Project Experiment

Run a DOS attack on each network configuration and validate the ranking metric correctly identifies the most and least resilient configuration (availability)

Assess Progress Towards the Larger Problem

- Periodically evaluate progress
  - If components of the problem are well characterized, they should respond to perturbations in predictable ways
  - As models mature, their predictions should align with experimental results – if not, update the model instead of rejecting the data
  - Modified models should still predict prior experimental results

- Do results and models of the sub-problem provide insights to the hairball problem?

Implementation in the ARC Initiative

- Proposals to the Initiative are required to have well defined research problems, as opposed to grand statements of intent
- Proposals and research plans indicate the maturity of previous research and whether the proposed work is exploratory or hypothesis driven
- Each funded project works with the Science Council to:
  - Refine their research questions
  - Develop testable hypotheses
  - Document and challenge assumptions
  - Generate an experimental plan – approved by the Science Council
- Projects plans are designed with initial experiments and conduct initial proofs of concept, where feasible, leading to a decisions point to continue or abort

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Nick Multari, PhD
Initiative Lead

nick.multari@pnnl.gov
1-509-375-2043

Asymmetric Resilient
Cybersecurity Initiative

cybersecurity.pnnl.gov