Building an Isolated Wireless Lab Space on a College Campus

Project Plan

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 3

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. 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 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.

1.4 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.

1.5 Assumptions and Limitations

1.5.1 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.

1.5.2 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.

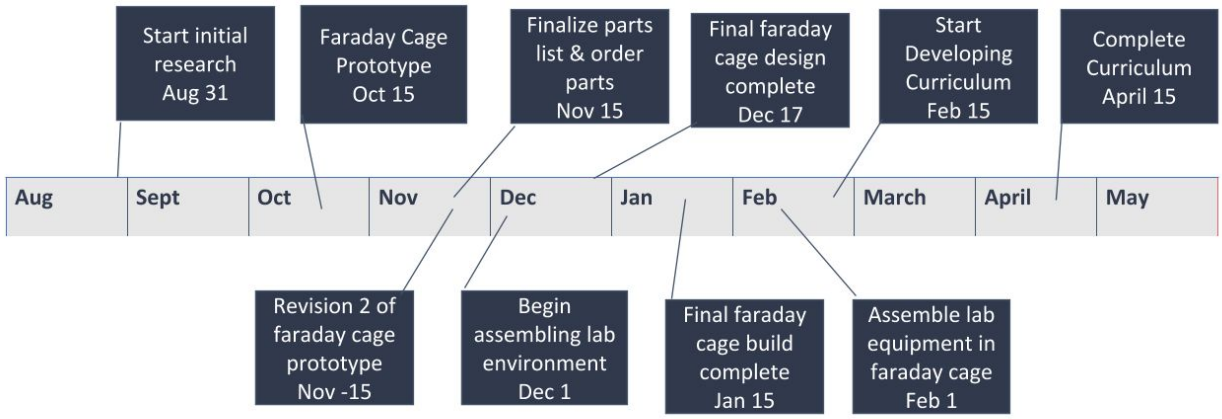
1.6 Goals

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.

2 Deliverables

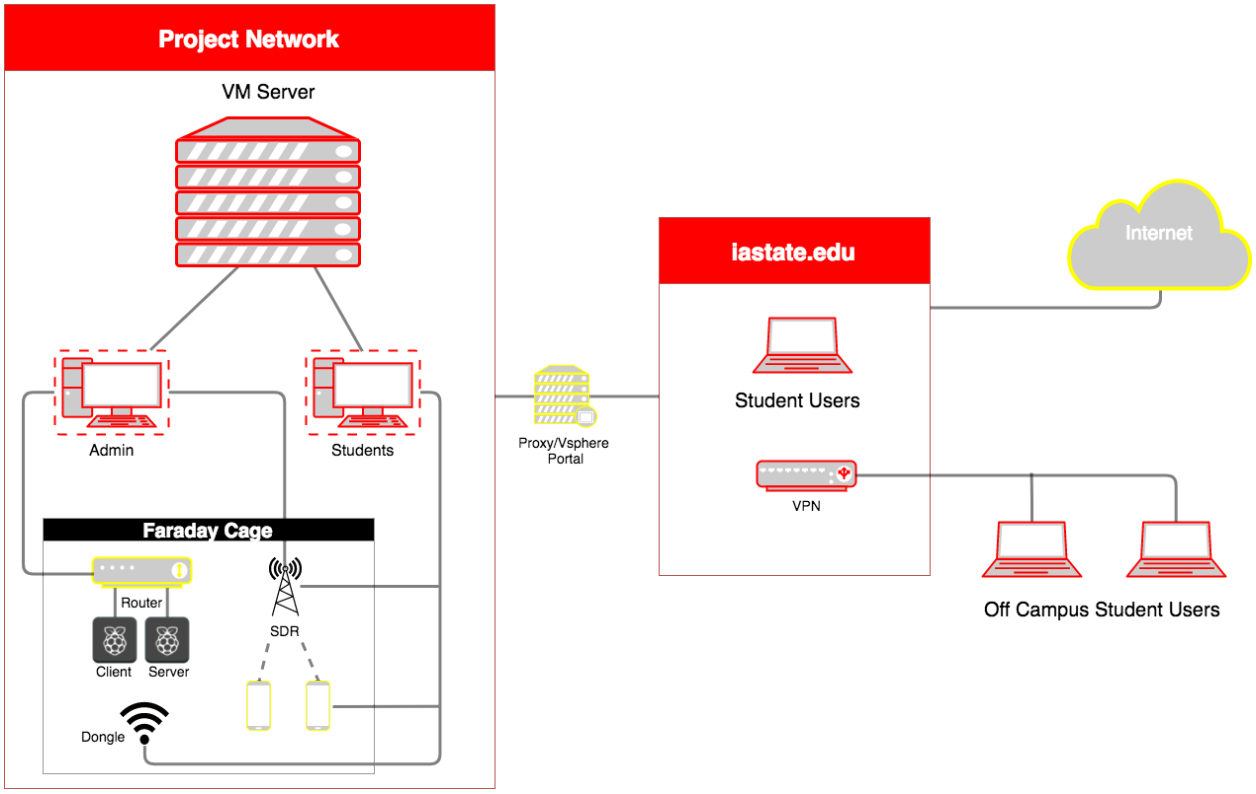
Timeline for major deliverables is as follows. General steps include researching, acquiring parts, and prototyping designs. In the second semester the team will look to finalize the products.



