Building an Isolated Wireless Lab Space on a College Campus

SDMAY18-15: The Iowa State Faradays

Alec Sauerbrei — Curriculum Lead | **Colin Ward** — Communications Manager | **Dalton Handel** — Networking Lead
Hope Scheffert — Git/Documentation Manager | **Omar Taylor** — Software Design Lead | **Tyler Much** — Physical Design Lead
Client/Faculty Advisers: Dr. Doug Jacobson and Dr. Julie Rursch

Introduction

Problem Statement

Currently wireless security courses utilize ***wired*** testing environments which generate "dummy" traffic so that students may observe and interact as if they are on a real network..

- Hard to scale
- Requires a lot of equipment
- Difficult to contain

Our Solution

Create an isolated wireless facility for coursework in wireless security

- Build a Faraday cage to encapsulate the networks
- Secure internal networks from the external campus network using a proxy server to prevent undesirable traffic from escaping into the wild
- Provide lab experiments to highlight the educational value of these isolated networks

Intended Users and Uses

- Students in wireless security courses at ISU
- Educational purposes only.

Requirements

Functional Requirements

1. Encapsulate 802.11 WiFi & GSM cellular networks
2. Isolate all internal and external network signals
3. Software Defined Radio (SDR) configured with OpenBTS to create a GSM network that will act as a cell tower
4. ONLY our Android phones accept and connect to the SDR as their cellular network
5. Cage environments available via virtual machines on a Linux server
6. Cage environments accessible off campus through VPN to the ISU network
7. Networks include "dummy" clients that autonomously generate network traffic.
8. Android phones configured with scripts to automate network traffic such as calling and texting each other over the SDR's GSM cellular network
9. Raspberry Pi 3 configured with scripts to automate network traffic such as sending/receiving emails and logging onto websites

Non-Functional Requirements

1. Curriculum delivered with the assembled environments
2. Hardware in the cage shall be accessible remotely
3. Cage shall fit next to linux server in the basement of Durham Hall or on the third floor of Coover Hall
4. Cage shall regulate airflow to prevent overheating

Operating Environment

- Requires the solution to incorporate remote access to the cage and it's isolated networks
- Utilize a server machine
- Cage must avoid producing too much heat, as this could be dangerous in an enclosed space
- The cage must be portable to be easily transferred to classrooms for students to use it directly

Engineering Constraints

- Must be affordable and easily replicable
- Must be remotely accessible
- Signals must not interfere with campus network
- Signals from outside and inside the cage should be isolated from each other

Most Relevant Standards

- IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012) - IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
- IEEE Std 1703-2012 - IEEE Standard for Local Area Network/Wide Area Network (LAN/WAN) Node Communication Protocol to Complement the Utility Industry End Device Data Tables
- GSM 04.08: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification"

Technical Details

Hardware

- Faraday Cage
  - Houses all of the wireless equipment
- ANTEC Server
  - INTEL Server Board S5500BC
  - 8 CPUs x Intel Xeon CPU E5606 @ 2.13GHz
  - 32 GB RAM
  - Running ESXi Hypervisor
- 2 Raspberry Pi 3's
  - Generates WiFi network traffic
- NI USRP-2920 Software-Defined Radio
  - Acts as a cellular tower
- Linksys AC1200+ Wireless Router
  - Broadcasts internal WiFi network
- 2 Samsung Galaxy J3 unlocked phones
  - Generates cellular network traffic
- Netgear N300 USB Adapter
  - Sniffs the WiFi traffic

Software

- ESXi 6.5
  - Hosts VM's within virtual networks
- OpenBTS
  - Software-based GSM access point
- GSM scripts
  - Simulate traffic on a cellular network
- WiFi scripts
  - Simulate traffic on an 802.11 based network
- Virtual Machines
  - Kali Linux - Student - Learning
  - Kali Linux - Admin - Configuration
  - pfSense - Router
  - Ubuntu 64-Bit 16.04 - SDR Configuration

