SAND2015-2320C

Emulytics™ at Sandia National Laboratories

Vincent Urias, Brian Van Leeuwen,
Brian Wright (P), William Stout

Overview

- Introduction
- Methodology
- Modelled Systems and Testbed
- Models and Emulations
- Data Collection
- Applications

Introduction

Networked information systems play a key in role supporting critical government, military and private information systems. Securing these information systems is not only about creating secure system architectures and configurations but also heavily relies on well trained defenders of the systems.

What kind of system might enable cyber analysis and cyber training with high-levels of fidelity and realism?

Sandia National Laboratories

FIND THE OPPORTUNITY IN CHANGE. INNOVATE, SIMULATE....EVOLVE!
MODSIMWORLD 2015

Introduction

Current cyber defender training and system analysis often performed via:

Operational Systems

→ Conducted with benign levels to prevent disruption

Testbeds

→ Typically expensive/time-consuming to construct and deploy; single-use

Simulated Models

→ Simulation codes developed on-the-spot; inaccurate and buggy

Methodology

Sandia's Emulytics solution provides:

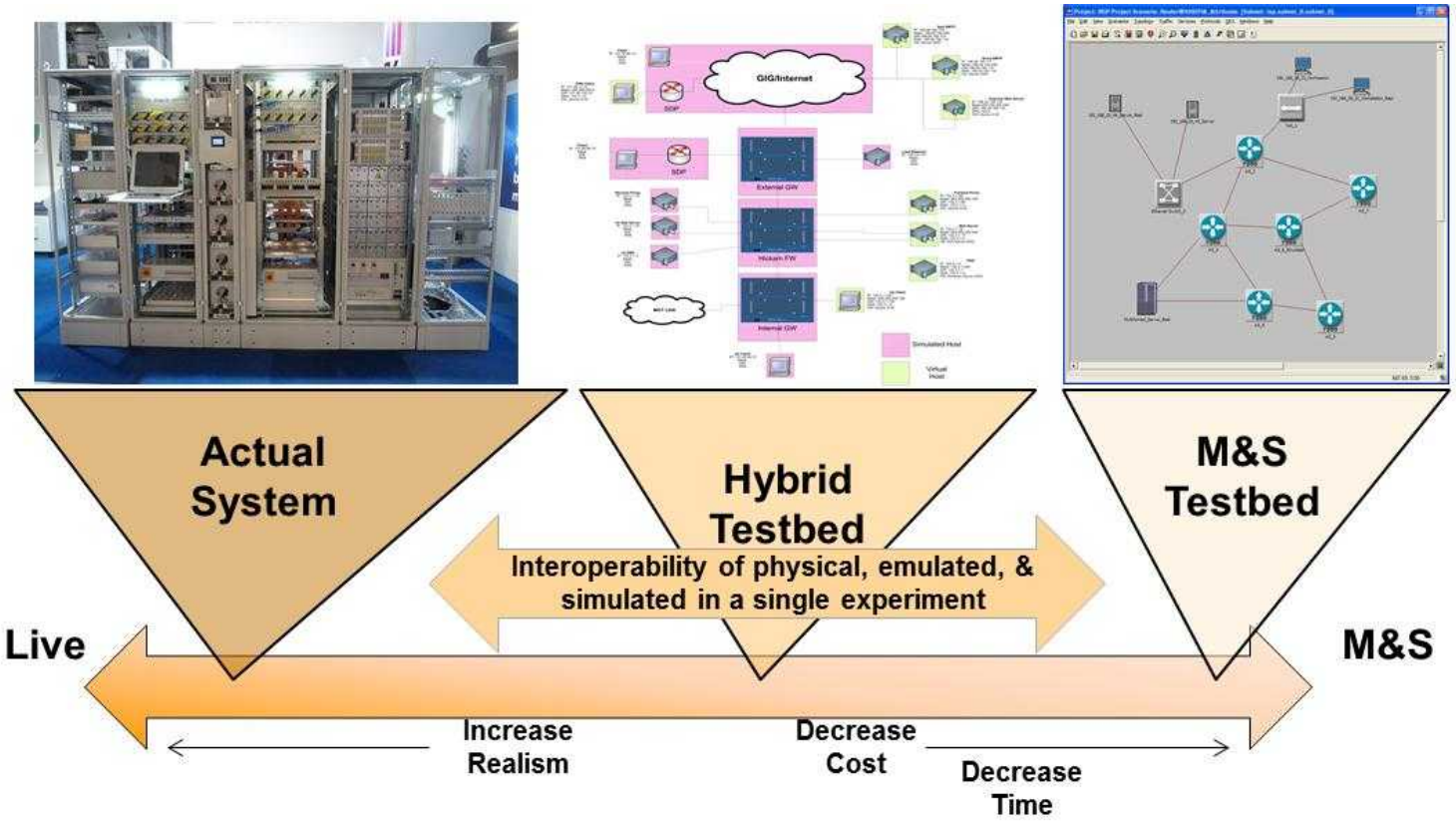
- Networked endpoints (OS, virtual, HITL)
- Instrumentation
- Data collection
- Analysis backend capability