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.

3 Design

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 the 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. Administrators will also have access to the router and SDR. The diagram below illustrates the design described above.



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 cage such as its cellular base station, what phones have worked in the cage for simulating traffic, and some hurdles that still need to be overcame. Below lists information received by the advisor of the project in early September.

- Cellular basestation: They use OpenBTS with an Ettus B200 radio. It works well, but there are many challenges to getting the software setup. They are happy to help/provide a preconfigured VM.
- 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.
- Isolation: In their in-classroom setups, they generally remove the antennas from the radios, which limits the range. The problem is that the cell phones have a very high powered radio that will reach a great distance. For their final version of the lab (where it will be accessible to others from the internet), they are working on Faraday cages. There's also the issue of heat dissipation. They are ordering a custom server rack built by HM Cragg that will be able to handle the servers and store the equipment while allowing ventilation.

This information was helpful because it allowed the team to narrow down research for compatibility of the SDR, to use strictly Android phones, and to have a warning about the signal strength of the SDR.

3.2 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, or having a mobile lab that can used anywhere on campus. Physical connection to the server would 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 cage be portable and relocate it 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.

3.3 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 networks inside the cage cannot be accessed by an outside device outside except via the access point designated for the curriculum. The final confirmation will come from ensuring all requirements listed below have been implemented.

4 Project Requirements/Specifications

4.1 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.

4.2 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.

4.3 Risks

This project comes with a very clear risk: if the Faraday cage does not isolate its 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

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.

4.5 Test Plan

At any point when a prototype has been made or updated, the following tests will be conducted:

1. Cellular Tests

Test 1: Starting Call from in the Cage

i. Team member A will place their cellphone in the cage.
ii. Seal the cage, placing the lid on top.
iii. Team member B will call A's phone.
iv. Record the results of the call.

Test 2: Start Call from outside the Cage

i. Team member B will call Team member A's phone.
ii. While B is on the line, A will place phone inside the cage.
iii. Seal the cage, placing lid on top.
iv. Record the results of the call.

Test 3: Sending Text form in the Cage

i. Team member A will place their cellphone in the cage.
ii. Seal the cage, placing the lid on top.
iii. Team member B will send a text message to A's phone.
iv. Record the results of the message.

2. Wireless Tests

Test 4: Starting Device Ping from inside the Cage

i. Ensure Raspberry Pi and an external device are connected to the same wireless network.
ii. Team member will place Raspberry Pi in the cage.
iii. Seal the cage, placing the lid on top.
iv. Team member will ping the Raspberry Pi from the external device.
v. Record the results of the ping.

Test 5: Starting Device Ping from outside the Cage

i. Ensure Raspberry Pi and an external device are connected to the same wireless network.
ii. Team member will ping the Raspberry Pi from the external device.
iii. Team member will place Raspberry Pi in the cage.
iv. Seal the cage, placing the lid on top.
v. Team member will ping the Raspberry Pi from the external device again.
vi. Record the results of the pings.

