SAND2015-3454PE

Exceptional service in the national interest

Sandia National Laboratories

Differentiating Capabilities for Defense Against Cyber Threats – SNL Cyber Activities & Research

Keith Vanderveen, Scalable & Secure Systems Research

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multi-program 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. SAND NO. 2011-XXXXP

Internet Emulation & Large Scale Data Analysis

- Internet-scale network emulation and analysis tools (Emulytics™)
  - Large scale virtualization of Windows, Android, and other OS (10^5 – 10^6 VMs)
  - Tools to instantiate network topologies of interest
  - Tools to configure and manage large-scale experiments
  - Fuzzing
- Algorithms and computing architectures for large-data analysis
  - Expertise with large graphs (DARPA FEAST project, others)

Sandia been working on Emulytics™-for almost a decade

Sandia National Laboratories

- We've developed tools/techniques that enable:
  - Testing, evaluation
  - Performance Analysis
  - Training
  - Effects Based Analysis
  - Malware Analysis
  - Next-Gen Cyber Capability Development
- The ease and ability to do the following is critical to the success of future systems…
  - Pose a question/hypothesis/ reason
  - Standup an experiment
  - Test
  - Analyze the data
- Emulytics is still developing and evolving as a capability, a community, and as a science

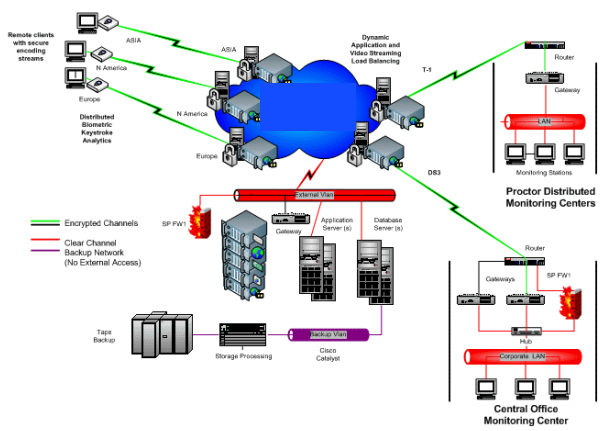
Why Emulate? Why Create Environments?

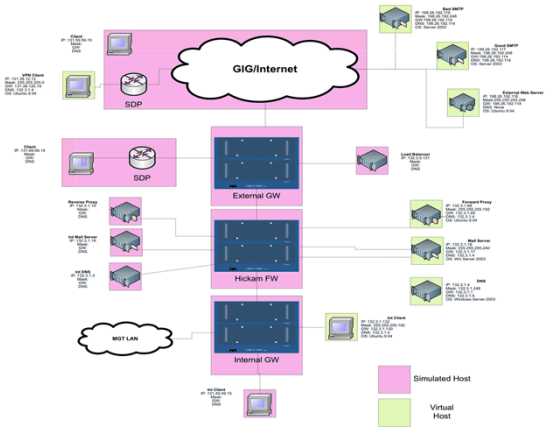
Sandia National Laboratories

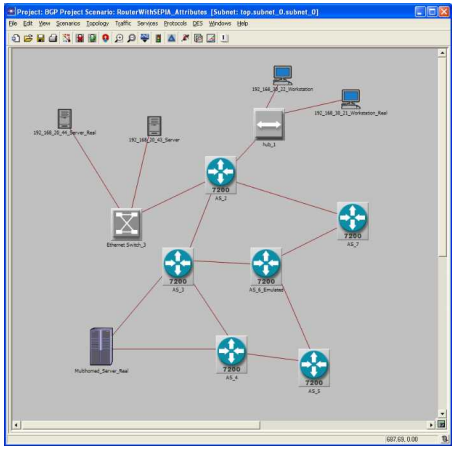
- Conducting high-fidelity testing (cyber and otherwise) is hard, expensive, or policy prohibitive
- Current tools and techniques do not provide the ability to:
  - create rapidly configurable, validated*, repeatable tests
  - create scalable solutions
  - quickly rollback to start state
  - test and evaluate technologies
  - heavily instrument the system (host, network app, …) to learn from system
  - understand the system

