# Building an Isolated Wireless Lab Space on a College Campus

Team 15
Client/Advisors: Doug Jacobson & Julie Rursch
Team Members/Roles:
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
Team Email: sdmay18-15@iastate.edu
Team Website: http://sdmay18-15.sd.ece.iastate.edu/

Revised: 9/22/17 Version 1

# Table of Contents

# 1 Introduction

## 1.1 Acknowledgments

Special thanks to Dr. Julie Rursch and Dr. Doug Jacobson for the proposal, guidance, and funds to complete the project. We would also like to thank ETG for assistance with parts and components to build our faraday cage.

We would also like to acknowledge Dakota State University for sharing their initial ideas and experiences with us so that we can reproduce and build upon their original work.

## 1.2 Problem Statement

Connecting cell phones, tablets, laptops, and desktops to a network is commonly done through wireless access. Many times these connections are not secure and/or can be easily monitored or intercepted. While we can somewhat replicate simple wireless scenarios in a lab for students, it involves a great deal of equipment and the overlap of the wireless channels makes it difficult to set up more than a few wireless access points for students to work with. Further, wireless connections can be accidentally used by unsuspecting innocents as they connect with real world communication and that traffic finds itself on the laboratory wireless network being sniffed.

The proposal is for the creation of wireless facility to be created for graduate coursework in wireless security. This wireless network would require creating a Faraday cage around the wireless equipment such that only those in the labs could connect to it and additionally that it would be secured from the campus network using a proxy server so that undesirable traffic would not escape into the wild.

## 1.3 Operating Environment

The faraday cages will likely be stored in a cabinet or other closed space in a room. This requires our solution to incorporate remote access to the cages and their isolated networks. Our first design of the network requires that we utilize a server machine, which could potentially extend our environment outside the lab room. Another possible requirement may be that they avoid producing too much heat, as this could be dangerous in an enclosed space. The cages must be portable to be easily transferred to classrooms in order to be used with students directly.

## 1.4 Intended Users/Uses

This project was proposed so that students in wireless security courses at Iowa State can safely learn about network security. Intended users are students enrolled in said wireless security classes as well as professors and teaching assistants. The intended use is for educational purposes only.

## 1.5 Assumptions and Limitations

Assumptions:

1. The maximum number of simultaneous users will be the size of a typical class (~50).
2. All users will have Iowa State credentials.
3. The cage will properly ventilate heat when running for long periods of time.

Limitations:

1. The system must be accessible from the Iowa State network.
2. The system must be physically connected to an Iowa State Linux server.
3. A finite number of devices will be able to be used inside each cage

## 1.6 Goals

The goal of this project is to build two portable faraday cages for use as part of security labs in future classes. Inside one cage, a network will be set up consisting of a wireless access point with multiple clients sending traffic to each other to simulate a real network. The second cage will be similar, but instead contain a cellular network. The networks will be impossible to connect to from outside of the cage except through a single point which is designed to allow students to observe and learn about the traffic generated in the cage.

Part of this project includes the development of curriculum regarding how to use these cages in labs for students. The goal of this portion is to create lab exercises that are clear, concise, and informational--but also interesting for students.

# 2 Deliverables

By the end of second semester, two cages will be built with one blocking wifi signals and the other blocking cellular signals. There will also be curriculum developed for exactly how they can be used in labs, including a proof of concept so that other curriculum can be developed for them in the future.

# 3 Design

The wireless faraday cage will consist of a router to broadcast the isolated wifi network that is configured with a proxy to separate it from the Iowa State network, a wifi dongle that will do the sniffing, and two Raspberry Pi's to simulate traffic. The cellular faraday cage will consist of a software defined radio (SDR), also configured with a proxy, which will act as a cell tower and a sniffer, and two android phones which will simulate traffic. In order to access these environments, students must VPN to the Iowa State network and access a virtual machine.

Refer to Section 3.2 for the proposed network diagram.

