SAND2011-2455C

Live Virtual Constructive Networks for CNO

Vincent Urias
Sandia National Labs

Sandia National Laboratories

The Setting

- The World is highly reliant on computer network infrastructure
- Interdependencies of systems are complex and often misunderstood
- Computer networks can be very costly

CNO Challenges

- Conducting high-fidelity CNO is hard, expensive, or policy prohibitive
- Current CNO tools and techniques do not provide the ability to:
  - create rapidly configurable, validated, repeatable tests
  - scalable solutions
- Understanding the system

What is needed…

- Enable analysis and understanding of complex computer network systems
  - without building large, costly, physical representations
  - early in CNO lifecycle
  - without relying on live systems
  - to ascertain cyber impact on a mission
  - portraying advanced cyber threats and representative environments

Goals

- Create a modeling, simulation & analysis framework using a Live, Virtual, Constructive (LVC) approach
- Ascertain IO effects and IO systems behaviors to inform cross-domain cyber operations
- Represent threat and target systems with sufficient fidelity to assess the effects of cyber adversary behavior
- Enable the analysts to *rapidly* and *cost-effectively* analyze complex networks

How do others solve it now?

- Penetration testing on restricted, non-representative networks
- Gaming and role playing during mission rehearsal
- Limited scope experiments during exercises
- Modeling and simulation testing of limited, selected environments

Our path to a solution

- CORONA offers some solutions to some of these problems – we're not the oracle though
- It is a funded DoD Modeling and Simulation Coordination Office (MSCO) project
- We are developing both technical solutions and a structured approach
- Rigorous scientific approach to each module
- Design of Experiments
  - Chose the right dependent variables (observables), understand your controlled(static) and independent(changed) variables
  - Look for confounding issues and iterate

Unique Approaches

- Modular approach to measure cyber effects on operational missions
  - Addresses heterogeneity and scale issues
  - Correct by construction approach (Dijkstra)
  - Enables incorporation of existing best suited model
- Closed environments reduce risk
  - Complete system representations
  - Fosters analysis of alternatives and COA
  - Facilitates realistic threat characterization

More Unique Approaches

- Ability to specify experiment in a high level language
  - Helps to eliminate the accidental complexities
  - Helps the SME put their brain power where we get the most benefit from it
  - Aids in revision control and Design of Experiments
- Analysis tools will help SME understand
  - The system
  - The tradeoffs
  - The experiment

M&S Objective's

- Create experiment with models and integrate emulation to perform security analysis
- Test hypothesis that LVC networking approach can be taken on systems of record
- Participate in joint IO Range experiment

Why Focus on an LVC Network?

- Timely flow of information is the warfighter’s lifeline
  - Impacted by myriad *invisible threats, including* environmental, technical and cyber attacks
- The network is a platform
- Many experiments :
  - assume perfect communications
  - simulate only the physical layer of communications.
  - don’t account for realistic delays in information dissemination

L-V-C Alone Is Not Enough

- Live
  - Highest form of *realism for vulnerabilities, exploits and impact*
  - Limited scalability, high cost.
  - Time and resource intensive for configuring and managing testbeds.
  - Limited network infrastructure; typically wired only
- Virtual
  - Higher-fidelity, real software on fake hardware
  - Non-scalable, poor performance, limited supported emulators
- Constructive
  - Hardware, operating system, applications, traffic and user behavior are abstracted or not considered.
  - Scalability, repeatability, low cost, quick turnaround time
  - Lack realism of cyber attacks and defenses; rely on probabilistic models
  - Generic Simulators have very limited suite of cyber attack and defense models

Technologies Used

- OPNET
  - Configurations
  - Extensions
- VMWare ESX:
  - Application services
  - Flexibility
  - Collaboration
  - Replication
- SEPIA:
  - Simulation
  - Emulation (virtual machines, Dynamips routers)
  - Physical (hardware, real operating systems)

