# AC 2007-406: AN ISOLATED DISTANCE EDUCATION LAB ENVIRONMENT FOR THE STUDY OF WIRELESS DEVICES

**Lee Toderick, East Carolina University**

Lee Toderick received a B.S. in Computer Science from East Carolina University and an MS in Computer Information Systems from Boston University. His professional certifications include CCNP/CCDP and RHCE. His currently serves as teaching instructor in the Department of Technology Systems at East Carolina University. Research interests include remote lab access for distance learning students, firewall implementation, and applied computer network security.

**Jingyuan Deng, East Carolina University**

Jingyuan Deng received a B.S. in Communication Engineering from Tianjin University, China. She is currently working on a Master Degree in Technology Systems of East Carolina University, concentrating in the fields of Digital Communication and Networking. She is employed by the College of Technology and Computer Science as the graduate assistant. She is the President of the Epsilon Pi Tau - Beta Mu Chapter.

**Philip Lunsford, East Carolina University**

Phil Lunsford received a B.S. in Electrical Engineering and a M.S. in Electrical Engineering from Georgia Institute of Technology and a Ph.D. in Electrical Engineering from North Carolina State University. He is a registered professional engineer and is currently an Assistant Professor at East Carolina University. His research interests include system simulation, telemedicine applications, and information assurance.

# An Isolated Distance Education Lab Environment for the Study of Wireless Devices and Protocols


## Abstract

Many educational institutions that offer curriculum classes in wireless technologies include protocol investigation and security configuration. Wireless technology labs help to reinforce theory and concepts, and to provide educational experiences not available through classroom lecture. Secure, remote access to lab equipment enables students to perform experiments 24/7 from any location thus maximizing the utilization of the equipment and providing scheduling flexibility to the students. Student laboratories for wireless devices can be problematic in institutions that offer wireless network access. This production wireless environment can be disrupted or even disabled if a student misconfigures the laboratory equipment.

This paper describes our success with the adoption of an isolated, remotely-accessible faraday cage that houses wireless equipment, permitting even the most invasive wireless projects to be performed in an area that offers production wireless network access. Our lab isolation is optimized for the ISM 2400-2483 MHz frequency band thus providing isolation for IEEE 802.11b/g radio communication. Current laboratory exercises include wireless access point configuration, wireless network interface card configuration, wireless network sniffing, WEP cracking, rogue access point detection, and wireless-based DoS attacks.

Remote control of devices inside a faraday cage is inherently problematic. Any wiring penetrating the wall of the cage is a potential source for RF leakage. Our approach is to use fiber optic cable for all data transmission into and out of the isolation area. Power delivery into the isolation area requires care to provide grounding filters for the frequency range of concern. Heat dissipation from the isolation area is aided by forced airflow through the cage. Details of our implementation are given.


## Purpose

The goal of this project is to provide the student with a fundamental understanding of wireless network security principles and implementation scenarios. To that end, a variety of security topologies, technologies and concepts used to provide secure communications channels are presented. An abbreviated list of subjects[1,2] include:

- Explain the goals and factors involved in a wireless network security strategy.
- Explain several popular wireless network attacks and configure wireless security to mitigate vulnerabilities.
- Explain popular wireless protocols, and apply the protocols in a wireless networked environment.
- Explain and demonstrate the concepts of wireless data transfer security issues and techniques used to secure wireless data, such as WAP, WTLS, and WEP.
- Explain, model, and configure wireless network security perimeters.

- Define and implement wireless intrusion detection system (IDS), honeypots, and provide examples of several detection methods.

**Implementation**

This section describes the composition of the lab, the physical connectivity of the lab hardware, and software used to control lab and pod access.

General hardware requirements for the project include four computers with wireless access, a wireless access controller, and ancillary equipment. Specific hardware requirements include a Faraday Cage manufactured by LBA, Greenville, NC, two Axis Copper to Fiber Converters, AT-MC13, a remote portal computer, and

Physical Connectivity of Lab Devices relies on different OSI Layer 1 mediums. Shown in Figure 1, equipment is arranged in a Pod, enclosed inside a Faraday Cage, and accessible to students through a fiber hole.

