2006-559: A REMOTELY CONTROLLED AND ISOLATED COMPUTER NETWORK TEST BED FOR ATTACK UNDERSTANDING BASED INFORMATION ASSURANCE DISTANCE EDUCATION COURSES

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.

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. He currently serves as lecturer in the Department of Technology Systems at East Carolina University. Research interests include remote lab access for distance learning students and information security as it applies to computer networks.

Daniel Brooker, East Carolina University

Daniel Brooker is currently working towards a B.S in Computer and Information Technology with a concentration in Computer Networking. He is employed by the College of Technology and Computer Science as the Undergraduate ICT Online Lab Support Technician. He is involved with the campus chapters of both AITP (Association of Information Technology Professionals) and IEEE (Institute of Electrical and Electronics Engineers).

A Remotely Controlled and Isolated Computer Network Test Bed for Attack Understanding Based Information Assurance Distance Education Courses

Abstract

Information assurance (IA) education has become an important topic in information technology related curriculums. Within the culture of IA educators, there are two pedagogical strategies: defense assurance and attack understanding. Defense assurance focuses on appropriate ways to build and maintain systems that are less vulnerable to attack. Attack understanding focuses on strategies for attacking and how to defend against them. Curriculums that focus more on attack understanding can use isolated test beds to provide laboratory experiences for the students to attack and defend networks. In a face-to-face environment, the test bed isolation can be accomplished by excluding wireless, infrared, and EoP (Ethernet over Power) interfaces, disabling any removable media, and by having only power cables (i.e. no network cables) extend beyond the test bed.

Unfortunately, the use of air-gap isolation is unsuitable in a distance education (DE) environment. Remote students must control equipment in the test bed and therefore must have some sort of access. Computer and networking equipment laboratories are provided in some defense-assurance-focused DE courses, but the access methodology is usually designed to only prevent external access by unauthorized machines. This can be accomplished by using a VPN concentrator or other access firewall. In the case of attack-understanding-based laboratories, the access methodologies employed must guarantee the prevention of any attack escaping the confines of the test bed.

Take the example of a demonstration of worm propagation via email attachments. The attacking machine sends an email to the victim machine that has a worm attached as an executable file. As part of the lab exercise the victim machine executes the file, installing the worm on the victim machine. The attacking machine then gains access to some resource on the victim machine. In a DE environment, the educator is responsible for ensuring that the worm cannot escape the isolated environment.

This paper discusses secure student access and network isolation techniques for DE network test beds and proposes the use of IP-based KVM switches as a mechanism for guaranteeing test bed isolation while maintaining remote access for the students. Tradeoffs of cost, capability, maintainability, and degree of isolation are also discussed.

Introduction

The Internet has provided us quick and easy access to many information technology (IT) resources, and it has also provided access to those individuals that want to compromise those resources. Thus the importance of teaching students the basics of information security and the more general information assurance topics has become a necessity in curriculum related to computer information systems. Some curricula have allowed for in-

depth study of these topics. However, the advancement of distance education (DE) has provided challenges to teaching these topics.

As discussed by Frincke [1], the teaching philosophies for information assurance educators can be divided into two camps: defense assurance and attack understanding. Defense assurance focuses on the mechanisms to provide defenses to a system. Very little discussion is dedicated on how to attack a system, rather the focus is on defense. On the other hand, the attack understanding philosophy focuses on the study of attack strategies and how to defend against them. This focus gives the students an in-depth look from the attack side and arguably a better foundation for devising and understanding defenses against attack. Of course this philosophy also teaches the students the ability to carry out attacks. This implies the duty of the educators to provide assurance that the students will not apply their knowledge for criminal use, a task not easily done.

Remote Lab Topologies

In addition to the need to teach information assurance topics, there is also a need to deliver courses in a DE environment, allowing students to live and possible work in a geographic location removed from the college or university. DE laboratory exercises have been developed and used in non-information systems courses [2]. DE labs have the advantage of being available 24/7 allowing fewer laboratory devices to serve a large student body.

