Building an Isolated Wireless Lab Space on a College Campus

Design Document

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: 12/4/17 Version 2

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. The team also appreciates Dr. Mani Mina's advice and suggestions for signal blocking techniques and materials.

Additionally, Dakota State University should be credited and thanked for sharing their initial ideas and experiences to help with the reproduction and expansion upon their original work.

1.2 Project Statement

Currently, wireless security courses here at Iowa State University utilize wired testing environments which generate “dummy” traffic so that students may observe and interact as if they are on a real network. This method is hard to scale, requires a great deal of equipment, and is also difficult to contain. Therefore, the proposed solution is for the creation of an isolated wireless facility for graduate coursework in wireless security.

In order to isolate these networks, a Faraday cage must be created which encapsulates the equipment such that only authorized users can connect to it. Additionally, these networks would be secured from the campus network using a proxy server so that undesirable traffic would not escape into the wild, and outside traffic will not be visible in the cage. Another part of the project is to provide curriculum in the form of lab experiments which will be developed to highlight the educational value of these isolated networks.

1.3 Purpose

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 existing courses can somewhat replicate simple wireless scenarios in a lab for students, it involves a great deal of equipment. Overlap of the wireless channels also makes it difficult to set up more than a few wireless access points for students to work with. Further, these 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.

By creating these isolated networks, the possibility of sniffing the traffic of innocent bystanders is eliminated and a simple environment for students to learn about wireless security is created. Professors will be equipped with a strong learning tool that can always be expanded upon by creating realistic scenarios in these mini environments and allowing students to observe and even play along. The cage will create an opportunity to learn about cellular networks, which have yet to be explored in existing courses at Iowa State University.

1.4 Operating Environment

The Faraday cage will likely be stored alongside the existing closed network laboratory equipment used in current courses. This requires the solution to incorporate remote access to the cage and it's isolated networks. The network design requires that the team utilize a server machine, which could potentially extend the environment outside the lab room. Another requirement is that the cage avoids 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.

1.5 Intended Users/Uses

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

1.6 Assumptions and Limitations

Assumptions:

1. The maximum number of simultaneous users will be the size of a typical lab session (24).
2. All users will have Iowa State University credentials.
3. The cage will properly ventilate heat when running for long periods of time.
4. The cage will be directly accessible by TAs and professors.

Limitations:

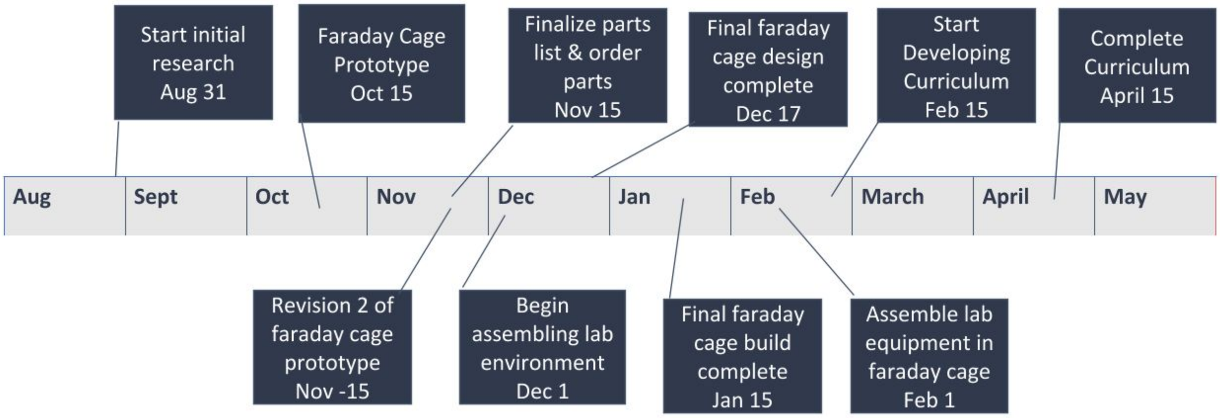
1. The system must be accessible from the Iowa State University network.
2. The system must be physically connected to an Iowa State University Linux server.
3. A finite number of devices will be able to be used inside the cage.
4. The cage will be built for the functionality that the curriculum requires, if those plans change in the future they will still have to abide by the physical limitations of the cage.

