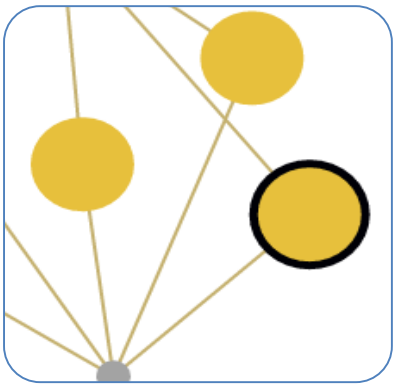
Emulytics™ Tool - minimega

Emulation, modeling, and analysis for large-scale cybersecurity research



minimega is an Emulytics™ tool developed at Sandia to launch and manage large scale virtual machine based experiments. Minimega is scalable, allowing us to study small or very large VM networks.

Problem

When attempting to study contemporary internet threats and mitigation technology, scale is everything. Malware, botnets, and distributed denial of service attacks, which can involve millions of endpoints, demonstrate emergent behavior that cannot be studied without dynamic behavioral analysis at scale. Complex patterns of malicious behavior, such as that manifested by botnets, emerge only at scale. Even benign behavior, such as the fast evolution of network topologies, present a challenge to researchers to fully understand.

Why it Matters

Scalable emulation for training, test and evaluation, and operations is needed to address urgent national security concerns. Internet technology is deeply embedded into the fabric of the nation's economy, electrical grid, and other aspects of critical infrastructure.

Sandia's Approach

Sandia's minimega platform leverages expertise in high performance computing, cybersecurity, and virtualization to provide a novel suite of emulation, modeling, and analysis tools for predictive simulation, exercises, training, and real-time dynamic defense. Sandia supports activities at classified and unclassified levels. The objective of Sandia's Emulytics™ program is to develop and deploy next-generation emulation and analytic tools to advance the state of the art of experimental cyber security and improve the utility of cyber range resources.

Key Features and Technologies

Investments in minimega at Sandia have resulted in a number of novel Emulytics™ technologies and capabilities:

- Open source, available at minimega.org
- Rapid, turnkey deployment on general purpose computers and clusters
- Very fast experiment description and launch
- Hardware-in-the-loop
- Scales to at least 100,000 endpoints
- Android-based mobile support with numerous emulated sensors/radios
- Integrated command and control layer for endpoints
- VNC-based framebuffer and keyboard/mouse record and replay
- Supports QEMU/KVM and container-based VMs
- Ephemeral network connection support
- Feature-rich, real-time experiment visualizations

Research Funding

minimega is funded by Laboratory Directed Research and Development.

Contact Us
emulytics@sandia.gov

Sandia National Laboratories is a multi-mission laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2017-1850M