INFORMATION WARFARE IN THE TRENCHES

Experiences from the Firing Range

Scott D. Lathrop, Gregory J. Conti, and Daniel J. Ragsdale
U.S. Military Academy, West Point, NY 10996

Abstract: With the increased potential of a bona fide cyber terrorist attack and the possibility of a future "war in the wires", we must continue to improve the education and training of individuals responsible for defending our national borders—whether those borders are physical or electronic. The Information Analysis and Research (IWAR) laboratory at the United States Military Academy (USMA) has proven to be an exceptional resource for such an education for our cadets and faculty studying information warfare and information assurance. The laboratory has also been successful in motivating the need for continued education and training in this area on a much larger scope. This paper justifies why information warfare laboratories are necessary, describes the phenomenon that is occurring as a result of the IWAR lab, explains the current configuration, and presents lessons learned that others might use in designing an Information Warfare laboratory. While this paper has a military context, the results apply to any university, corporation, or non-profit organization desiring to increase awareness and improve education in the area of information warfare

Key words: Information warfare, information assurance, education, educational laboratories

1. INTRODUCTION

Two years ago, the Information Technology and Operations Center developed the initial Information Warfare Analysis and Research (IWAR) laboratory to support undergraduate education and faculty research in Information Assurance (IA) at the United States Military Academy (USMA). Since that time, it has matured into a much larger and robust laboratory. What began as a single, isolated network has matured into three separate networks and a library. Each component has a distinct purpose but all are

C. Irvine et al. (eds.), *Security Education and Critical Infrastructures*

aimed at furthering education in Information Assurance at USMA and throughout the IA community. With the increase in size and scope of the laboratory, technical and social issues in manageability have risen.

The original purpose of the IWAR laboratory focused on providing an isolated laboratory where students enrolled in our Information Assurance course could familiarize themselves with various known computer security exploits and employ technical measures to defend their network against such exploits. Additionally, the laboratory provided a facility for faculty members to conduct research in Information Assurance. [1] Currently, the laboratory serves not only the Information Assurance course which is limited to computer science and electrical engineering majors, but also provides a "clubhouse" atmosphere for our ACM SIGSAC student chapter; supports the annual CyberDefense Exercise (CDX) conducted with the other military institutions of higher learning and in conjunction with the NSA penetration teams, the 1st Information Operations Command, and the Air Force 92d Information Warfare Squadron [2]; is used as a focal point for congressional, academic, military, and other visitors interested in observing or replicating our work; and is used for information warfare demonstrations during a once-per-semester "Tech tour" for the freshman students. The purpose of this demonstration is to motivate the plebes to take advantage of the laboratory and IA course while they are at West Point.

There are several other courses at USMA that use the laboratory in addition to the computer science-based, Information Assurance course. Almost every CS course uses the laboratory for computer security related lessons. A political science course entitled, "The Policy and Strategy of Cyberwar" uses the IWAR laboratory exclusively as their classroom in order to demonstrate the technologies that common hackers and cyber-terrorists use to gain access to computing resources and then to relate those experience to strategic level policy issues. The Cyber Policy course includes hands-on exercises where the students build viruses, worms, and malicious applets. The "Cyber Law" course uses the laboratory for a lesson to give pre-law students an appreciation of the tactics and techniques used by cyber-criminals. Finally, the IWAR laboratory provides faculty with a facility to learn about emerging information warfare. Computing infrastructure upgrades and initiatives often begin in the IWAR laboratory before inflicting them on the user base. For example, the laboratory has been used to install a Windows 2000 Active Directory infrastructure before deploying it on a larger scale. It has been also used to familiarize, test, and validate wireless security solutions prior to decisions being made on whether or not to install a wireless network. What was originally designed primarily for a single undergraduate class has blossomed into an institution-wide resource, but

with that has come additional administrative overhead and technical requirements.

The intention of this paper is to provide an overview of the current state of the laboratory, the methodology used to obtain this condition, impart lessons learned to managing the increased overhead of others considering such an endeavor, and discuss future improvements.

2. BACKGROUND AND MOTIVATION

It can be argued that education in information warfare is paramount for the students at the United States Military Academy and the other military institutions of higher learning. Nearly a year ago, the Secretary of Defense summarized a long-standing national discussion when he stated that our dependency on information networks makes attractive targets for new forms of cyber attack. [3] In the recent Department of Defense Report to Congress, the assertion was made that "In the future, the network will be the single most important contributor to combat". Furthermore, the report asserted the *information domain* must be protected and defended in order to generate and sustain combat power in the face of offensive actions taken by an adversary.[4] With the military's increased reliance on information systems coupled with the cyber-coordinated events of September 11th 2001, the reasons for educating our students in information warfare are readily apparent.

Current systems being developed by the Army depend on this network-centric warfare concept. For example, Land Warrior is a wireless networked system of computers. Each infantry solider in a 30-soldier platoon wears a personal computing device that communicates with other soldiers in the platoon through a wireless local area network (LAN). The system enables the exchange of terrain, enemy, and friendly information; digital maps; operations orders; and e-mail messages between the soldiers in order to facilitate information dominance.[5] [6] Such systems also are to provide a "just-in-time" logistics framework, enabling supplies such as ammunition and food to be pushed forward as the information indicating a logistics shortfall is autonomously sent to the supply forces. These systems will connect into the Army's tactical Internet. Without technically savvy soldiers and an information structure designed to protect and defend these critical assets, the Army's reliance on information dominance is a fragile one.