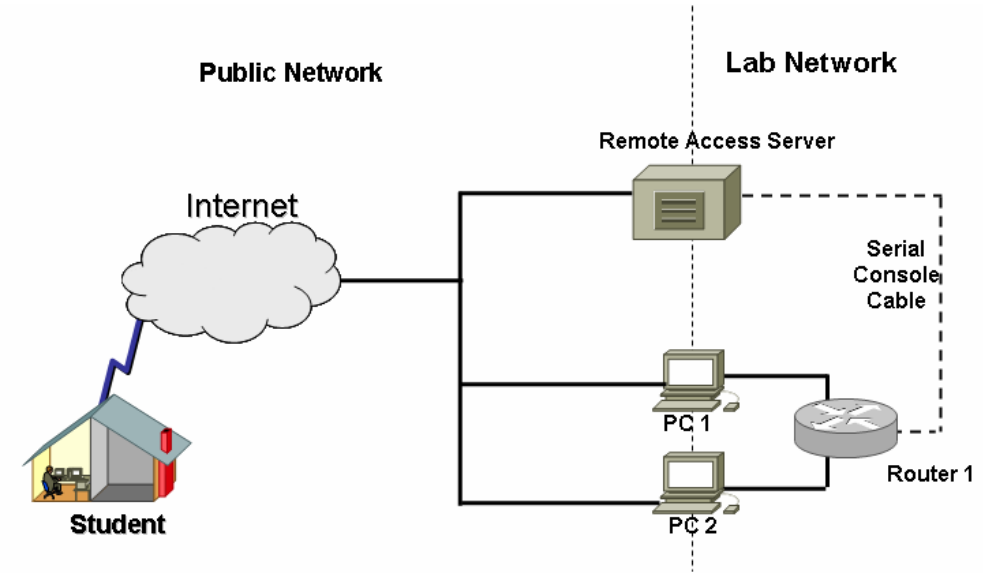

Figure 1. Minimum remote lab topology without a firewall.

Providing DE laboratory exercises in computer information systems curricula have evolved somewhat over the past years. As shown in Figure 1, a simple DE lab environment can be supplied by connecting laboratory equipment to the Internet. For the case of computers, remote access is easily obtained using technologies such as remote desktop for Microsoft based machines or secure shell (SSH) for Linux/Unix based

machines. Access to network equipment serial interfaces can be provided through a remote access server providing a remote virtual terminal to a physical serial administrative interface. Thus the student can control and configure one or several devices and test the interaction of these devices in a laboratory network. Note that the PCs must have two network interface cards, one for student access and one for access to the laboratory network. If a student mis-configures the access NIC, the connectivity is lost to the machine and a visit to the lab is required to fix the problem.

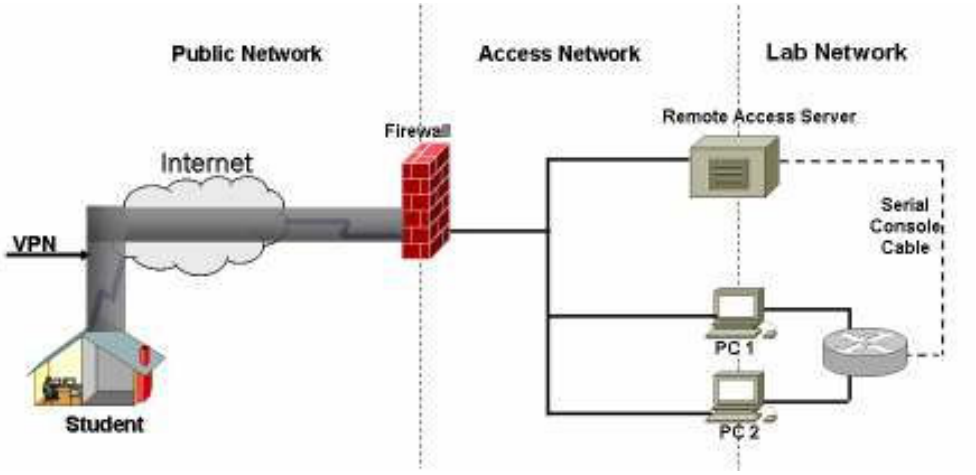

Figure 2. Remote lab topology using a firewall to isolate the access network from the public network.