1.7 Goals

The goal of this project is to build a portable Faraday cage for use as part of network security labs in future classes. Inside the 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. It will also contain a Global System for Mobile Communications (GSM) 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 the cage in labs for students along with a proof of concept on how the cage works. The goal of this portion is to create lab exercises that are clear, concise, and informational--but also interesting for students. The cage and it's components will be modular and new labs should be able to be implemented quickly and painlessly.

1.8 Deliverables


Start initial research Aug 31
Faraday Cage Prototype Oct 15
Finalize parts list & order parts Nov 15
Final faraday cage design complete Dec 17
Start Developing Curriculum Feb 15
Complete Curriculum April 15
Aug
Sept
Oct
Nov
Dec
Jan
Feb
March
April
May
Revision 2 of faraday cage prototype Nov -15
Begin assembling lab environment Dec 1
Final faraday cage build complete Jan 15
Assemble lab equipment in faraday cage Feb 1

A Faraday cage will be built which blocks wifi and cellular signals. There will also be curriculum developed for exactly how it can be used in labs, including a proof of concept so that other curriculum can be developed for it in the future. Ideally, 10-12 labs will be created of varying difficulty and covering both 802.11 and GSM network security.

2 Specifications and Analysis

2.1 System specifications

2.1.1 Functional Requirements

1. The cage shall encapsulate an 802.11 WiFi network as well as a GSM cellular network.
2. The cage shall isolate all signals from the outside world and block any outside signals from connecting to the enclosed network.

3. The Software Defined Radio (SDR) shall be configured with OpenBTS to create a GSM network that will act as a cell tower for the labs.
4. The Android phones inside the cage shall accept and connect to the SDR as their cellular network. No other phones shall accept and connect to the SDR.
5. Cage environments shall be available via a virtual machine on the Linux server.
6. Cage environments shall be accessible off campus through VPN to the Iowa State University network.
7. Each network shall include “dummy” clients that autonomously generate network traffic. An example of these environments can be seen in the network diagram.
8. The Android phones shall be configured with scripts to automate network traffic such as calling and texting each other over the SDR’s GSM cellular network.
9. Each Raspberry Pi 3 shall be configured with scripts to automate network traffic such as sending/receiving emails and logging onto websites.

2.1.2 Non-Functional Requirements

1. Curriculum shall be delivered in tandem with the assembled environment to be used in lab.
2. Hardware shall be assembled in a way that allows it to be used with all of the delivered curriculum.
3. Hardware in the cage shall be accessible remotely.
4. Cage shall fit next to an existing linux server in the basement of Durham Hall or on the third floor of Coover Hall.
5. Cage shall regulate airflow to prevent overheating.

