Galaxy: A Network Emulation Framework for Cybersecurity

NATURAL COMPUTATION LABORATORY, DEPARTMENT OF COMPUTER SCIENCE, MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY / LOS ALAMOS NATIONAL LABORATORY CYBER SECURITY SCIENCES INSTITUTE

Kevin Schoonover, Eric Michalak, Sean Harris, Adam Gausmann, Hannah Reinbolt, Joshua Herman, Daniel R. Tauritz, Chris Rawlings, Aaron Scott Pope
Outline

• Motivations
• Design
• Application
• Challenges and Lessons Learned
• Future Work
Who are we

Kevin Schoonover  Eric Michalak
• Undergraduate CS student  • Research Scientist at Los Alamos
• Researcher at Missouri S&T  • Missouri S&T CS Alumni

Our Team
• CEADS-LIN Project
• Missouri S&T’s export-controlled Natural Computation Laboratory
• Los Alamos Advanced Research in Cyber Systems
• Funding: Cyber Security Sciences Institute (Los Alamos and S&T)
What is Galaxy?

- Network emulation framework
  - Stateless evaluations with low overhead
  - Network fidelity
  - Result storage and collection
- Specialized for agent-based experiments
- Unique from current solutions
  - Rapidly runs successive, stateless evaluations
  - Built-in results reporting
  - Modular components
Design
Design - Layers

- Two logical layers
- **Host Layer** – Evaluation orchestration and persistent storage
- **Virtual Layer** – Facilitating and running evaluations
Design - Infrastructure

- **Libvirt** – Virtualization API utilizing KVM as hypervisor
- **Virtual Machines** – High fidelity emulation of physical hosts
- **Virtual Bridges** – Layer 2 “switches” that network virtual machines together
- **Control Bridge** – Point-to-point command network connected to each virtual machine
Mothership

- Primary data storage/retrieval for researchers and agents
- Provides access to persistent evaluation metadata through REST API
  - /queue/
  - /evaluations/
  - /results/
  - /nodes/
UFO

- Manages evaluations
- Sends commands to agents
  - **START** – Begin an evaluation and perform your actions
  - **UPDATE** – If an agent has an update action, send the update to Mothership.
  - **END** – End the evaluation and gracefully shutdown
Drone

- Metric / data collection agent
- Performs ping tests to ensure network consistency
  - Alerts researcher of infrastructure problems
  - Researcher can then determine to restart or fail an experiment
Node Configuration

- **<<node name>>**
  - overlay
  - **<<node name>>.conf**
  - network.yaml
Scaling Galaxy
Experiment Procedure

1. Query Mothership for list of nodes on the topology
2. Revert each VM to initial snapshot, starting VM
3. Send the START command
4. Send the UPDATE command every five seconds
5. Send the STOP command after 60 seconds
Application: CEADS-LIN

- CoEvolution of Attacker and Defender Strategies for Large Infrastructure Networks
- Represents Attackers and Defenders as evolutionary agents operating within an emulated network
- Utilizes Galaxy for creating the network, running evaluations, and reporting results
CEADS
Network Layout

Domains Contain:
- A Firewall
- A DHCP Server
- End Nodes
Evolutionary Algorithms
Results

Example Enumeration Strategy

- Primary Search: $A.B\pm 8.C\pm 1.D$
- Secondary Search: $A.B.C.[0-255]$
- Root Node: own IP address
Results

- Moderate success – 75% of network discovered
Challenges and Lessons Learned

- Overhead time
- Dynamically building networks
- Complex attack strategies
- Simulation vs Emulation
Future Work

• Containerization
• Web application to interact with components
• Additional infrastructure support: AWS, Baremetal, etc