The next evolution of DE IT labs included the use of a firewall to isolate the access network from the Internet as shown in Figure 2. Note the difference in the access network and the laboratory network. The access network is adjacent to the firewall and contains traffic for remotely configuring and controlling the laboratory equipment. The laboratory network is the network where the laboratory equipment interacts. This configuration has several advantages:

- Access to the laboratory equipment is more easily controlled.
- With the appropriate software, the firewall can act as a scheduler, allowing students to reserve times for access to the remote laboratory. The firewall can also enforce these reservations by allowing only access to students with reservations.
- Access to the remote equipment can be logged. The amount of time that a student uses the equipment can be verified via the logs. These logs can also be used to justify the purchase of more equipment.
- By utilizing a virtual private network (VPN) all of the traffic in the public network (the Internet) can be encrypted, allowing an extra layer of security against anyone wishing unauthorized access to the equipment.
- The firewall can restrict unauthorized traffic coming out of the access network. For instance, if a laboratory machine is compromised and the intruder tried to use the machine as an open email relay to propagate spam, the firewall could block this unauthorized traffic.

- Public IP addresses can be conserved. With the use of a VPN, the access network can use private IP addresses instead of public addresses.

When considering this topology for a DE laboratory focusing on attack understanding, there is no guaranteed isolation similar to what can be found in a non-DE laboratory. For a face-to-face class, laboratory equipment can be separated with an air gap as long as the following equipment is excluded: wireless interfaces, infrared interfaces, EoP (Ethernet over Power) interfaces, and any removable media carried in by students. In a face-to-face lab there is no access network because the students are sitting in front of the machines. Are DE networks configured as in Figure 2 adequately isolated for attack understanding exercises? For the case of closely monitored networks, the answer may be yes. For instance, the cyber Defense Competitions between the students at the five U.S. Service Academies has used a topology connected via VPNs [3,4]. But in this case the network is closely monitored and the students are not novices and are closely supervised. Moreover, the students in this competition are not acting as the attacker. For the case of a 24/7 available DE lab used in conjunction with an attack understanding based course, many would argue that this isolation is not adequate.

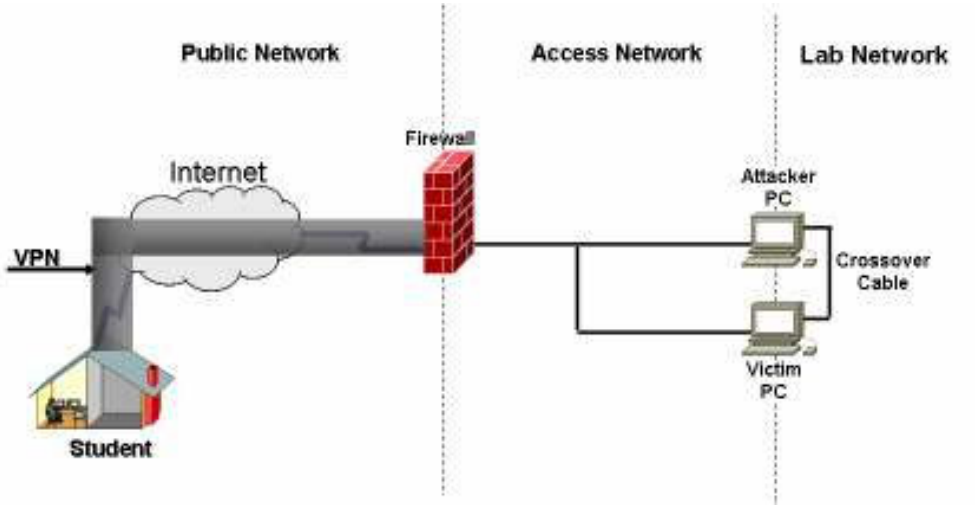

Figure 3. Minimum remote lab topology for investigating attacker-victim machine interaction. This topology does not supply adequate isolation because the attacker PC is only isolated from the public internet by a single firewall.