2.1.3 Standards

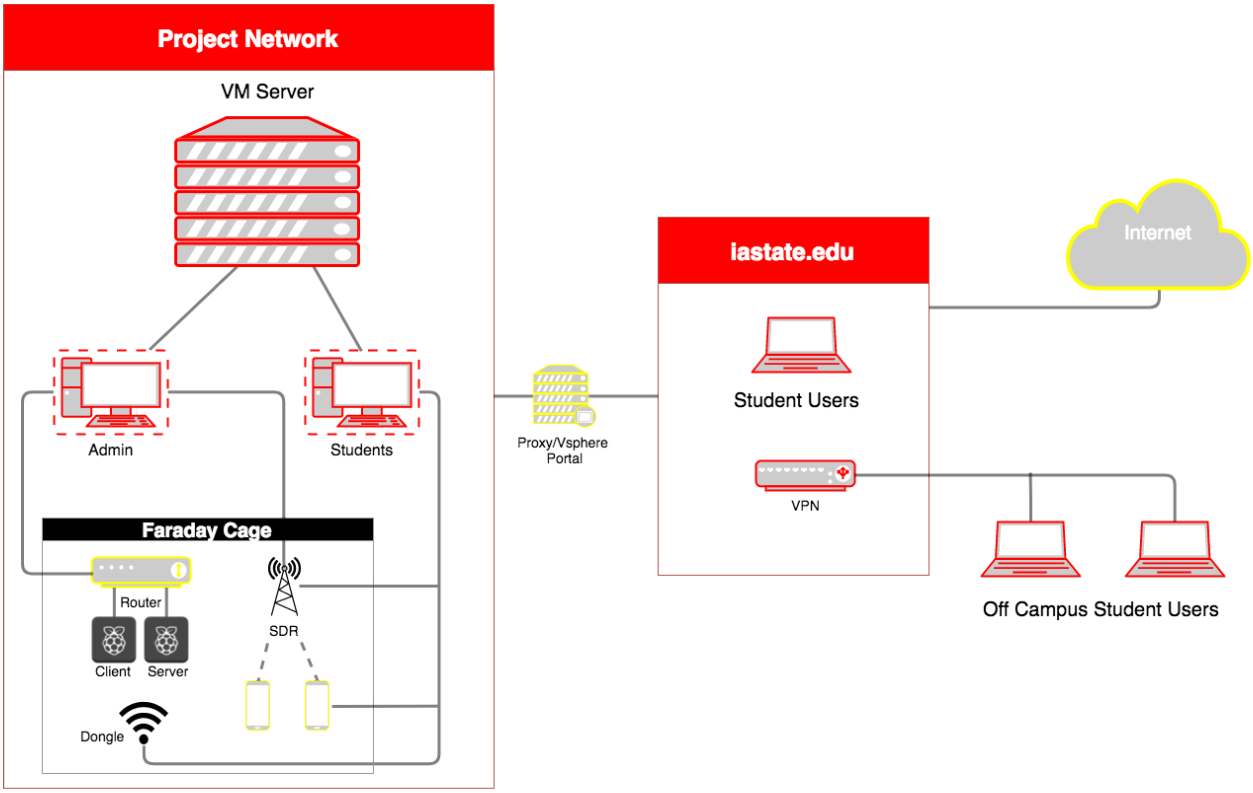
Because this project involves interfacing with and allowing external access to the Iowa State University network, the team will be ensuring that the security matches the standards used by Iowa State University. Also, as the project itself involves creating safe environments for wireless security learning, the environments will be tested to make sure that no real personal data can be compromised during a lab session.

The cage itself will be tested to block the standard wavelengths for 802.11 (2.4 GHz) and GSM (300-2500MHz) communications.

Curriculum will be developed to the standards of the client-advisors so that it may serve as an effective tool for learning. Packet parsing labs will be developed for both the wireless and cellular networks.

2.2 Proposed Design/Method

The Faraday cage consists of a router to broadcast the isolated WiFi network that is configured with a proxy that separates it from the Iowa State University network, a WiFi dongle that does the sniffing, and two Raspberry Pi 3's that simulate traffic. It also consists of a software defined radio (SDR), also configured with a proxy, which acts as a cell tower and a sniffer, and two Android phones that simulate traffic. In order to access these environments, students must VPN to the Iowa State University network and access a virtual machine. The diagram below illustrates the design described above.



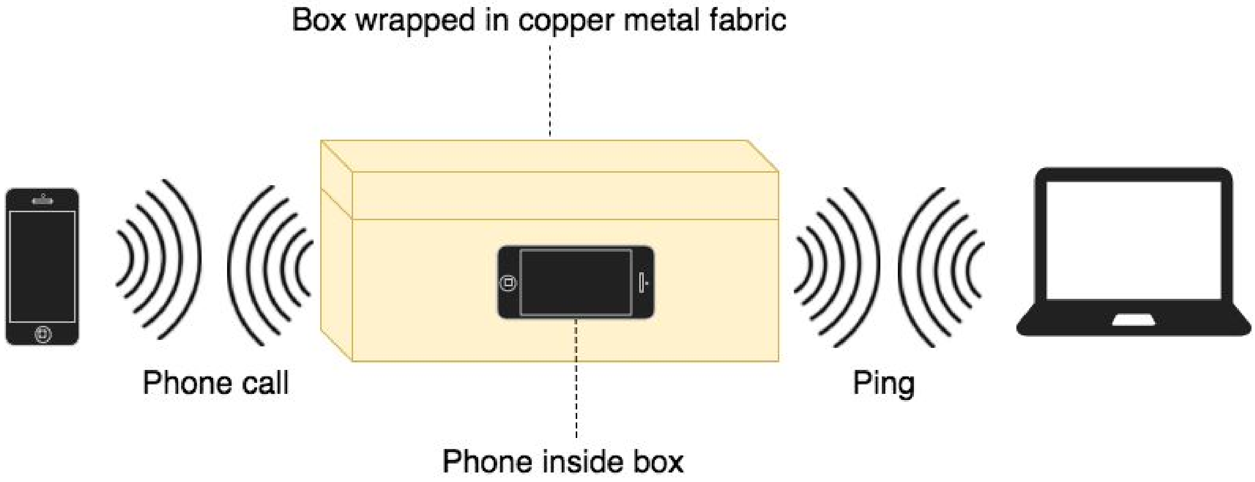
The Faraday cage is designed as a two foot by three foot plastic container with a removable lid. Inside, the container is completely lined with a copper metal fabric designed to block frequencies as well as two layers of heavy duty aluminum foil.

