Carnegie Mellon University
Software Engineering Institute

WELLE-D

A Wireless Traffic Transport for Wired Networks

WIRELESS DEVICES ARE MORE PREVALENT NOW THAN EVER BEFORE. New Wi-Fi-enabled smart devices are being introduced at a rapid pace now that security and infrastructure monitoring systems are becoming commonplace. Everything from monitor cameras to HVAC and lighting systems are now being modernized to include data monitoring and control, and it's common today for new, off-the-shelf systems to contain built-in wireless capabilities. With the pervasiveness of these devices, there is a growing need to train people on how to keep them secure.

Training Challenges

Organizations training their staffs in wireless security must provide access to physical devices. Doing so is a challenge because physical devices are expensive and time consuming to configure and deploy. Also, organizations often restrict the use of wireless devices inside their facilities.

Maintaining the training environment can also be difficult because uncontained outside attacks can compromise it. Instructors can also struggle to exercise complete control over the environment.

WELLE-D for Virtual Networking

Virtual networking can provide organizations with a way to overcome these challenges. With a virtual network, you can ensure security and control because it is isolated from wireless attacks, free from outside interference, and allows instructors to remain in control of the environment. It also saves you time and money since you don't need to provide physical devices to all cyber-training participants, and setup and configuration can be automated.

At the SEI, we developed a new, virtual wireless networking environment called WELLE-D (Wireless Emulation Link-Layer Exchange Daemon). With WELLE-D, your cyber workforce can develop wireless security skills by performing realistic attack-and-defend scenarios in a cost-effective, safe, and controlled environment.

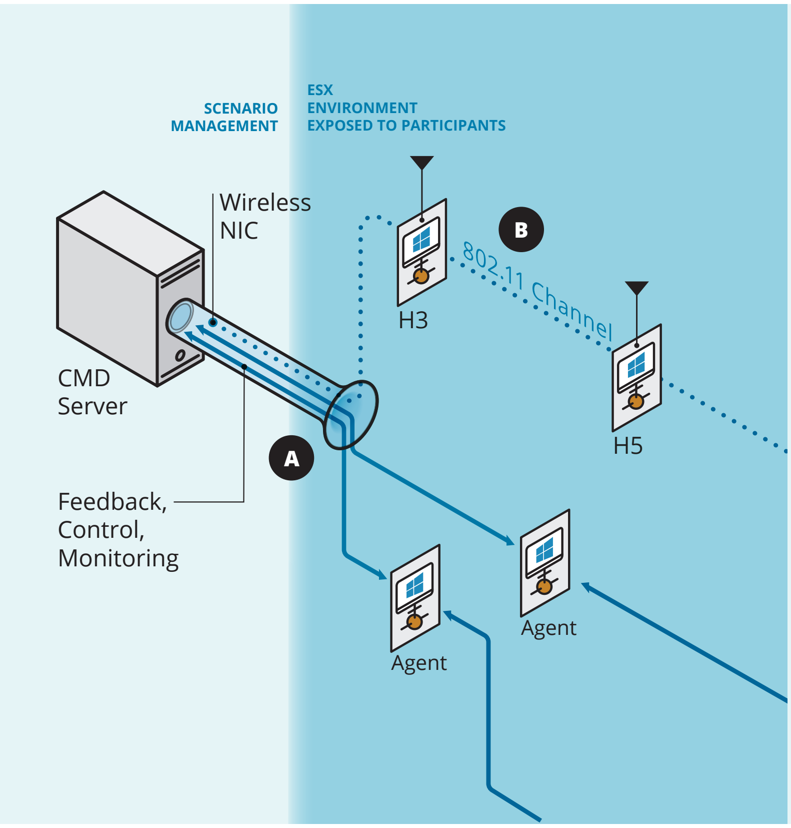
WELLE-D provides many benefits, including the following:

- You can use it for free since it's open source.
- It's scalable, so you can deploy and configure it according to your organization's unique needs.
- You can control the lab environment using the same characteristics each time you deploy it.
- System administrators can configure wireless access points and client software running a Linux kernel.
- Penetration testers can practice different wireless attacks and methods for penetrating the system.
- Training lab developers can create training labs that allow learners to exploit wireless communication protocols, such as WPA.

The Innovative WELLE-D Solution

As the SEI developers of WELLE-D, we created a way to transmit 802.11 frames in a simulator environment without using radios. We identified several benefits in designing a solution based on the mac80211_ hwsim driver for the Linux kernel and developed a custom set of programs to transfer the simulated wireless frames between multiple guests residing on the same host. This set of programs uses the VSOCK address family to communicate between the guests and host.

WELLE-D has three components: a device driver, a guest agent, and a host agent. These components work together to extend the virtual wireless network across multiple guests.



WELLE-D Highlights

WELLE-D enables the use of wireless frames in virtual-machine environments without having to use radios.

A. WELLE-D is based on the mac80211_hwsim driver for the Linux kernel. The Linux 802.11 driver creates Wi-Fi frames and redirects those frames through a VSOCK cloud that is enabled through vTunnel.

B. Because WELLE-D uses actual 802.11 protocols, the environment supports use of 802.11 monitoring and malware tools and attack-defend scenarios. And because it doesn't use radios, the traffic can run in any VMware environment, including classified workspaces.

Explore Our Tools Online

SEI cyber training tools can be used to create cybersecurity training to help students learn in near-real-world situations without risking organizational assets.

See the latest information about these tools on our website at **sei.cmu.edu/go/cwd-tools**.

About the SEI

The Software Engineering Institute is a federally funded research and development center (FFRDC) that works with defense and government organizations, industry, and academia to advance the state of the art in software engineering and cybersecurity to benefit the public interest. Part of Carnegie Mellon University, the SEI is a national resource in pioneering emerging technologies, cybersecurity, software acquisition, and software lifecycle assurance.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu