Summer 2011 Quarterly

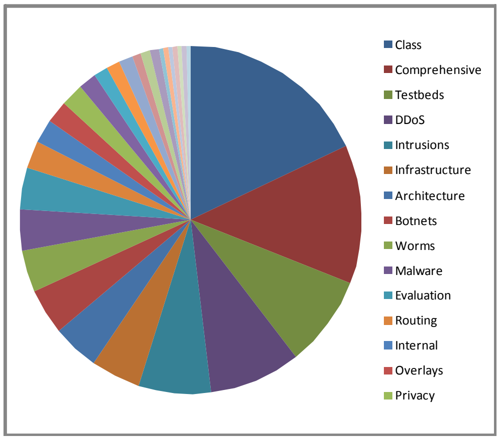
dē•ter

Elevating the Science of Cybersecurity

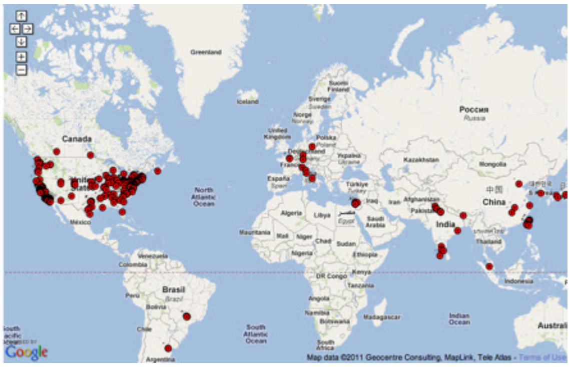
DETER at a Glance

DETER is an open community-based facility available to academic, industrial, and government organizations for research, testing, and computer security evaluation.

Types of DETER Projects



Where is DETER Used?



Useful Links

DETER Project Web Page:
http://www.isi.edu/deter
DETER Testbed Web Page:
http://www.deterlab.net
User Support:
testbed-ops@isi.deterlab.net

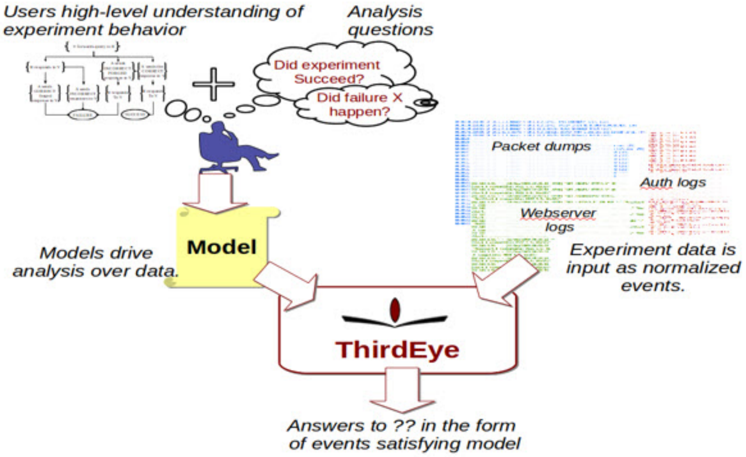
ThirdEye for Semantic Analysis of Experiment Data

Arun Viswanathan(aviswana@isi.edu), Alefiya Hussain(hussain@isi.edu)

As a network or cyber security experimenter, have you ever wished for an ability to analyze your experiment with high-level questions such as “did my experiment run as expected?” or “did X occur in my experiment?” Have you ever felt the tedium of manual analysis or writing problem-specific tools for every situation and wished for a better approach? Read on as ThirdEye might just be the right tool for you. [1]

ThirdEye enables analysis, reasoning, and discovery over experiment data at a semantic level. ThirdEye achieves this by providing a simple modeling language for experimenters to describe the experiment or analysis inquiry as an abstract behavior model. Experimenters can use existing models or build models to formulate analysis questions as semantically-relevant assertions over data. Given such a model and the experiment data, ThirdEye provides algorithms to present the relevant events in the experiment. To get started with ThirdEye, please visit http://thirdeye.deterlab.net and download the latest release.

