Proceedings of the 9th Colloquium for Information Systems Security Education
Georgia Institute of Technology
Atlanta, Georgia, 6-9, June 2005

Design and Development of an Information Security Laboratory

S. Srinivasan, *Senior Member, IEEE*

Abstract: Information Security courses such as Network Security and Database Security require the need for students to test the concepts taught. In order to develop effective countermeasures the students must first learn about the effects of attacks on networks. In a live network of an academic institution it is impossible to provide such a facility for testing and development. A stand-alone Information Security Lab was envisioned for this purpose and was developed over the past two years.

Index Terms: Network security, laboratory, attacks, countermeasures, simulation

I. INTRODUCTION

Information Security is an important component of curricula in Computer Science, Decision Science, and Information Systems programs. Over the past five years, thanks to Presidential Decision Directive 63 [1] and the efforts of the National Security Agency (NSA), five comprehensive curriculum standards have been developed. These standards have been released under the auspices of the Committee on National Security Systems (CNSS). Of these standards, the National Security Telecommunications Information Systems Security Implementation (NSTISSI) 4011 standard is an important standard that emphasizes the fundamental principles of information security [2]. The extensive details presented under this standard cover topics in Network Security, Information Security, Operating System Security, Cryptography, Security Policy, Privacy, and Ethics.

In addition to developing several curriculum standards, CNSS has been designating four-year academic institutions and graduate-level universities as National Centers of Academic Excellence (CAE) in Information Assurance Education using a very rigorous standard [3]. Since the start of this program in 1999, so far 59 institutions have been awarded the CAE designation. The designation is for an initial three year period, after which the institutions must reapply for continued designation as a CAE. The complete list of CAE institutions is available at the National Information Assurance Education and Training (NIETP) website [4].

The University of Louisville (UofL) started offering Information Security courses in summer 2002. The first course offered was at the graduate level. Since then both undergraduate and graduate courses in Information Security have been offered at UofL. The University also successfully mapped the existing Information Security (IS) courses and non-IS courses to the NSTISSI 4011 and 4012 standards in 2003 and 2004 respectively.

II. OUR PROGRAM

The University of Louisville has an undergraduate concentration in Information Security as part of the Computer Information Systems (CIS) degree [5]. The CIS degree program is housed in the College of Business and Public Administration. The college of Engineering at the university has separate undergraduate and graduate programs in Computer Science.

The CIS and Computer Science departments at the university have been offering information security courses for three years now. In courses such as Network Security and Database Security we discuss security design, attacks on networks and possible countermeasures to protect the networks. As part of the learning experience for the students we have tried to assign projects that the students could do to get a firsthand experience in network protection. Attempting an assignment involving a denial of service attack on a live network of any institution is impossible. The best that we have been able to do has been to work with the university's academic computing liaison and give the privilege for the students to do an email

* College of Business and Public Administration
University of Louisville, Louisville, KY 40292
srini@louisville.edu

ISBN 1-933510-99-4/05/$15.00

spoofing. All other attacks and countermeasures remained as theoretical discussions in class.

The students were disappointed to see that they could not get better experience with the types of attacks, viruses and worms that they learn about in classes as well as notice wreaking havoc on the Internet. Occasionally, we were able to put together a few computers and a router and a switch to simulate some of the attacks such as Address Resolution Protocol (ARP) poisoning and keystroke capture. The first and foremost hurdle for developing these types of temporary networks has been the availability of space for safely keeping the system for a semester at least.

After some small successes with the temporary network labs, we started to explore the possibility of designing a permanent Information Security Lab. In the meanwhile, as noted earlier, we had successfully mapped our curricula against the NSTISSI 4011 and 4012 standards. This gave us the opportunity to apply for National Science Foundation's (NSF) Capacity Building grant. The Capacity Building grant is administered by the Division of Undergraduate Education at NSF as part of the Cyber Corps program. The external validation of our Information Security curriculum by CNSS and the number of information security courses that we had offered in the two years prior to that helped us in obtaining a two-year Capacity Building grant from NSF in the amount of $300,000. In seeking this grant we also partnered with the Kentucky State University, located 50 miles from the University of Louisville. The Kentucky State University is designated as a Historically Black College or University (HBCU) by the U.S. Department of Education. Both the University of Louisville and the Kentucky State University were independently awarded $300,000 for two years as part of a single collaborative grant proposal. The Capacity Building grant is limited to $150,000 per year for a maximum of two years. It is possible to apply for renewal of the grant. The NSF grant enabled us to purchase the computers. It also provided summer releases for two faculty members to work on the curriculum aspects of Capacity Building for the Information Security curriculum.