An issue arises when considering the way the wires are routed from the inside of the cage through a drilled hole to feed outside of the cage. The concern here is that some signals may escape through the drilled holes and reach the wild--which is exactly what is to be prevented by this project.

2.3 Design Analysis

2.3.1 Initial Prototype

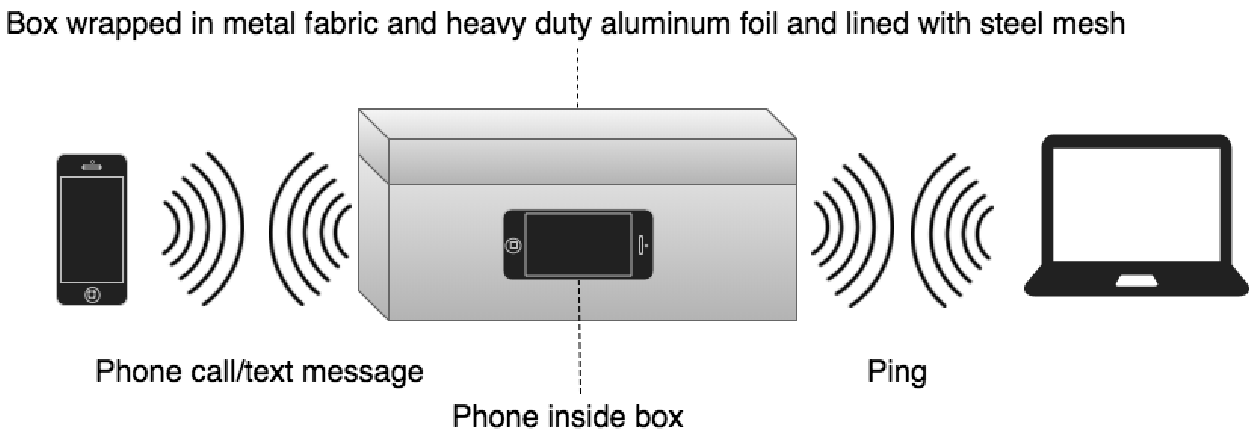
After receiving a sample of the Faraday fabric, it was wrapped and secured around a shoebox to create an extremely simple initial prototype. On October 12, simple tests were conducted with a cell phone in the box and it was determined that, unfortunately, the fabric alone may not be enough to adequately block all signals. Refer to section 4.1 for the detailed results. However, the team has considered that another layer of the fabric may increase the blocking power and lead to a better solution. Below is a diagram of the initial prototype and tests.



Despite how easy it was to create this prototype, it doesn't address the main concern. The cage must house equipment and successfully route wires from inside the cage out to the wild without also letting signals escape. The team will need to construct another prototype that feeds wires out of the box to get an idea of how difficult it will be to keep signals inside.

2.3.2 Reinforced Prototype

Due to the lack of signal blocking of the initial prototype, the team reinforced it with additional signal blocking materials. Firstly, pieces of steel metal mesh were stapled to the inner walls of the box. This only slightly improved the blocking power. After speaking with Mani Mina, the team wrapped the box with one layer of heavy duty aluminum foil, as he suggested. This has significantly improved the signal blocking, leading the team to believe this is the design to be used for the final cage. Below is a diagram of the reinforced prototype and tests. Refer to section 4.2 for test results.


Box wrapped in metal fabric and heavy duty aluminum foil and lined with steel mesh
Phone call/text message
Phone inside box
Ping

3 Testing and Implementation

3.1 Interface Specifications

The cage must be accessible remotely via VPN on the Iowa State University network and connect to a set of virtual machines on a Linux server. Preemptively, around 50 virtual machines will be needed to support the desired curriculum. However, the design emphasizes the ability to support more students if needed. These will be orchestrated using VMware Vsphere. In order to service this, the host server will require 32 GB of RAM and 64 processors. The cage must have a physical connection to the server. The server will have one VM for the cage. This will be used for network configuration and provide the activity within the cage.

