Wireless Security Lab & Open BTS

Project Plan

Iowa State University

Senior Design Group Dec13-14

Faculty Advisor/Client: Dr. George Amariucai

Team members:
Xiaofei Niu
Thuong Tran
Chris Van Oort
Matt Mallett
Yuqi Wang
Khan Rahman

Disclaimer

This document was developed as a part of the requirements of an electrical and computer engineering course at Iowa State University, Ames, Iowa. This document does not constitute a professional engineering design or a professional land surveying document. Although the information is intended to be accurate, the associated students, faculty, and Iowa State University make no claims, promises, or guarantees about the accuracy, completeness, quality, or adequacy of the information. The user of this document shall ensure that any such use does not violate any laws with regard to professional licensing and certification requirements. This use includes any work resulting from this student-prepared document that is required to be under the responsible charge of a licensed engineer or surveyor. This document is copyrighted by the students who produced this document and the associated faculty advisors. No part may be reproduced without the written permission of the senior design course coordinator.

Thursday, March 28, 2013

Table of Contents

1) Background Information

The purpose of this project is to provide students enrolled in Computer Engineering 537: Wireless Network Security at Iowa State University with an environment in which they can carry out various experiments involving different wireless communication protocols. Our goal is to build a sandbox style environment capable of supporting four simultaneous users with the tools and hardware needed to carry out a multitude of different experiments, and make this environment accessible from anywhere in the world to support the needs of both on- and off-campus users. The rest of this document deals with the project plan and major categories listed in the table of contents.

2) Concept Sketch and Statement of Need

Senior design project DEC13-14 was prompted by Dr. George Amariucai, professor of CprE 537: Wireless Network Security. It was noted that some students in the class may find it difficult to construct an environment in which wireless security experiments may be run, which may result in inability to expand their knowledge or temptation to run exploits unlawfully against a public network.

This project attempts to create a laboratory with real-world equipment that mimics a real-world network, complete with legitimate traffic, and also provides the user with the hardware and software tools necessary to exploit this network, all within the safe confines of a controlled environment. This way, the student can avoid needless time spent acquiring and configuring equipment and gathering software tools, and get directly to experiment with the network.

The system will consist of not only the hardware implementation to support wireless security experimentation but also laboratory experiments designed to complement the lecture material. Students will be able to experiment with the laboratory environment on their own, but will also be guided through structured laboratory procedures.

The lab must support multiple users, be accessible via GUI from a remote machine either on or off campus, and have ample documentation for both students and faculty administrators.