Consider the fact that the Code Red worm infected more than 250,000 systems in approximately nine hours on July 19, 2001.[7] Had even one percent of those computer systems been military end systems such as Land Warrior, rather than commercial or home-based computers, the effects would

have been to cripple the unit's reliance on such systems—infrastructures which our doctrine advocates as being a combat multiplier by increasing situational awareness (that is the ability to spatially and temporally know where the enemy is and where friendly units are). If such systems are denied service, or worse compromised, then clearly information dominance is no longer established. The future of the military's information dominance on the battlefield hinges on the security of the networked information systems providing the necessary services—thus, the increased requirement that future officers educated at the military institutions of higher learning become aware of such issues and their potential solutions.

The issues in assuring our information are much larger than just what the military foresees. Our nation's critical infrastructures and economic structure are becoming increasingly reliant on information systems and the Internet that provides connectivity between such systems. Addressing these issues requires an education in information warfare that does not merely theorize and describes such concepts. A hands-on, *active learning* experience entails that we provide an environment where students, employees, and anyone managing or administrating information systems can apply theoretical concepts in an isolated environment [8]. Such an environment allows the unleashing of viruses, worms, and Trojan horses so as not to have an effect on a production network. Kaucher and Saunders found that even for management-oriented graduate courses in Information Assurance, a hands-on, laboratory experience enhances the students understanding of theoretical concepts [9]. The above reasons justified the original creation of the IWAR laboratory and validate continued expansion and improvements to the laboratory.

Recent success in the Cyber Defense Exercise and the educated, yet tough, information assurance questions coming from our former students further justify the usage and improvements to the IWAR laboratory. Our Cyber Defense team showed vast improvement between the first and second years of the competition. The Cyber Defense Exercise (CDX) is an annual competition between the United States Military, Naval, Air Force, Merchant Marine, and Coast Guard Academies. At USMA, the competition serves as the final project for senior-level computer science majors enrolled in the Information Assurance (IA) course. Participating students are required to design, implement, configure, and secure a network of computers. Required services are determined by the exercise's operation's order and allowed red team attacks are controlled by a set of rules. After verifying all services are running, the students must secure that network using open source tools. Each school's network is then attacked by members of the NSA's red team, the Army's 1st Information Operations Command, and the Air Force's 92d Information Warfare Aggressor squadron while the students attempt to

maintain the required services; prevent and detect attacks; and then recover and restore any loss of information or services.

The main goal of the CDX is to reinforce the knowledge that students have acquired in academic courses addressing the protection and defense of information systems. To take part in the exercise, the participating students are required to design and implement a security plan for a network comprised of various operating systems, services, and applications. Their plans must address the issue of maintaining confidentiality, integrity, availability, and authentication of all services and resources. The National Security Agency's Director of Information Assurance sponsors the event and awards a trophy to the school with the best overall showing in the competition. The trophy is a traveling award that resides at the winning school for a given year.

In the first CyberDefense exercise, our students struggled to maintain services and provide security simultaneously. Much of their effort was aimed at maintaining the required services leaving little time for analysis and improvements in their defensive plan. [2] In the recently completed 2002 CyberDefense exercise, the students not only maintained the majority of the required services throughout the exercise, but also had a very high success rate in defending their network from the red team. Not only did they secure the network with the tools and technologies learned during their course work, but they also were able to explore various other security options such as Bastille Linux, one-way Ethernet cables for intrusion detection systems, and *honeypots*. A majority of their success is due to the fact that both students and faculty had access to a facility such as the IWAR laboratory and even more of an opportunity to work with the various technologies such as firewalls, vulnerability scanners, system integrity tools, and intrusion detection systems that are required to defend such a network.

Another recent example, which validates the continued usage and improvements to the IWAR laboratory, are the experiences a former student, now an Army second lieutenant, had when attempting to determine a technical solution to a typical information assurance issue in determining the appropriate balance between service and security. The problem the lieutenant was trying to solve was providing access to .mil sites from IP addresses originating from within the Republic of Korea (ROK). Soldiers in the lieutenant's organization were attempting to take continuing education courses offered on-line through the Army's .mil portal. However, the soldiers could not access the sites through their ASDL and cable modem connections from their homes located off Army installations. The problem had existed since the September 11th, 2001 attack on the World Trade Center, when the Army decided to block access to all .mil sites from IP addresses originating from within the Republic of Korea and from several

other foreign countries. Therefore, soldiers could only take the online courses from computers, which were on a military installation. The security solution imposed by the Army defeated the purpose of after-hours education for those soldiers living off an Army installation in any oversea location. [10]

The lieutenant, based on his experiences in the IA course and specifically, in the IWAR laboratory, realized that technical solutions should exist (VPN, PKI, proxy servers, etc) that would both provide soldiers with access to .mil URLs while simultaneously protecting the Army servers in Korea. The lieutenant fielded the question with a proposed, well-informed solution to the USMA IA faculty and Computer Emergency Response Team (CERT) who made minor changes to the lieutenant's solution and then proposed an Army-wide recommendation for overseas units.

Such examples highlight that the experiences learned in the IWAR laboratory directly translate to solutions in real world applications. The IWAR laboratory component of the IA educational program at West Point provides a much richer experience for students than what classroom instruction alone could provide.

3. RELATED WORK

Primarily due to the increasing importance of IA education, many colleges and universities are beginning to invest resources towards the construction of information security laboratories. [9, 11, 12] Others have been looking at using simulation-based tools to educate their students. [13] To the best of our knowledge, no one has attempted to design and implement a laboratory on the scale or complexity currently exhibited by the IWAR laboratory. Others have created laboratories, primarily to serve different purposes, but none have the similar heterogeneous nature or scale that the IWAR demonstrates.

