



Cyber Simulator Showcase

CERT Cybersecurity Workforce Development

Part 4 of 6: vTunnel and WELLE-D

Adam Welle
03 JUN 2019

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0578

vTunnel

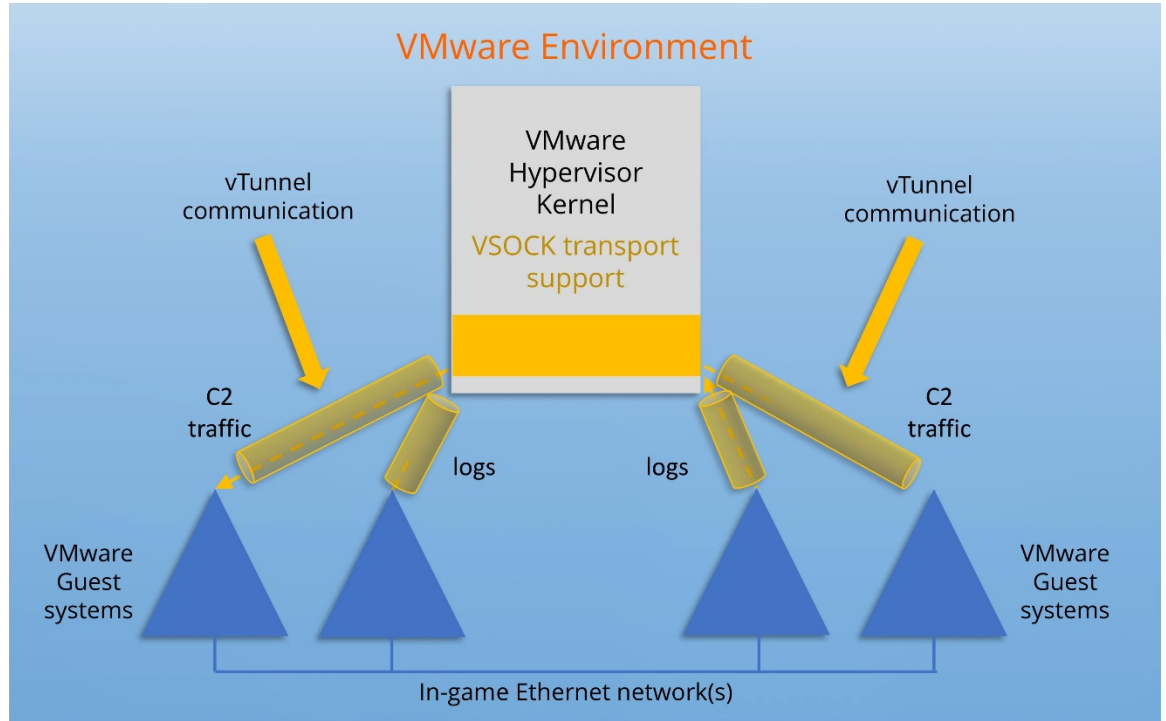
Adam Welle

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

vTunnel

Allows a tunnel to be established one way:

- Guest side to host side
- Host side to guest side



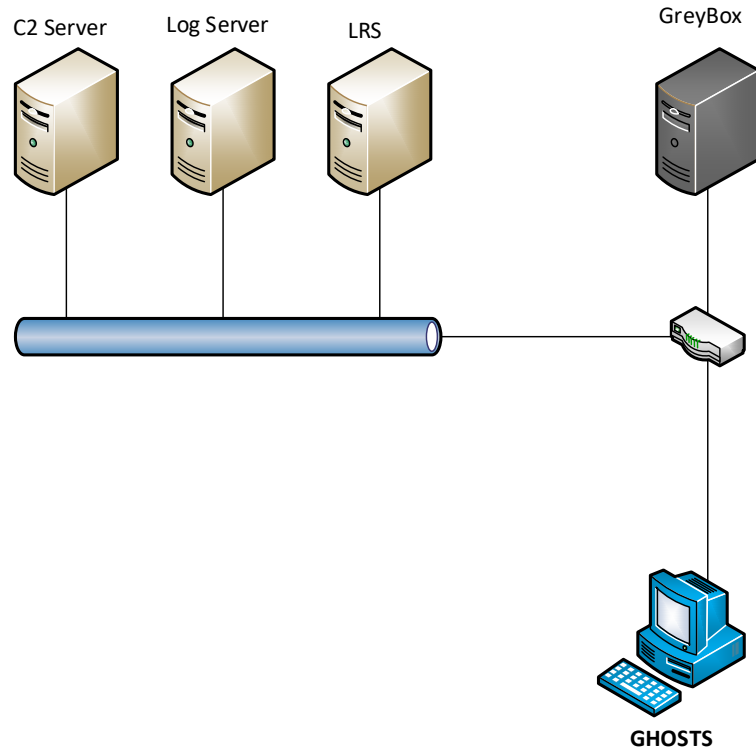
Range Management Traffic

Relies on networked applications

Injects activity into exercise

Logs network and system activity

Scores student actions

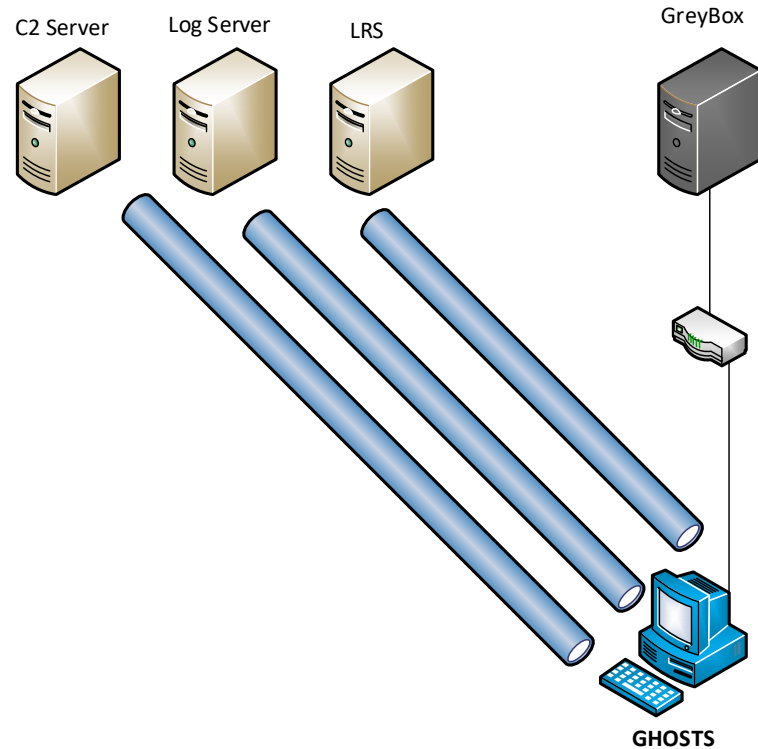


vTunnel

Tunnels IP traffic between guest and host networks

Uses VSOCK to transmit data via hypervisor

Traffic is hidden from participants



vTunnel

Disadvantages of in-game management traffic

- Participants can be tipped off to injects
- Participants can block the traffic
- Participants can manipulate the traffic

Advantages of using vTunnel to hide management traffic

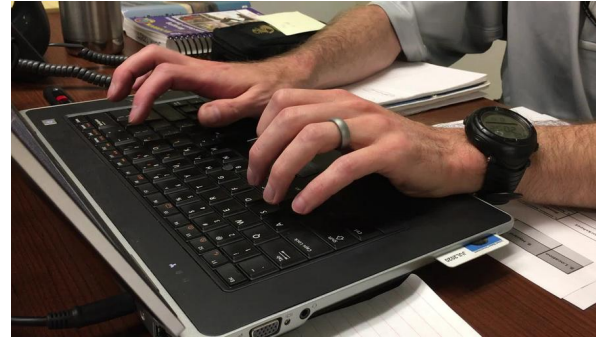
- Traffic in game stays on localhost
- Simplifies client configuration