The cage will route mobile traffic through an SDR being controlled by an Ubuntu Server 14.0 virtual machine. This will require an ethernet connection from within the cage to the VM server. This server can control the throughput of the traffic being routed through the SDR’s, thus allowing the network to be malleable to support different amounts of devices if needed.

3.2 Hardware/Software

3.2.1 Hardware

The most important part of these tests is the prototype Faraday cage that blocks all other signals from entering the enclosed environment. This “cage” can be simply a shoebox wrapped with signal blocking fabric, or it can be a more durable solution such as a plastic container.

Both the software defined radio and the wireless router are needed to broadcast network signals within the cage.

The cage will have two Raspberry Pi 3's and two Android phones. These components are vital to the testing phase because they are responsible for creating the traffic for these environments. These networks are useless to observe if no traffic is being generated on them.

3.2.2 Software

In order to observe and interact with these networks, one must access a virtual machine on an Iowa State University server.

There will be a set of scripts to autonomously generate network traffic so that students have packets to sniff. Raspberry Pi scripts may include logging onto websites such as Facebook or sending emails. Android phone scripts may include calling and texting the other phone to simulate a real cellular network.

The virtual machine will be equipped with Wireshark, a popular network protocol analyzer. This will be used extensively in testing to observe packets sent over the networks.

3.3 Functional Testing

With respect to cage testing, the procedure will be simple. Once a prototype is finished, the wireless and cellular components will be placed inside. The team will then attempt to contact the devices inside to see if the signals are being sufficiently blocked.

Further, the cage needs to successfully trap its own signals. This means that the wifi network broadcasted within the cage should not be accessible or even visible from outside the cage. To test this, the team will stand next to the cage and see if they can see the SSID of the cage's router. This test would especially fail if they were able to connect the the network inside the cage.

Similarly, the cage should not allow any bystander to connect to its cellular network. In fact, failure to isolate the SDR's signals would mean breaking the law, as it is a *spoofed* cell tower. Because this test is so critical, the team will be using the Faraday room on the third floor of Coover Hall to test the cage until they are sure it is completely secure. This room already blocks signals from the outside world, so it will be a great testing environment. The cage will be placed in the room and signals will be monitored closely. If there are any signals in the room, it is safe to say that the cage is not sufficiently trapping it's signals. Even if this happens, there will be no risk of those signals escaping the room, as it is itself a Faraday cage.

Android phones will be rooted in order to gain administrator privileges, then they will be connected to the SDR's GSM network. The scripts should automate calling and sending SMS text messages and will be first tested outside of the cage to ensure expected behavior.

In order to test that the networks are generating sufficient traffic, the team will access the environments through virtual machines and use Wireshark to sniff packets, just as students will be doing in future labs.

3.4 Non-Functional Testing

Students must log in to the Iowa State University network via VPN in order to access the virtual machines, therefore security is not a main concern. VPN access will be tested using team member Iowa State University credentials. If these tests are successful then it is sufficient for other student access. Access will be tested on and off campus, as this should cover all possible connection use cases that students will experience.

If students are trying to learn through observation of these networks, it is important that they produce enough traffic in a sufficient timeframe. It is a team goal that there will be network traffic to observe at all times. This way, students avoid having to wait for the chance to sniff packets and perform other lab exercises.

Once labs are developed, at least two team members will complete each lab and ensure that the instructions are clear, the content is helpful and educational, and the environment develops adequate traffic for the purpose of the lab.

3.5 Modeling and Simulation

While this project does not require much modeling, there is the challenge of simulating an active wireless environment. These simulations will change based on what the purpose of the given lab curriculum is. On a basic level, the network traffic will be simulated using custom shell and python scripts that will transmit packets within each cage.

3.6 Implementation Issues and Challenges

As stated many times, the challenge of this project is creating a cage that will completely trap it’s own signals in while blocking all others. The first prototype was not as successful as the team had hoped, but the second was more promising. Nonetheless, precaution is needed when designing the final product to ensure two secured networks.

Another interesting challenge will be creating scripts for Android phones to automate phone calls and SMS text messages. This topic is not all that common, so it requires some research and experimentation. Currently, the best option is the custom Android app, which, when active, will send SMS and make phone calls based on a timer. This is not ideal, however. The team is still researching other ways to automate this traffic.

