SAND2008-5245C

BGP Analysis using System-in-the-Loop (SITL) Testbed

Brian Van Leeuwen
Uzoma Onunkwo
Michael McDonald

Sandia National Laboratories
Albuquerque, NM 87185

August 2008

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company,
for the United States Department of Energy's National Nuclear Security Administration
under contract DE-AC04-94AL85000.

GOALS…

The goal of our project is to develop new theories and tools for analyzing network security.

To this end, we are developing a hybrid network testbed capability for Simulated, Emulated, and Real Investigative Analysis (SEPIA).

…AND SIGNIFICANCE

SEPIA tools will allow analysts to ***rapidly*** and ***cost-effectively*** analyze complex network security issues.

Motivation

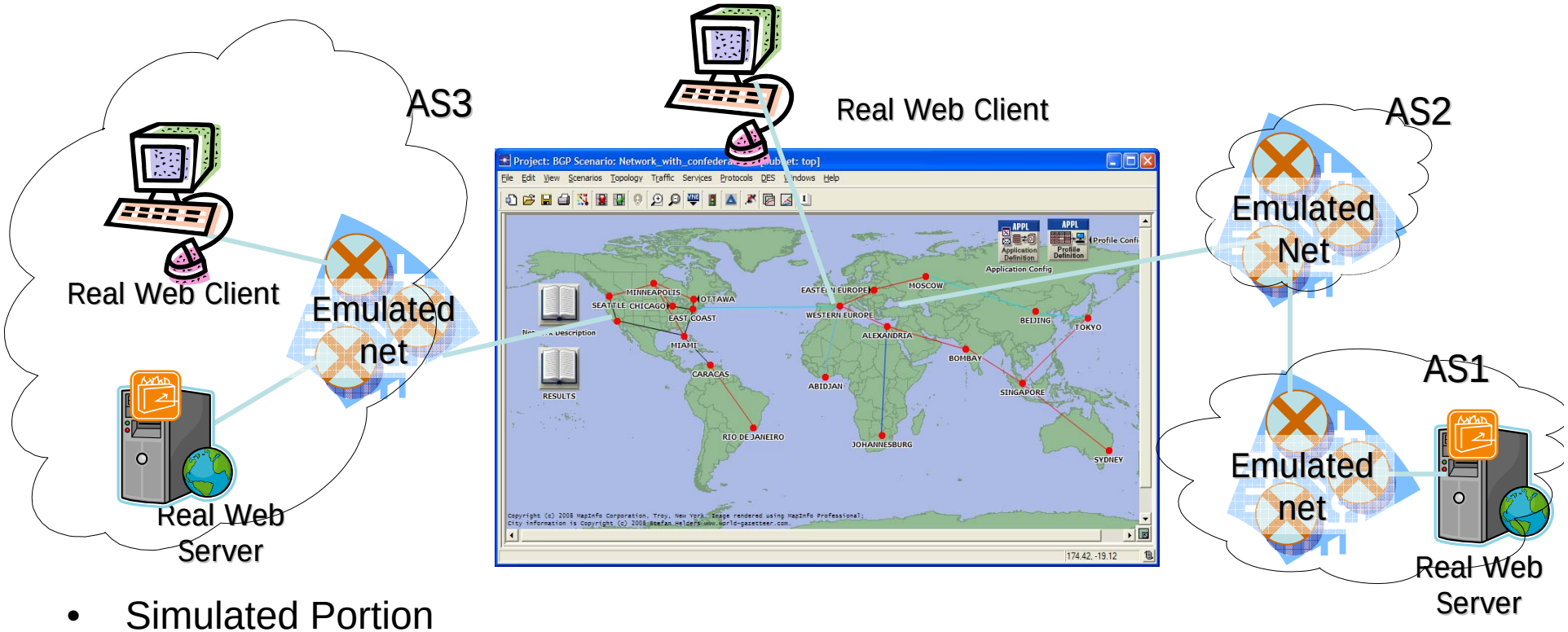
- Computer security and information assurance analysis
- Many important network security issues difficult to analyze at any specific scale
  - Dangerous to experiment on operational networks
  - Full-scale testbeds expensive to build and operate
  - Simulation alone does not provide sufficient fidelity for analyzing key network security issues
  - Models of key network elements often not available
  - Simulation models hard to develop and validate
- Reducing analytic costs allows us to address an increasing percentage of the critical security problems