vTunnel

Command and Control

- GHOSTS tasks
- Ansible configuration
- File copy

Allows system modifications

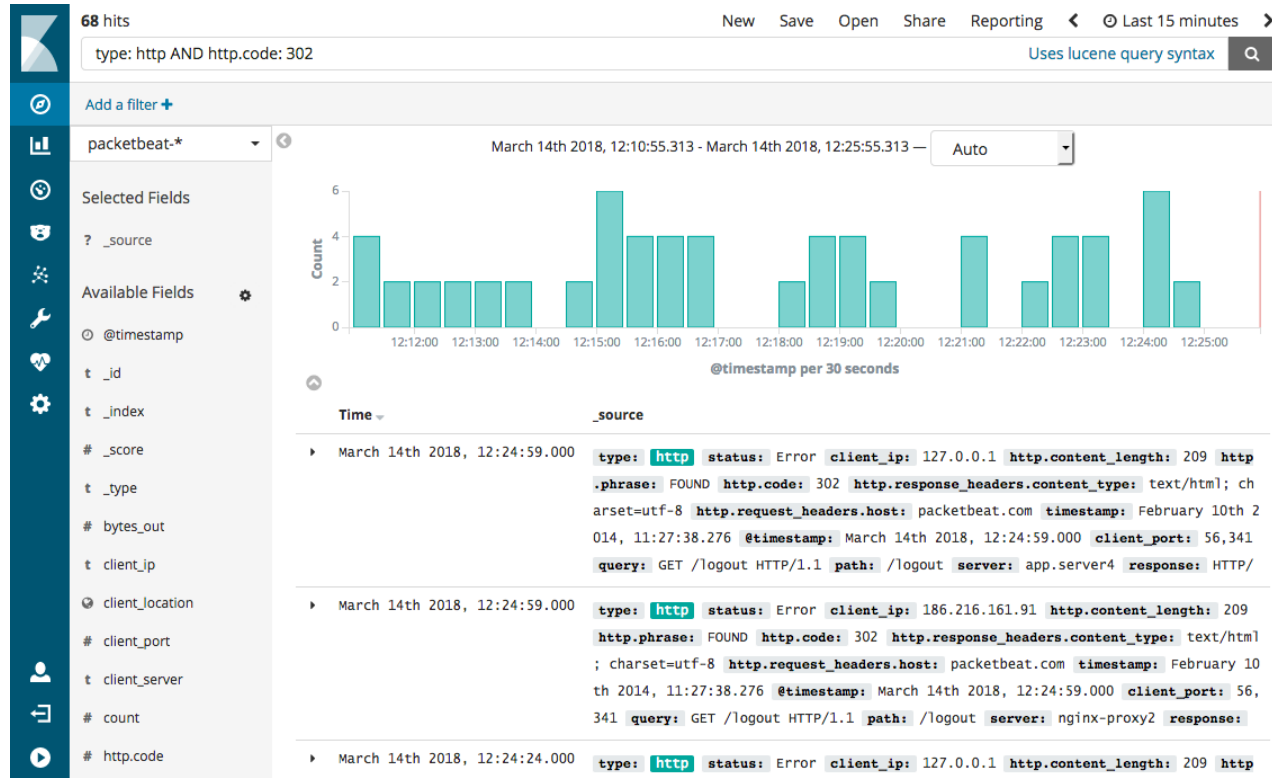


vTunnel

Logs

- Netflow records
- System logs
- GHOSTS results

Allows tracking of exercise performance



vTunnel

Student activity

- xAPI logs to LRS

xAPI

- Student activity
- Actor, Verb, Object

Learning Record Store

- Receives xAPI
- Multiple sources

```
{
  "version": "1.0.0",
  "actor": {
    "objectType": "Agent",
    "name": "Example User",
    "account": {
      "homePage": "http://example.com/moodle",
      "name": "1"
    }
  },
  "verb": {
    "id": "http://id.tincanapi.com/verb/viewed",
    "display": {
      "en": "viewed"
    }
  },
  "object": {
    "objectType": "Activity",
    "id": "http://example.com/moodle/course/view.php?id=1",
    "definition": {
      "type": "http://id.tincanapi.com/activitytype/lms/course",
      "name": {
        "en": "CMU Moodle Demo Course"
      }
    }
  }
}
```



WELLE-D

Wireless Emulation Link-Layer Exchange Daemon

Adam Welle

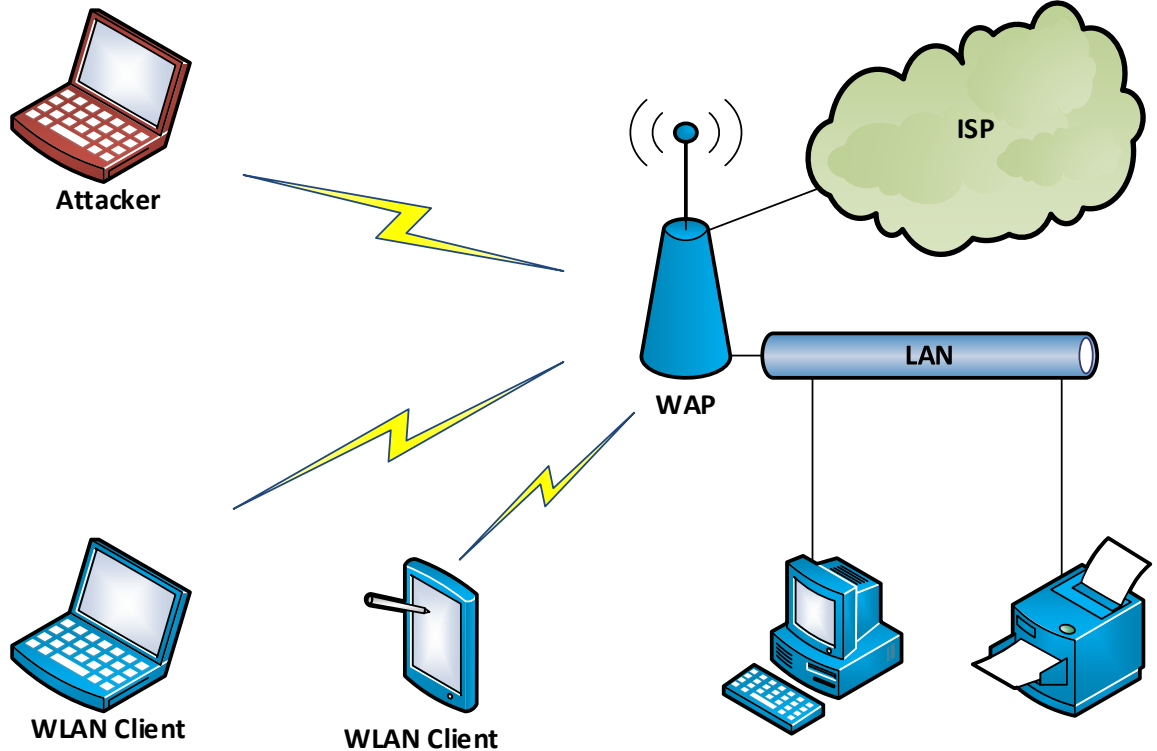
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Wireless Security Training