LIVE, VIRTUAL, CONSTRUCTIVE (LVC) Analysis

Sandia National Laboratories







Actual System

LVC Testbed

M&S Testbed

Interoperability of live, virtual, & constructive in a single experiment

Live

M&S

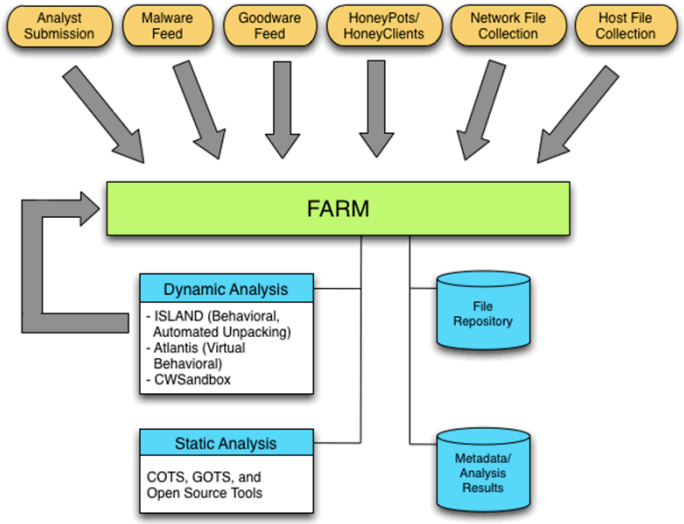
Increase Realism

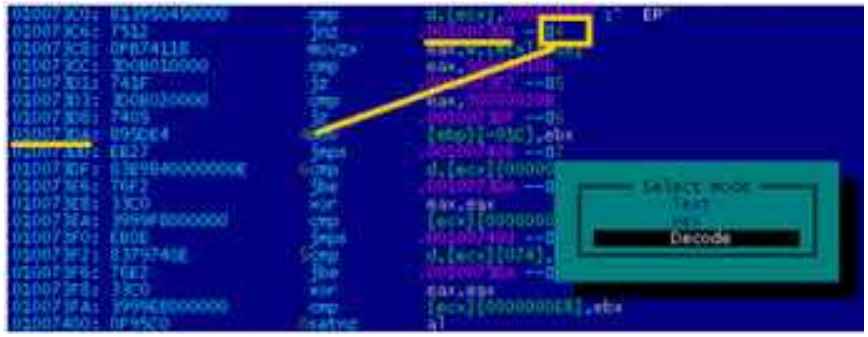
Decrease Cost

Decrease Time

Secure Cyber Networks and Systems

- Malware Analysis
  - Automated malware analysis and triage using static and dynamic analysis
  - Deep dive reverse engineering of malware
  - R&D in the area of file similarity detection
- Network Monitoring and Incident Response
  - Responsible for SNL enterprise cyber security (partnership between 8900 and 9300)
- Vulnerability Assessment
  - Red-teaming and penetration testing





FARM

- Forensic Analysis Repository for Malware
  - Sandia's automated malware analysis system
  - Modular – Easy to add **New Tools**
  - Growing repository of ~ 50 million (+ 100k / day)
  - Scalable framework based on cloud technology
    - Easy to add **Automated** analysis capacity
  - RESTful API – programmatic submission and data retrieval
    - Enables more complex analytics
  - Group permissions that control context
    - Enables **Information Sharing**
  - Email Alerting
    - **Focus humans resources**

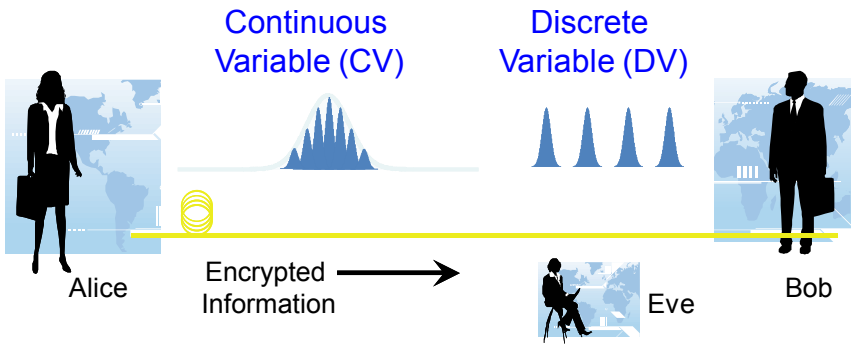
Formal Methods R&D

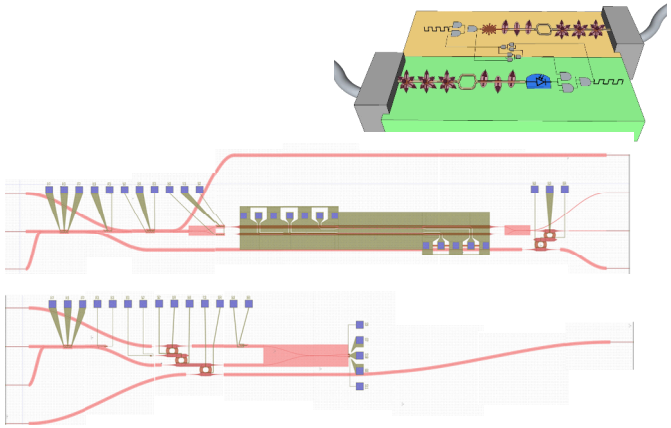
- Formal methods are increasingly commonplace in industry and academia
- What outside parties do:
  - Verify reliability
- What they don't do as much of:
  - Verifying security
  - Assessing trust in engineering
  - Addressing complex scenarios (e.g., situational awareness, cascading failures)
  - Off-nominal conditions (e.g. effects of radiation on logic)

Quantum Information Sciences

Sandia National Laboratories

Improving Quantum Key Distribution

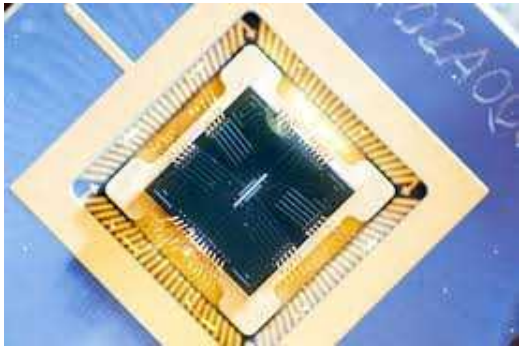




Transmitter design

Receiver design

Building components for future quantum computing platforms



Sandia on-chip ion trap

- Assembling well-characterized qubits
- Fault tolerance
- Control of quantum systems