DESIGN OF A LABORATORY FOR INFORMATION SECURITY EDUCATION

Vikram Anantapadmanabhan, Nasir Memon, Phyllis Frankl and Gleb Naumovich
Polytechnic University
Brooklyn, NY 11201.
vikram@isis.poly.edu, memon,frank,gleb@poly.edu

Abstract It has been recognized for some time now that education in information security is better served by a laboratory component that reinforces principle and theoretical analysis learnt in the class room with a follow-up hands-on component performed in an appropriate laboratory. In this paper we present the design of a highly reconfigurable laboratory for information security education. The design has been implemented successfully in ISIS - The Information Systems and Internet Security Laboratory at Polytechnic University. We also describe the rationale for our design and give examples of a few typical assignments that the laboratory facilitates.

Keywords: Laboratory Education, Network Security Laboratory, Information Security Laboratory, Network Security Eduction, Information Security Education, Information Assurance Education

1. Introduction

The recent focus on security education, kindled by the NSA Center of Excellence in Education program [3] has seen a variety of universities add a security component to their computer science and engineering curriculum. As a result, we now have 36 universities that have been designated as Centers of Excellence in education. However, a significant number of programs continue to teach information security in the decades old traditional framework, focusing solely on theoretical principles and their analysis. Although theoretical concepts are essential and need to be taught, it is very important to also show students how to apply the theory they have learnt in very different and important practical situations. Hence, a good part of an information security course should

also focus on applications and operational concerns. In order to do this, a supporting laboratory becomes necessary.

Recent years have seen an increased awareness on the importance of a laboratory component in information security education [7, 1, 5, 6]. In [7], Irvine points out that securing a system requires a "marriage" of good science and engineering. And that engineering components are best taught by reinforcing concepts taught in the class by hands-on experiences in the laboratory. She further points out that just as it is unreasonable to expect a student to learn programming only by reading about it, it is also unreasonable to expect students to learn "security engineering" solely from discussions in the class room. Similarly, [5] and [6] also make the case for laboratory based instruction in information security and in fact provide detailed examples of specific courses and lab projects that accomplish this goal.

A laboratory for information security education can be designed in a different manner depending on the nature of the program and the course being serviced. However, there are certain general principles that guide the design of such a laboratory. Specifically, a well designed laboratory should possess the following characteristics:

- *Reconfigurable:* The lab should be highly flexible and re-configurable. Different topics and assignments require different operating systems and/or network topologies and it should be possible to change the configuration of hosts and networks easily and efficiently.

- *Heterogeneous:* The lab should comprise of multiple platforms from multiple vendors. A lab with homogeneous environment does not effectively train students to cope with real world situations.

- *Scalable:* The lab should be scalable and should be able to sustain many students, and still have enough duties for each student to handle. Student groups should not get large due to lack of resources.

- *Cost Effective:* The cost of setup and maintenance of the lab must be far less them whats being simulated by the lab. For example, the lab should effectively simulate a small to medium enterprise network but the cost for building and maintaining the lab should be far less then the cost of a moderate enterprise network.

- *Robust:* The lab should be able to sustain and handle inadvertent damage by the students. For example, it should be possible to quickly recover the set-up and configuration of a host node even

after a student accidentally causes a malicious program to erase the hard disk.

- *Maintainable:* The lab should be easy to maintain. Routine tasks like back-up and application of software patches should be easy to perform and automated to whatever degree possible.
- *Realistic:* The lab should provide practical and first hand experience to students in a network environment that is close, in terms of complexity, to a network that they might encounter in a a real world enterprise.
- *Insulated:* Activities in the lab should not effect traffic on the campus network. There should be sufficient amount of separation and isolation enforced between the lab network and the external network. The presence of the lab should not be a cause of concern to campus network authorities.

In the rest of this paper we describe the design of ISIS - An Information Systems and Internet Security Laboratory at Polytechnic University, which aims to achieve the above listed design goals. ISIS was initially started as the result of an NSF CCLI grant to develop a sequence of undergraduate courses in computer and network security and an accompanying laboratory. Initial lab and course design was done with the assistance of ISSL [2] at Iowa State University which has long been an NSA designated Center of Academic Excellence in information assurance education and research. ISIS has been running for more than two years now and the lab and the courses it supports have proved to be immensely successful. In fact the role of ISIS has been significantly expanded beyond its original scope and design and it now serves as a center of education and research in information assurance at Polytechnic University.

The rest of this paper is organized as follows: In the next section we describe the overall architecture of ISIS and two of its smaller components - the student workstation network and the server cluster. In Section 3 we describe in detail the design of the core of ISIS, a secure systems experimental testbed. In Section 4 we describe briefly some typical assignments supported by ISIS and in Section 5 we conclude with a brief discussion on future plans for expanding ISIS.