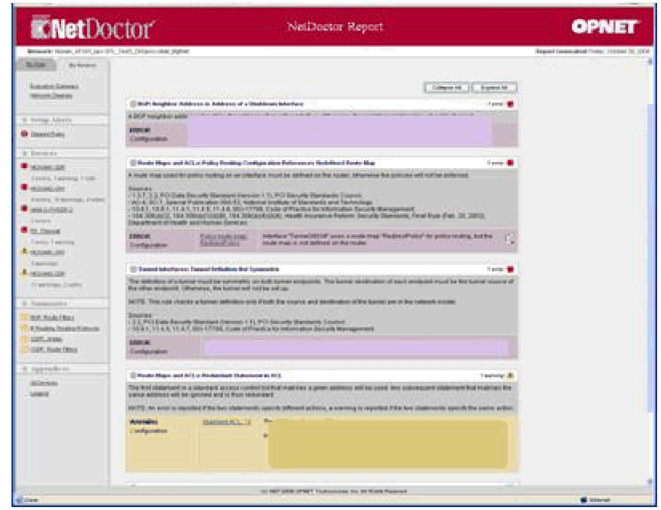
Flexibility to vary where to put the fidelity - Attach physical devices to the network that include simulated and emulated devices

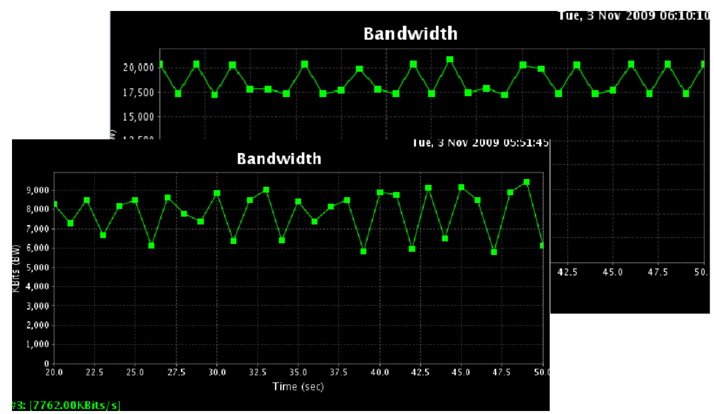
Talking Points

- Leverage existing open source, freeware, and COTS
- Effects faithfully replicated from physical testbed
- No relevant artifacts introduced
- Analyzed LVC trade-offs between LVC
- Imported several hundred of thousands of lines of operating configurations from gateway devices
- Provided method for describing and deploying configurations to LVC components
- Moved between L<->V<->C
- “Gateway-in-a-box”

LVC Testbed Successes

- Models configured with actual Cisco configs
- Port Scan analysis
- NetDoctor reports
- VPN replication
- Bandwidth optimization
- Services represented
- Vulnerability analysis





Sandia National Laboratories

Demonstrations

- Technical demonstrations show fundamental IT capabilities
  - ICMP, DNS, HTTP, SMTP/POP3, SSH
  - Proxy
- Dataflow is faithfully with surrogate systems
- Show that malicious payloads can cross LVC boundary multiple times and effect an intended target

Other Efforts

- Incorporated IPS/IDS
- Introduced more emulation
  - Used emulated PIX firewalls to enclave parts of network
  - Several Dynamips emulated routers
- Created SCADA network topology
  - Instantiated VCSE
  - Conducted several "scenarios"

Lessons Learned

- LVC makes sense - let's do it.
- Model Test Model makes sense – let's do it more…
- Cyber threat replication makes sense – let's make it formal and do it some more

Who does this impact?

- Combatant Commands – exercise support
- Testing, training, acquisition, experimentation, intelligence communities – Enhanced assessments and training
- Existing and emerging ranges – needed capabilities & technology break through
- Armed Services – Individual and joint operations
- Conduit for Intel support to warfighter

Where else can this be used?

- Training, Exercises, Wargames
  - *How do we train our defenders without using the live networks?*
- Defensive Strategy Development
  - *How do we avoid the "disconnect while under attack" mentality?*
- Testing/Evaluation/Assessment
  - *How do we test, evaluate, and assess new defensive technologies and devices at scale?*
- Malware Analysis
  - *How can we observe behaviors or mission impact at appropriate scales?*
- Policy Analysis
  - *How can we ensure government cyber policies will have the right effects without negative unintended consequences?*

Successes – How and Why?

- Our approach evolved from a systems engineering & lessons-learned mentality (experience & expertise)
- Overcame significant technology barriers
- Demonstrated cyber Modeling and Simulation capability in multiple forums

Conclusions

- Successful hybrid use of:
  - *Physical devices (Live)*
  - *Emulated devices (Virtual)*
  - *Simulated devices (Constructive)*
- Flexible experiment deployment
- Varying degrees of fidelity as needed
- Rapid deployment of experiments
- Analyze actual events in test bed to understand threats and vulnerabilities