For instance, take the example of a laboratory exercise that demonstrates the use of an email Trojan Horse. As shown in Figure 3, only two laboratory machines are needed to demonstrate this exercise. The attacker machine sends an email to the victim machine with an attachment such as Sub7 (http://www.hackpr.net/~sub7/main.shtml). The victim machine executes the attached file and a backdoor is silently installed on the victim machine. The attacker machine then can surreptitiously gain control of the victim machine through the laboratory network. This exercise provides a powerful demonstration to students, especially students majoring in non-computer related fields. For an example such as this, many would argue that the DE topology provided in Figure 2 is inadequate. That is, there is no total guarantee that the remote student is absolutely

prohibited from either unintentionally or intentionally downloading the Trojan Horse to the student's computer. Of course there exists layered defenses against this such as the firewall, but most information assurance educators would consider this defense as inadequate. However, in a face-to-face lab where the lab is monitored, and there is an air-gap isolation (i.e. no access network), this may be acceptable if other safeguards are in place (e.g. no wireless interfaces, no removable media allowed).

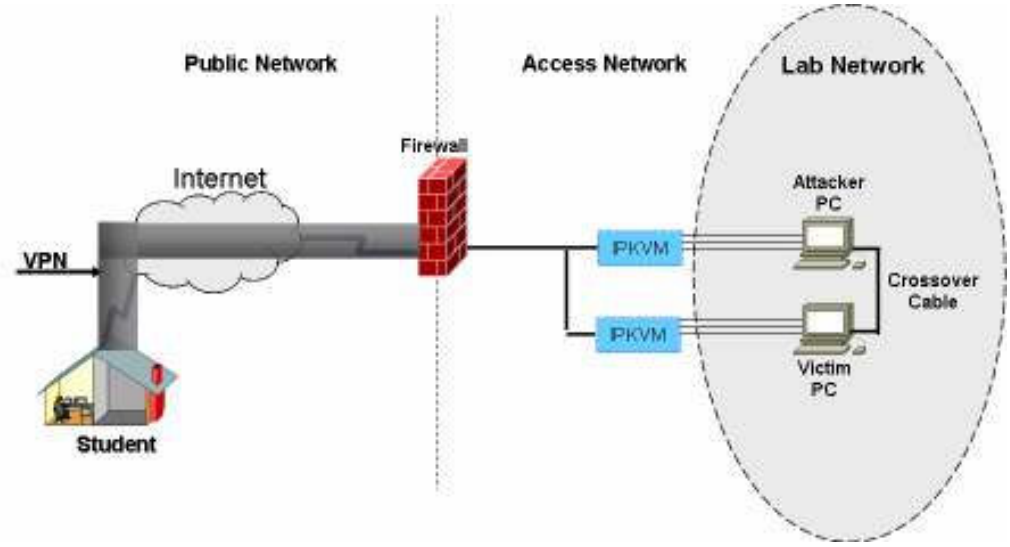

Figure 4. Remote Lab Topology using IP based KVM Switches. Note that only one student can work simultaneously and independently.

Figure 4 introduces a new DE topology that makes use of IP based KVM (Keyboard-Video-Mouse) switches. As before, a firewall acts as an interface between the public network and the access network. However, instead of the access network connecting directly to the lab machines the access network connects to the IP-KVM switches. These switches have been developed for remote server configuration and maintenance, but are applied here to add an extra layer of almost-air-gap isolation to the laboratory network. Note the dotted isolation boundary shown in Figure 4. The only cables that cross this boundary are the cables for the keyboard, mouse, video, and power for the laboratory network and devices. Many keyboard/mouse connections now can be USB based and some IP based KVM switches support this along with other functions such as remote floppy drive support. The use of USB-based connections is not recommended by the authors as this provides a weaker layer of security especially if the KVM switch is compromised. For the configuration shown in Figure 4, only PS/2 cables, video cables, and power cables should cross the isolation boundary.