A Hypothetical Problem

- **Imagine**
  - Your job is to understand exactly how a particular BGP router configuration elsewhere could hijack your network.
- **You could**
  - Run the code on your network to see what happens
  - Build testbed networks of routers and computers to run the codes
  - Use emulation to save money on the testbed
  - Use network simulation models alone to test various theories about the software
- **Problem is**
  - In-situ testing is forbidden
  - Physical testbeds are very expensive to build and operate
  - It's hard to analytically model most cyber threats correctly

We suggest using hybrid SEPIA testbeds to provide the needed middle ground

Conceptual SEPIA Experiment for Analyzing the BGP Router Hijack Issue

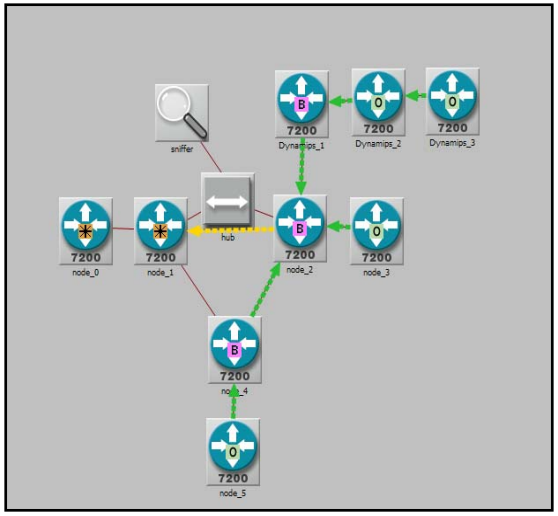


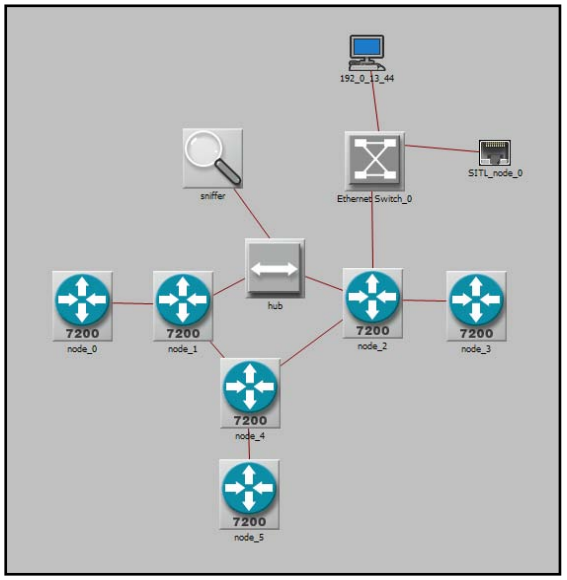
- Simulated Portion
  - Large BGP network in OPNET
- Emulated Portion
  - AS1 represents the hijacker network
  - AS2 is AS1's service provider
  - AS3 represents your network

- Physical (real)
  - Web server representing your site
  - Web server at hijacker's site
  - Web browsers throughout the network

Making The Experiment Work

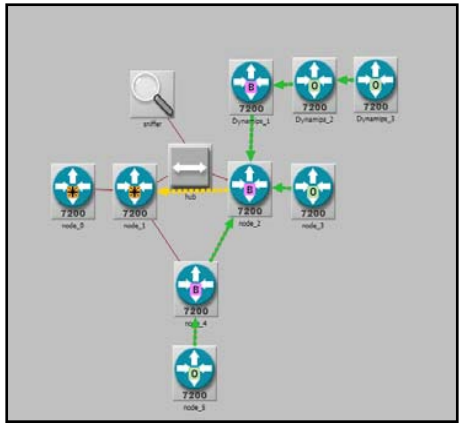
- OPNET's SITL provides the needed simulation-to-real and real-to-simulation interface.
- Unfortunately, out of the box SITL has very limited TCP support through proprietary and closed libraries
- In addition, out of the box SITL lacks specific protocol translator functions
  - This means that the standard OPNET router models don't interact with real routers and share BGP information
- A key element in making this experiment work is to develop the needed BGP and TCP translation functions.
- Here, we developed new
  - TCP packet translation functions
  - BGP packet translation functions