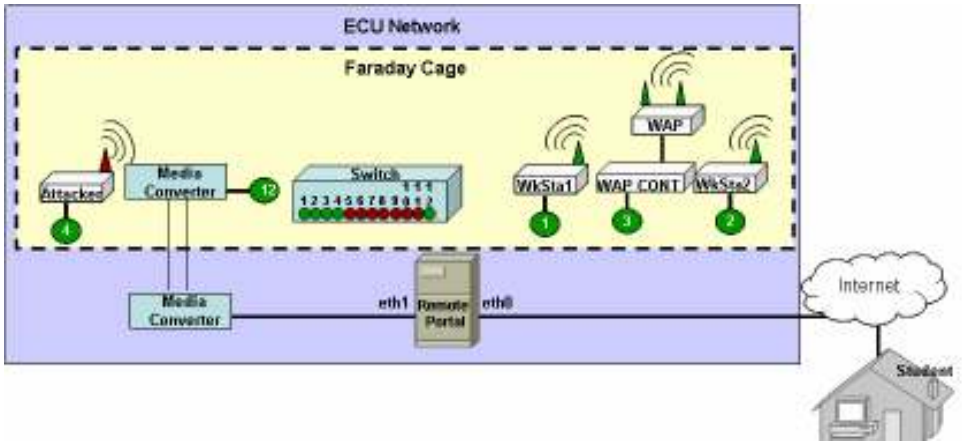


Figure 1. Topology for the various lab components.

Students control four computers and a Wireless Access Point (WAP). Computers are labeled WKSta1, WKSta2, Attacker, and WAP Controller. WAP Controller is used to directly connect to the WAP for configuration. Four computers are the maximum number required by any lab module. Each computer is connected to the Remote Portal through the Catalyst 2950 switch via two media converters.

Two AT-MC13 media converters[3] are used to pass external and internal network signals through the Faraday Cage without interfering with other wireless transmissions. These signals are passed into and out of the faraday cage[4] through fiber optic cable passing through waveguide openings. These physical configuration of these waveguides are designed to block the specific RF frequencies. One of the waveguide openings can be seen in Figure 2. They will allow other out-of-band frequencies to pass through the opening.

One converter receives network traffic from the network 10Base-T port and converts the traffic to light signals. The light signals are transmitted across SC/ST fiber optic cables to the other converter, where the signals are converted back to electronic form and sent through a 10Base-T port to the destination network. Figures 3 and 4 show the faraday cage with the cover on and off.

Figure 2: Faraday Cage side showing waveguide opening at the upper right hand corner.

Figure 3: Faraday Cage with cover on.

Figure 4: Faraday Cage with cover off.

Remote portal operation consists of a firewall[5], student reservation system, and access to pod devices. This section describes remote portal operation and student access.

Unnecessary services should not be run on the remote portal. Only the secure shell (SSH) daemon is needed, and all other unnecessary services should be disabled or uninstalled.

The firewall routing table permits only SSH traffic to the remote portal from the Internet. From the internal network, only VNC ESTABLISHED traffic is permitted into the remote portal. VNC traffic is tunneled from the student to the remote portal, the encryption is stripped, and resulting VNC traffic is passed to the pod devices. On return, the VNC traffic is encrypted by the firewall and passed to the student. In this way, no malicious traffic can leave the remote portal and infect or attack outside computers.

Student access is controlled through a reservation application on the remote portal. Students make a reservation and have exclusive access to the equipment during that time. When the reservation has finished, the next student reservation becomes active. This permits the lab to be scaled for optimal equipment usage.

In order to access computers inside the secure network lab, students must initiate a SSH connection to the firewall. Normally, users are not permitted to connect to a perimeter firewall, but the student has no access to the firewall beyond a restrictive menu that permits only reservation scheduling and changing the user's password. SSH Connectivity must be maintained for VNC traffic to be tunneled.

A student with a current reservation to the lab Pod is able to make a ssh connection to the firewall. The student then initiates a VNC session with VNC client. The VNC information is tunneled to the firewall, where the VNC information is stripped from the SSH encryption. The firewall initiates a 3-way TCP handshake with the Pod computer. However, VNC traffic from the source (student) to the destination (remote computer) is blocked by the firewall. The reservation

database is checked to confirm that the user has a valid reservation and the IP network address is correct. If the information is valid, then the connection process continues. Periodically, the current time is compared against the reservation expiration time. If the two times are the same, then the student is blocked from access.

VNC server is loaded on each Pod computer and used by students for access remote Pod computers.

