Wireless Security Lab & OpenBTS

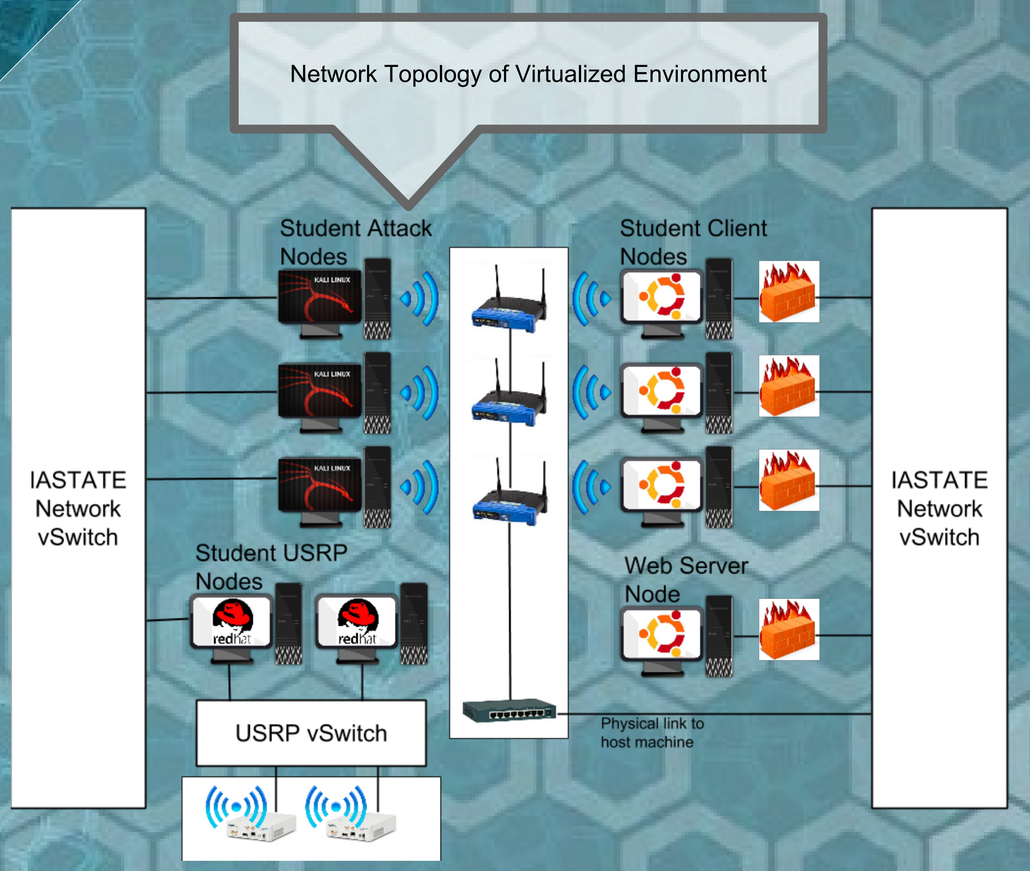
Dec 13-14

Introduction

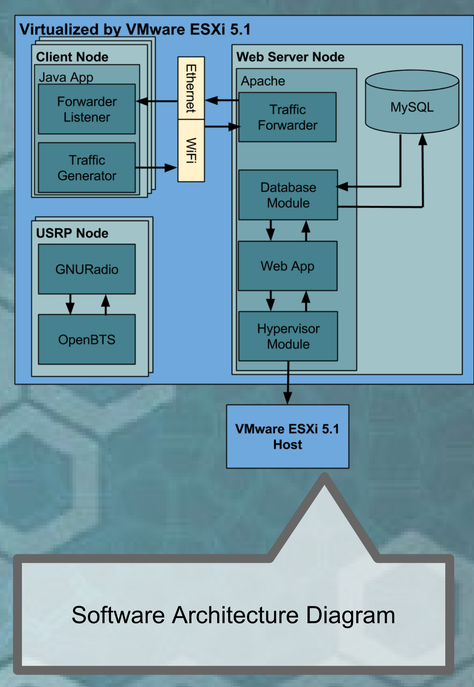
The purpose of this project is to provide students enrolled in Computer Engineering 537: Wireless Network Security at Iowa State University with an environment in which they can carry out various experiments involving different wireless communication protocols.

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.

OpenBTS (Open Base Transceiver Station) is an open source software allowing a USRP (Universal Software Radio Peripheral) to act as a GSM (Global System for Mobile Communications) network access point. The end goal for the hardware portion of the project is to make a phone call through the USRP.



Network Topology of Virtualized Environment



Software Architecture Diagram

Requirements

Functional

- ❏ The system consists of a web server, OpenBTS client, and attack/defend clients shall be made functional.
- ❏ The system shall be remotely accessible.
- ❏ The system shall implement a functioning OpenBTS sub-system using the USRP as communication hardware.

Non-functional

- ❏ Design actions shall be taken to prevent end-user students from breaking the law by any means of illicit activity.
- ❏ System shall conform to any and all operational and environmental requirements and regulations.
- ❏ Overall system user experience shall not be learning prohibitive.