[1] A. Viswanathan, A. Hussain, J. Mirkovic, S. Schwab, and J. Wroclawski. A Semantic Framework for Data Analysis in Networked Systems. In Proceedings of the 8th USENIX Symposium on the Networked Systems Design and Impelentation (NSDI), April 2011.


Users high-level understanding of experiment behavior
Analysis questions
Did experiment Succeed?
Did failure X happen?
Packet dumps
Auth logs
Webserver logs
Model
Models drive analysis over data.
Experiment data is input as normalized events.
ThirdEye
Answers to ?? in the form of events satisfying model

Profile of a DETER User: Esteban Mocskos

Researcher at the University of Buenos Aires, Argentina

1. What are you using the testbed for?
**We use the DETER testbed to run a modified locality-aware BitTorrent client in order to analyze traffic patterns and optimize resource usage. Eventually, we want to analyze if using this local gathered information can be used for a client to take advantage of the system.

2. What kinds of experiments are you running?
**We are currently running three experiments: 1) a small, controlled environment with 12 nodes, 2) a medium-size network composed of 33 nodes, and 3) a big network with 64 nodes. Running time is long (5-6 days), as it runs series of batch experiments with different fine-tuning parameters. Each run is about 1 hour in length.

3. What kinds of resources are you using? **We are currently using PC nodes only.

4. Any positive remarks about the testbed? Is there anything we need to improve for users such as you?
**Some issues we noticed and reported: Occasional traffic loss in long runs and link-test failures.

5. Any interesting results or items that could be newsworthy?
**Not yet. These simulations consist of the core experiments in a Licentiate Thesis (a six-year career final work). We are working hard to analyze the obtained results. The Deter facility was absolute necessary for carry on this work, we are really thankful with this initiative.

The Hive Mind Project -- Digital Ants for Intrusion Detection

By Sean Peisert of UC Davis

This article describes the Hive Mind project—performed by researchers at the University of California, Davis—that explores an innovative method of intrusion detection based on mobile agents and swarm intelligence. The project's goal is to provide a lightweight, decentralized, intrusion detection method that is adaptable to changing threats while communicating suspicious activity across hierarchical layers to humans who can respond when needed.

The Hive Mind approach to intrusion detection provides event correlation over an infrastructure comprised of one or more administrative *enclaves*, each made of a collection of device-level nodes. These represent the devices in the network being monitored. Swarming sensor agents modeled after biological elements such as ants, wasps, termites, crows, and/or immune systemsroam from node to node, searching for security relevant activity, leaving markers to communicate with other wandering agents.

The Hive Mind interposes logic-based rational agents between humans and the swarm, providing a basis for communication, interaction, and shared initiative. The goal is to augment, not replace, more traditional security mechanisms. For example, the Hive Mind should be effective where computing power is highly limited, e.g.,where host-based IDSs would be impossible or in highly distributed systems without well-defined monitoring points, making network-based detection infeasible. The Hive Mind could then be used in parallel with traditional firewall and intrusion detection systems.

Antness

The Hive Mind approach can be thought of as a directed online search algorithm. It has similarities to swarm intelligence models, such as Ant Colony Optimization (ACO) and Particle Swarm Optimization (PSO), but it contains important differences. Rather than be about path minimization, it is about resource direction.

This research will explore the elements of biology that are useful to security monitoring. For example, how "ant-like" should sensors be? When does "antness" over-complicate or interfere with goals, such as accuracy, ease of use, and performance? Also, how might influence from other insects such as wasps or termites enhance or detract from this approach?