4 Results

4.1 Initial Prototype

The initial prototype is simply a shoe box wrapped with copper metal fabric that was designed to block signals.

The first test was to place a cell phone in the box and call it. When the phone rang, it caused the team to stop and think why the cage wasn’t doing it’s job. After some thought, the conclusion was that the cellular connection was extremely strong because of the proximity of the cell tower. After simply walking around the corner about ten yards away, the phone does not ring.

The second test was to ping the IP address for the same phone while it was inside the box. At first, the phone was responding, so the box was moved about ten feet away. Although it took a few seconds, sure enough, the phone stopped responding to the pings. From there, the lid was taken off of the box and again--after a few seconds--it was responding as expected. This was tested a few times and it was found that there is a 3-10 second delay for the signals to be blocked after fully enclosing the phone in the box. Further, it only worked when the box was roughly ten feet from a wireless access point.

This makeshift shoe box “Faraday cage” has only one layer of copper metal fabric surrounding it. The team has decided to obtain more of this material and see if another layer will improve its signal blocking power.

4.2 Reinforced Prototype

The Reinforced Prototype builds off of the initial design and uses the same box structure. Steel mesh was added to the inside of the box and heavy duty aluminum foil was wrapped over the existing metal fabric.

Identical tests were performed on this prototype. The big difference with these results is that while the phone is in the box, an incoming call does not go through. Similarly, the phone does not respond to pings. The real win, however, is that an existing call will be dropped when the phone is put inside the box. This was something that the first prototype could not quite handle. Another benefit is that the time taken for the phone to stop responding to pings or to drop a phone call has dropped to only 2-5 seconds.

The team is very pleased with these results and has decided that this is the general design to be used for the final cage.

5 Conclusion

Over the next two semesters, the team will design, prototype, test, finalize, and finally develop curriculum for the proposed isolated networks. The team has currently created and tested their initial and reinforced prototypes and have modified their designs accordingly.

The team has decided that a plastic container lined with metal fabric and heavy duty aluminum foil is be the best solution to house the components and isolate these networks from the outside world. The container offers the a simplistic design very similar to the prototypes. A hole will be drilled at one corner of the container in which all cables will be routed through. It also allows for easy component access with the removeable lid and is sturdy enough to avoid any damage to the inner equipment.

These environments are extremely useful in educational settings. With the construction of this cage and automated scripts to generate traffic, students will be able to observe and learn about wireless and cellular network security without worrying about breaking the law. The ability to manipulate the cellular network alone is very valuable because this is not legal in the real world. The team hopes that professors at Iowa State will utilize this cage and the created lab exercises in the near future. It is exciting that this small proof of concept gives professors the option to build upon their curriculum to include GSM network security or even experiment with the interaction between WiFi and GSM networks.

6 References

Information regarding GSM networks was obtained from

- Cai, Jain, and D.j. Goodman. “General Packet Radio Service in GSM.” *IEEE Communications Magazine*, vol. 35, no. 10, 1997, pp. 122–131., doi:10.1109/35.623996.
- *GSM World Coverage Map and GSM Country List*, www.worldtimezone.com/gsm.html.

The team has consulted with Dr. Mani Mina at Iowa State. Dr. Mina is an Electrical Engineering professor who has worked with signal blocking in the past.