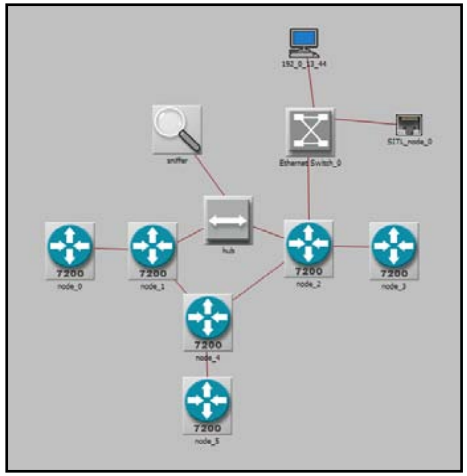


Process for Developing the Custom Interface

- Develop side-by-side Models for comparative analysis
  - Simulation-only model
  - Emulated Model
- Use protocol sniffing to understand network traffic
  - Wireshark
  - Custom probe node
- Gradually link the networks together through a SITL model



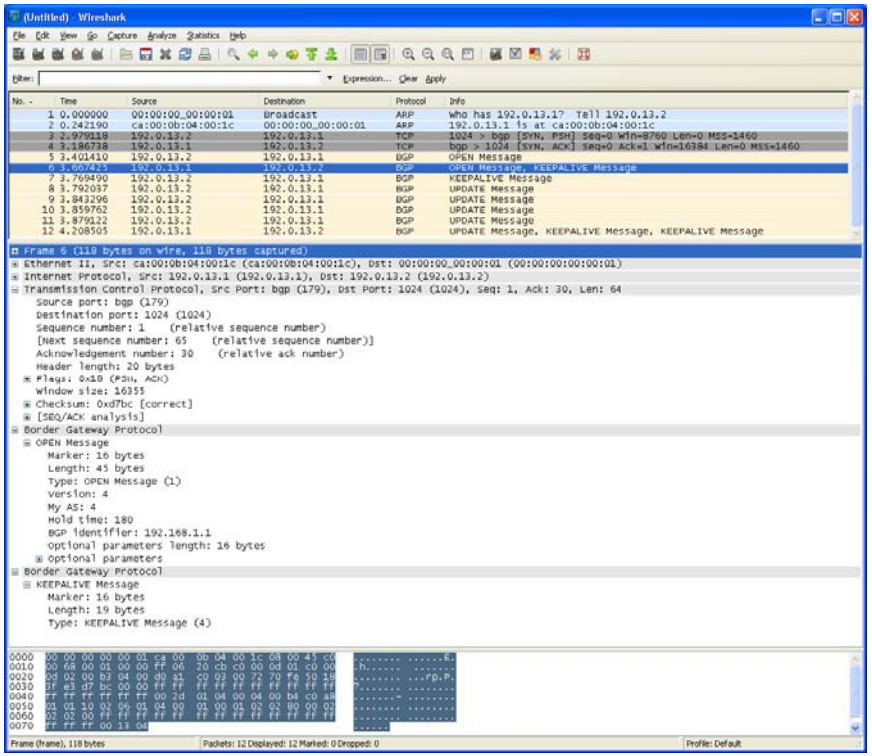
Model of basic SEPIA Network



SITL part of SEPIA network

Interesting Issues in Developing Custom TCP & BGP Translation Functions

- OPNET TCP uses a “key” to retrieve the connection handle
  - Translation function must map real-side TCP to corresponding keys on simulated-side.
- OPNET BGP differs from standard (RFC 4271) on message type codes (e.g. Update message in OPNET is 3, standard is 2)
- OPNET BGP message size must match real message size to keep TCP synchronized – some packet fields types are different sizes
- Cisco IOS sends multiple BGP packets in a single TCP packet, whereas OPNET BGP sends single BGP packet in each TCP packet – use OPNET segmentation & reassembly



Screen capture from Wireshark showing detailed protocol investigation

Future Work

- Develop and deploy additional network protocols of interest in computer security studies
- Test and understand overall SEPIA model performance issues, especially at the OPNET-to-real SITL interfaces.
- Develop tools that can predict the performance of the hybrid test networks
  - We plan to build OPNET models that let us size SITL experiments
- Develop partitioning approaches for right-scaling experiments
  - Use prediction results to partition network experiment models
  - Address performance, time synchronization and packet exchange issues
- Develop tools (e.g. GUI and processes) to rapidly configure large experiments
  - We are investigating using OPNET as a key GUI element

CONCLUSION

- SEPIA tools will allow analysts to ***rapidly*** and ***cost-effectively*** analyze complex network security issues.
- This experiment demonstrated that simulation models could be practically linked to physical equipment to support in-depth studies
  - Beyond simply passing network traffic, the physical nodes in this experiment actually interacted at a protocol level
- In addition, this experiment demonstrated a viable process for developing the needed middleware between the simulation and physical elements
- We expect to make further refinements in this process
- OPNET's Simulation In The Loop is an enabling feature for SEPIA experimentation