Report on the Workshop on GENI and Security

or, What Happens When the GENI Leaves the Bottle?

Matt Bishop
Department of Computer Science
University of California at Davis
Davis, CA 95616-8562
bishop@cs.ucdavis.edu

Workshop Particulars

- Held on January 22–23, 2009 at UC Davis
  - 56 attendees
- Sponsors
  - National Science Foundation
  - GENI Project Office
- Co-chairs
  - Matt Bishop, UC Davis
  - Chip Elliott, GENI Project Office

Importance of Thinking Sideways

From the March 15, 2001 Blue Springs, Missouri, *Examiner*:

PICK 3

ST. LOUIS—The winning numbers drawn Tuesday night in the daily Missouri Lottery Pick 3 game were 9-9-9.

A winning $1 ticket with the numbers in the correct order paid $500; a winning $1 ticket with the numbers in any order paid $160.

Steve Wolfe

Goals

- To engage the security community in GENI's design and prototyping, to ensure that security issues are properly considered
- Specific questions:
  - What classes of experiments should GENI support? What capabilities will GENI require to do this?
  - How can GENI itself be secured and protected from attack? How can networks and CPS mechanisms connected to GENI be protected from attacks originating on GENI, or from malfunctioning GENI experiments?

The Shortest Version

- *GENI must foster a culture of scientific experimentation from the very beginning*

The Shorter Version

1. GENI must provide capabilities to enable a science of security that involves the experimental validation of security-related hypotheses that could not be validated in current testbed settings.
2. The construction of formal security experiments with hypotheses, controls, and well-articulated measurements will require substantial care and review to assure reproducibility and scientific and statistical validity.

The Shorter Version

3. GENI must provide the capabilities to enable experimenters to capture *all* the data needed to enable others to reproduce the experiment.
4. The deployment of GENI will require the development of mechanisms to reconcile conflicting requirements, constraints, and customs in different parts of the network.

The Shorter Version

5. The operation of GENI will require careful planning to enable communication among the federated organizations to handle (security and other) problems. The GENI infrastructure should support security testing, to ensure that security breaches can be handled quickly and effectively.

The Short Version

- See the Executive Summary
- Highlights follow

Resource Management

- Who has the right to use resources?
  - Identification, credentialing, delegation
- Implies cross-federation agreements, mechanisms
  - This includes accountability
- How are slices managed?
  - In particular, how do you prevent an experiment in one slice from interfering with experiments in other slices?

Recording Events

- Speaks to *reproducibility* for validation
- Record events at various layers of abstraction
  - *tcpdump*, etc. not enough as new protocols may not use IP
  - Privacy issues abound
- Requires *replication* of environment
  - Also need to be able to restore this to replicate experiment
- Anyone must be able to do this, not just experimenter

Privacy

- Definition of this varies among jurisdictions (countries, states) and organizations
  - Impacts what can be recorded
- Gathering data for experiments
  - Record data elsewhere, anonymize it, develop framework for seeding it with attacks
  - Encourage ordinary users to use GENI
- Key question:
  - Under what conditions can we decide whether an experiment is doing something that violates the rules of usage without compromising the privacy of the experiment?

Architecture and Infrastructure

- Human and policy aspects *critical* here!
- What is security?
  - Automated mechanisms problematic
- What security support services must federated networks provide?
  - Not understood because of boundaries
- How will disputes be arbitrated?

Architecture and Infrastructure

- Infrastructure should supply timely answers, take action promptly
  - Requires someone be available at all time
- How *exactly* does the federation work?
  - Who decides who is allowed to use the federation's resources, and establishes priority?
  - Centralized vs. distributed mechanisms

Stakeholders

- These set requirements for security services
  - Those who provide the resources
  - Those who provide the data
  - Those who will use the resources
  - Others?
- Use a clearinghouse to track who has what resources, and under what conditions other may use them

User Requirements

- Who owns the experiments?
  - Think "Intellectual Property" here ...
- Ease of use
  - Volunteers cannot have to spend lots of time, effort, resources to do their tasks
  - If management difficult, configuration and other errors may disrupt experiments or compromise results
    - Principle of psychological acceptability

Experiments

- Must provide capabilities to enable science of security
  - Experimental validation of security-related hypotheses that cannot be validated in current testbed settings
  - Can also be used as a teaching tool for how to carry out scientific experimentation in computer science, especially computer security

Experiments

- GENI should provide set of detailed examples of experiments
  - Culture of sharing is critical
- Methodology must address features in GENI
  - Validation of experiments
  - Validation of data used in experiments
  - How GENI itself affects experimental results due to its unique features

Experiments

- Example experiments on GENI
  - Validation of models of DDoS attacks and defenses on large scale
  - Development of new models, architectures to inhibit botnets
- Other types
  - Evaluate security of solutions deployed on large-scale distributed network
  - Test high cost but low probability events
  - Run exercises like CyberStorm to prepare plans, procedures for large scale attacks

GENI Itself

- Cannot prevent attacks on GENI
  - So, how do we minimize their effects?
- Legal liability
  - This is trans-border, remember
- Possible approach: use penetration teams to compromise GENI
  - This tests ability of GENI administrators, federated network administrators, to respond and recover
- Have social scientists study GENI, work on it?

Conclusion

- Security is a key part of GENI
  - As a topic for experiments
  - As a topic for protecting other experiments
- GENI has unique features making security considerations unique (for now)
  - Scale
  - Interconnection with outside world
  - Policy and procedural issues

For More Information ...

- Go to the workshop web site:

  http://seclab.cs.ucdavis.edu/meetings/genisec

Final Thought: The Tension

You can observe a lot just by watching.
—Yogi Berra

A little knowledge is a dangerous thing.
—*Old proverb*