Kaucher and Saunders describe an Information Assurance laboratory that they use at the National Defense University for educating information assurance and information security professionals. Their network serves a different purpose and thus does not need to be the same scale or complexity as we have built into the IWAR laboratory. Similar characteristics include a heterogeneous network. One of the unique features of their network is that they expose the entire network to their students. This works well for their particular situation, as their students often need to see the entire network to "demystify the technology." [9] However, for this particular application major portions of the network are not revealed to the computer science and electrical engineering majors taking the IA course. This forces students to

conduct reconnaissance using port scanners and similar tools. Exposing the network might be a better idea for Cyber Policy and Cyber Law courses, but the administrative overhead to perform such a task makes it unfeasible.

Others have taken heterogeneous networking to another level by implementing different layer 2 architectures such as Ethernet, Asynchronous Transfer Mode (ATM), and Fiber Distributed Data Interface (FDDI) on a token ring. [12] Their network design is different from ours in that they are using it more for system modeling and simulation, networking, and special projects rather than information warfare. The scope of their network is also much smaller and where our heterogeneous nature consists of multiple operating systems and services, their heterogeneous flavor is a result of different link layer protocols. Some similarities also exist, however. We have begun establishing a wireless network using the 802.11b protocol in order to further investigate the security issues surrounding this wireless protocol.

Yasinsac describes a computer security laboratory project for outreach, research, and education. Their laboratory serves a similar purpose as the IWAR laboratory but on a smaller scale. Similar to the IWAR laboratory, they have been challenged to provide an environment where students are free to explore without creating administratively challenging headaches when systems break because of the use of certain tools. One of their solutions is to use a virtual machine software wrapper created by Vmware. [11] We also use Vmware but more so to provide a heterogeneous environment of operating systems rather than to control computer configuration. We control the configuration by re-imaging the systems or swapping hard drives when a student has applied a technology that causes unrecoverable damage. We place certain machines in an "administrative" mode and specify that these machines are off-limits. While this approach has worked thus far, we realize that in future years we may have to impose further constraints. However, we encourage our students and researchers to attack the various servers that exist in our laboratory.

Others have begun designing or looking at simulation based-tools to educate others in IA. However, to the best of our knowledge, many tools exist that model networks, but no tool exists that accurately models the specific decisions that must be made to simulate an IA education. [14]

The implementation and maintenance of an IWAR type laboratory requires significant investments in terms of hardware, software, and human resources to build and maintain the physical networks of computers and communication components. This is not a unique problem. We agree that a tool or model that can be used by students to assess the quality of their information system design choices prior to (or instead of) a physical implementation is required in an IA education. Simulations also allow the proposed network to be tested by a larger variety of conditions and attacks

than would be feasible with a real network. There may also be a number of attacks that are too dangerous to perform on the real system. [13] As is true in military training exercises however, simulation-based tools will always complement, rather than replace a hands-on "live-fire" experience.

4. LABORATORY ORGANIZATION

The design goals for the IWAR laboratory were that it consist of heterogeneous operating systems, networking equipment, defensive security tools, and offensive exploits; contain "soft" and "hard" targets; be large enough to provide a real world signature; and be robust enough to withstand the attacks from students and faculty—that is we wanted to make the laboratory conducive to exploitation experiments without creating a lot of administrative overhead in repairing the network. We selected open-source security tools to allow students to "look under the hood" and identify what each tool is doing. Our requirements were that we have a facility for the IA course and other IA-related courses, a network for the CyberDefense competition, a network for our ACM SIGSAC student chapter, dedicated browsers where users could locate and download exploits posted to hacker websites, and the reference material necessary to build and maintain the laboratory. What evolved were four separate networks: (1) The IA network, (2) the CyberDefense network, (3) the SIGSAC network, and (4) a small "search box" network. Additionally, we began building an IWAR library with reference material gathered during the re-design of the current laboratory.

The remainder of this section will focus on each component separately with emphasis being placed on the IA network.

4.1 Information Assurance Network

The Information Assurance (IA) network is the original IWAR laboratory as cited by Schafer.[1] Its primary purpose is to provide a facility for course instruction and hands-on exercises for our Information Assurance course taught in the spring semester each year. Secondary purposes include using the laboratory as the primary classroom for the Social Science's course on "The Policy and Strategy of Cyberwar," provide a resource for other CS courses to use in order to demonstrate information warfare principles, and using the facility to display and provide demonstrations to our many guests from outside of USMA.

The IA network is a completely isolated network that we often compare to a firing range. The Army uses firing ranges to train soldiers on individual

weapons and firing systems. Likewise, the IA laboratory is a range where students and faculty may use and experiment with port scanners, vulnerability scanners, Trojan horses, worms, and viruses without running the risk of releasing malicious code onto our production network or into the "wild". Just as a solider would only fire a weapon on the range or in combat, the IA network policy only permits users to use the malicious tools in the controlled confines of the laboratory.

Malicious software that exploits system vulnerabilities is installed on select systems within the laboratory, allowing students and faculty to learn about, and experiment with, the capabilities of potential adversaries. Through experimentation with malicious software, users gain an appreciation of the numerous vulnerabilities existing in currently deployed information systems. With this knowledge IWAR laboratory users are better equipped to protect and defend the information and information systems for which they are, or will be, responsible.

