Design of a Network Security Teaching and Research Lab

Jeffrey L. Duffany, Ph.D.
Universidad del Turabo, Gurabo, PR, USA, jduffany@suagm.edu

ABSTRACT

Important considerations in the design of a network security teaching and research lab are discussed in the context of the Universidad del Turabo's Graduate Network Security Certificate program. The main objective is to provide a learning and research environment for the student to enrich their understanding of the network and computer security theory taught in the classroom with an extensive set of complementary hands-on laboratory exercises.

Keywords: Network Security, Certificate Program, Education

1. INTRODUCTION

Many industries have become more and more dependent on computer systems, networks and the internet as an integral part of their day-to-day operation. These systems and networks are vulnerable to a wide variety of security threats which can adversely affect the productivity of these industries (Stallings:2006, Amoroso:1994). As a result, there is a need for industry professionals in the information technology areas to gain increased proficiency in the area of network security. Traditional electrical and computer engineering programs at the undergraduate and graduate level do not typically provide the in-depth kind of training and state of the art information required to perform effectively in this rapidly changing branch of information technology. As a result it was desired to develop a one-year certificate program in Network Security targeted towards information technology professionals. This project was also designed to complement the new Masters degree in Telecommunications that was introduced by the University of Turabo in August 2003.

The typical student will already hold a college degree and be already working in industry in an information technology or management position. The expected outcome of the completing the certificate is to allow interested students and employees in local industries to raise their overall level of proficiency in the area of network security within a relatively short time frame. It requires a laboratory of equipment geared towards providing the student with hands-on experience in setting up secure networks. Experience gained can be brought directly into the work environment. Over the longer term, this initiative can provide a laboratory for research investigations in the areas of network and computer security.

2. NETWORK SECURITY LABORATORY DESIGN CONSIDERATIONS

The main goal is to develop a one-year Network Security Certificate program that provides a solid technical foundation for the student and at the same time addresses the immediate needs of a networking professional in terms of practical skills to maintain acceptable operating security levels and to respond to threats, intrusions and attacks on a network. To provide this type of learning experience a laboratory dedicated to network security was designed and implemented at the Universidad del Turabo.

The approach taken was to first look at the various types of industry accreditations available which includes primarily the GIAC (Global Information Assurance Certification) and the CISSP (Certified Information System Security Professional) (Harris:2005). It was decided to base the program on CISSP since it is more closely aligned with the list of core topics that can be found in textbooks such as Stallings (Stallings:2006) and Pfleeger (Pfleeger:2005). This provides a significant value-added aspect to the program which makes it easier for the student to leverage off of the material learned in the Network Security Certificate Program and apply that knowledge to obtain the industry-recognized CISSP Certification. The curriculum and the textbooks are a major consideration in the design of a laboratory environment that can be tightly coordinated with the material and theory taught in the classroom. Another consideration was an attempt to align the curriculum to the required topics specified by the National Security Agency (NSA) center of excellence (NSA:website).

3. NETWORK SECURITY CURRICULUM

The certificate program is composed of a combination of both classroom theory and hands-on laboratory practice. Some of the core topics (Northcutt:2002, Stallings:2006, Sheldon: 2000, Bolinger:2000, Pfleeger:2005, Bryant:1988) that are covered include:

- Public/Private Key Cryptography
- Modular Arithmetic
- Galois Field Theory
- DES/AES/RSA
- Message Authentication
- Message Integrity
- Digital Signatures
- Digital Watermarking
- Key Management
- Kerberos
- Electronic Mail Security
- Secure Hash Functions
- X.509 Certificates
- IPSec (IP Security)
- Virtual Private Networks
- Wireless Network Security
- Remote Access Security
- Password Administration
- Transaction Processing (SSL)
- Steganography
- Firewall design principles
- Trusted Systems
- Computer Viruses
- Database Security
- Intrusion detection
- Hacker techniques and exploits
- Denial of service attacks
- Operating System Security: Windows, Unix, Linux
- Computer Forensics, investigation and response
- Security planning and security audits
- Legal and Ethical Issues

The curriculum is split about equally between network security and computer security. Generally speaking any time information is moved between computing devices it is considered network security. All other topics involving a single computing device are all covered under computer security. The curriculum includes all major topics in the areas of network and computer security which are covered in a four-course sequence:

- Network Security I
- Computer Security I
- Network Security II
- Computer Security II

The student can complete the course of study in one year by taking two classes per semester with each class meeting once a week. Alternatively the student can take two years to complete the program by taking one course per semester. Another possibility is to have a basic certification after completing the first two courses and an advanced certification after completing all four of the courses. The student will learn about the course topics through a combination of class lecture, homework assignments, in-class group exercises and laboratory assignments. The student may be required to take an overview networking class in the first semester if they enter the program without sufficient background in this area.