Testing the Hive Mind

The Hive Mind project plans to test and explore this new concept in several network testbed environments, including ProtoGENI and DETERlab. ProtoGENI, part of the GENI project, federates resources from multiple Planetlab and Emulab-based testbeds such as DETERlab. DETERlab needs no introduction here. GENI (Global Environment for Network Innovations) is an NSF-funded, BBN-operated testbed designed to support experimental research in network science and engineering.

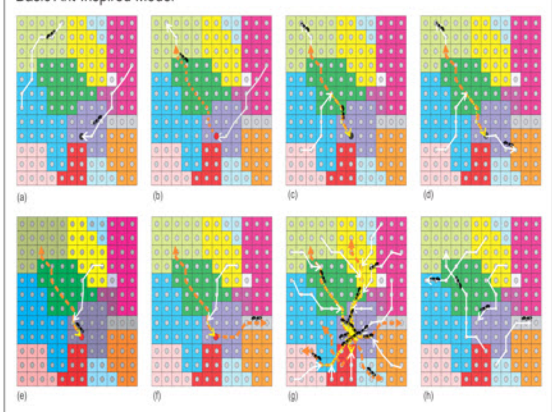
The Hive Mind is designed to meet a key challenge for GENI security: disparate administrative domains that may encompass numerous, potentially conflicting security policies. Another challenge is that networking experiments run on GENI, and security mechanisms need to have limited and predictable impact on those experiments. A final challenge of GENI is security of low-power devices, specialized components, and/or possibly even non-compute devices.

Thus, the evaluation of the Hive Mind on DETERlab and ProtoGENI seeks to determine (a) the set of security policies that the mechanism can enforce, (b) its ability to detect attacks, and (c) its resource usage, and compare with more traditional IDS systems.

Researchers at UC Davis have developed a functional Python prototype of the Hive Mind. They have also successfully mapped the concept to the ProtoGENI and DETERlab testbeds. Their current focus is on using the DETERlab testbed to evaluate competing algorithms and study how effectiveness and resource use are affected by parameter changes and scale. They are also using ISI's "Benito" containerized virtualization system to create large tests with thousands of nodes to study behavior of the HiveMind system. In some ways the tests are races between competing designs in which the ones with the most detections using the fewest resources wins.

Another task is to study the system's ability to detect different types of attacks. These include simple attacks targeting a single host, complex attacks targeting many hosts, and attacks where nodes are used to launch a DDoS attack. The Hive Mind team will be initiating these test attacks on their DETERlab experiments and monitoring the outcome.

Basic Ant-Inspired Model



The above grids represent the collection of monitored nodes, the different colors represent different Enclaves.

(a) Patrolling mobile sensor agents, aka "Ants", move between nodes spanning multiple GENI Aggregators, evaluating their specific sensor functions looking for "interesting" activity at each node (white). (b) An Ant discovers activity matching its sensor function's target. The Ant moves away leaving a trail of "virtual pheromone" markers at nodes it transits (orange). The trail leads back to the node where the discovered activity occurred. After a while the Ant stops marking nodes and returns to patrolling. (c) Another patrolling Ant intersects a node with a marker and follows the trail to the originally discovered node (yellow). (d) No activity matches this Ant's sensor function. The Ant returns to patrolling. (e) Another Ant intersects the trail and follows the markers to the discovered node. (f) Activity on the node matches this Ant's sensor function. The Ant moves off leaving its own trail. (g) As this behavior is repeated, more trails direct more Ants to the target. If Ants continue to find interesting activity, this escalates into a swarm of ants converging on the nodes in the target's vicinity. If the problem has spread to nearby nodes, this will also increase the swarm. When the information gathered from the combined sensor functions, is sufficient to indicate reportable activity, alerts are sent to a supervising process where response may be initiated. (h) After time the marker trail dissipates and the Ants return to patrolling.

Acknowledgements

This material is based on was supported in part by the National Science Foundation and the GENI Project Office under grant CNS-0940805. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of any sponsors. More information about the Hive Mind project can be obtained at the project web site: http://hivemind.cs.ucdavis.edu/