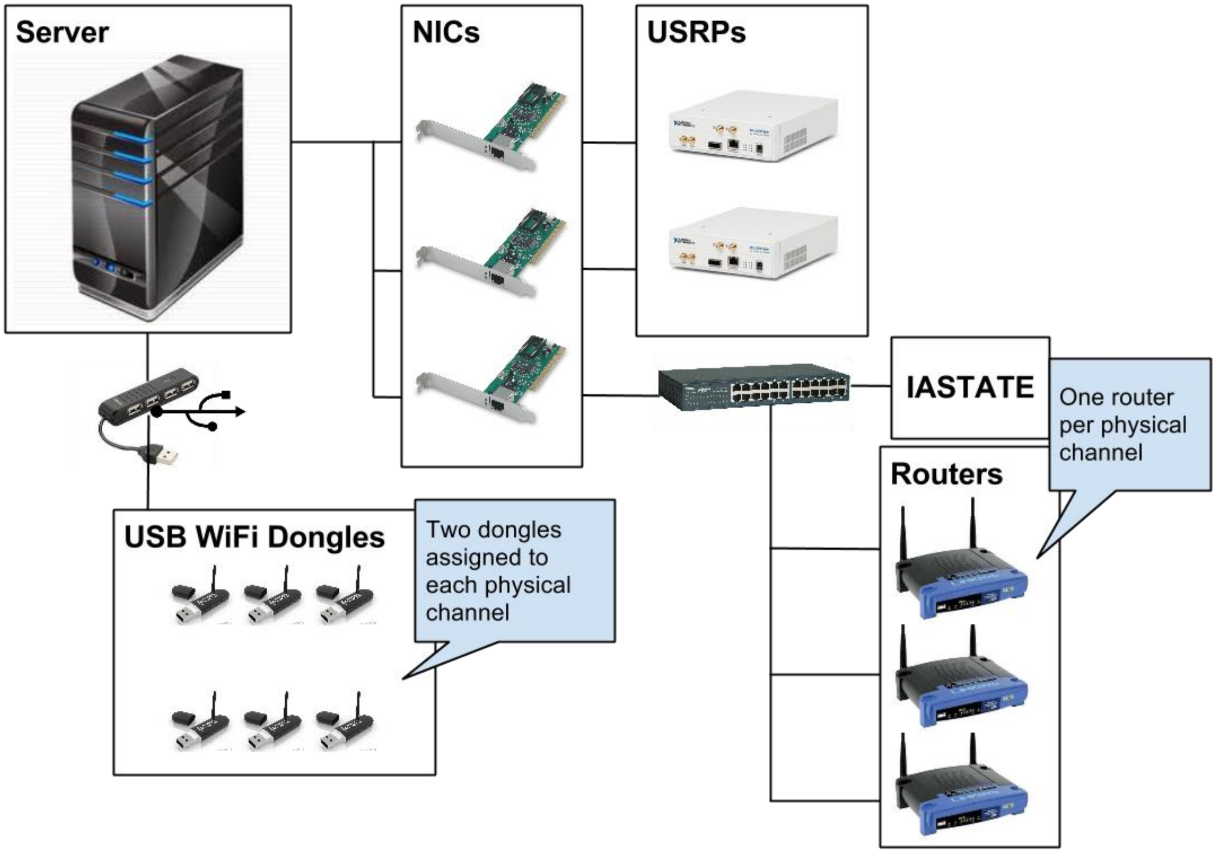
The hardware for the lab will be installed in a computer room in Nuclear Engineering. Testing will have to be completed to determine required computing power to implement all lab functions.

The team plans to implement this system using commodity server hardware and virtualization technology to make the system as compact, easy to administrate and cost-effective as possible. In addition to hardware, the team will install operating system environments and all necessary software tools, write extensive documentation in their proper use, and provide novel experiments to run with the given equipment. The instructor and/or students will then be free to modify these experiments to satisfy their own curiosities in the subject.

3) System Block Diagram

The following page demonstrates a preliminary sketch of the system configuration of a laboratory environment which is configured to concurrently support four students. This example shows a configuration example wherein multiple Wi-Fi routers would be run in parallel with different encryption schemes, such that students could experiment with any scheme without having access to the router's configuration.

All virtual machines will be run on a single host. The final decision on host machine architecture will be made as a joint agreement between the team and the client based on performance testing of several classes of machines.


Server
NICs
USRPs
IASTATE
One router per physical channel
Routers
USB WiFi Dongles
Two dongles assigned to each physical channel

4) System Description

The laboratory structure will be reconfigurable to suit the different wireless system architectures under study. For experiments dealing with Wi-Fi, a two-node setup will be pursued, with each node equipped with a Wi-Fi interface. In this configuration, one node acts as a legitimate client transferring data across a Wi-Fi network via a router. The second node will be under full student control and will be capable of executing a variety of exploits and tests on the network, including packet sniffing and injection. This functionality will be implemented through a combination of compatible hardware and commercially- or freely-available software packages.

Generally, students will be given access only to the attack node, or will be given extremely limited access to the legitimate clients or other equipment (e.g. routers). This will simplify administration of the environment and allow a level of control and repeatability to be expected of the experiments. In certain cases, students may be able to choose the type of traffic generated or the encryption technology implemented between nodes, if this is within the scope of the experiment.