2. ISIS Architecture

ISIS consists of heterogeneous platforms and multiple interconnected networks to facilitate hands-on experimentation and project work in

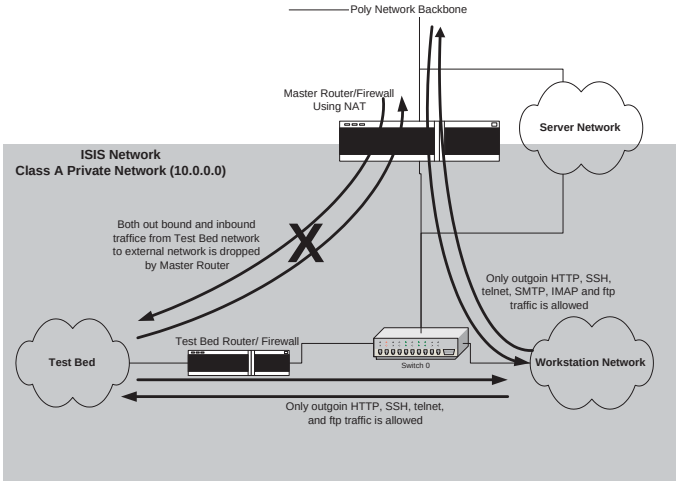

Figure 1. ISIS lab architecture overview showing its three main components - 1) ASSET - A Secure Systems Experimentation Testbed, 2) The Student Workstation Network, and 3) The Server Cluster - and their interconnection with each other and with the campus network backbone.

issues related to information security. ISIS lab is divided physically and logically into three areas, namely:

- The Student Workstation Network,
- The Server Cluster,
- A Secure Systems Experimentation Testbed (ASSET).

Figure 1 shows how these three components are interconnected with each other and also with the external campus network. The student workstation network and the testbed ASSET are inside a class A private network so that they are isolated from traffic on the campus network and the internet. The private network is created using a router with NAT capabilities. This router is shown in Figure 1 labelled as the"Master Router". Usually a private network is created to hide internal network topology and expand the range of IP address availability. In our case it is critical to separate our network traffic from the external network in order to stop internal traffic, malicious and otherwise, from reaching the external network. The router will prevent packets from internal traffic to escape out into the external network.

The second advantage that a Class A private network provides is the large number of subnets that can be created within it. We could potentially have 2^{16} subnets with 250 hosts in each subnet in the network.

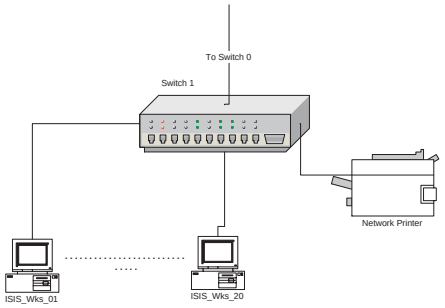

Figure 2. Physical network layout of the student workstation network.

This fact is critical to the design of our testbed network, as is explained in the Section 4.

In addition to performing NAT, the master router also is configured to act as a firewall in order to impose restriction on traffic flowing to and from the internal network. Furthermore, traffic from and to the testbed network from the workstation network and the server network is restricted by a second firewall labelled as the Testbed/Router Firewall in Figure 1. This ensures that any attack traffic in the testbed network does not enter the workstation network or the server network.

2.1 The Student Workstation Network

The primary purpose of the workstation network is to provide students a means to access the ASSET network. Typically, for most assignments, students have to be physically present in the lab and logged on to a workstation in order to access ASSET. The workstations themselves are Pentium 4, 1.5 GHz general purpose machines, running Windows 2000 and equipped with standard university lab software, like compilers, editors etc. They are members of the ISIS active directory server present in the server network. Currently there are 20 workstations as shown in Figure 2.

Individual workstations in this network are completely locked down physically by using padlocks on the machines and also by appropriate configuration of BIOS settings and Windows domain policies and restrictions. For example, students cannot reboot these machine using bootable floppies or CD's. They cannot install or remove any software, and connect or disconnect these computers from the network. They are only allowed to use the applications that are installed on the workstations. The software restrictions are enforced using Windows 2000

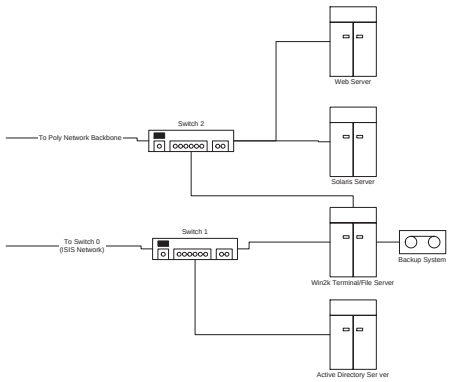

Figure 3. Physical network layout of the server network.

domain policies and restriction suggested by NSA's Windows 2000 lock down guidelines (http://www.nsa.gov/snac/index.html).

