CyberVAN (Cyber Virtual Assured Network)

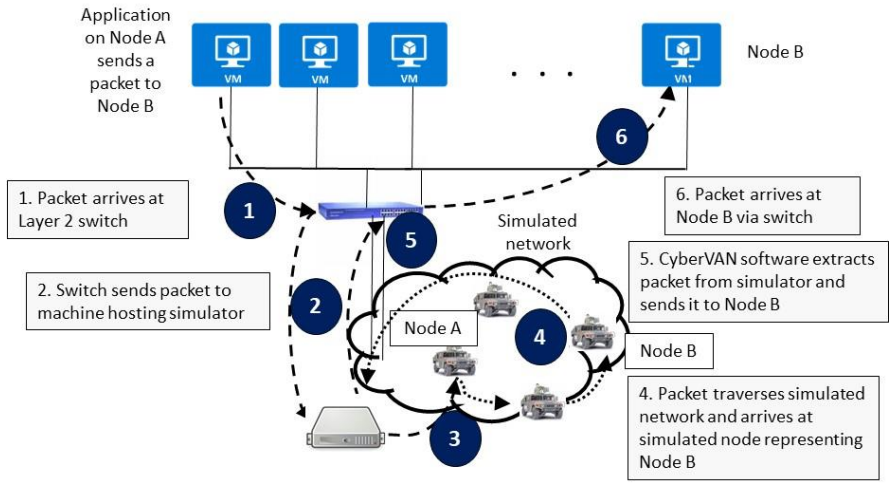
A FLEXIBLE, HIGH-FIDELITY, SCALABLE, RAPIDLY DEPLOYABLE CYBER ENVIRONMENT FOR EXPERIMENTATION, OPERATIONAL PLANNING, VALIDATION, AND TRAINING

The Challenge

New and improved cyber security capabilities are emerging at a rapid pace to counter new and evolving cyber threats. In order to ensure that resources are focused on the most promising approaches, there is a need for capabilities that enable **efficient** and **accurate** evaluation and validation of cyber security tools in a **realistic, high-fidelity cyber environment**. Isolated and contained environments are needed for operational planning and what-if scenario experimentation. In addition, cyber specialists need high-fidelity reproducible cyber environments for **training.** Such environments must be easy to define and specify, manage and maintain, and deploy and modify. They must scale to tens of thousands of cyber elements which hosts, routers, switches, firewalls, WiFi, LTE cellular, tactical waveforms, etc. Finally, capabilities are required to easily define highly diverse computing environments, which could include multiple versions of different operating systems and services, each with their own known and unknown vulnerabilities, organized in different topologies, with different levels of access.

The CyberVAN Solution

How does one create a cyber environment, say, representing an enterprise network? The easiest and highest fidelity solution is to deploy an exact replica of a known network by procuring the same equipment and deploying it in the same configuration, including the network elements' setup and connectivity, and the host software and user configurations. Clearly, such an approach is prohibitively expensive, in terms of hardware cost, physical space required, and human labor. A natural alternative is to take advantage of virtualization capabilities to deploy a virtual cyber environment using commodity hardware or hardware supplied by a cloud service provider. Cloud providers already provide sophisticated tools for defining and deploying such computing resources. So, why is a product like CyberVAN required?



CyberVAN provides the **highest possible fidelity representation of a network** next to actually deploying the real network, by representing the network in a **discrete event network simulator**, and enabling hosts represented by **virtual machines (VMs) to communicate over this simulated network**.

CyberVAN Differentiators

High-Fidelity Network Representation

Although existing cloud service offerings can provide high-fidelity representations of different host environments, they are limited in the networking capabilities. For example, it would not be possible to

connect two cloud-hosted VMs via a WiFi Link. Network simulators like ns-3 provide high-fidelity simulation all of the network effects, including latencies, link capacities, routing protocols, etc. In particular, wireless networks can be modeled with mobility, interference, and propagation effects, as well as the details of different waveforms. This becomes critical when cyber attacks that target aspects of the wireless protocols need to be included in a scenario. Accurate modeling of Internet-scale networks is also not achievable using existing cloud service environments because of the inability to model Internet protocols and services accurately. CyberVAN's innovative **transparent forwarding** technology enables IP traffic generated by services running on VMs to be sent via a **simulated network segment** to its destination VM. To accommodate large or complex scenarios, CyberVAN incorporates our **TimeSync** technology that synchronizes the rate of time advancement between the simulator and the VMs, thereby enabling experiments to run slower than real time and maintain accuracy of test results.

Scenario Design and Management

CyberVAN provides sophisticated capabilities for managing the design, deployment, and archiving of cyber scenarios. Users access CyberVAN via a Web Portal and use a **Scenario Design GUI** to design their network. CyberVAN automatically allocates the required hardware resources for the scenario. A **Scenario Management GUI** provides an environment for accessing and managing the elements of a scenario, including logging in to the VMs in the scenario, running various analytics tools on these VMs, saving the results of experiments, pausing and restarting experiments, and so on.

Cyber Effects Library and Realistic Benign Traffic Generation

CyberVAN provides a substantial, growing library of cyber effects, including a configurable botnet, tools for assessing vulnerabilities via scanning, and an ability to generate vulnerable scenarios and executable attack blueprints from high-level user specification, with attacker TTPs based on the MITRE ATT&CK framework. A realistic cyber environment must include realistic traffic, which is generated by users of the network. CyberVAN provides a capability for simulating user activity that drives real applications on end hosts, which in turn generate realistic network traffic.

Rich Simulated Networking Model Library

CyberVAN offers a comprehensive set of commercial and military models within a single testbed.

ns-3 Model Library
Focus on commercial wireless and wired network technologies

- Commercial waveforms
  - LTE, 802.11a/b/g/n/ac/ah, 802.15.4, 802.16, LoRaWAN, WRAN…
- Spectrum-based wireless propagation loss models
  - Free-space, Terrain-aware…
- Energy consumption and battery models
- Terrestrial and airborne mobility
- Wired Models: 802.3, WAN links…
- Routers, Switches, Hubs, Firewalls, NAT…
- Layer 3 protocols
  - DHCP, DVRP, OLSR, BGP, SMF, B.A.T.M.A.N.
- SDN (OpenFlow, P4)
- DVB-S2 Satellite Waveform
- Transport and queuing models (tc)

EMANE Model Library
Focus on military waveforms

- Extensive library of military waveforms:
  - SRW
  - Link16
  - TTNT
  - MADL
  - CDL
  - Satellite, …
- High fidelity, validated models

Data Collection

CyberVAN offers a number of data collection capabilities, including network packet captures and flow records, host log files and system call interception, and a user activity tracker tool to collect human-computer interaction such as window, mouse and keystroke events, and shell commands.

For more information: http://www.peratonlabs.com E-mail: cybervan@groups.peratonlabs.com