7 Appendices

Figure 1: Project Timeline

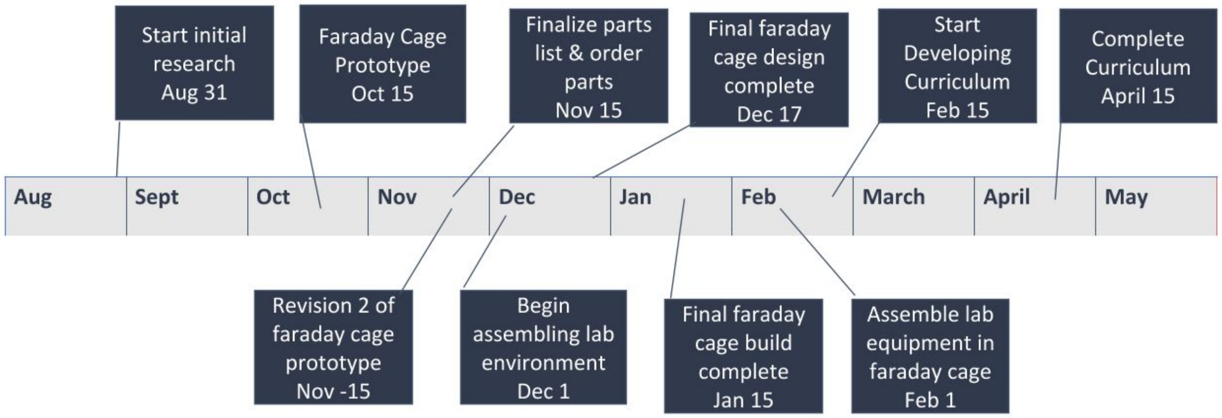

Start initial research Aug 31
Faraday Cage Prototype Oct 15
Finalize parts list & order parts Nov 15
Final faraday cage design complete Dec 17
Start Developing Curriculum Feb 15
Complete Curriculum April 15
Aug
Sept
Oct
Nov
Dec
Jan
Feb
March
April
May
Revision 2 of faraday cage prototype Nov -15
Begin assembling lab environment Dec 1
Final faraday cage build complete Jan 15
Assemble lab equipment in faraday cage Feb 1