Around the time we were applying for the Capacity Building grant from NSF, the Kentucky Council on Postsecondary Education (CPE) called for collaborative proposals for growing the IT Workforce in the state. We have been collaborating for two years with the Jefferson Community College (JCC) in Louisville as they have a Cisco Academy. The JCC's Cisco Academy offers both Cisco Certified Network Associate (CCNA) and Cisco Certified Network Professional (CCNP) certifications. Usually, the students earning the CCNA or CCNP certifications do not pursue the bachelors degree as they would have to take many more courses at a four-year institution to earn the bachelors degree. The University of Louisville, in partnership with the Jefferson Community College, submitted a collaborative proposal in response to CPE's request for collaborative proposals. The principal component of our proposal was developing a seamless path for high school students to earn a bachelors degree from the university after completing the associate degree at JCC. The program aimed at students who take A+, Network+ or Security+ courses in high schools to get college credit at JCC and earn the CCNA or CCNP certification. After that the students will be able to block transfer their credits towards the bachelors degree in CIS with the Information Security concentration. The bachelors degree would then enable the students to join the workforce at a higher salary level than they would otherwise earn with their Cisco certification alone.

The Kentucky Council on Postsecondary Education favorably viewed our collaborative proposal and funded us for one year at $180,000, with a requirement to get matching corporate support for $20,000. We had planned to purchase Cisco equipment for our proposed Information Security Lab. We came to know about the grants available through the Cisco Critical Infrastructure Assurance Group (CIAG). We invited a CIAG representative to visit our campus to learn more about our Information Security program. After the visit, the CIAG representative donated Cisco equipment valued in excess of $20,000 that helped us meet the matching corporate support requirement from the CPE grant.

III. INFOSEC LAB

The vision of creating a dedicated Information Security Lab was beginning to take shape in summer 2004. The College of Business and Public Administration, where the CIS program is housed, made available 500 square feet of space for the lab. The CPE grant provided funds for

ISBN 1-933510-99-4/05/$15.00

space renovation and furniture for the lab. The NSF grant enabled us to purchase the computers and a network printer. Our Corporate Partners donated three servers. The Cisco equipment grant provided all the routers, switches and a firewall. Figure 1 shows a layout of our InfoSec Lab.

outlets. Our goal is to use the router and configure two different LANs out of the 16 workstations overall.