Test 6: Signal Strength Test

i. Ensure Raspberry Pi and an external device are connected to the same wireless network.
ii. Team member will start signal strength script on the Raspberry Pi.
iii. Team member will place Raspberry Pi in the cage.
iv. Seal the cage, placing the lid on top.
v. Monitor signal strength of the Raspberry Pi, this is an opportunity to add or remove fabric from the cage to see what is most effective for the next round of tests

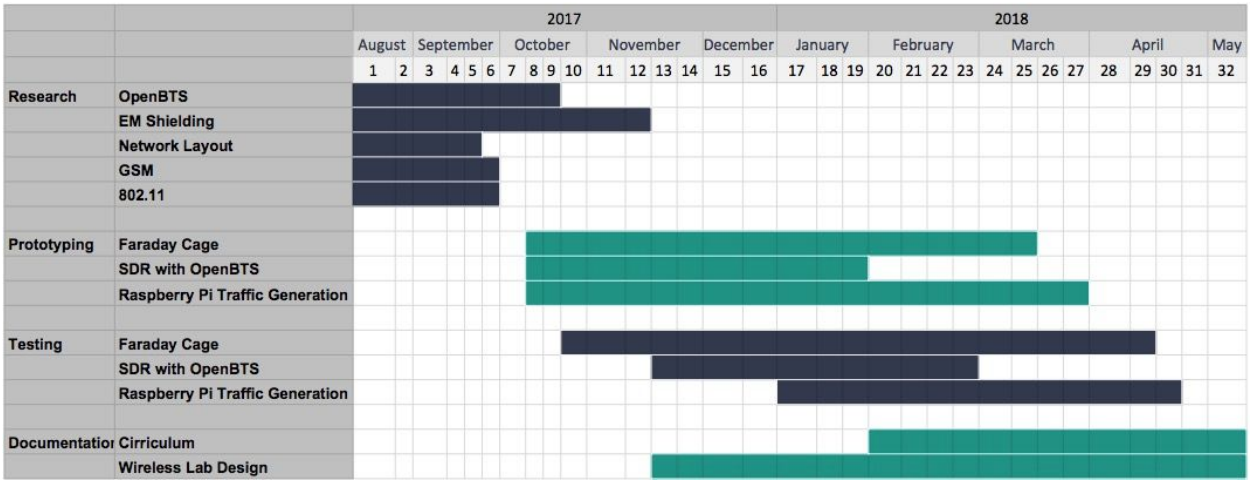
The tests are designed in this way because the core problem with the project is efficient signal blocking. Through experience, the team has identified a difference in signal blocking success depending on whether or not there was an existing connection before the device was placed in the cage. The tests may seem very simple, but they are designed this way in order to be easily replicated.

5 Challenges

This project induces a few challenges. A Faraday cage is something that can be purchased for a high price or built with a little hard work. This requires acquisition of materials needed to physically build the cage. There are also several components that must safely fit inside of the cage that require power sources and need to connect to devices outside the cage. These all require wires to be routed through a wall in the cage, which in turn creates a hole through which signals can get in or out of the environment. How these wires are routed needs to be taken into consideration to make sure that no signals are in fact escaping. Which leads to the biggest challenge thus far, blocking all of the signals required to be blocked. Because all of the frequencies that are being dealt with are meant to be accessible to all related devices, it is challenging to block these signals from getting inside or outside the cage. In addition, there is also the fear that the equipment will produce too much heat in such an isolated space. Ventilation isn't as easy as it sounds because the more holes there are, the more likely signals can escape into the wild.

6 Timeline

Timeline for the major deliverables is as follows: First semester includes researching technologies such as SDR's, OpenBTS, Raspberry Pi 3's, and virtual machines, acquiring parts for building the cage, and prototyping cage designs. Second semester focuses on finalizing the cage and creating lab curriculum.



7 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.

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.

