ENGINEERING

CyberVAN™

A Flexible, High-Fidelity, Scalable, Rapidly Deployable 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. To ensure that resources are focused on the most promising approaches, there is a need for efficient and accurate evaluation and validation of cyber security tools in a realistic, high-fidelity cyber environment where isolated and contained environments enable operational planning and what-if scenario experimentation.

Cyber specialists need high-fidelity, reproducible cyber environments for training. These environments must be easy to define and specify, manage and maintain, and deploy and modify. They must also scale to tens of thousands of cyber elements including hosts, routers, switches, firewalls, Wi-Fi, LTE cellular, tactical waveforms, etc.

In addition, capabilities are required to easily define highly diverse computing environments, which can 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.

CyberVAN SOLUTION

Cyber Virtual Ad-hoc Networking (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 (VM), to communicate over this simulated network.

Creating a representative cyber environment as an alternative to deploying an exact replica of a known network takes advantage of virtualization capabilities to deploy a virtual cyber environment using commodity hardware or hardware supplied by a cloud service provider. A critical benefit of this approach is that any required analysis can be performed prior to procuring potentially expensive equipment and spending valuable time configuring and deploying it.

High-Fidelity Network Representation

Although existing cloud service offerings can provide high-fidelity representations of different host environments, they are limited in their networking capabilities.

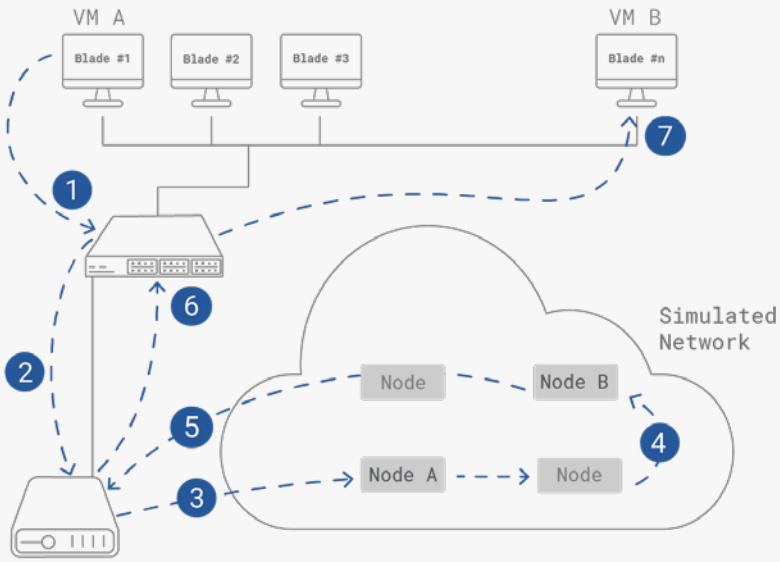

Figure 1. Journey of a packet in CyberVAN

1. Packet arrives at Layer 2 switch
2. Switch sends packet to machine hosting simulator
3. CyberVAN software injects packet into simulated network at the simulation node representing Node A
4. Packet traverses simulated network and arrives at simulated node representing Node B
5. CyberVAN software extracts packet from simulator and sends it to simulator machine
6. Packet is sent from simulator machine to switch
7. Packet arrives at Node B via switch

For example, it would not be possible to connect two cloud-hosted VMs via a Wi-Fi 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 to synchronize the rate of time advancement between the simulator and the VMs. This enables experiments to run slower than real time while maintaining the 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 graphical user interface (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 into the VMs in the scenario
- Running various analytics tools on the VMs
- Saving the results of experiments
- Pausing and restarting experiments

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.

CyberVAN provides a capability for simulating user activity that drives real applications on end hosts, which then generates 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: Commercial Wireless and Wired Network Technology

- Commercial waveforms: LTE, 802.11a/b/g/n/ac/ah, 802.15.4, 802.16, LoRaWAN, WRAN
- Spectrum-based wireless propagation loss modes: 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 protocals: 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: 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.

cybervan@groups.peratonlabs.com