Cyber security training relies heavily on virtualization

But not for wireless training...

No native virtual wireless adapters



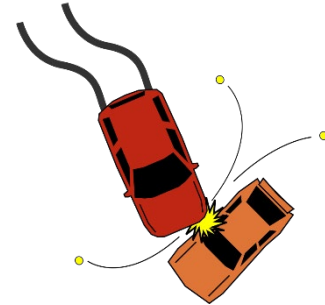
Problems with Physical Devices

Cost

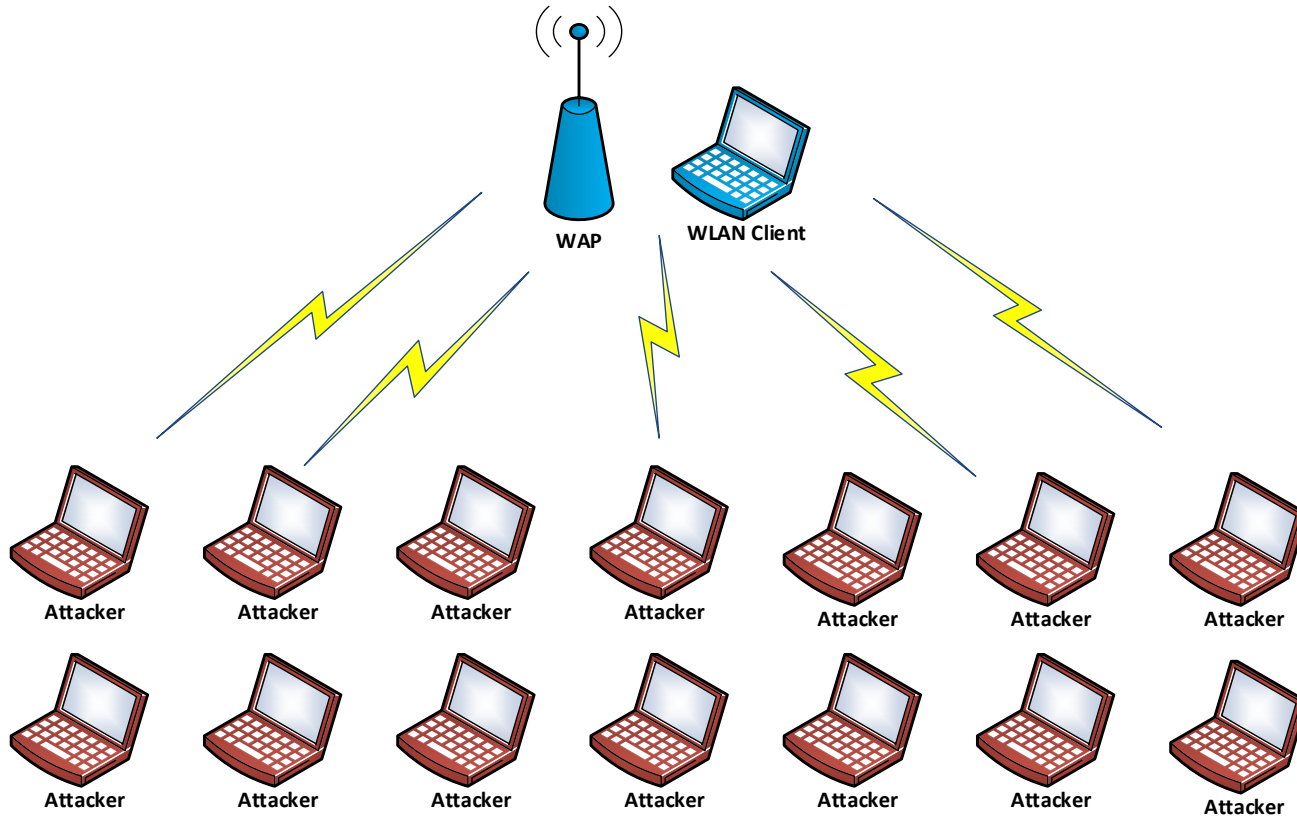
Time

Security Policy

Interference



Problems with Physical Devices



Advantages of Virtual Devices

Cost effective

Efficient

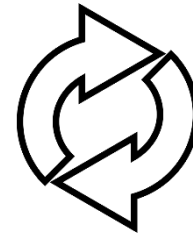
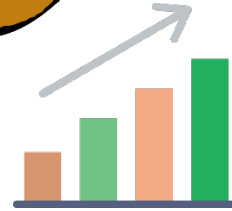
Compliant