**Survey Results of Wireless Labs and Wireless Networks**

A survey was conducted in December of 2006 using 35 randomly selected 4 year colleges with a student population of less than 7,500 and 99 randomly selected 2 year colleges

20 total replies were received and results are summarized below.

Questions and Response Information

1. Does your college or university currently teach or plan to teach wireless technology?

| Response | Response Total | Response Percentage |
|---|---|---|
| No plans to teach wireless technology | 8 | 40% |
| Currently teach wireless technology | 10 | 50% |
| Plan to teach within the next 1 year | 1 | 5% |
| Plan to teach after 1 year | 1 | 5% |

2. What is the status of a campus wireless network?

| Response | Response Total | Response Percentage |
|---|---|---|
| No plans to implement a wireless network | 0 | 0% |
| Currently have a campus wireless network | 14 | 70% |
| Plan to implement a campus wireless network within 1 year | 4 | 20% |
| Plan to implement a campus wireless network after 1 year | 2 | 10% |

3. What plans or procedures do you have in place to prevent wireless laboratory exercise from interfering with the campus wireless network?

| Response | Response Total | Response Percent |
|---|---|---|
| Do not or will not offer laboratory exercises | 5 | 25% |
| We use simulated labs | 1 | 5% |
| The lab does/will not overlap with campus network | 7 | 35% |

| | | |
|---|---|---|
| Close faculty supervision and/or limited lab times | 5 | 25% |
| Other (please specify)* | 2 | 10% |

*Two specific answers were given to this question
Wireless capability will only be available in and around our new Technology Building. Students will have to register IP addresses and students who use the wireless will not be able to access our campus network.
We began with teaching 802.11A; we now tone down the AP and use the available security to prevent unauthorized access.

4. Would your capital budget support a shielded wireless laboratory environment including wireless equipment and laboratory exercise supporting 12 students?

| **Response** | **Response Total** | **Response Percent** |
|---|---|---|
| No. | 12 | 60% |
| Yes, if less than $5000 | 7 | 35% |
| Yes, even if between $5000 and $15000. | 0 | 0% |
| Yes, even if over $15000 | 1 | 5% |
| Other (please specify)* | 1 | 5% |

*One specific answer was given to this question
Cisco Networking, Wireless, and Security Budgets are limited and often have to be made up with funding from grants. At this time we can work around the wireless interference, but in the long term we would prefer the labs to be in an environment.

The results of this survey demonstrate that the problem of interference with a production network in a college setting can be an issue when teaching lab based courses on wireless networking.

**Heat Dissipation**

Testing of the system indicated that the faraday cage was successful in shielding the radio transmitters, however the temperature inside the cage rose to unacceptable levels when the front cover was put in place. To date, we have not successfully solved this heat issue but are convinced that it can be overcome with appropriate airflow. Plans are to add fans and possibly more waveguide openings to be function as ventilation ports to overcome this issue. Additionally, conditioning (cooling) of incoming air to the faraday cage might also be needed to ameliorate the problem.

**Conclusion**

This paper presents our implementation strategy for an isolated, remotely-accessible, secure wireless equipment pod to allow even the most invasive and potentially destructive wireless lab exercises to be performed within an area that is physically adjacent to a wireless production

network. A survey of a random sample of universities and colleges received a low return rate and thus strong conclusions cannot be deduced. Several student experiments using this project have been designed and ready for use although heat dissipation issues have not yet been fully solved. Plans are to eventually use this system in both face-to-face and distance education classes on wireless network configuration and security.

**References**


1. Mark Ciampa " Security + Guide to Network Security Fundamentals, Second Edition" ISBN 0-619-21566-6 ©2005
2. Michael T. Simpson " Hands-on Ethical Hacking and Network Defense" ISBN 0-619-21708-1
3. Allied Telesis Company. Available: **http://www.alliedtelesyn.co.uk/site/files/documents/datasheet/MC1X_G.PDF** downloaded January 17, 2007.
4. Raza, I, "Containing emissions from a microprocessor module", IEEE International Symposium on Electromagnetic Compatibility, Volume 2, 21-25 Aug. 2000 Page(s):871 – 876 vol.2.
5. Phil Lunsford, Lee Toderick, "Firewalls for Remote Computer Labs", presented at the 2003 Convention of the National Association of Industrial Technology, Nashville, TN.