Since the original publication of the IA network, it has been re-designed and refurbished with new equipment. The current configuration is shown in Figure 1. Including the virtual machines, there are approximately 200 nodes in this *isolated* network. The current network consists of two primary LAN segments based on USMA's school colors. The *black* segment contains the classroom machines, "soft" server targets, and a few administrative machines. The *gold* segment, separated from the *black* network by a router and a firewall, consists of a few administrative machines and several "hard" targets. "Soft" targets are computers that have a default operating system installation and configuration with no patches applied. The only "hardening" that has been done to these machines is to insure that all local and domain administrative passwords are strong. Otherwise, the systems are wide open. The "hard" targets are harden using the SANS and NSA guides and applying the current patches to the operating systems.

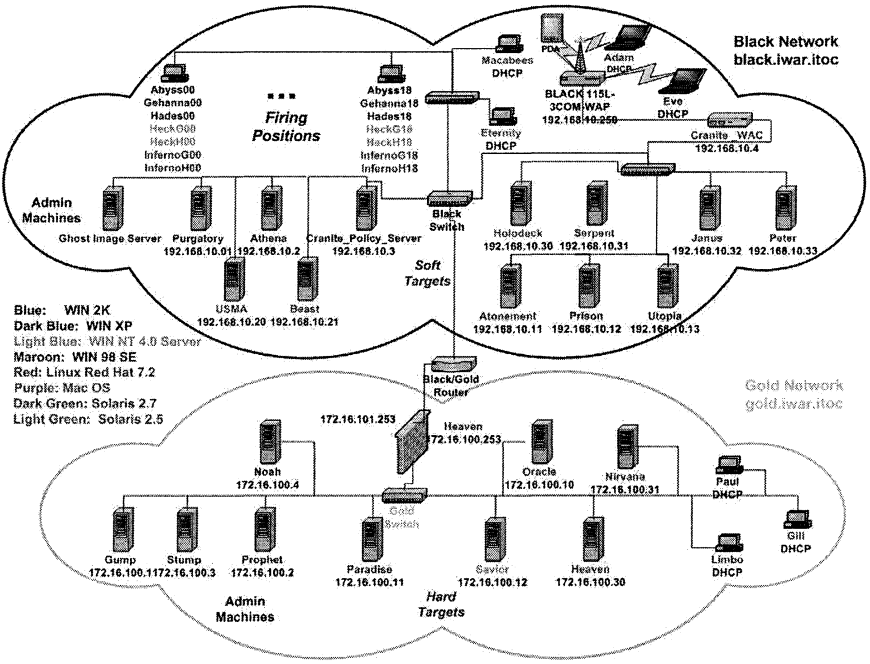

Figure 1: IA Network

The *black* network serves as the laboratory's "LAN" while the *gold* network attempts to portray the remaining *Internet* from the perspective of the users on the *black* network. The majority of the *black network* is contained in our IA classroom and consists of the 19 classroom computers (18 for students and one for the instructor), which we refer to as the "firing positions". These computers are the systems from which students may launch offensive exploits against the soft or hard targets that are arrayed throughout the network. Each of the 19 classroom computers is a DTK 733 MHz Intel Pentium with a 750 MB swappable hard drive. The systems contain a standard classroom image consisting of a Windows 2000 Server as the base operating system and VMware 3.0 installed on each machines. VMware is a virtual machine software solution that allows one to run multiple operating systems on one personal computer. By simply switching between windows, the user can switch between host operating systems. The VMware software isolates each virtual machine from the others (including the base operating system). This separation prevents an improper configuration in one system from affecting another virtual machine. VMware allows users to install and configure Windows 2000, Windows XP, Windows NT, and Linux operating systems. Each virtual machine has a unique IP address and a full complement of hardware devices. In our IA network, each virtual machine is registered as an individual node on the

black network. Additionally, one can establish a "virtual network" between the virtual machines residing on the same computer. [15] We found VMware to be particularly useful in teaching the students both offensive and defensive operations.

Including the virtual machines, each classroom computer effectively has eight machines (Figure 2). Individuals with accounts on these machines have administrative privileges on all the virtual machines on that particular computer. Windows 2000 Server is the base operating system with one Windows XP and Windows 98 virtual machines. We also installed two Windows NT4.0 Servers and two Red Hat Linux 7.2 virtual machines. There are two of these operating systems in order to allow students in each of our two sections to have their own virtual computer with this type of operating system. Finally, we have an additional Red Hat Linux 7.2 virtual machine that we use as a machine on another "external network". This configuration allows gives each student a "virtual network" on their machine and provides some flexibility and creativity for the instructors and the students (Figure 2).