Secure

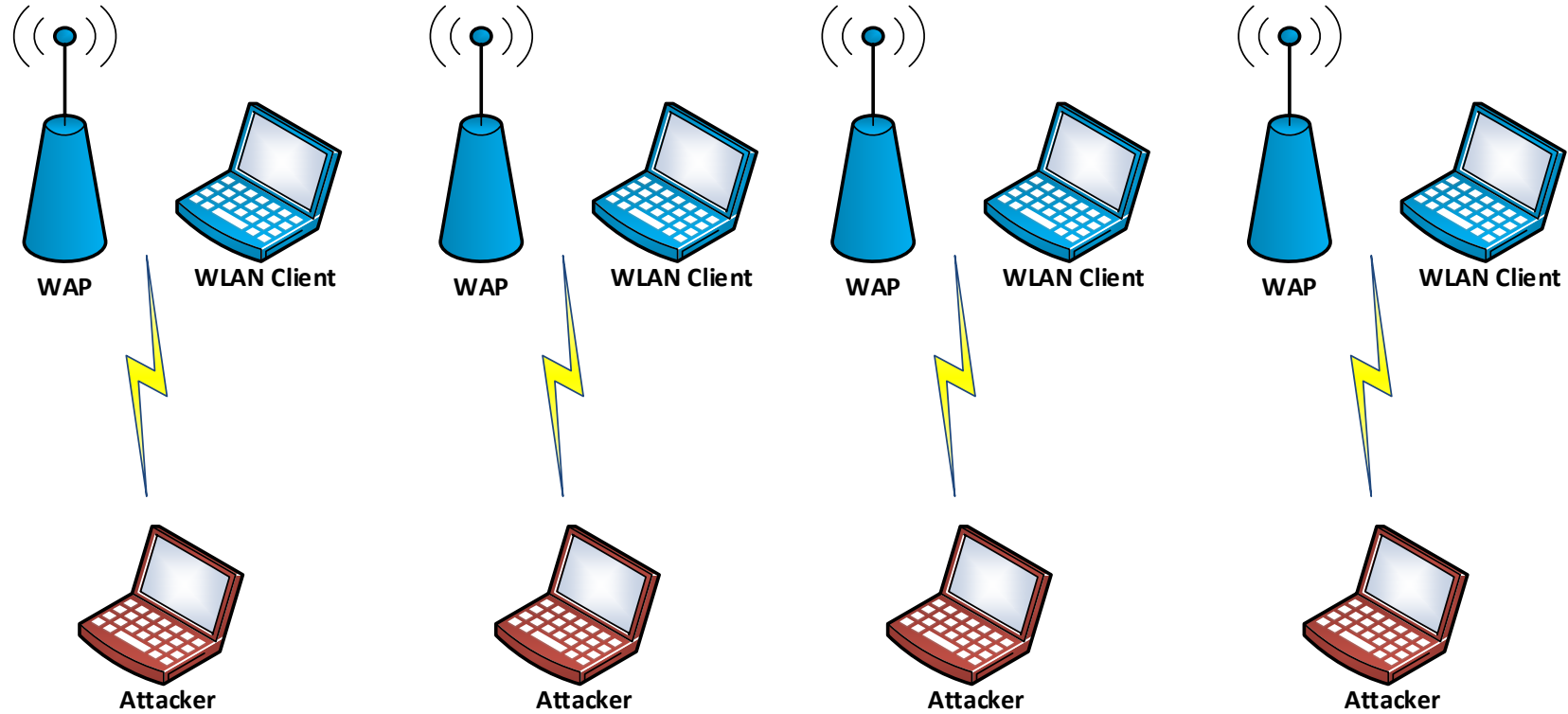
Scalable

Repeatable training

Enables distance education



Advantages of Virtual Devices



WELLE-D

Implementation

WELLE-D

Wireless Emulation Link-Layer Exchange Daemon

Leverages frames from mac80211_hwsim driver

Uses VSOCK to transfer frames

Simulates wireless medium

Provides GPS simulation

Enables high-fidelity use of full-featured operating systems

Open Source: <https://github.com/cmu-sei/welled>



WELLED

Wireless Emulation Link-Layer Exchange Daemon

```
[user@Fedora-WLAN ~]$ iwconfig
lo          no wireless extensions.

virbr0     no wireless extensions.

wlan0      IEEE 802.11  ESSID:"OpenWrt"
          Mode:Managed  Frequency:5.18 GHz  Access Point: 00:0C:41:00:00:00
          Bit Rate=6.5 Mb/s   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on
          Link Quality=47/70   Signal level=-63 dBm
          Rx invalid nwid:0   Rx invalid crypt:0   Rx invalid frag:0
          Tx excessive retries:0   Invalid misc:23   Missed beacon:0

virbr0-nic no wireless extensions.
```

WELLE-D

Wireless Emulation Link-Layer Exchange Daemon

Hosts

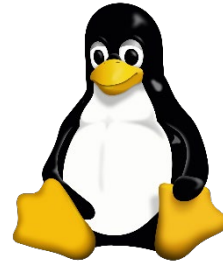
- Linux
- ESXi
- Windows

Linux Guests

- OpenWrt
- Fedora
- Android
- Ubuntu



OpenWrt
Wireless Freedom





WELLE-D

Implementation

Host Configuration

WMASTERD

Wireless Master Daemon

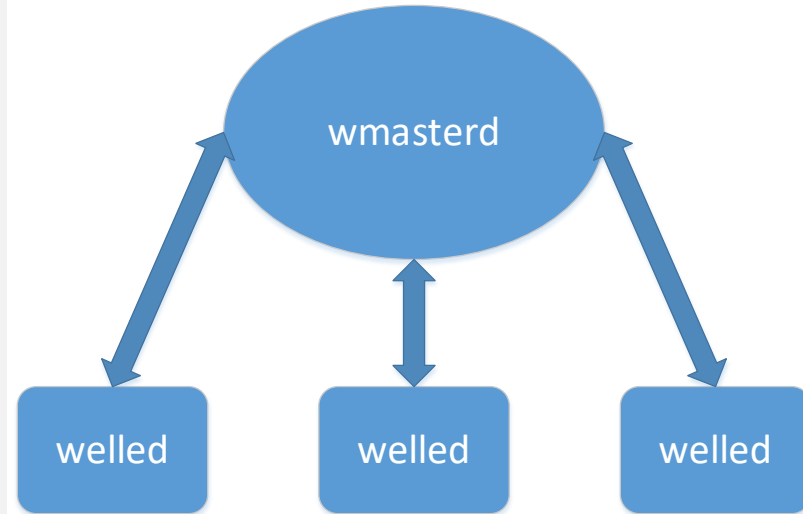
Receives frames from virtual machine nodes