In addition to clients and attackers, one additional host is planned, which would provide usage statistics, environment data such as spectrum analysis, downloadable tools, and other lab-specific data to the student. This host would not be console-accessible to the student under any circumstances, and would run autonomously with little or no configuration from the lab administrator. This would be implemented using the USRP - Universal Software Radio Peripheral - acting as a base station for wireless signals.

All machines will run a distribution of Linux to be determined by the team. The choice of Linux will allow fine control over student access privileges on the machines. It also ensures compatibility with the most popular wireless security related software packages. The particular distribution will be chosen on basis of stability, configurability and resource efficiency. Currently Red Hat Enterprise Linux is the distribution of choice.

5) Operating Environment

The goal of the Wireless Computer Security Lab is to provide the students of the Computer Engineering 537 class a practical environment for experimenting with wireless security. Since this class is taken by distance education students, the lab must be setup with special considerations that a normal computer lab may not consider. One consideration is how the students will access the lab as they will not have physical access to the lab equipment. Another consideration is the physical environment the lab will reside in. Things like temperature, space and wireless signal interference are critical to the operation of the lab. Finally, due to the type of experiments, the students will require a fairly high level of control over the equipment. The lab must be built with this in mind.

Since some experiments will require the student to have direct control over different equipment, there is a concern over the possibility of the student breaking the lab environment that has been set up for them. This concern makes the lab a prime candidate for virtualization. For example if a student were to delete an important configuration file while editing it the system may no longer work the way it was intended to or work at all. However since the machine is a virtual image, the system administrator would be able to back up the machine to a previously working state very easily. Besides making the lab easy to administrate, virtualization also makes the lab more cost effective. Instead of having one physical computer running one lab session for one student, the lab will be able to run multiple sessions on one physical machine for multiple students. Now that the amount of physical equipment needed is significantly less, the amount of space needed to run the lab is also significantly less.

By choosing to run the lab in a virtual environment as well as having the lab only remotely accessible to students, the amount of space required to set up and run the lab is small enough not to warrant entire room. It has been decided that, since the amount of space required is relatively small, the lab will be set up and run in the Nuclear Engineering Building along will other machines of the same type. This raises the concern that with so many computers so close together that the temperature may excide the level of safe operation. This has yet to be seen and probably will not be testable until the weather becomes significantly warmer. However, it still remains a concern. Another concern that arises from having so many computers so close together is with so many wireless signals on the airwaves there may be a considerable amount of interference. To counter this when the machine is set up in Nuclear Engineering an audit of wireless traffic must be done. Once this information has been analyzed the correct configuration should allow the lab to co-exist with the rest of the computers.

6) User Interface Description

The laboratory structure will be reconfigurable to suit the different wireless system architectures under study.

For experiments dealing with Wi-Fi, a three-node setup will be pursued, with each node equipped with a Wi-Fi interface. In this configuration, two nodes act as legitimate clients transferring data across a Wi-Fi network via a router. The third node will be under full student control and will be capable of executing a variety of exploits and tests on the network, including packet sniffing and injection. This functionality will be implemented through a combination of compatible hardware and commercially- or freely available software packages.

Students will be given root access to the exploit node, and user level access to one of the client nodes. The other client node will be our web server, which will act like a target and reply to traffic. This will simplify administration of the environment and allow a level of control and repeatability to be expected of the experiments. In certain cases, students may be able to choose the type of traffic generated or the encryption technology implemented between nodes, if this is within the scope of the experiment.

All machines will run a distribution of Linux to be determined by the team. The choice of Linux will allow fine control over student access privileges on the machines. It also ensures compatibility with the most popular wireless security related software packages. The particular distribution will be chosen on basis of stability, configurability and resource efficiency. Currently Arch Linux is the distribution of choice.