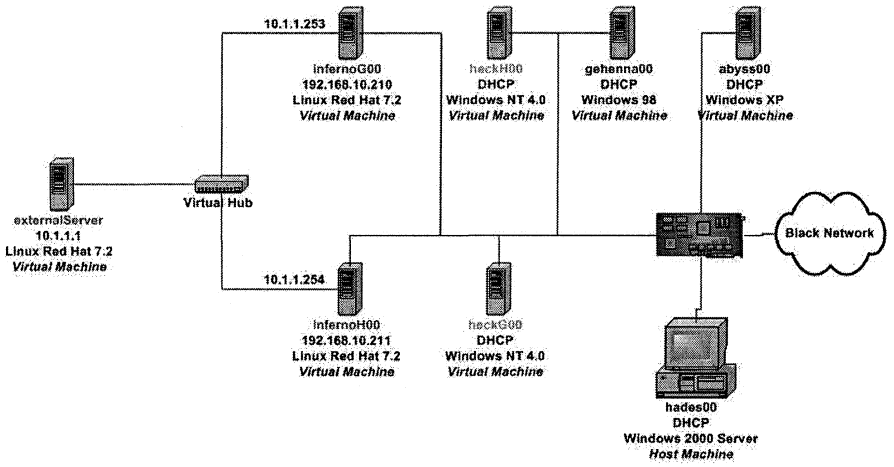

Figure 2: Classroom Machine

For example, a student may want to test an exploit against an IIS 3.0 sever running on Windows NT. The individual can create the malicious virus, worm, or applet and launch it from their Linux virtual machine and target the IIS server running on their Windows NT virtual machine. The entire attack sequence is isolated to their classroom PC. Once the student has perfected their exploit, they can then attempt to target the "soft" and "hard" targets existing in the larger network. The virtual network configuration "exposes" a portion of the network, similar to Kaucher and Saunders idea. [9]

From a defensive perspective we have used the virtual machines' to demonstrate the concept of firewalls. The Linux virtual machine running on the "external" network portion serves as the outside world from which the student wants to protect their internal network. The internal network consists of the remaining virtual machines. The student can configure their Linux virtual machine as a firewall between these two networks. Using *ipchains*, a stateless packet-filtering firewall, we can demonstrate the advantages of a packet-filtering firewall. In order to show a stateful packet-filtering firewall we can then use *iptables*. Finally, in order to take the exercise to the final level, we can install a proxy server such as Squid on the student's Linux machine and demonstrate the firewall that separates the *black* and *gold* networks.

Other uses we have found for the virtual machines is using them in a hands-on laboratory where students install, configure, and then harden an operating system using a security checklist such as from SANS or the NSA. The virtual machines enable the student to perform these functions without having to worry about tampering with the base operating system's configuration.

The remainder of the *black* network is contained in a server room next to the classroom and contains six administrative machines, seven "soft" target servers, three additional workstations, and a small wireless network. Additional funding allowed us to purchase Dell Poweredge 1550 rack mountable servers to replace the desktop computers we originally used. Each server is a 1 GHz Intel Pentium processor with two, 8-GB hard drives. All of the servers except for the Solaris servers run on these machines in order to save space in our server room. The operating systems within the *black* network include Solaris 2.8, 2.7, and 2.5; Windows 2000 Advanced Server and Windows NT 4.0 Servers; Linux Red Hat 7.2 servers; and MAC OS 8 and MAC OS 9. Administrative machines include domain controllers, file servers, Samba servers, and a NIS server. Our "soft" targets currently include web servers, ftp servers, SNMP servers, telnet servers, Exchange 5.5 server, and several other wide-open, services without patches. The router currently has unnecessary services running such as an http server, telnet, and SNMP server.

We attempt to provide an "enterprise" appearance to the users of the network. For example, we have a two web servers running on the various machines. The course web page is on an Apache web server running on a Linux operating system and another web server is running on a Windows based Internet Information Server (IIS) 3.0 server. The Exchange Server is used not only for email within the IA network, but also as a "soft" target. Other services are added as required by the instructors, students, or other users of the laboratory. Finally, there are three additional workstations. One

is identical to the classroom computers and is used primarily by instructors during class preparation. The other two workstations are Macintosh computers used as other potential targets that can be used as a launching pad for other attacks.

The *black* network also has an IEEE 802.11b wireless basic service set (BSS) infrastructure. The wireless network is tied into the *black* network with a wireless access point. Currently there are two laptops with wireless cards and a personal digital assistant (PDA) device with a wireless card used in the network. Primarily used for familiarization and research, we plan on incorporating wireless security into our IA curriculum. We are also using the wireless network to evaluate current wireless security solutions such as the Cranite Systems' Wireless Wall™ architecture.

The *gold* network is contained entirely in the server room. It consists of five administrative machines and seven "hard" targets. It is similar in setup to the servers running on the *black* network except that the machines are configured with the most recent patches and hardened using the NSA and SANS security checklists. Services similar to those in the *black* network are running with the exception of improved, more secure services running where applicable. For example, instead of running NIS, the *gold* network runs NIS+. The IIS Server 5.0 is running and configured with the latest patches rather than IIS 3.0 or 4.0. Additionally, the *gold* network sits behind a Solaris based firewall product in order to provide increase security. The *gold* network is where small groups of students and faculty working on research projects normally operate because of the added security and less risk of losing their work. However, everyone understands to back up their work and store any important files on the file server that is off limits. For example, we have a group of students working on plug-ins and a Java based client for the Nessus vulnerability scanner. Their work is currently stored on the *gold* network. This gives the laboratory a "real-world" look-and-feel and also provides the individuals working on their projects some additional security. However, all users understand that any node in the laboratory is subject to an attack. Therefore, most computers are configured with a zip disk in order to provide an additional storage method for backing up work.

4.2 CyberDefense Network

The CyberDefense network supports the CyberDefense exercise as described in Section II. The CyberDefense network serves as the initial configuration for the CyberDefense exercise. Each school's networks are connected via a VPN to the red team and white cell's observers. This configuration allows the red team to attack each network without fear of repercussions from a stray attack, and allows the white cell evaluators to

verify that required services are running and observe the actions of each of the schools respective teams. Each year the configuration is changed based on the students' design within the constraints of that year's exercise guidance.