A platform capable of adequately representing the operational system for cyber red and blue teams to exercise their techniques and develop tools, tactics and procedures.

Methodology

- Mechanisms to **rapidly specify and deploy** complex networked information systems of routers, switches, hosts, services, and applications.
- Extensive **protocol support** for network devices such as switches and routers.
- Instantiate **10,000's hosts**, such as servers or workstations, in high-fidelity. Windows/Linux operating systems but can be extended to support a greater variety of systems and devices including VoIP phones, printers, etc.
- **Instrumentation** at the hosts and network layer to capture, in **high-fidelity, data** describing system operation.
- Create **complex scenarios** (e.g., of deployments, intrusion attempts, user impact, etc.) that can be scripted for execution within the experimental platform.
- Incorporate **application-layer overlay systems** such as those used for Supervisory Control and Data Acquisition (SCADA)
- Represent **mobile communications** and their interoperability with fixed-networks
- Represent the latest and upcoming security approaches such **as Moving Target Defenses (MTD**).

Methodology

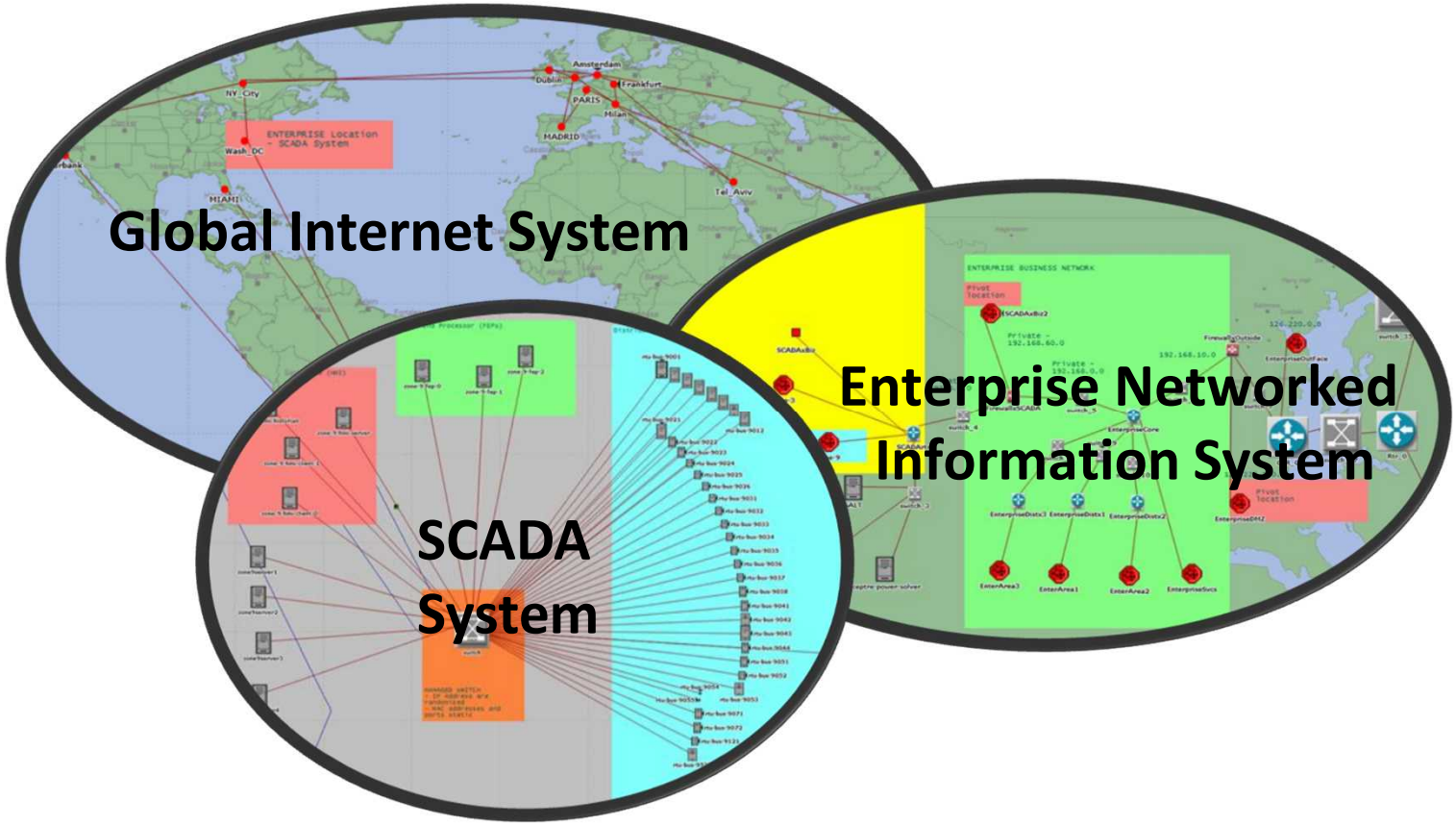


Modeled Systems and Testbed

An example system deployed using Emulytics, employing emulation, physical hardware, and extensive virtualization – consisting of:

- Global Internet-like System
- Enterprise Networked Information System
- SCADA System

Modeled Systems and Testbed



Sandia National Laboratories

FIND THE OPPORTUNITY IN CHANGE. INNOVATE, SIMULATE....EVOLVE!
MODSIMWORLD 2015

Models and Emulations

- Do the local and wide area networks respond appropriately? Do routes and paths converge as expected? Are quality-of-service (QoS) parameters and metrics comparable to those in the real world?

- Do devices perform as expected? Are servers, SCADA devices, and security stack devices well integrated? Do the devices offer the same, if not extended capabilities to monitor and introspect upon?