Figure 2: Proposed Network Diagram

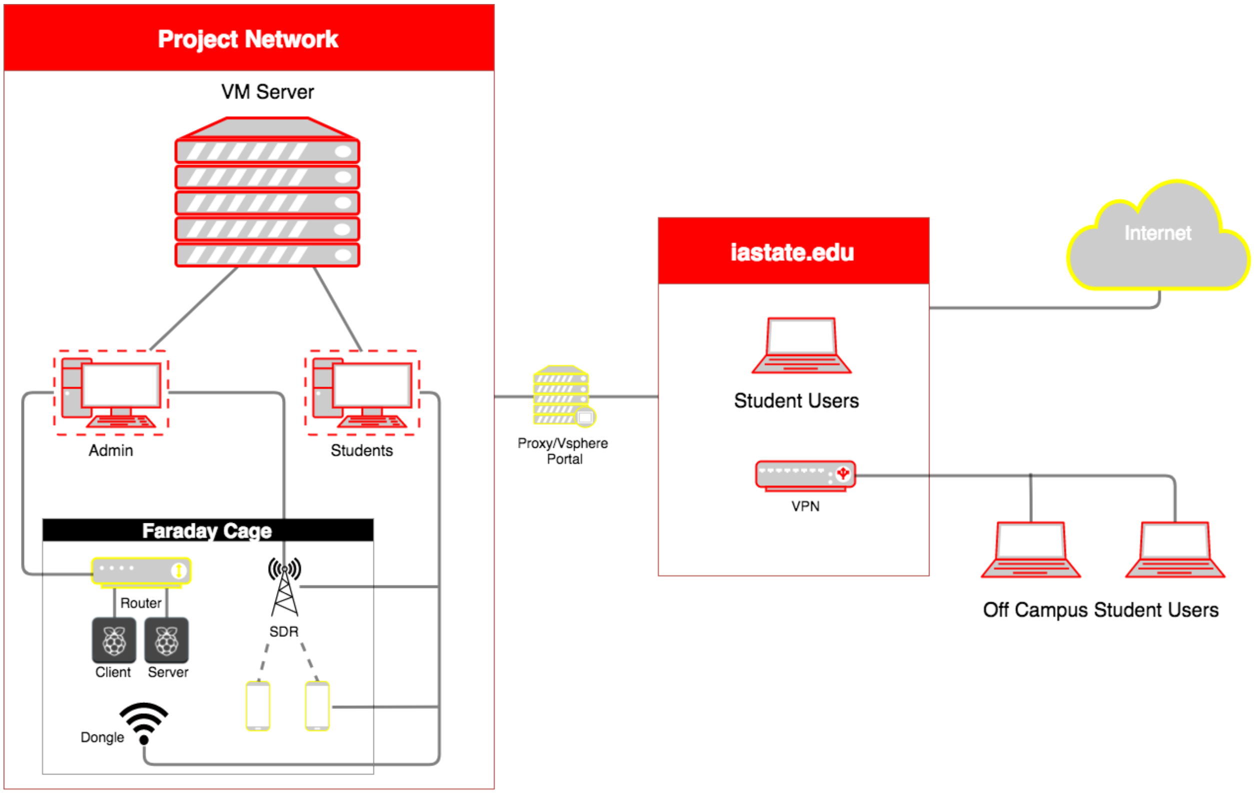


Figure 3: Initial Prototype Diagram

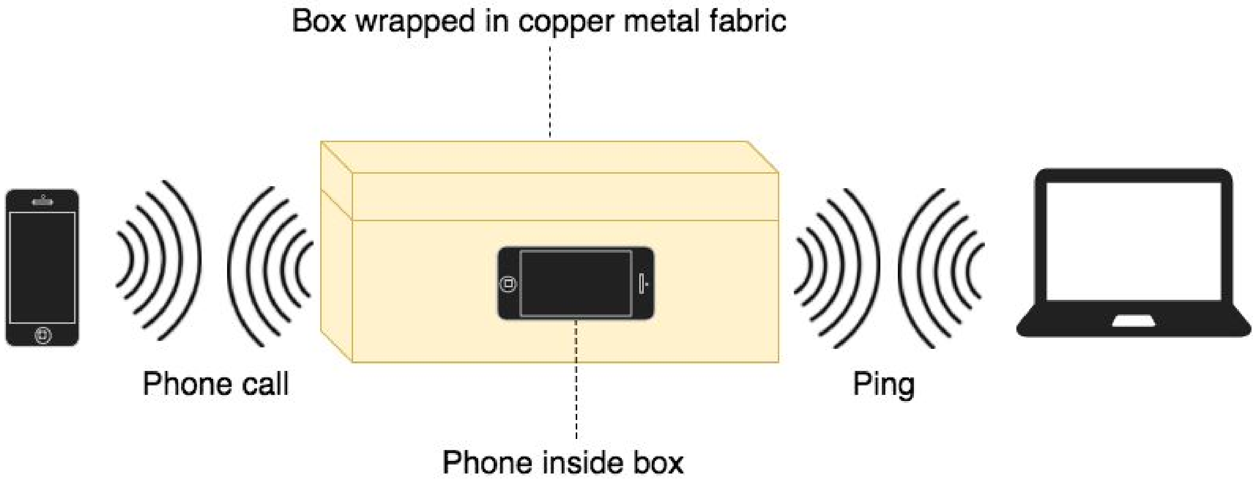
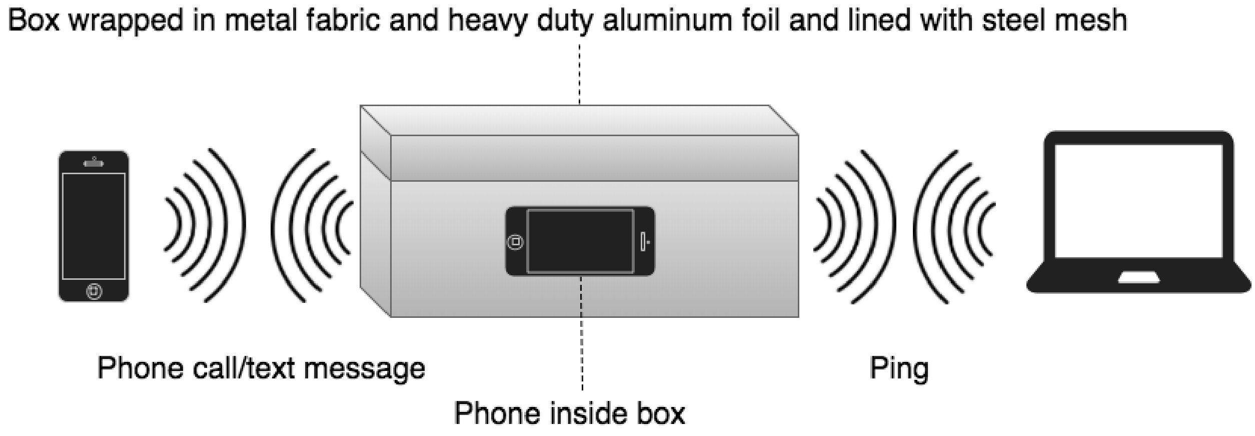


Figure 4: Reinforced Prototype Diagram


Box wrapped in metal fabric and heavy duty aluminum foil and lined with steel mesh
Phone call/text message
Ping
Phone inside box