CALL FOR PARTICIPATION

Workshop on GENI and Security

Date: January 22–23, 2009
Location: Davis, California, USA

The Global Environment for Network Innovations (GENI) is a suite of network research infrastructures now in its design and prototyping phase. It is sponsored by the National Science Foundation to support experimental research in network science and engineering.

The goal of this workshop is to engage the security community in GENI's design and prototyping, to ensure that security issues are properly considered during its development.

First, what classes of security experiments should GENI support? What capabilities will GENI require to allow the conduct of these experiments? The capabilities may be intrinsic to GENI (such as equipment or software of a particular kind) or extrinsic (such as organizational management, or external interfaces and connectivity). Experiments involving malware or vulnerabilities analysis may require that parts of the infrastructure suite be partitioned from other parts. Deploying and testing new protocols may require that the suite be partitioned to prevent errors in the implementation or in the protocol itself from interfering with other uses of the infrastructure.

Second, how can GENI itself be adequately secured and protected from attack? What forms of authentication, authorization, and accountability would be most appropriate? As access to GENI will be from the Internet, GENI will be exposed to potential attackers. Other types of attack may involve physical compromise of the systems making up GENI, or of the Internet (or other) infrastructure that provides support for GENI. Protocols, management and organizational procedures and processes, and access control mechanisms must be developed to safeguard both the GENI resource and the data and software that researchers deploy on it.

As the GENI Project Office expects to issue its 2nd solicitation for GENI analysis and prototyping subcontracts in the middle of December, with proposals due in mid-February, it is anticipated that topics discussed at the workshop will lead to proposals from the security community.

Participation. We invite short (1 paragraph preferably; at most 1 page) statements of ideas addressing these two issues. For example, what security-related experiments would you like to run on GENI, and what benefit would you expect from them? What constraints or requirements would you need to carry out the experiments? How can we shield other experiments and work being done using GENI from the effects of your (or others') experiments? How can we prevent GENI from being attacked? The workshop is designed to discuss these, and other, questions.

The GENI System Overview (http://www.geni.net/docs/GENISysOvrvw092908.pdf) provides an overview of the GENI system design. The GENI Spiral 1 Overview (http://www.geni.net/docs/GENIS1Ovrvw092908.pdf) discusses the first phase of GENI prototyping. More information on GENI is available at the GENI web site (http://www.geni.net).

Submission Information. Submit your statement to geni-workshop@cs.ucdavis.edu by December 18. Please use either PDF or text. The steering committee will evaluate the responses, and notify senders of the results, by December 22.

Travel. Limited travel support is available, so please indicate in your submission whether you require assistance. This will not be a factor in selecting participants.

Web Site. For up-to-date information about the workshop, please visit the workshop web site at http://seclab.cs.ucdavis.edu/meetings/genisec.

Steering Committee.

Matt Bishop, *co-chair*, UC Davis
Chip Elliott, *co-chair*, BBN
Heidi Picher Dempsey, BBN
Deborah Frincke, PNNL
Suzanne Iacono, NSF
Karl Levitt, NSF
John Mitchell, Stanford
Vern Paxon, UC Berkeley
Taieb Znati, NSF
Others to be added