- Do users, such as red or blue teams, feel comfortable in the environment? Do workstations, servers and applications accurately reflect the settings they're accustomed to?

Models and Emulations

- Device Representations
  - Virtual Machines, HITL
    - Windows, Linux, Appliances
  - File insertion
    - Custom configurations
  - SNMP, DHCP/DNS, in-band configuration
  - Heterogeneous network devices
    - Virtual/physical L2/L3 switches, routers

Models and Emulations

- Application and Traffic Representations
  - Enterprise systems
  - Vulnerable hosts

  - Realistic end user traffic
  - Small cross-platform injected application

Data Collection

Host, Network, Management

- SNMP
  - Performance metrics, CAM tables, …
- Virtual machine introspection (Sandia specific)
- VNC Capture/Replay
- PCAP, network performance monitoring, netflow

Applications:
Cyber Training Platform

Train teams responsible for network defense and hunt; understand their roles, tasks, and how their actions supported (or impacted) overall mission.

- Stand up experiments quickly and repeatably
- Introspect into actions and processes
- Adequately gather data to reason about the experiment and team member performance

Applications: Cyber Training Platform

- Three Zones (A, B, C)
- VPN Connectivity
- Enterprise Elements
  - HITL, Routers, Firewalls, IDS, Enterprise Services (DNS, Mail, Web)
- Global Internet, SCADA, Business Networks
- Exploitation, Hunt, Blue Team, Red Team

Applications:
Cyber Training Platform

- Team workstations from the customer site were brought directly into the Global Internet system, occupying virtual workstations in the Tokyo domain.
- With presence established team members were free to roam the environments and put their training to work.
- Data collection techniques allowed Sandia to capture their movements through virtual/physical networks.
- Collection revealed actions from the networking perspective, but also on host down to points, clicks and keyboard entries on the virtual machines.

Emulytics™
at Sandia National Laboratories

Vincent Urias, Brian Van Leeuwen,
Brian Wright, William Stout

Questions/Comments?