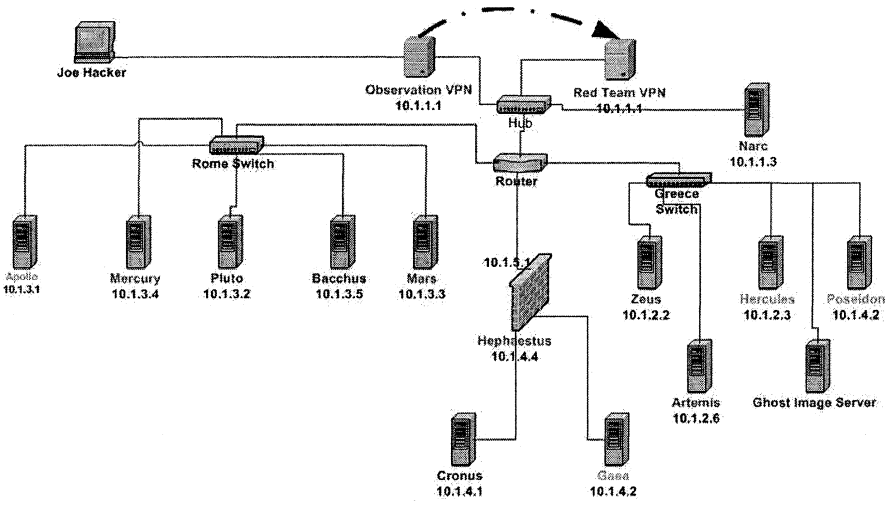

Figure 3: CyberDefense Network

The design philosophy of the CDX network is similar to the IA network, but on a much smaller, more manageable scale. The network is designed to have heterogeneous operating systems provide services such that an outside observer would view it as a real-world environment. Unlike the IA network, however, the students implementing the CyberDefense network wish to make it secure as possible—thus there are no explicit "soft" targets.

The CyberDefense network consists of platforms running Sun Solaris 8.0, Red Hat Linux 7.2, Windows 2000, and Windows NT 4.0 operating systems. Internet access is allowed through the VPN for downloading the latest patches and software updates; however, students are not allowed to purchase any additional software in order to implement their defense. The network systems are configured to provide various services such as: web servers, database servers, file servers, e-mail servers, and the normal contingent of network utilities.

During the preparation phase of the exercise, students harden the systems using the SANS and NSA security checklists. They also use a variety of open-source port scanners, vulnerability scanners, network monitoring tools, intrusion detection, and host-based and network-based firewalls in order to establish a defense-in-depth and defense-in-breadth posture. For example, in the recently completed exercise, the students established an intrusion

detection system using Snort running on a Linux machine. In order to prevent traffic from leaving their network interface card, they built a one-way Ethernet cable that allowed only one-way traffic into their intrusion detection machine, aptly named *Narc*.

The intent of the exercise is to force the students to pull together what they know theoretically and from what they learned using the IA network and apply it to a real network, under attack, in an environment in which mistakes will not cause catastrophic loss of life or information.

Responses to attacks were limited to network reconfiguration. Offensive operations were limited to the Red Team only, and social engineering by either the attackers or defenders is not allowed. Social engineering is a major threat that we face in information assurance; however, it would have introduced undesirable complexity to the CDX without corresponding benefits. As you might imagine in an undertaking of this complexity, the execution of the Cyber Defend Exercise involved a number of lessons learned for future iterations.

4.3 SIGSAC Network

The SIGSAC network supports USMA's Special Interest Group for Security, Auditing, and Control (see figure 3.). Designed and built in 2002 by members of SIGSAC, the network, otherwise known as the SIGSAC "clubhouse" supports the group of over 300 members by providing an isolated network of computers from which members of the club may learn and explore both offensive and defensive tools used in cyber warfare. The network equipment co-exists with the CyberDefense Network in order to take advantage of the most recent information technology available to students at West Point. Additionally, the co-location of the two networks facilitates the exchange of ideas between the current CyberDefense team and the future Cyberdefenders that are currently involved in the SIGSAC club. Members of the club learn about the threat of information warfare and how to defend against it--having fun in the process. It is not a hacking clubhouse, per se, although students have the opportunity to learn and apply hacking type tools in an isolated environment.

The advantages to having a network specifically set aside for our SIGSAC club is that it allows them to experiment with offensive and defensive tools, again, in an isolated network without the concern of interfering with our IA classes. Since the individuals using the SIGSAC network are generally less experienced, they work on a smaller network separate from the IA network, minimizing the risk due to a mistake and minimizing the time to rebuild. At a minimum the laboratory provides them

with a resource where they can "play" on a network with administrator privileges--something unlikely in a traditional university setting.

Currently, the SIGSAC network consists of seven computers interconnected by a hub. It is also a heterogeneous network with two Windows 2000 servers, and two Windows 2000 workstations, one Windows NT4.0 server, and one Red Hat Linux 7.2 server. The computers share the keyboard, mouse, and monitor with the computers in the CyberDefense network through a KVM (Keyboard, Video, Mouse) switch.

4.4 IWAR Library

The final component to the IWAR laboratory is one that we began building slowly, but over time has evolved into a significant resource for our students and faculty. The library provides reference material for faculty to use in their classes, for students to use throughout their various IA course and in the CyberDefense exercise, and most importantly by our SIGSAC student members excited to learn about information warfare. We found that as we built the various networks and installed various services, often times it was useful to have a book explaining, in detail, what it was we were trying to configure. As we acquired books over the past few years, we began receiving requests from students and faculty alike to borrow the references. The library was organized and is currently maintained by members of our SIGSAC club. They are currently building an on-line checkout system for the library.

