EMULYTICS

Emulate, analyze, and understand complex systems

Networked Information Technology systems play a key role supporting critical government, military, and private computer installations. Many of today's critical infrastructure systems have strong dependencies on secure information exchange among geographically dispersed facilities. As operations become increasingly dependent on the information exchange they also become targets for exploitation. The need to protect data and defend these systems from external attack has become increasingly vital while the nature of the threats has become sophisticated and pervasive making the challenges daunting. Enter Emulytics!

The term "Emulytics" was coined at Sandia Labs in 2008 when a need for two kinds of computing environments was noticed: information analytics and graph analytics. Emulytics™ is derived from the terms emulative network computing and analytics. Emulytics™ includes and seeks to include:

- Large-scale, vastly heterogeneous networked systems
- Integrated systems that can be configured and used both for controlled experimentation and interactive exploration of system behavior
- Components that may be real, emulated, or simulated
- Network(s) creation, management, and instrumentation
- Large HPC platform management and monitoring
- Data extraction and warehousing
- Analysis and result visualization.

Screenshot of the Supercomputing model, running in Sandia's Emulytics platform. This graph shows an abstraction of the network which we can compare to the model for first-order validation.

Sandia supports an open-source project "minimega" (minimega.org) to support creating virtualized models of computer-related networks. This is the core capability that enables much of the Emulytics™ program at Sandia. Key features allow:

- Scalable experiment development: design and test an experiment on a laptop, and then upload and run it on a large cluster to increase the number of nodes in the model
- Performance considerations: thorough experimentation requires many repetitive runs. Minimega orchestration can tear down and re-provision extremely large networks (on the order of 10,000 elements) in seconds thus enabling many iterations of studies on a consistent model

The tool has been used by academic researchers and enables Sandia's cyber-range and operational systems testing analysis and training efforts.

Emulytics™ blends simulation, virtualized hardware and software, emulated devices, and the direct deployment of actual hardware and software to create live-virtual-constructive (i.e., real-emulated-simulated) environments. Emulytics enables rich analyses through scalable infrastructures while being deployable with great efficiency. Among its many applications, Emulytics provides cyber defender training, helps to characterize otherwise unmanageable systems, and has even been used to understand and provide quantitative evidence of potential cyber threat impacts on the performance of physical protection systems. Securing today's sophisticated information technology facilities involves not only creating secure system architectures and secure system configurations, but also heavily relies on well-trained defenders. Thus, there is a need for flexible cyber security training, testing, and analysis platforms that can replicate information systems with high levels of realism to enable training and analysis.

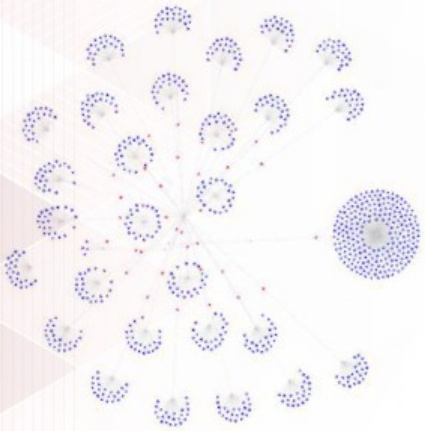
Minimega feeds thousands of emulated Android devices synthetic GPS locations to emulate users walking and driving around Livermore, CA as part of the MegaDroid LDRD.

Scan with SNLSimMagic App to see our work come to life.

Sandia has engaged in multi-year research projects to develop new strategies and methodologies that enable researchers to quickly and accurately model information systems' hosts and networks of interest for cyber analysis and training. Emulytics™ provides the capability to combine real, emulated, and simulated devices—i.e., live, virtual, and constructive—into a single controlled experiment to enable system-wide cyber training, while answering a wide variety of cyber-related questions. high performance computing capabilities enable the Emulytic platform to represent complex, large-scale, complicated system enterprises, such as government facilities like Sandia, or to model threats across the national power grid infrastructure like the recent Mirai internet-of-things botnet.

Sandia advises the Department of Homeland Security on policies and protections related to the cyber defense of civilian government networks (.gov). Emulytics™ is used to model portions of the nation's infrastructure to answer "what if" questions for technology, architecture, and policy changes. Sandia aims to be able to create models of the entire national infrastructure.

Information System: According to the *Business Dictionary,* an information system is "a combination of hardware, software, infrastructure and trained personnel organized to facilitate planning, control, coordination, and decision making in an organization."



Minimega models a simple enterprise network with dozens of subnets (represented in red) each containing dozens of endpoints (represented in blue). A core router connects the subnets to the outside world.

What's at Stake?
The Importance of Emulytics capabilities

Currently, cyber defender training and system analysis are performed on operational systems, on limited scale testbeds, or on simulated models of the system. However, each approach has some disadvantages.

- Operational systems: Analysis and training on operational systems is limited to the most benign levels because any disruption to the operational system has potentially severe consequences. While defenders gain experience with the actual system, this approach reduces operators' ability to test and analyze the system. The scale of operational systems can be the size of entire nations or even the global routing infrastructure (the Internet). Creating full-scale replicas for experimentation is not economically feasible, so operators turn to virtualization and modeling techniques.
- Testbeds: Testbeds for analysis and training are typically expensive, time-consuming to construct and deploy, single-purpose, and difficult to maintain due to fast-paced technological advances. Testbeds are also typically limited to small subsets of the larger system, which limits their realism.

Sandia Lab's Emulytics™ solution provides: Networked endpoints (OS, virtual, HITL), instrumentation, data collection, and analysis backend capability. Sandia provides a platform capable of adequately representing the operational system for analysis and for cyber teams to exercise their techniques and develop tools, tactics, and procedures.