The text by William Stallings (Stallings:2006) provides most of the material for both semesters of Network Security I and II covering chapters 1 through 10 in the first semester and chapters 11-20 in the second semester. There is a very strong emphasis on cryptography. Students are given a rigorous introduction to the basic elements of number theory, Galois field theory, modular arithmetic, Euclid's algorithms, Fermat's theorem, Euler's phi function, prime numbers and tests for primality. Students are required to demonstrate a complete mastery of these topics to the level of the William Stallings text (Stallings:2006). DES, AES and RSA public key cryptography are covered in detail along with key distribution and management.

The text by Pfleeger (Pfleeger:2005) is used for the first semester of computer security (Computer Security I). The second semester of computer security (Computer Security II) is a series of in-depth projects derived from a number of sources and is variable depending on the instructor. However it usually focuses deeply in the area of computer forensics and other advanced topics such as intrusion detection systems.

4. DESIGN OF LABORATORY FACILITIES AND EQUIPMENT

The network security laboratory consists of a variety of equipment including desktop PCs and servers connected in a local area network configuration. The laboratory supports both wired (Figure 1) and wireless configurations (Figure 2). In Computer and Network Security I the focus is on Microsoft and wired networks while in Computer and Network Security II the emphasis shifts onto Solaris/Linux operating systems and wireless networking. All of the PCs support multiple boot capability and VMWARE (Vmware:website) so that they can run different operating systems such as (Windows 2003 Server, Windows XP, Linux, etc.). Identical hard drives should be provided on all servers so that advanced Microsoft Server 2003 features such as disk mirroring can be deployed. Connections to the internet are provided along with hardware and software firewalls (e.g., Cisco Pix 501 firewall) (Hucaby:2005). The lab should be placed on its own VLAN and be easily disconnected from the campus network so that worm and virus experiments can be conducted without risk of affecting other computers on the network.

Routing equipment, VPNs, WiFi and Wireless access points are also required for a complete configuration (Northcutt:2000, Pahlavan:2002). Traffic loading software and a specialized server for virus incubation/retention are also required along with network monitoring and protocol analysis hardware and software. The laboratory itself will also be used for the classroom environment. Ideally there should be a classroom area and a research area with deskspace for a technician and researcher, cabinets for equipment and shelf space for at least a small research library. The laboratory should be designed so that all students have a good and unobstructed view of the whiteboard and LCD projection screen.

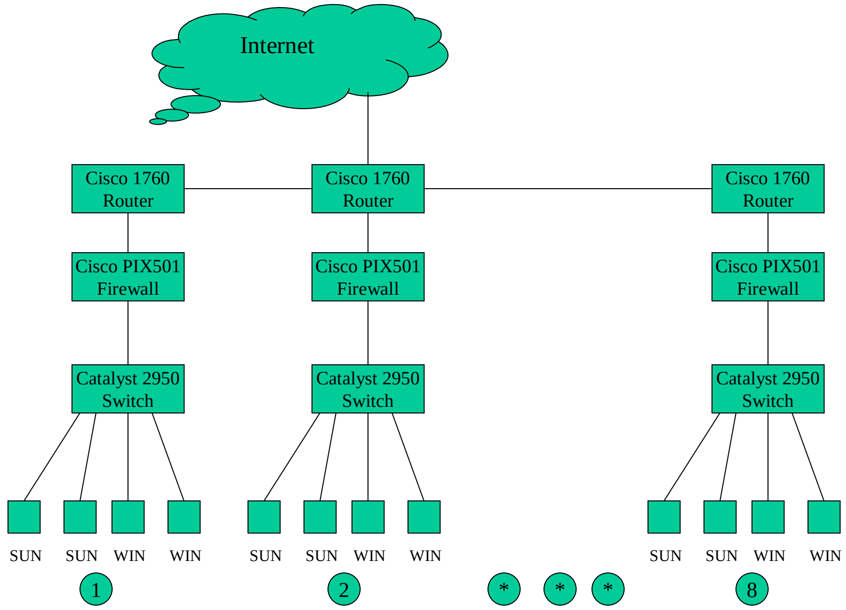

Figure 1. Universidad del Turabo's Network Security Lab (Wired Network Configuration)

Laboratory equipment should include the following as a minimum requirement:

- Desks, chairs, office furniture
- PCs, laptops, servers
- Routers, switches, access points
- Equipment racks and lockable cabinets
- High speed internet connection
- Modems and WiFi cards
- Phone lines for testing remote access
- Hardware Firewalls
- Laser Printer
- Application software
- Whiteboard and supplies
- LCD projector and screen

The Universidad del Turabo's Network Security Lab supports two configurations: ***wired*** as shown in Figure 1 and ***wireless*** as shown in Figure 2. Switching between the two configurations involves only powering down the Catalyst 2950 switch and powering up the Aironet 1100 access points. There is no need to reconfigure any wires.