## 3.1 Previous Work/Literature

Individuals from Dakota State University have been developing a product similar to the cellular faraday cage proposed here. They have shared ideas regarding what they have used in their faraday cages such as their cellular base station, what phones have worked in the cage for simulating traffic, and some hurdles that still need to be overcame. This is the message received by the advisor of the project on what they have accomplished thus far:

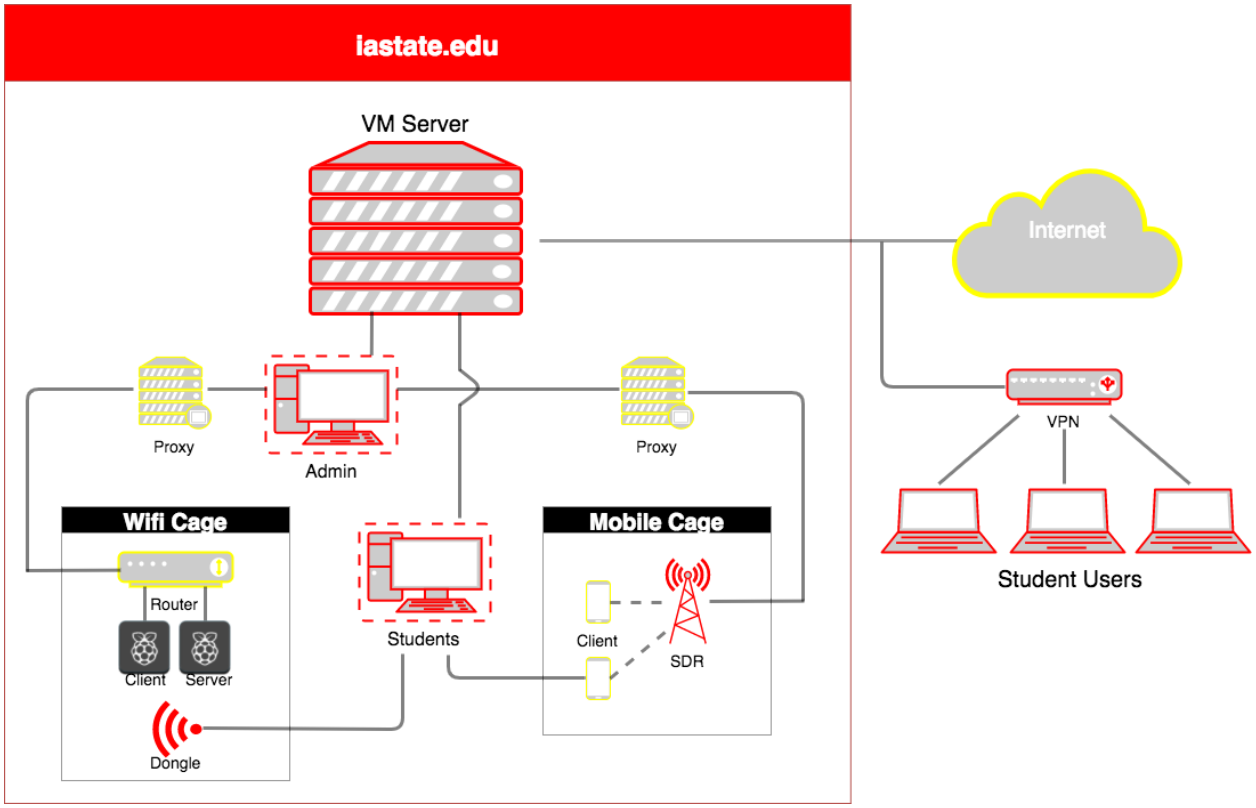
- Cellular basestation: For us, we use OpenBTS with an Ettus B200 radio. It works great, but there are many challenges to getting the software setup. I'm happy to help/provide a VM that's preconfigured if you'd like too! There are other radios, both made by Ettus Research and others that will work, but the B200 has been the most cost effective and functional. This is the one side that we have tested/implemented and it works great!