5. LESSONS LEARNED

There were numerous lessons learned from the creation of the IWAR laboratory. At a larger scale, we found that (1) following an engineering design process, (2) limiting the networks to their specific purpose(s), (3) developing a viable recovery plan, (4) creating a policy, and (5) delegating responsibility to individuals or groups were keys to our success.

As computer scientists, we are trained in engineering thought process, but often times fail to follow such a procedure whether it be creating software or building a laboratory of networks. In the IWAR project we often times began moving equipment, cabling, and software services from machine to machine without thinking of the consequences. Only after sitting down and insuring that we understood the requirements and what functionality we desired, did a design and implementation succeed.

The first step is to understand what your requirements and desired functionality are. We realized that we wanted a network for educational

purposes, for our CyberDefense exercise and for the use of our SIGSAC club so the original idea of three separate networks was readily apparent. However, the hardware and software resources were not readily available and had to be acquired over time using "unwanted", older systems, and eventually through acquisition of new systems. The funding for these new systems came only after we were able to demonstrate the potential for the IWAR laboratory and exercises such as the CyberDefense exercise.

The modular design of four separate networks provides us with the flexibility to combine networks, if we determine it would be beneficial in the future. Domain names and IP addresses were carefully chosen so as not to have conflicting namespace issues. If for example, we decide to create a mini-CyberDefense exercise with our SIGSAC club members, we could combine the SIGSAC network and all or portions of the IA network (for example the *gold* network) through either a CAT-V cable or wireless connection. The design of the IWAR laboratory's networks tried to anticipate such future requirements.

Determining requirements also involves how you want your network to appear to the general user, what operating systems and services you wish to provide, and at what level of security. A conscious decision has to be made about where to emplace those services and the administrative burden that you place on the faculty maintaining those systems when a service breaks. There is a point where the number of services to install, configure, and then maintain becomes unmanageable. One has to decide this breaking point based on the number of qualified administrators and faculty you have at your particular location.

Once you have decided on the requirements and functionality you can then design the network. Drawing the network on paper and using a chart to manage the nodes provides a good starting point for your design. An example network node chart is shown in table 1.

Table 1: Network Nodes

NAME	SERVICES	HARDWARE	OS VERSION	IP ADDRESS
Purgatory	Domain Controller	DELL PowerEdge 1550	Windows 2000 Server	192.168.10.1
Athena	File Server	DELL PowerEdge 1550	Windows 2000 Server	192.168.10.2
Beast	SSH, FTP Server	Sparc LX	Solaris 2.7	192.168.10.21
Atonement	Web Server	DELL PowerEdge 1550	Linux Red Hat 7.2	192.168.10.11

After finalizing the design, it is essential to discuss its features with those who will implement it. In our case, we were able to leverage the knowledge of the staff and faculty in the USMA Department of Electrical Engineering and Computer Science. In particular, we exploited their knowledge of UNIX and Windows system administrators in installing, configuring, and "hardening" of operating systems and various services. After working together with the administrators, one becomes proficient enough to venture into the systems in more depth. Finally, when building the network, as in any design project, manage it in an incremental fashion.

Developing a viable restore and recovery plan is vital to the long-term maintenance of networks such as the IA network and the CyberDefense network. Although we have not reached our goals in this area we have a plan to implement some of our ideas. Currently, in the IA laboratory, prior to the beginning of the semester, we ghost each of the classroom images and keep an archive on a removable hard disk. Furthermore, we use a disk duplicator device to make backup copies of the master classroom image. When an IA classroom machine crashes we can simply swap the hard drives with a fresh image and manually enter a few configuration changes (IP address, machine names, etc.). Ultimately, we would prefer to have this capability for the *black* and *gold* network servers also. Currently, if one of these machines crashes we have to either troubleshoot the problem or reinstall the software. Neither course of action is suitable for our current operation.

During the CyberDefense exercise the students planned on ghosting their server images, but never put their plan into action. Consequently, when our

Microsoft Exchange 5.5 Sever crashed, we had to re-install not only the service, but also the underlying Windows NT 4.0 Server operating system. Another academy, on the other hand, successfully replicated their images prior to the start of the exercise so when they lost a service, they were able to efficiently re-image their servers.

A written and verbal policy must be created by a few with input from many. Our current policy is mainly communicated through verbal means and is gradually being recorded in written form with the creation of the IWAR laboratory user's guide and Standard Operating Procedures (SOP). Certain policies draw on our analogy to a live fire range. The range (i.e. IWAR laboratory) is used for training individuals on live fire weapons (i.e., offensive and defensive information tools). Individuals are not allowed to take their weapons off of the range.

Other policies address the administrative issues in the laboratory. Certain servers in the IA network are designated "administrative servers" and are off-limits to attack. Viruses, worms, and other exploits that are downloaded using the search boxes are stored on the zip disks and not allowed outside of the IWAR laboratory area. Finally, certain reference material is available for checkout and other is required to stay in the laboratory area. These policies are just the beginning of our user's guide but provide a baseline for general user behavior.

