The Center for Cyber Defenders

Expanding Computer Security Knowledge

SAND2015-6109C

FIRESTORM - Firewheel Instrumenting Realistic Environments while Starting Topologies on Running Minimega

Nicholas Hilbert, Missouri University of Science and Technology

Project Mentor: Kasimir Gabert/5638; Steven Elliott/5634

Problem Statement:

Over the past 10 years, Sandia has been researching and developing a platform for emulating and analyzing large complex information systems. From this research, two different tools have emerged: Firewheel and Minimega. On a cursory level, these tools seem similar; however, they both excel at resolving different emulation challenges.

- Combining these tools is the next step forward for Sandia's Emulytics™ (emulation + analytics) program and my summer goal.

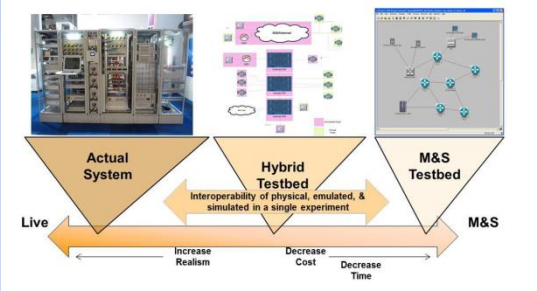

Figure 1. Emulytics™ platform

Objective and Approach:

Unlike Firewheel, Minimega does not have an automated experiment configuration.

- Utilize the topology created by Firewheel to construct a virtual network within Minimega.
- This should be done through a process that can convert Firewheel's graph into a series of commands Minimega can interpret and execute.

Results:

- Minimega and Firewheel commands can be used to control the setup and execution of the virtual machines.

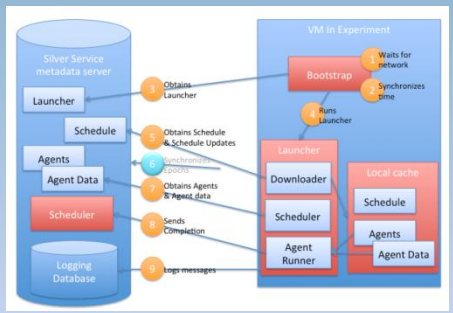

Figure 2. Firewheel Agent System

Impact and Benefits:

- Now, Firewheel's scalability along with its automated topology and experiment generation are combined with Minimega's graphical user interface (GUI) and easy-to-use controls.
- Customers previously familiar with only one of these tools can now expand their capabilities with minimal educational overhead.

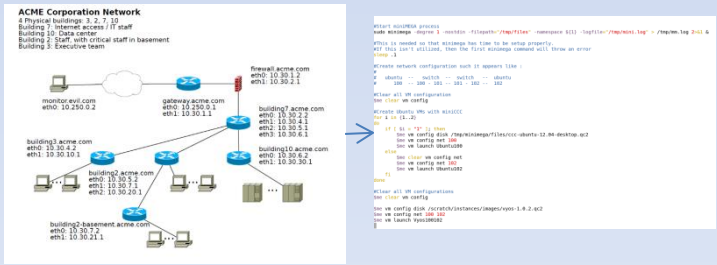

Figure 3. Firewheel topology to Minimega Script

Sandia National Laboratories operated by Lockheed Martin

Sandia National Laboratories is a multi-program laboratory operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin company, for the U.S. Department of Energy's National Nuclear Security Administration under con-

NNSA