Although students are only allowed to store their files on the file server and not in the workstation they work on, they are still provided some writable space in each workstation. Without user writable space, Windows will not allow any user to log on. This space is very small (10MB) and each workstation is cleaned occasionally by erasing all users temporary directories, and/or re-installing a fresh image, if necessary, during the cleaning process.

2.2 The Server Cluster

The server component of ISIS currently is composed of four serves: 1) A Web server, 2) A Solaris server, 3) A Win2k Terminal/File server and 4) An Active Directory server. The BSD web server is used to host labs and students web pages. The Solaris and Win2k terminal servers are used by the students for compute intensive tasks like password cracking and cryptanalysis. These servers also contain a repository of security related tools that students need for their projects and assignments. The active directory server is used to manage the ISIS lab active directory. The Win2k server is also used as a file server to store student files. Each student is allowed to store up to 5GB's in the file server and their files are automatically backed up by the backup system and also screened for common viruses frequently. The total storage capacity on the server network exceeds half a terabyte.

The server network can facilitate secure remote access to our network via the Windows terminal server. We use a dual homed Win2k terminal

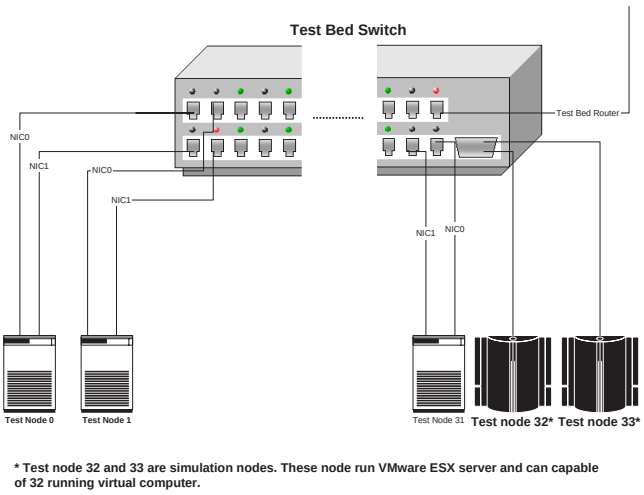

Figure 4. Physical layout of ASSET.

server for remote access. The remote access server is also part of the ISIS active directory, so all users in the active directory can potentially access the secure systems experimental testbed from a remote location. This was done to facilitate students who cannot be physically present in the lab.

3. ASSET - A Secure Systems Experimentation Testbed

In this section we describe the third component of ISIS - A Secure Systems Experimentation Testbed (in short ASSET). ASSET is the core of the lab and this is where most of the lab activities take place. It consists of a highly reconfigurable network built around a layer 2 switch, 32 computers fitted with two or more NICs and removable hard drives, and two mainframe class hosts as shown in Figure 4.

ASSET is designed to be flexible and highly reconfigurable. Flexibility in terms of network layout and software running on end nodes is necessary as this allows us to support assignments of vastly different nature and scope with the same resources. The need for flexibility in terms of operating system can be seen in assignments like Linux and Windows hardening. These assignments follow each other and its important that we are able to change the operating system on a large number of nodes in a reasonable amount of time (say a few hours). A dual boot architecture will not suffice as we need the ability to load ASSET hosts with

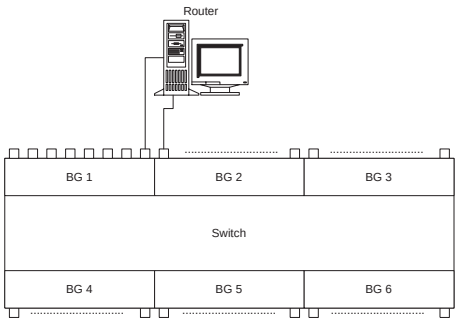

Figure 5. A switch divided into 6 bridge groups, each bridge group represents a VLAN. Figure also shows how two bridge groups could be connected using a router.

selected versions of an operating system with deliberate misconfigurations for students to discover and fix. It is also important that we have the ability to restore these nodes to a default state in minutes, after inadvertent damage by a a student. In order to achieve these goals we use nodes with removable hard drives. This way we can load or restore a node by simple replacing its hard drive. A hard drive duplicator allows us to load the same configuration in multiple hosts. Disk images of different versions of different operating systems, and applications with and without flaws, are stored on the server network and can be copied on to a disk in minutes, and can then be duplicated and loaded in multiple hosts.