The final lesson learned is more of a leadership or management issue rather than a technical solution. However, delegating the work, following through with supervision and refinement of the delegated task, and then rewarding the individuals involved in the task pays enormous dividends and sets conditions for a successful experience. The IWAR laboratory reached its current state by the dream of a few individuals; the ideas of a few more persons; and the assistance and guidance from many parties. For example, the original vision of the laboratory was created by its original designers. [1] With a fresh crop of faculty and students with new ideas, purchasing of upgraded equipment, a new design, and assistance from the department's system administrators during implementation, the IWAR laboratory has evolved to its current configuration. The current CyberDefense network was designed and primarily implemented by a student working on an Advance Individual Study project. Finally, the library and SIGSAC network was built and organized predominantly by the SIGSAC student body members. Each individual or group was rewarded either through an Army award, a certificate, special priority on SIGSAC sponsored trips, or simply with a time honored pat on the back and public recognition.

6. FUTURE WORK

The key to implementing future work is to make incremental changes and learn from their lessons. We plan to follow this approach as we continue to refine and improve the laboratory so that we continue to provide a quality IA education to our students and sustained research work for our Army.

One of the first issues we must address is the search box network. Because those workstations ultimately connect to our local area network and the Army's backbone, some "hacker" sites are often blocked. What we are proposing is the installation of a cable modem through a local Internet Service Provider along with a small honeynet on the far side of our firewall. This solution provides the students in our programs the ability to scan the Internet freely while still being constrained to a controlled environment. The search box computers will not be on our local area network and will continue to force the students to save downloaded exploits to their zip disks. Second, the honeynet will allow us to capture live attacks enabling us to use that information in the classroom and further our education on forensics analysis.[16] We would also like to add a few more workstations to this search box network to improve the availability for the students.

Our final issue for immediate improvements is to expand the SIGSAC network either by connecting it into the IA network or by adding more nodes to the existing network. Currently, the size of the network only allows a small number of students to work on the network. One way to add more nodes to the network would be to establish a wireless network with a few laptops as thin clients. Since real estate is an issue in the SIGSAC Clubhouse, the mobility provided by the laptops would provide us with more space and also enable us to expand our wireless networking infrastructure. The other alternative is to connect the SIGSAC network to the IA network in order to provide more targets for the club members.

7. CONCLUSION

The IWAR laboratory began as a small experiment, but with continued visibility resulting in funding, the IWAR laboratory continues to grow. The justification for the laboratory is clear—in order to provide a quality Information Assurance education for our students, the hands-on experiences acquired using the laboratory's networks cannot be replaced by PowerPoint presentations or simulations.

Neither Rome nor an IWAR laboratory is built in a day. The influence that Rome had on Western civilization is well documented in history. The long-term influence that the IWAR laboratory will have on the education of

students and faculty at the United States Military Academy remains to be determined, but initial signs indicate that the experiences observed in the laboratory will provide a positive impact on the future leaders of our country for years to come. These are the same individuals who will ultimately have to make critical decisions concerning the assurance of information.

REFERENCES

1. J. Schafer, D. J. Ragsdale , J. R. Surdu, and C. A. Carver, "The IWAR range: a laboratory for undergraduate information assurance education," presented at Consortium for Computing in Small Colleges, Middlebury, Vermont, 2001.
2. D. W. Welch, D. J. Ragsdale, and W. Schepens, "Training for Information Assurance," IEEE Computer, pp. 2-9, 2002.
3. J. Garamone, "Capabilities, Strategy Must Converge to Face New Threats," http://www.defenselink.mil/news/Jun2001/n06222001_200106221.html, accessed on May 9, 2002.
4. Department of Defense Report to Congress, "Network Centric Warfare," http://www.c3i.osd.mil/NCW/, accessed on April 23, 2002.
5. J. Garamone, "Land Warrior Coming to a Grunt Near You," http://www.defenselink.mil/news/May2001/n05092001_200105094.html, accessed on April 15, 2002.
6. G. Blackwell, "802.11's in the Army Now," http://www.80211-planet.com/columns/article/0,4000,1781_1000821,00.html, accessed on April 15, 2002.
7. CERT/CC Advisory CA-2001-23, "Continued Threat of the "Code Red" Worm," http://www.cert.org/advisories/CA-2001-23.html, accessed on April 15, 2002.
8. R. M. Felder, "Reaching the Second Tie--Learning and Teaching Styles in College Science Education," Journal of College Science Teaching, vol. 23, pp. 286-290, 1993.
9. C. E. Kaucher and J. H. Saunders, "Building an information assurance laboratory for graduate-level education," presented at 6th National Colloquium for Information System Security Education, Redmond, WA, 2002.
10. M. Brakewood,"Question," email to D. J. Ragsdale, March 05, 2002.
11. A. Yasinsac, J. Frazier, and M. Bogdanov, "Developing an Academic Security Laboratory," presented at 6th National Colloquium for Information System Security Education, Redmond, WA, 2002.
12. G. A. Francia and R. K. Smith, "The Design and Implementation of a Heterogeneous Computer Networking Laboratory," presented at 6th National Colloquium for Information System Security Education, Redmond, WA, 2002.
13..J. H. Saunders, "Simulation Approaches in Information Security Education," presented at 6th National Colloquium for Information System Security Education, Redmond, WA, 2002.
14. C. A. J. Carver, J. R. Surdu, J. M. D. Hill, D. J. Ragsdale , S. D. Lathrop, and T. Presby, "Military Academy Attack/Defense Network," presented at 3rd Annual IEEE Information Assurance Workshop, West Point, NY, 2002.
15. VMware, VMware Workstation 3.0 User's Manual, 2001.
16. The Honeynet Project, Know Your Enemy Revealing the Security Tools, Tactics, and Motives of the Blackhat Community. Boston: Addison-Wesley, 2002.