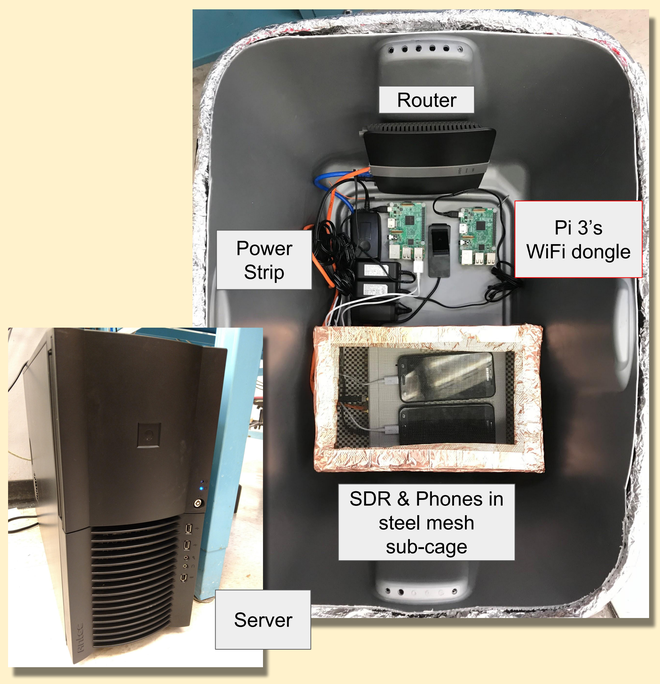
Design Approach

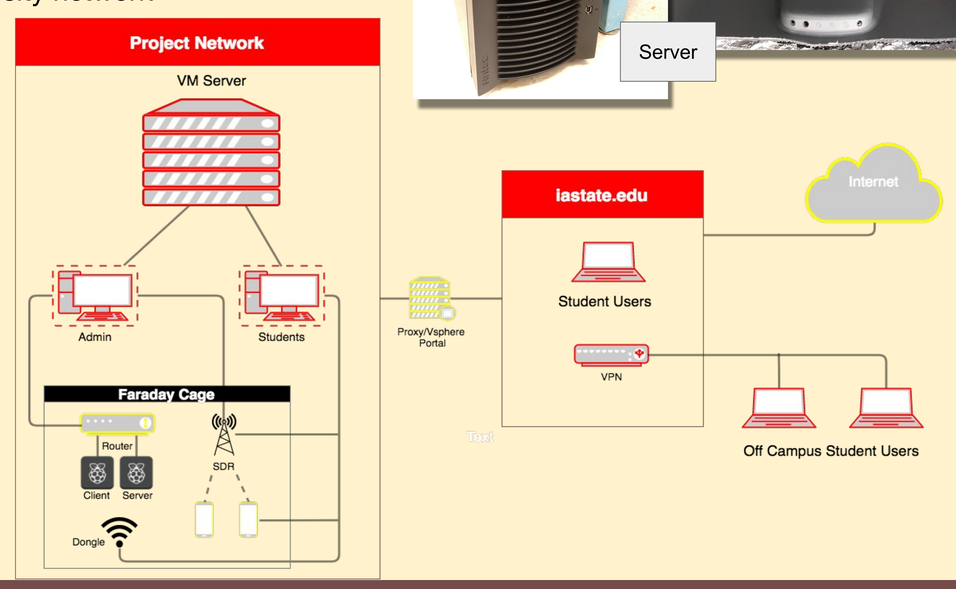
Cage Design

The Faraday cage is designed as a 2 ft x 3 ft plastic container with a removable lid. Inside, the container is completely lined with six layers of heavy duty aluminum foil. Then--to avoid the components touching the foil and boosting their signals--an additional container of the same dimensions was placed inside. The outside of this container was sprayed with MG Chemicals SUPER SHIELD Nickel Conductive Coating aerosol spray for further signal blocking strength. The 1mm steel mesh material was built as a sub-cage surrounding only the SDR and phones because through testing it was found that this material was only effective for blocking the cellular signals. A power strip is placed between the two containers so that all components can be plugged into this, and only one cord is fed outside the cage versus six.

Network Design

- Server
- Router to broadcast the isolated 802.11 WiFi network
- WiFi dongle that does the WiFi traffic sniffing
- 2 Raspberry Pi 3's that simulate traffic
- Software Defined Radio (SDR) which acts as a cell tower and a GSM sniffer
- 2 Android phones that simulate GSM traffic
- Accessible via VMs on the Iowa State University network

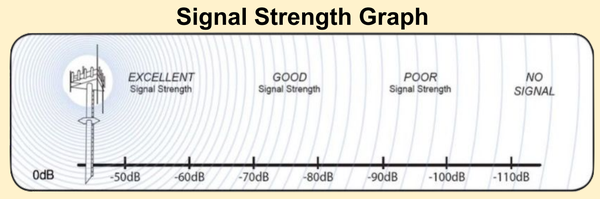




Testing

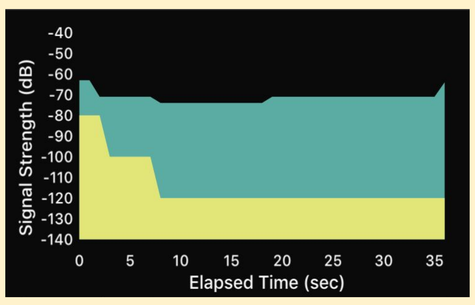
Environment

- Senior design lab
- Within the Faraday cage
- Inside the Faraday room in Coover Hall



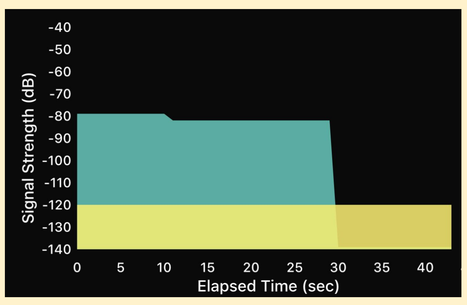
Strategies

Test	Passed (✔/X)
Failure to contact devices inside the cage	✔
WiFi network does not allow any devices outside of the cage to connect	✔
GSM network does not allow any cell phones outside of the cage to connect	✔
Achieving at least -110 dB in signal strength measurement (no effective signal)	✔



Test with only the steel mesh sub-cage shows the robustness of GSM signal blocking (in yellow) which dropped 40 dB

Though not its purpose, it also helps 2.4GHz signal blocking.



Test on blocking signal between router in cage and device outside
(WiFi signal in teal)

The lid to the cage was placed at 10s, after 20 seconds the signal was lost completely.