The documentation for the laboratory environment will be comprehensive. It will contain step-by-step instructions for the proper administration of the environment, as well as recovery strategies for if and when machines become corrupted. Instructions for reallocating laboratory resources from one experimental setup will be given. Finally, complete hard copy backups of the final state of all machines will be provided with instructions for rebuilding the laboratory environment if necessary.

7) Functional Requirements

OpenBTS & USRP Requirements

1. The system shall implement a functioning OpenBTS sub-system using USRP's as communication hardware.

> Fit Criteria: USRP's run on the GSM network and are the hardware available for with OpenBTS to communicate with.
> Rationale: OpenBTS will be provide the communication software to give function to USRP's.

2. The system shall act as a wireless base station for the purpose of injecting, receiving, and sending wireless data.

> Fit Criteria: The purpose of the lab is to non-destructively interact with wireless traffic.
> Rationale: The basic ways to interact with data are create/rename/update/delete – as a wireless base station students will be able to entertain all possibilities.

3. Between OpenBTS and USRP's, LabVIEW shall be used to transfer data and interact as an interstitiary application.

Fit Criteria: OpenBTS doesn't directly interface with the USRP's.
Rationale: In order to create a wireless base station the hardware must have a line of communication with the software.

4. The existing web control interface shall be updated to reflect control of the new USRP & OpenBTS functionality.

Fit Criteria: Users control the system through a web interface.
Rationale: In order to utilize our updates and changes, users will need to have an updated and functional interface to do so.

5. Ubuntu virtual machines will be created to interface with the USRP's and run the OpenBTS system.

Fit Criteria: Users are interacting with the system entirely remotely.
Rationale: OpenBTS is software designed to run on *nix systems; LabVIEW is also compatible with *nix systems.

System Requirements

1. The system consisting of web server, open BTS client, and attack/defend clients shall be made functional.

Fit Criteria: The existing system maintains much functionality that is useful to build upon to further the project goal of student lab experiments.
Rationale: The existing system is already built and simply needs to be reconfigured for new hardware.

2. The existing system shall be made current to any security patches.

Fit Criteria: The system deserves up to date security software.
Rationale: This would provide the most relevant learning experience with the latest and greatest techniques employed.

3. The existing system shall be remotely accessible through VMware vSphere Clients and VMware workstations for administration, in addition to SSH and SFTP for students.

Fit Criteria: This is a remote access, wireless lab for students.
Rationale: Students will be unable to gain physical access to the server / peripherals and must be able to still interact with the lab.

8) Non-Functional Requirements

Documentation

1. Updated documentation shall be created and merged with existing documentation where possible.

Fit Criteria: The system is to be used for students for a number of years.
Rationale: To maintain longevity, the system must be well documented to have a hope of being well maintained.

2. Updated system passwords and account access shall be enacted.

Fit Criteria: Passwords are regularly compromised.
Rationale: System administrators and maintainers shouldn't have to worry about the insecurity of passwords or have to hunt for them in many places.

Legal

1. Design actions shall be taken to prevent end-user students from breaking the law by any means of illicit activity.

Fit Criteria: System must be legal to operate.
Rationale: If a student breaks the law unknowingly using a lab from Iowa State, the University is put in a compromising legal position.

2. System shall conform to any and all operational and environmental requirements and regulations.

Fit Criteria: System must be legal to operate.
Rationale: System must conform to all regulations imposed by governing bodies.

User Experience

1. Overall system user experience shall not be learning prohibitive.

Fit Criteria: The user interface must be intuitive to use.
Rationale: If end-users are unable to use the software the system functionality is nullified.

9) Market Analysis

As an academic project intended for student use rather than marketability, the market survey for this project may be considered less relevant than it may be for an industry client. Nevertheless, the existence of similar wireless security laboratory environments at other universities and organizations was investigated. Although such environments are found at many universities, including Arizona State, Northeastern University, and St. Mary's University, TX, the team has been unable to find an example of a wireless security laboratory which has been designed for remote access or experimentation in the ways we have designed for this environment. Furthermore, most university wireless security labs are geared towards research rather than student learning and experimentation, so it may be stated that for its purpose, this laboratory would be the only one of its kind.