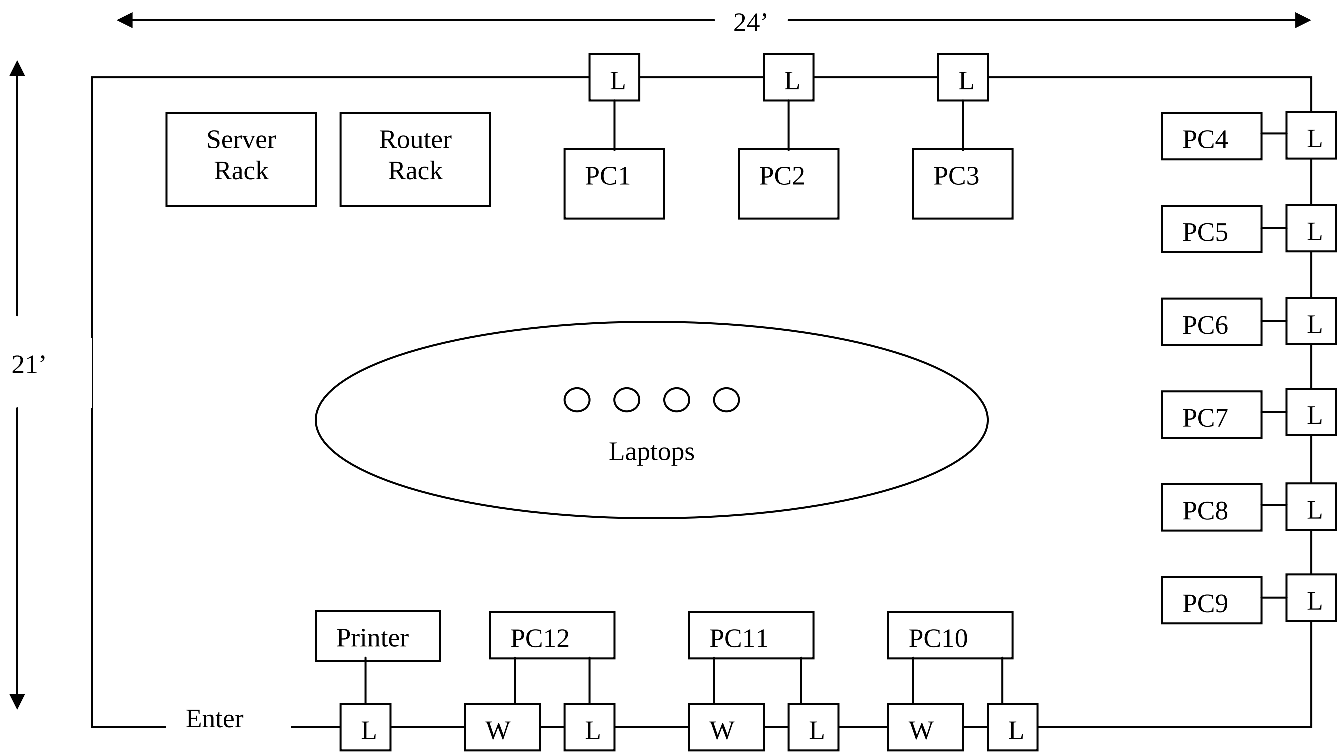

Figure 1

The Lab has a number lock and each student has been assigned an access code for the Lab. Thus, the Lab is basically available for student use at all times the building is open. The Lab has three dedicated servers. We have a different operating system in each server. The operating systems in use are: Windows 2000, BSD Unix and Red Hat Linux. There are 12 workstations that are connected to one server at a time through a Cisco switch. Changing the connection from one server to another is simply a matter of changing one patch cable connection to the switch. Nine of the twelve workstations are on the LAN only. Three of the twelve workstations can be connected to either the LAN or the WAN. In addition to the workstations, we have provided a facility for four laptops to be connected to the network, for a total of 16 nodes on the network. All nodes have access to a network printer. For each workstation, we have provided two LAN

The Lab became operational in January 2005. Students in the Database Security class are currently using the Lab. We are running SQL Server 2000 in the Windows Server and My SQL in the Unix and Linux servers. The nodes on the network are controlled by an Active Directory on the server. Since the Lab is dedicated for the Information Security program students only, we were able to set up the SQL Server first with SQL Server authentication and test some of the vulnerabilities posed by that setting. Then we changed the authentication to Windows authentication which is much stronger. First, we let the SQL Server 2000 unpatched and the students tested the software version using SQL Ping, a tool usually used by hackers to identify the patch level on application software. After the students had a chance to test that aspect of a database security, we applied Service Pack 3a for SQL Server 2000. Students then used the SQL

ISBN 1-933510-99-4/05/$15.00

Ping command again to note that the SQL Server version number changed. Next, the server setting was changed to "hidden" and the students were able to note using SQL Ping that the port number changed to 2433 from 1433.

The students in the class were divided into four groups of four students each. Two standalone computers were added to the Lab for additional testing purposes. Each group was asked to install SQL Server 2000 on one of the standalone computers and choose the appropriate settings and create accounts for students in other groups. Students were given an assignment in which the students were asked to grant suitable permissions first, then deny the permissions and then finally revoke the permissions. This exercise gave the students a hands-on experience with SQL Server installation and the security settings allowed by the software. The next assignment involved testing buffer overflow attack. The students were able to simulate the buffer overflow attack on the two standalone computers that were not patched by executing extended stored procedures and see how the buffer overflow brings down the server. The students then tried to execute the same extended stored procedures on the main Windows server that had been patched and note how the buffer overflow attack failed.

In the next assignment, students in the Database Security course tested SQL Injection. This assignment involved testing various types of injection commands, ranging from simple access to SQL for an unauthorized user, to deleting the users file, and running queries that are prohibited. Students tried these assignments on the unpatched and patched servers. Additional assignments planned at this time include testing the use of firewall to prevent attacks on the database as well as using appropriate encryption for protecting the database. The encryption assignment is intended to help the students understand the performance issues related to databases.

