



GEC9 Demo : The Hive Mind: Applying a Distributed Security Sensor Network to GENI

Participants: Matt Bishop, Sean Peisert (PI), Steven Templeton, *UC Davis*
 Glenn Fink, Deborah Frincke (CoPI), *Battelle*
 Carrie Gates (CoPI), *CA Labs*
 Michael Crouse, Errin Fulp, *Wake Forest University*

URL: <http://hivemind.cs.ucdavis.edu>

Abstract

This project seeks to define and prototype a security layer underlying GENI that will allow providers of the system to collaboratively defend against attacks and misuse of GENI resources.

Specifically, it seeks to investigate the reporting requirements that GENI will need to provide to support certain forms of networking and security experiments. To do this, they will use decentralized security algorithms (in the form of agents, sentinels, and supervisors) that communicate between sensors, in some sense simulating the function of an ant hive. The result of this will enable GENI to support experiments where there is communication between internal nodes (sensors or routers).

In the context of networking, such experiments might be used to test if bandwidth usage can be improved through the communication of capacity and usage information between routers.

In the context of security, such experiments might be used to test the tradeoffs among different approaches to exchanging security information between sensors, and where that information might affect firewall rules or pro-active, forensic logging efforts.