10) Deliverables and Objectives

Objectives:

- Working wireless security lab.
- Full documentation.
- Working Base Station.
- Web server.
- Skype call through base station using smart devices.
- LabVIEW/Virtual lab compatible with current server.
- Remote access with GUI for on/off campus student.
- Support multiple users at the same time.

Deliverables:

- Working implementation of VMware lab.
- Interface Open BTS with LabVIEW and USRP.
- Website for interaction.

The website interface for launching attack nodes will greatly simplify the process of learning for students. They will not have to download the relevant software and setup an environment in order to practice wireless security principles, but will be provided with one with a simple web based user interface.

This will allow for hands on experience in addition to the learning that takes place in the classroom. Students will be able to apply the principles they learn in class and apply them in a real world scenario.

The base station will allow for students and instructors to view the waveforms generated by the wireless signals through LabVIEW. It also serves as an introduction to how calling works and will also act as a miniature cell phone tower.

11) Division of Labor and Responsibilities

Work Breakdown Structure

This is a general breakdown of team roles and responsibilities, members can help with each and every aspect of the project and are not necessarily limited to these particular roles.

Xiaofei (Frank) Niu - Team Lead/Documentation
Frank will be responsible for the majority of the documentation such as the project plan and design document as well as acting as a general secretary for the weekly reports. Another major responsibility is making sure that others keep on track and providing assistance if needed.

Khan (Tahsin) Rahman/Yuqi Wang – Hardware Specialists
Tahsin and Yuqi will be responsible for all things related to the USRP, including the embedded programming and base station setup; along with LabVIEW integration in order to collect and view waveforms.

Matt Mallet/Chris Van Oort – System/Software Specialists
Matt and Chris will lead the setup of the entire system architecture for the lab including but not limited to OS setup, remote setup, network setup, server setup, user interface and any software integration for new technologies. In addition, Chris is the webmaster for our project.

Thuong (Dustin) Tran – Security Specialist
Dustin will lead the design and implementation of the security related wireless experiments including but not limited to individual experiments, test experiments and any security related experiments.

Task No. 1 – Project Analysis and Requirements Analysis

Objective:
To understand client vision and identify requirements for a working environment.

Approach:

- Interview the client
- Study class material

- Research technology
- Test feasibility / constraints
- Expected Results:
- Environment definition
- Requirements / feasibility / constraints / risks analysis

Task No. 2 – Environment Design and Implementation

Objective:
To set up a working environment to carry out remote wireless security experiments.

Approach:

- Design system
- Implement system
- Test System
- Validate system

Expected Results:

- Working environment

Task No. 3 – Experiment Design and Implementation

Objective:
To design and implement individual wireless security experiments.

Approach:

- Research technology
- Design experiments
- Implement experiments
- Hardware
- Software
- Validate experiments

Expected Results:

- 3-4 WiFi experiments

Task No. 4 – Laboratory Documentation

Objective:
To create documentation to support laboratory administration.
To create documentation to support the individual experiments.

Approach:

- Identify administrative tasks
- Create documentation
- Identify experiment instructions
- Create documentation

Expected Results:

- Administration documentation
- Experiment documentation

Task No. 5 – Testing and Validation (Individual Part / Full System)

Objective:
To test the environment and validate experiments.

Approach:

- Extensive testing under different conditions
- Usability testing
- Client validation
- Student response

Expected Results:

- Ensure that the laboratory setup and experiments meet client vision and support class instruction.