The description presented in this section so far gives an overview of how the lab has been used by the students. The lab is for use both in teaching and research. The following tables summarize the use of the lab for teaching and research.

Table 1. InfoSec Lab use for Teaching

Course	Planned use
Network Security	Email spoofing, IP-spoofing, ARP poisoning, Network sniffing, use of Firewalls and Virtual Private Networks, Development of countermeasures to attack scenarios
Information Security	Centralized and distributed management of policies and procedures, Periodic updates, Impact of Social Engineering attack on policies implementation
Cryptography	RSA algorithm implementation, Simple cipher techniques development, Evaluation of encryption methods for response time in practical scenarios
Database Security	SQL Server 2000, Oracle and MySQL installation, creation of new accounts, and security settings on multiple operating systems (Windows 2000, 2003, Unix and Linux), Buffer overflows, SQL injection, and Bulk copy

Table 2. InfoSec Lab use for Research

Lab setting	Planned use
Wired lab	Vulnerability identification, Development of patches, Integration with wireless nodes for high speed, high security communication
Wireless lab	Mobile Ad hoc Network security and performance evaluation, Mobility management

IV. FUTURE UPGRADES

The first upgrade planned for the lab is the purchase of a video surveillance system. The next planned upgrade is the purchase of a high-performance server. This server will have VMware installed and run Windows Server 2003, BSD Unix and Red Hat Linux. Each of the workstations will then have the VMware client software installed to choose the appropriate operating system from the server. Next, the laptops will be equipped with high security wireless cards and the laptops allowed to roam outside the Lab and connect to the server wirelessly. This will help us test the wireless security aspects of the network. After this upgrade, the laptop communications will be monitored using another system for packet sniffing. The workstations in the Lab will be equipped with network sniffer software and attacks such as Address Resolution Protocol (ARP) poisoning will be simulated. Voice over IP (VoIP) software will be loaded in one of the servers and VoIP phones installed in the Lab for testing purposes.

V. IDEAS FOR BUILDING A SIMILAR LAB

The details provided in this paper lay out our experience in building an InfoSec Lab for teaching and research. Any institution that is planning to offer courses in Information Security area will find it beneficial to consider the following points:

1. Identify the courses that your institution is interested in teaching
2. Identify at least a 600 square feet of space for building a dedicated lab
3. Explore the availability of funding from internal sources as well as external sources such as the National Science Foundation and businesses specializing in security of communication and storage
4. List the benefits of a dedicated lab for information security that does not interfere with the institutions computer network
5. Plan the use of the dedicated lab both for teaching and research as well as curriculum development. Organizations such as Microsoft and Cisco Systems have curriculum development grant possibilities.

VI. SUMMARY

The availability of the dedicated Lab for Information Security has tremendously helped our students to test various aspects of database security at this time. In the semesters to come we will be using the Lab for testing attacks on Networks and developing countermeasures. The ability to add and remove software quickly as well as to apply various levels of patches for learning purposes has given a good exposure to managing security. Also, the availability of two additional computers that were not on the network gave the students the opportunity to learn about the various security settings involved in installing SQL Server as well as setting the user permissions appropriately. Such tests could not be performed on a live network of an academic institution. Overall, the availability of the dedicated InfoSec Lab has helped the learning environment significantly as evidenced by the positive student comments.

VII. REFERENCES

[1] PDD-63,
http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (accessed on March 5, 2005)

[2] NSTISSI Standards
http://www.nsa.gov/ia/academia/cnsstesstandards.cfm (accessed on March 5, 2005)

[3] CAE Criteria
http://www.nsa.gov/ia/academia/caeiae.cfm?MenuID=10.1.1.2 (accessed on March 5, 2005)

[4] CAE Institutions
http://www.nsa.gov/ia/academia/caemap.cfm?MenuID=10.1.1.2#completeList (accessed on March 5, 2005)

[5] InfoSec Program at University of Louisville
http://www.louisville.edu/infosec (accessed on March 5, 2005)

ISBN 1-933510-99-4/05/$15.00 © 2005 IRI/CISSE