It was clear from the beginning that it was desired to have a lab that could be used for both teaching and research and that also included both wired and wireless networking. The core of the system was built around Cisco networking equipment and Microsoft 2003 Servers. The choice of Cisco equipment for the networking was influenced by having a standard web based user interface for configuring equipment. Cisco was chosen for its reputation and industry leading feature sets. It was also decided to be in the best interest of the students who could transfer the expertise in Cisco over to an existing job environment. The specific equipment models were chosen for both versatility of use in a teaching and research lab environment and also based on cost-effectiveness.

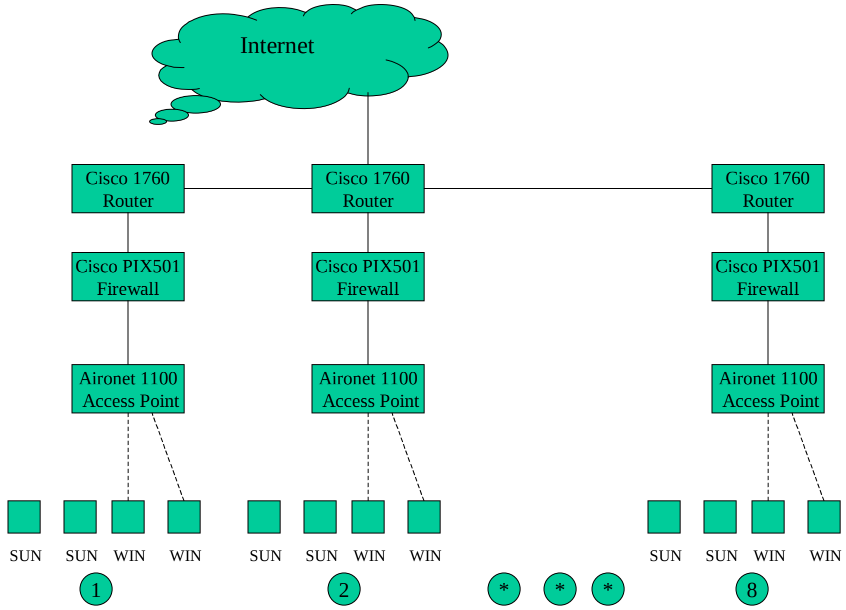

Figure 2. Universidad del Turabo's Network Security Lab (Wireless Network Configuration)

A list of the network security laboratory's computing and networking equipment follows:

- Cisco 1760 router (x8)
- Cisco 2950 switch (x8)
- Cisco PIX 501 firewall (x8)
- Cisco Aironet 1100 Access Point (x8)
- Redhat Linux OS (x16)
- Microsoft Windows 2003 server (x16)
- Sun Solaris Blade Servers (x16)

The network security laboratory was designed for a maximum of 15 students. To ensure a quality teaching environment, each student has their own dedicated server for Windows 2003 and SUN Solaris while networking equipment (such as the router, switch, access point and firewall) are shared by each pair of students. Linux is inexpensive and the computers in the lab can dual boot to Linux essentially for free. Sun equipment is relatively expensive compared to Linux however it can serve a dual purpose by providing SUN training courses to industry. Also SUN gives its software for free or nominal charge to educational institutions which can provide significant leverage to the investment. Both SUN and LINUX have versions that support a trusted OS - Trusted Solaris (now outdated) and SE Linux (security enhanced Linux). The budget of a network security lab should also be funded to include biometric authentication devices such as iris/retinal scan equipment and fingerprint scanning.

Since much of computer security focus is on the operating system and a lot of software is freely available relatively little of the budget was spent on software except for VMWARE and the entire forensic suite from Paraben (Paraben:website). VMWARE (Vmware:website) allows virtual machines to be set up on top of the base operating system. This is useful for experimenting with worms and viruses in virtual machines without any harm to the host system thus and avoiding the need to frequently reinstall the operating system images.