12) Schedule

Week Number	**Start Date**	**End Date**	**Tasks**
1	1/14/13	1/19/13	Obtain group members
2	1/20/13	1/26/13	Meet with advisor
3	1/27/13	2/2/13	Research project
4	2/3/13	2/9/13	Review wireless security documentation, read USRP manual, install virtual machine and connect to client server

5	2/10/13	2/16/13	Create website, USRP research, VMWare download/connect to server
6	2/17/13	2/23/13	Access attack client, research hardware compatibility, install Ubuntu 12.4 on server, finish design document
7	2/24/13	3/2/13	Update design document, create use cases, consult with Doug about network architecture, GNU radio install on server, update hardware section for design document
8	3/3/13	3/9/13	Use cases/use case diagrams, check out situation with virtual machine, researched firewall, get website onto IAstate website
9	3/10/13	3/16/13	Set up git hub repo, schedule for project, use cases and functional/nonfunctional requirements for USRP
10	**3/17/13**	**3/23/13**	**Spring break**
11	3/24/13	3/30/13	Hardware Setup
12	3/31/13	4/6/13	VM Install and Configure
13	4/7/13	4/13/13	Software Setup
14	4/14/13	4/20/13	Administrative/UI Setup

15	4/21/13	4/27/13	Debug current issues
16	4/28/13	5/4/13	Client/Student Validation
17	5/5/13	5/11/13	Presentation
18	8/26/13	8/31/13	Environment Design and Implementation
19	9/1/13	9/7/13	Environment Design and Implementation
20	9/8/13	9/14/13	Environment Design and Implementation
21	9/15/13	9/21/13	Environment Design and Implementation
22	9/22/13	9/28/13	Environment Design and Implementation
23	9/29/13	10/5/13	Environment Design and Implementation
24	10/6/13	10/12/13	Environment Design and Implementation
25	10/13/13	10/19/13	Laboratory Documentation
26	10/20/13	10/26/13	Administration Documentation
27	10/27/13	11/2/13	Experiment Documentation
28	11/3/13	11/9/13	Testing and Validation
29	11/10/13	11/16/13	Full System Testing
30	11/17/13	11/23/13	Client/Student Validation
31	**11/24/13**	**11/30/13**	**Thanksgiving break**
32	12/3/13	12/9/13	Final presentation

33	12/10/13	12/16/13	Prepare for graduation/ celebration

13) Resource Requirements

Since we already have the necessary hardware and all of the software we are planning to use is either free or will be written by us, the total cost of this project will be what it takes to supply electricity to keep the server up.

14) Risk and Mitigation

1. Risk: No access to web server
Mitigation: We can request members of the previous group to send us the web server materials, and create a virtual machine image from it, so that this problem is never encountered again by us, or subsequent groups.

2. Risk: USRP/OpenBTS has unknown level of compatibility with a virtualized environment
Mitigation: Depending on levels of compatibility, we could limit the number of virtual machines that have access to the devices, or in the extreme case, run this portion of the project on a standalone server.

3. Risk: Serious ethical and legal boundaries involved in the project
Mitigation: Carefully explore and define these boundaries. Make them absolutely clear, and possibly limit what software can do to avoid crossing these boundaries.

15) Conclusion

Upon completion of this project, the team shall present to the client a complete hardware-software implementation of a multi-user virtualized environment. This may consist of one or more physical machines as deemed necessary by the team, as well as any networking equipment or other hardware devices required for completion of the lab experiments. This shall be accompanied by ample documentation outlining the proper assembly and configuration of the laboratory environment, including software install media and backup images of virtual machines. Guidelines for basic environment administration will also be provided, including reassignment of resources between machines and instructions on building and deploying new machines.

16) Project Team Information

Client and Faculty Advisor Information

Dr. George T. Amariucai, gamari@iastate.edu
212 N Nuclear Eng. Bldg.

Student Team Information

Xiaofei Niu - Team Lead/Documentation, xniu@iastate.edu
Thuong Tran - Software Design, thuong88@iastate.edu
Chris Van Oort - Webmaster/Software Design, chrisv@iastate.edu
Matt Mallet - Software Design, mmallett@iastate.edu
Yuqi Wang - Hardware Design, xiaoqiqi@iastate.edu
Khan Rahman - Hardware Design, mtrkhan@iastate.edu