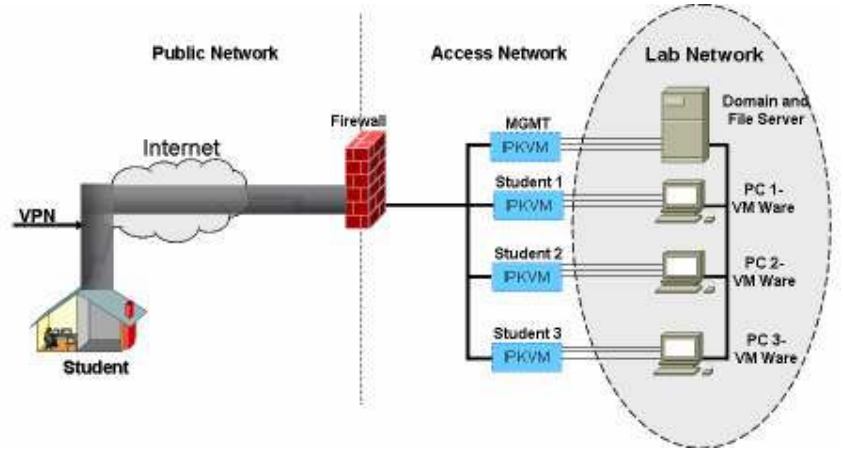

Figure 5. Remote Lab Topology using IP based KVM Switches and VMWare emulation software. Note that 3 different students can work simultaneously and independently. Students returning for follow-on labs can use any of the three PCs because the previous work is stored on the file server in the isolated lab network. The MGMT IP-KVM switch is used only by the instructor to remotely manage the laboratory network.

Figure 5 shows the addition of the use of a virtual environment such as VMWare (http://www.vmware.com/). The use of this kind of software has been applied to face-to-face air-gap isolated labs and has several advantages:

- The topology and computer configuration can easily be reset by just copying the (very large) configuration files. If the file system is configured correctly, this can even be accomplished by the student without instructor intervention, a very important aspect in labs that are available 24/7.
- Multiple devices can be emulated by a single machine.
- Network topologies and configurations can easily be changed in software, thus the same setup can be used for different laboratory exercises or even different classes.
- The file server provides access to laboratory exercise configuration files and to store student specific data. This provides several more advantages:
    - The system scales easily by adding more client lab machines and associated IP-KVM switches.
    - The system easily supports multiple classes and courses. Machine access is managed by the firewall system.
    - The instructor may monitor student progress by viewing files on the file server.
    - Students are not tied to a single lab machine.
- There is no access NIC that the student can mis-configure.

There are several disadvantages to this network system that include:

- Cost: The lab machines hosting the virtual environment must be powerful and have a large amount of memory.
- Non-PC based machines (e.g. routers, switches) are difficult to implement.
- Attacks based on timing are difficult to accurately emulate.

- Network size is limited.
- The large file sizes associated with virtual machines effects the file server performance.

A configuration similar to Figure 5 using AMI MegaRACK IP-KVM switches, a Windows-based laboratory host OS, and VMWare Workstation version 5 was used to teach an advanced network security course with 21 students during the fall semester of 2005 and used only two lab PCs. Remote laboratory access was available 24/7. Informal student surveys indicated general student acceptance and success. Formal assessment studies that reflect student learning, remote lab comfort level, and hardware usage will be published as data is acquired.

Conclusion

The teaching of attack understanding based information assurance requires the use of guaranteed isolation of laboratory networks. Providing Distance Education courses with a remote laboratory network presents challenges to providing adequate isolation. The use of IP-KVM switches adds a very strong layer of isolation, and in combination with the use of emulation software such as VMWare or other virtual operating system environment, provides an adequately isolated laboratory network for some exercises.

References

[1] Frincke, D., "Who watches the security educators?", Security & Privacy Magazine, IEEE Volume 1, Issue 3, May-June 2003 Page(s):56 – 58

[2] Eppes, T. & Schuyler, P., "A General-Purpose Distance Lab System", International Journal of Modern Engineering, Volume 5, Number 2, Spring 2005

[3] Dodge, R.C., Jr.; Ragsdale, D.J.; Reynolds, C., "Organization and training of a cyber security team" Systems, Man and Cybernetics, 2003. IEEE International Conference on Volume 5, 5-8 Oct. 2003 Page(s):4311 - 4316 vol.5

[4] Dodge, R.C., Jr.; Ragsdale, D.J.,"Organized cyber defense competitions**",** Advanced Learning Technologies, 2004. Proceedings. IEEE International Conference on, 30 Aug.-1 Sept. 2004 Page(s):768 - 770