5. LABORATORY ASSIGNMENTS

For computer security classes many labs come from Microsoft Windows 2003 server training (Northrup:2004). There is much to be learned and the Windows 2003 server is very rich in features used for setting security policies, disk backup, disk mirroring, RAID, password administration, system auditing, system logs, configuring UPS (Uninterruptible Power Supply), etc. For network security there is a focus on firewall configuration and both wired and wireless security (WEP and WAP). Many lab exercises can be found in the excellent book by Nestler (Nestler:1998) including a live computer virus (the backdoor subseven virus). Also many resources are available on the internet. For example the Simon Singh black chamber web page (Simon Singh:website) is studied in detail to give the students their first introduction to classical cryptography. The laboratory should be equipped to allow the student to gain hands-on experience with as many of the course topics as possible. Some typical laboratory assignments include:

- Implementing Remote Access Security
- Setting up a Virtual Private Network
- System Security Policies and Auditing
- X.509 Certificate Generation and Administration
- Implementing IPSEC and Security Associations
- Setting up disk mirroring, RAID and UPS
- Setting up and use of auditing and event logs
- File encryption and public key cryptography
- Setting up and implementing a RADIUS Server
- Implementing hardware and software (linux kernel) firewalls
- Recovery from the *backdoor subseven* virus using the registry editor
- Implementing Password policies

6. RESEARCH

Students enrolled in the Universidad del Turabo’s Masters in Telecommunications Program can choose to do a thesis in the area of network security as a partial fulfillment of their degree requirements. The network security laboratory should facilitate this by providing all or part of the lab to be set up for testing environments. In practical reality, teaching and research goals of a laboratory have a tendency to conflict with each other as the lab requires one hardware and software configuration for teaching and a completely different one for research. Therefore the ability to quickly change between configurations is desirable. Virtualization software (Vmware:website) can be used for this as well as the remote installation service (RIS) feature of Microsoft Operating Systems which allows an image of a machine to be restored quickly without having to reinstall all of the software and service packs and software patches. Norton Ghost software can also provide a similar capability.

7. SUMMARY AND CONCLUSIONS

A network security laboratory was designed to support both teaching and research in the Universidad del Turabo's Network Security Certificate and Masters Degree in Telecommunications Programs. The main objective is to provide an environment for the student to enrich their understanding of the network and computer security theory taught in the classroon with an extensive set of complementary hands-on laboratory exercises. The laboratory also serves as the base for research and development of methods, strategies, protocols and procedures to address network and data security issues. The core of the lab is based on Cisco networking equipment for both wired and wireless network configurations which interconnect Microsoft and Solaris/Linux operating systems. Access to the internet is essential for both teaching and research. A network security laboratory should be designed to provide the ability to experiment with worms and viruses without the risk of endangering any other computers on the university-wide campus network. Also, alignment of the lab capabilities and curriculum to the NSA center of excellence guidelines would allow the university to compete for NSA research funding grants.

REFERENCES

Abler, R. "Georgia Tech Information Security Hands on Network Security Laboratory", *IEEE Transactions on Education*, February 2006.

Amoroso, E., *Fundamentals of Computer Security Technology*, Prentice Hall, 1994.

Bolinger, M. (Editor), *Microsoft Windows 2000 Network Infrastructure Administration*, ISBN-0-7356-0989-6, Academic Learning Series, Microsoft Press, Redmond, Washington, 2000.

Harris, Shon, "*All-in-One CISSP Exam Guide*", McGraw-Hill, 3rd Edition, 2005.

Hucaby, David, "*Cisco ASA and PIX Firewall Handbook*", Cisco Press, October, 2005.

Stallings, William, (2006). "*Cryptography and Network Security*", Prentice Hall, 4th edition, 2006.

Pfleeger (2005). "*Security in Computing*", Prentice Hall, 4th edition, 2005.

Macarty, Bill,"*SELINUX, NSA's Open Source Security Enhanced Linux*", O'Reilly Press, 2005.

Nestler, Vincent, J. (1998). "*Security Lab Manual*", Career Education Press, 2005.

Northcutt, Stephen, Zeltzer, Lenny, "*Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems,* Publisher: Que; 1st edition (June, 2002) ISBN: 0735712328.

Northrup, Tony, "*Implementing and Administering Security in a Microsoft Windows 2003 Server Network*", "Microsoft Press, 2004.

National Security Administration (NSA) web site: www.nsa.gov/ia/academia/caeiae.cfm

Pahlavan, K. and Krishnamurthy, P. "*Principles of Wireless Networks*, ISBN 0-13-093003-2, Upper Saddle River, NJ: Prentice Hall, 2002.

Paraben Corporation web site: www.paraben.com.

Sheldon, R. and Wilansky, E. *Microsoft Windows 2000 Server*, ISBN-0-7356-0988-8, Academic Learning Series, Microsoft Press, Redmond, Washington, 2000.

Simon Singh website: www.simonsingh.net/The_Black_Chamber/home.html

Tanenbaum, A. S., *Computer Networks*, Upper Saddle River, NJ: Prentice Hall, 2003.

VMware corporate web site: www.vmware.com.

Authorization and Disclaimer

Authors authorize LACCEI to publish the paper in the conference proceedings. Neither LACCEI nor the editors are responsible either for the content or for the implications of what is expressed in the paper.