Can calculate distance between nodes

Can produce GPS data as NMEA sentences

Enables simulation across multiple virtual machines

Isolates traffic from different users based on roomid



WELLE-D

Implementation

Guest Configuration

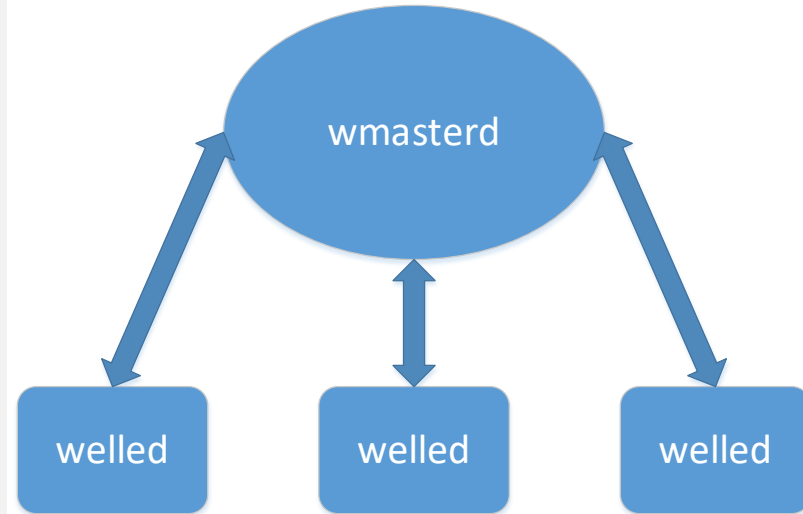
WELLED

Wireless Emulation Link-Layer Exchange Daemon

Receives frames from mac80211_hwsim,
transmits frames to wmasterd

Receives frames from wmasterd,
transmits frames to driver

Applies signal variations based on distance