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

9 Appendices

Figure 1: Network Diagram

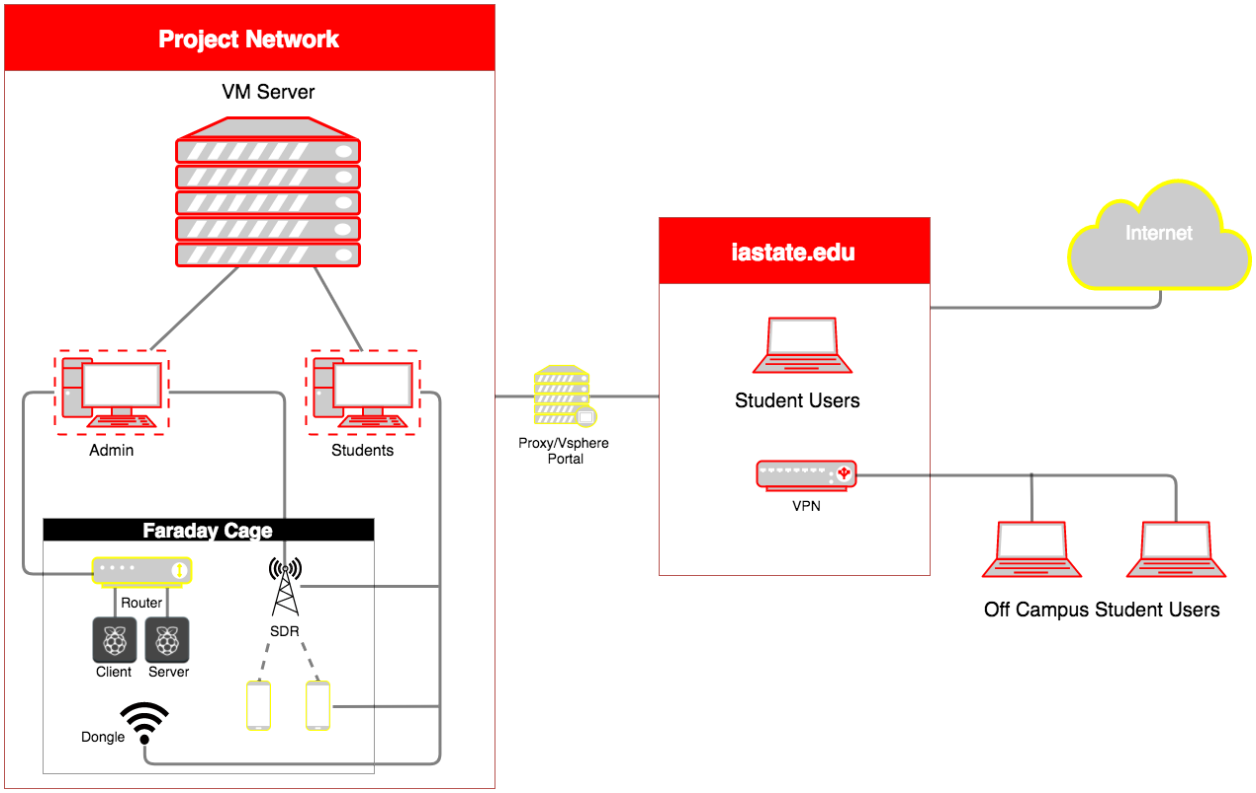


Figure 2: Deliverable Timeline

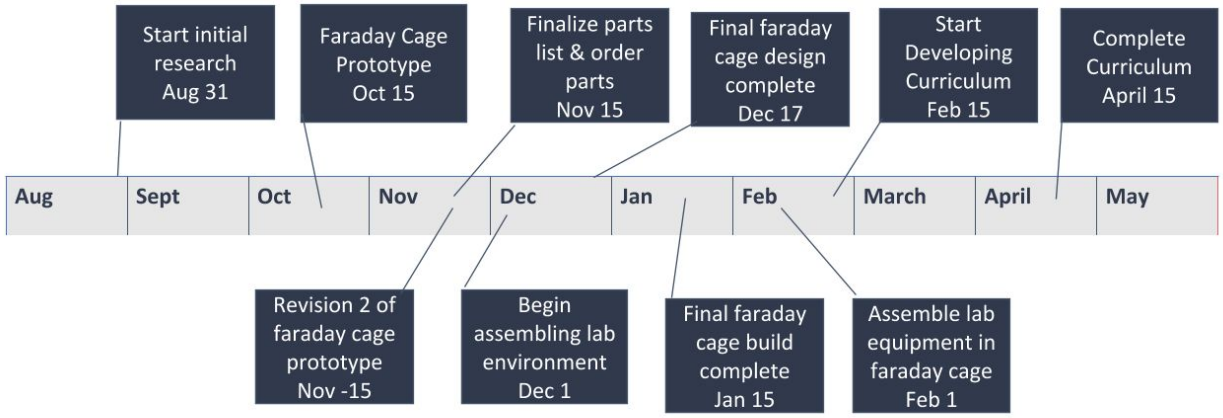


Figure 3: Gantt Chart