Summary

Problem Statement

- ❏ Students may find it difficult to construct an environment for wireless security experiments
- ❏ Results in inability to expand knowledge or temptation to run exploits unlawfully against a public network

Solution

- ❏ Design and build a website to automate the process of setting up laboratory environments
- ❏ Implement the necessary software to apply OpenBTS on the USRP

Operating environment

- ❏ Individual with internet access
- ❏ Operating system with Mac OS X, Windows, and Linux

Intended users and uses:
Students enrolled in CprE 537 for laboratory exercises

Approach

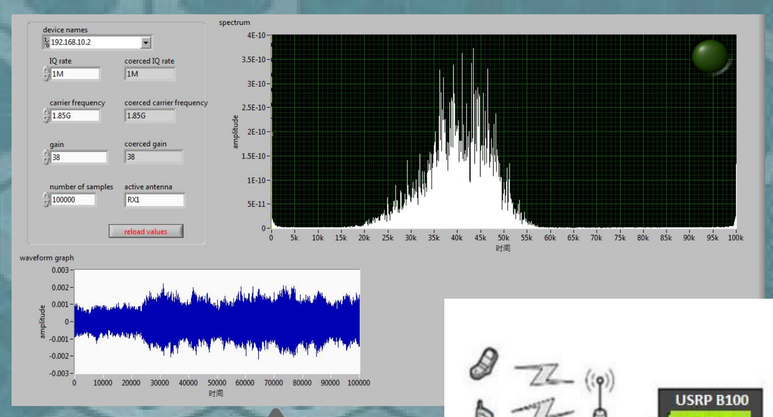
- ❏ All nodes will be allocated through a website interface
- ❏ VMware ESXi 5.1 hypervisor will allocate virtual machines
- ❏ Client Nodes running Ubuntu will send information to routers
- ❏ Attack Nodes running Kali Linux will be able to view/intercept signals
- ❏ USRP Nodes running Windows 7 will have LabVIEW for signal information viewing
- ❏ Network will be contained behind a firewall, only allowing traffic through internal virtual network

Technologies Considered

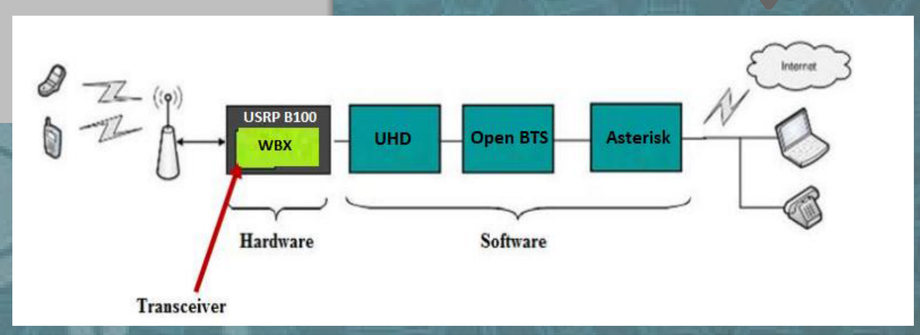
- ❏ Virtual Machine Managers
- ❏ Operating Systems
- ❏ Front-end and Back-end Implementations

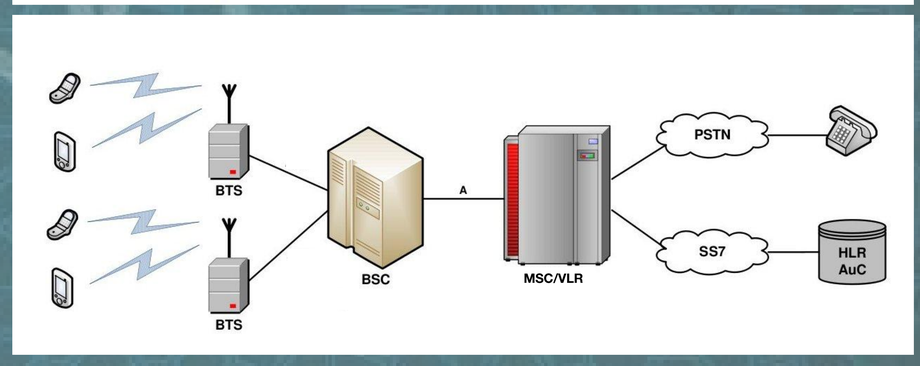
Testing Considerations

- ❏ Functional Verification User Testing
- ❏ System Infrastructure Testing
- ❏ System Integration Testing



Observing the GSM Spectrum with LabVIEW and USRP





OpenBTS GSM Network Architecture (Top), and Traditional GSM Network Architecture (Bottom)

Team members	Xiaofei Niu	Matt Mallett	Chris Van Oort	Yuqi Wang	Thuong Tran	Muhammad Tahsinur Rahman Khan	Advisor/Client
	CprE	CprE	SE	EE	CprE	EE	George Amariucai