The need for flexibility in terms of network layout arises from the variety of network security assignments that students are required to perform, ranging from network fingerprinting, penetration testing, intrusion detection and prevention, and finally war games. Again, such assignments follow each other in a logical sequence and one needs the ability to reconfigure the network topology from one assignment to the other in order to meet the specification of each assignment. Furthermore, in certain more complex assignments it is also desirable to mimic a slowly changing enterprise network and this leads to the need for an ability to automatically change network layout by means of scripts and without human intervention.

To make ASSET flexible in terms of network layout we use Virtual LAN's (VLANs) and create logical networks. We do this using a switch with VLAN support. In a conventional switch, all ports belong to the same broadcast domain (i.e. one switch represents a network segment) and many networks can be created using multiple switches interconnected with a router to represent an enterprise network. An example of

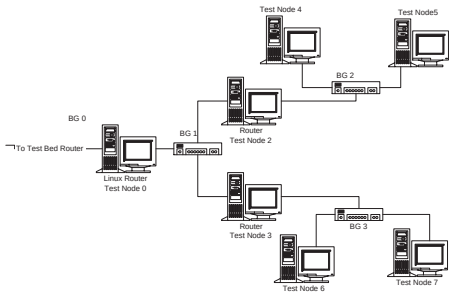

Figure 6. An example of small network with 4 network segments, built using an independent switch to support each network segment. Each network segment is interconnected using a Linux router.

such a network is depicted in Figure 6. With a switch that can support multiple VLANs, it is possible to create such a network without having multiple switches, and we can change the network layout without changing the physical layout.

With a switch with VLAN support, VLANs can be created and modified by changing the software configuration of the switch to which all the hosts on the network are physically connected to. Using VLANs it is possible to create independent virtual broadcast domains within a switch as shown in Figure 5. Also, a switch with VLAN support can have multiple broadcast domains. We could interconnect these domains by having a router between them (Figure 5) and the network in Figure 6 could be created by configuring the switch to have multiple VLANs and physically it would look like what is shown in Figure 7.

More complicated networks as shown in Figure 8, can be created using the two mainframe class computers (nodes 32 and 33 in Figure 4) in combination with the other 32 computers. These two machines can run up 32 virtual computers using VMwares ESX operating system. ESX server is a mainframe class computing environment, and is capable of having internal networks independent of the external network. Node 32 and 33 can be used to simulate a changing network. There are 16 virtual test networks inside each node and the network topology is dynamic. Using a skillfully crafted script one can periodically change the internal network configuration of the VMware network to simulate a changing network. This kind of a network, for example, could be used in routing vulnerability analysis assignments.

From the above discussion, we can see that ASSET meets the design goals of reconfigurability, heterogeneity, maintainability, and robustness. The dual firewalls and private network provide sufficient isolation to

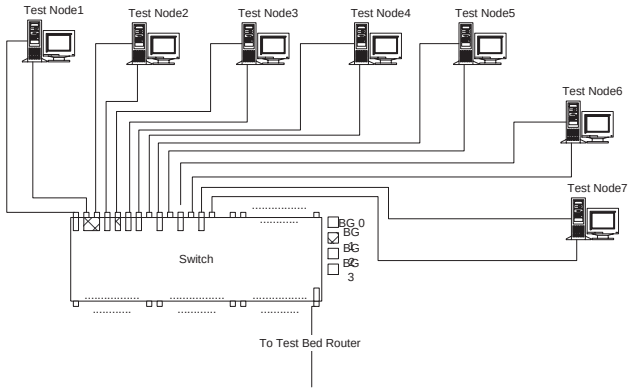

Figure 7. The network depicted in Figure 6 implemented in a single switch configured to support 4 bridge groups.