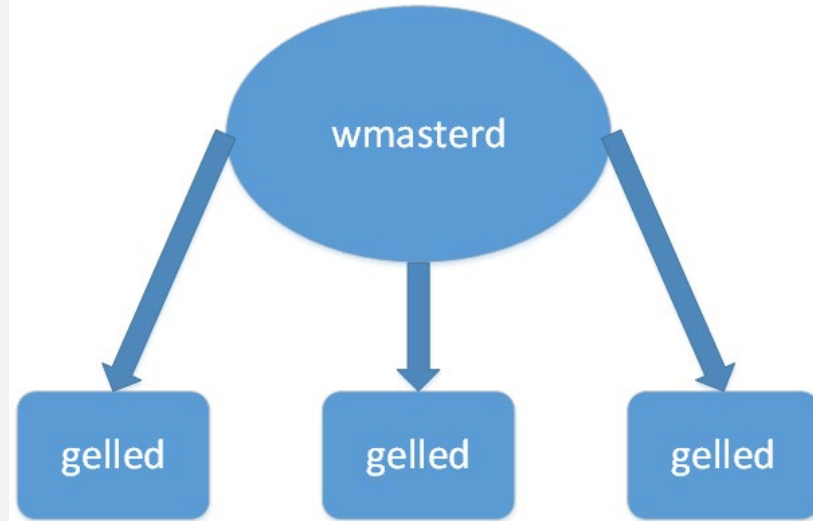
GELLED

GPS Emulation Link-Layer Exchange Daemon

Receives NMEA from wmasterd,
transmits NMEA to serial device

Allows GPSD to track location

Allows kismet to log network locations



GELLED-CTRL

GPS Emulation Link-Layer Exchange Daemon Control

Manipulates guest's GPS feed

Speed

Course

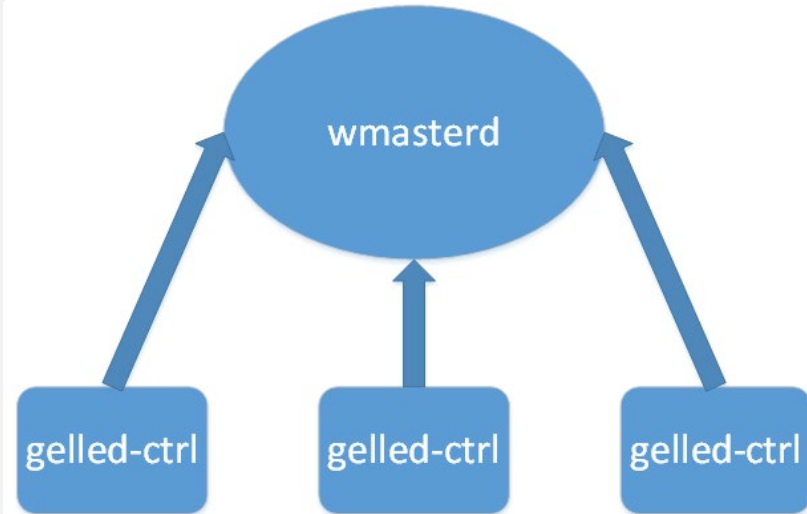
Climb

Follow

Latitude

Longitude

Altitude



GELLED-GUI

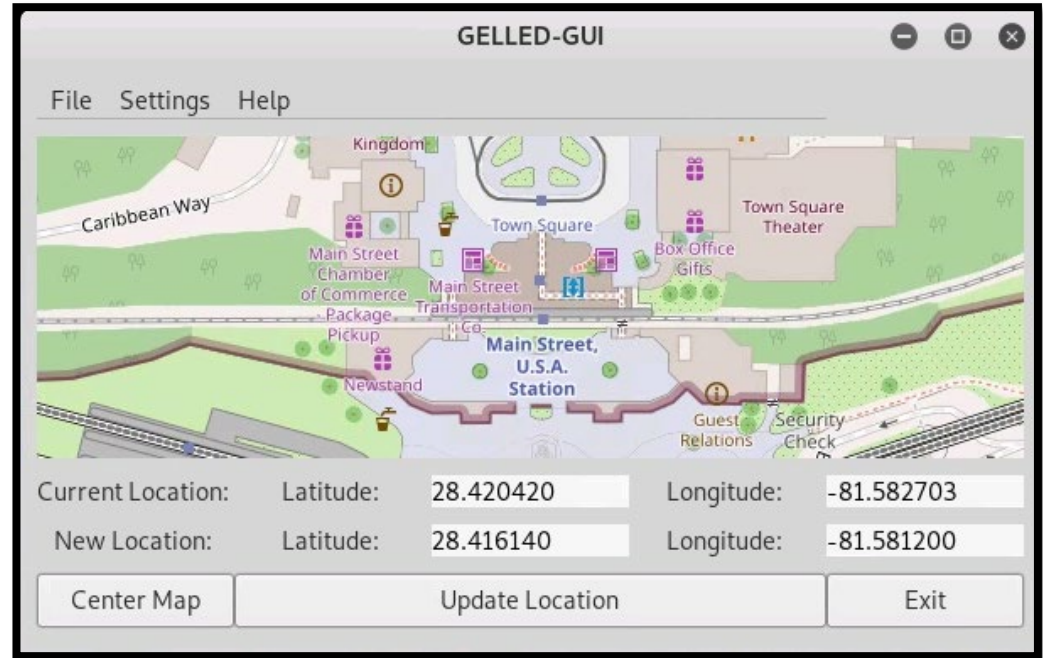
GPS Emulation Link-Layer Exchange Daemon GUI