- Phones: Some phones are better than others for actually connecting. Many students with Android phones can easily connect onto the new cellular network without any configuration or hardware changes. Those with iPhones will not be able to connect without replacing the SIM card in their phones with ones that are pre-configured. Most 2G/GSM style phones should function otherwise though

- Isolation: this is always the biggest worry—making sure the signals aren't going out into the wild. In our on-classroom setups, we generally remove the antennas from the radios, which limits the range. The problem is that the cellphones have a very high powered radio that will reach a great distance. For our final version of the lab (where it will be accessible to others from the internet), we're working on faraday cages. We've experimented with ones like this: http://ramseytest.com/product_list.php?category=1&series=1 they work pretty good but they're small and don't scale well for what we need. There's also the issue of heat dissipation if you have a lot of gear crammed in there. What we're ending with is having a custom server rack built for us by HM Cragg (out of Minneapolis), that will be able to

handle the servers and store the equipment while allowing ventilation (or so their specifications say!).

## 3.2 Network Diagram




## 3.3 Assessment of Proposed Methods

The physical manifestation of the wireless laboratory is the primary point of debate amongst design topics. There are two present options: having the system statically connected to a server in the basement of Durham Hall, and having a mobile lab that can used anywhere on campus. Actually connecting the faraday cages to a server in the basement of Durham Hall may be farfetched. It would likely have the benefits of proper environmental control for the machines to run safely in, but it is possible to have this perk in a mobile environment as well. Instead, it may be more realistic to have the cages be portable and relocate them from lab to lab as necessary. This would require having a router added to the system to connect the VM server to the iastate.edu network.

## 3.4 Validation

To confirm that the solution works, each lab exercise developed will be executed to ensure clarity and ease of operation. It will be proven that the network inside the cage cannot be

connected to by a device outside of it except from the access point designated for the curriculum.

# 4 Project Requirements/Specifications

## 4.1 Functional Requirements

1. Software Defined Radio (SDR) configured with OpenBTS to use with cellular communication
2. 2 faraday cages: 1 configured for 802.11 signals, and 1 configured for cellular network signals.
3. Both faraday cages must isolate their respective signals from the outside world.
4. Active dummy environments: Each contained environment will need to have a number of clients and servers that autonomously generate network traffic. An example of these environments can be seen in the network diagram.
5. Environment Components:
    a. Software Defined Radio
    b. Cell phone(s) (2 or more)
    c. Router
    d. Raspberry Pi 3(s) (used as wireless clients)

## 4.2 Non-Functional Requirements

1. Curriculum is to be delivered in tandem with the assembled environments to be used in lab.
2. The hardware is assembled in a way that allows it to be used with all of the delivered curriculum.
3. The hardware is accessible remotely.

## 4.3 Risks

This project comes with a very clear risk: if the faraday cages do not isolate their networks, students could unintentionally sniff public wireless and cellular traffic. To manage this risk, extensive testing will be done to ensure that no signals are allowed in or out of each cage.

## 4.4 Standards

Since our project involves interfacing with and allowing external access to the Iowa State network, we will be ensuring the security is on par to the standards used by Iowa State. Also, as the project itself involves creating safe environments for wireless security learning, the

environments will be tested to make sure that no real personal data can be compromised during a lab session.

# 5 Challenges

This project brings on a few challenges. A faraday cage is something that can be purchased or built. For earlier prototypes, it makes sense to build a cage for testing. This requires acquisition of materials needed to physically build the cage. There are also several components that must safely fit inside of each cage as well as wires which must connect devices inside the cage to devices outside the cage. Finally, a discussion with IT about setting up a proxy and obtaining access to an existing server will be needed.

# 6 Timeline

## 6.1 First Semester

- Completed Project Design
- Completed Component List
- Education goals outlined for the curriculum piece
- Functioning faraday cage for both WiFi and cellular signals

## 6.2 Second Semester

- Curriculum outlined for necessary courses
- Hardware accessible via VPN (off campus, remote)
- Working prototype
- (Stretch goal) Completed lab material (10-12 labs) for each necessary course

# 7 Conclusions

Over the next two semesters, the team will design, prototype, test, finalize, and finally develop curriculum for the proposed isolated networks. While some of us are comfortable with either networking, security, prototype building, or making curriculum, none of us are a jack of all trades. Each of us will have to learn what it is we can do, and when to ask for help.

# 8 References

The main source of advice and ideas come from a team from Dakota State which is working on a similar faraday cage to isolate cellular signals.

# 9 Appendices