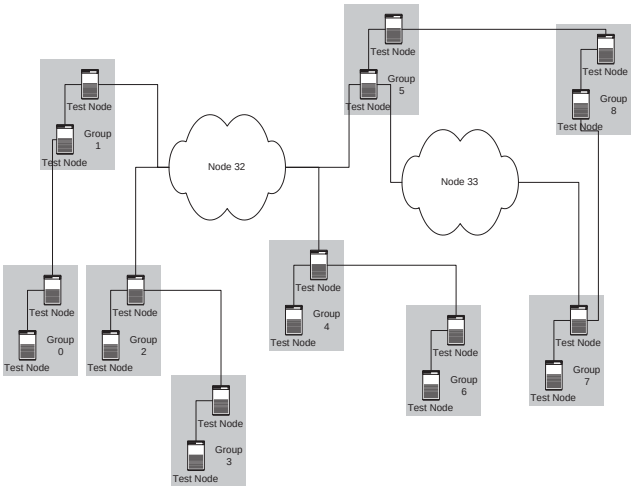

Figure 8. An example logical network that can be built in ISIS testbed network. This example can support 8 student groups. Node 32 and 33 simulate a changing network.

yield an insulated environment for experimentation. Since the entire lab can be constructed from cheaply available hardware and open source software, the design is also cost effective. The design is scalable as it allows us to have several networks, thereby facilitating smaller groups even with a class size of 30 or 40 students. Finally, the design allows us to configure different realistic environments for experimentation and exploration.

4. Example Class Assignments

The laboratory design that we have described facilitates a rich variety of class assignments. A detailed description of the different assignments we have created and their objectives is beyond the scope of this paper. However, in order to describe what is made possible by the laboratory, we give a few brief examples below.

4.1 Server Assignments

These assignments only utilize one or more of the servers in the server network. Often they are compute intensive in nature. For example, one assignment makes students explore the confusion and diffusion properties of modern cryptosystems like AES. Another explores the difficulty of a brute force attack as the key length increases. Students are able to successfully attack a 40 bit key using the computing resources of the server. Finally, assignments that involve password cracking also utilize the servers.

4.2 Host Assignments

Here the testbed network is configured as a flat network of hosts and each student or group of students is assigned a host. Assignments for this type of configuration typically explore security vulnerabilities in a stand alone computer system. One example of such an assignment is to make students harden a poorly configured Windows and/or Linux machine as per security guidelines specified by the NSA. Assignments involving malicious code are also performed with such a configuration. Finally, another example is provided by assignments that involve learning about robust programming techniques in general and exploring buffer overflow, and format string vulnerabilities in particular.

4.3 Network Assignments

These assignments require configuration of the testbed into a collection of networks or clouds of networks and student tasks include ex-

ploring, configuring, and defending a network. Example assignments include exploiting and understanding ARP vulnerabilities, such as ARP cache poisoning and denial of service attacks that can be done through ARP in the local subnet. TCP and UDP vulnerabilities such as session hijacking, spoofing, and other DOS attacks in TCP and UDP. Vulnerabilities in routing protocols such as RIP, and OSPF. Use of network mapping utilities. Secure communication using IPSEC, SSL, and other upper layer protocols. Implementation of secure echo and secure HTTP. Configuring firewalls using IP chains. Assignments involving intrusion detection and prevention. And finally, war game like assignments where students attack networks being administered by other students while at the same time defending their own network from attack.

5. Conclusions and Future Development Plan

In this paper we have described the design of a laboratory for information security education. We argued that the design goals of such a laboratory should include reconfigurability, scalability, robustness, maintainability, cost effectiveness, and heterogeneity. Furthermore the lab should be well insulated from the external network and should provide a realistic environment for student experimentation and learning. The design has been implemented successfully in ISIS - The Information Systems and Internet Security Laboratory at Polytechnic University.

Future plans for expanding ISIS include the addition of a wireless subnet, the addition of VPN and tunnelling capabilities, software and hardware for advanced intrusion detection and prevention and finally equipment that will facilitate lab work in computer and network forensics.

References

[1] M. Bishop. What Do We Mean by "Computer Security Education"? *22nd National Information Systems Security Conference*, Oct. 1999.

[2] ISSL: Information Systems Security Laboratory, Iowa State University: http://www.issl.org/.

[3] NSA Centers Of Academic Excellence in Information Assurance Education http://www.nsa.gov:8080/isso/programs/coeiae/index.htm.

[4] National Coordination Office for HPCC. Committee on Information and Communications (CIC) Strategic Implementation Plan. http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/cic/cic_plan.html.

[5] John M. D. Hill et. al. Using an Isolated Network Laboratory to Teach Advanced Networks and Security. *Proceedings of ACM SIGCSE Technical Symposium on Computer Science Education*, Charlotte, North Carolina, pp 36-40, Feb. 2001.

[6] Prabhaker Mateti. A Laboratory-Based Course on Internet Security. *Proceedings of ACM SIGCSE Technical Symposium on Computer Science Education*, Reno, Nevada, Feb. 2003.

[7] Cynthia E. Irvine. Amplifying Security Education in the Laboratory. *Proceedings IFIP TC11 WC 11.8 First World Conference on Information Security Education*, pp 139–146, Kista, Sweden, June 1999.