Changes guest's position

Uses open street maps

Executes gelled-ctrl

Enables war driving scenarios



Training Scenarios

Wireless Monitoring with kismet/kismon

Wardriving with kismet/gelled-gui

Eavesdropping

WPS attacks

WPA2 deauthentication

MiTM attacks with evil twin

Rogue APs

Krack attacks

Wireless surveys

WPA Enterprise

WELLE-D Training Lab Overview

Investigating WELLE-D Configuration

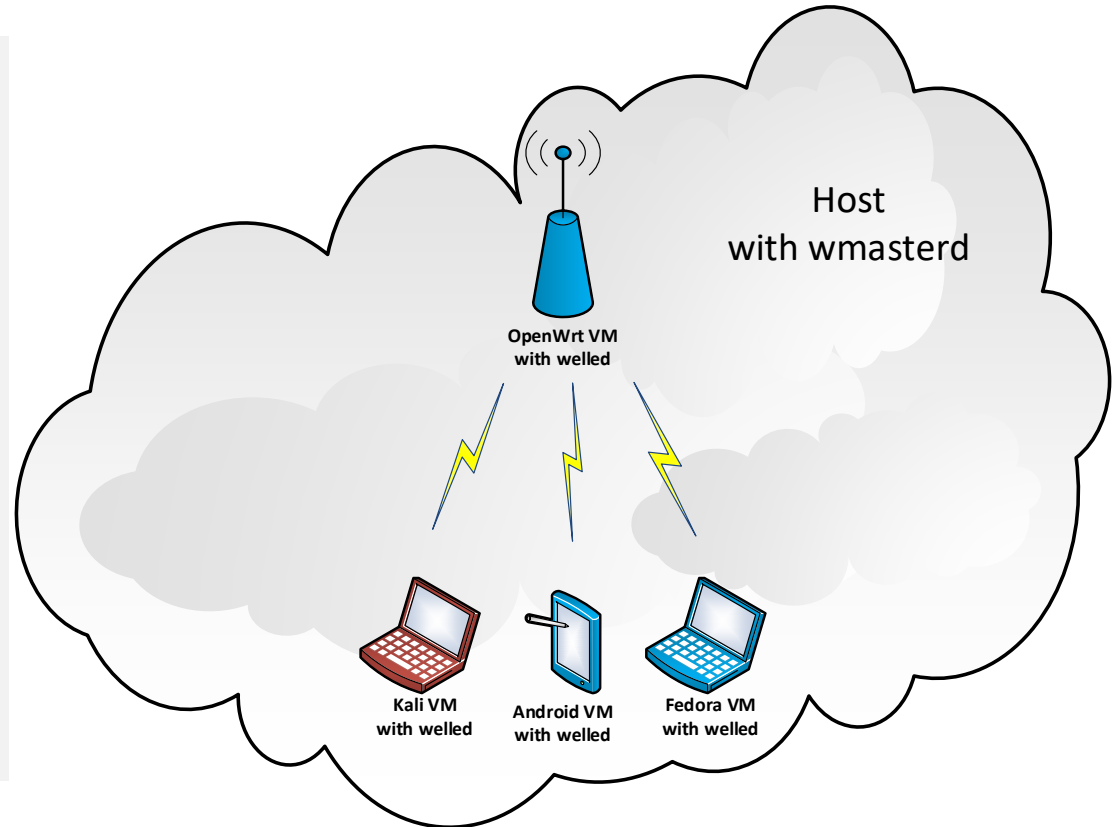
- wmasterd on host
- welled on Linux VMs

Performing a Wireless Attack

- Capture packets
- Perform deauthentication attack
- Perform dictionary attack
- Decrypt traffic

Wardriving Walt Disney World

- Run kismet and kismetmon
- Move VM using gelled-ctrl





Questions ?