THE CYBER DEFENSE EXERCISE: AN EVALUATION OF THE EFFECTIVENESS OF INFORMATION ASSURANCE EDUCATION

Wayne J. Schepens
National Security Agency
Information Technology Operations Center
United States Military Academy
West Point, NY 10996
Wayne-Schepens@usma.edu
845-938-7674

Daniel J. Ragsdale, John R. Surdu
United States Army
Information Technology and Operations Center
United States Military Academy
West Point, NY 10996
{dd9182 | dj6106}@usma.edu
845-938-2056/2407

Joseph Schafer
United States Army
U.S. Naval War College
New Port, RI
kj6rl@arrl.net
401-848-6200 x3816

ABSTRACT

The US Military Academy at West Point issued a challenge to the five United States service academies to participate in an inter-academy Cyber Defense Exercise (CDE). This exercise was initiated and implemented by faculty and cadets assigned to the US Military Academy, West Point, with funding and direction provided by the National Security Agency. The concept of "defending the network" was derived to evaluate cadet skills and the effectiveness of the Information Assurance (IA) education invoked at West Point. The Cyber Defense Exercise served as the final project for senior-level Computer Science majors enrolled in the Information Assurance (IA) course. The IA - Service Academy Group for Education Superiority (IA-SAGES), a group formed to plan, develop and share IA curriculum, proposed that all US service academies teaching an IA course participate in the exercise. The US Air Force Academy and US Military Academy accepted the challenge to compete in 2001.

The *distributed* facility in which this exercise will be conducted is known as the Cyber Defense Network (CDN). It was designed and developed by a West Point cadet (student) team, and is an extension of the Information Warfare Analysis and Research (IWAR) Laboratory. To understand the function of the CDN, it is necessary to understand all the resources at the disposal of USMA for IA education.

The IWAR Laboratory is an isolated laboratory used by undergraduate students and faculty researchers at the US Military Academy. It is a production-like, heterogeneous environment and has become a vital part of the IA curriculum at West Point. The military range analogy is used to teach the students in the class that the exploits and other tools used in the laboratory are weapons and should be treated with the same care as rifles and grenades. This paper describes the structure of the laboratory and how it is used in classroom instruction. It describes the process used to create the IWAR and the Cyber Defense Exercise (CDE). Finally, this paper describes the concept of the 2001 Cyber Defense Exercise and expectations for future participation.

INTRODUCTION

The Information Technology and Operations Center (ITOC) is a focal point for Information Assurance education at USMA. Soon after its creation in 1999, the ITOC built the Information Warfare Analysis and Research (IWAR) Laboratory. This facility was designed to support undergraduate education and faculty research at West Point. It was developed with the thought in mind that, one day, each US Service Academy would have similar resources and curriculum in which to train; therefore, representatives from the service academies created the Information Assurance – Service Academy Group for Education Superiority (IA-SAGES) in June 2000.

The mission of this working group is to share IA curriculum, resources, and experiences in order to align each academy's IA program in a similar fashion. The service academies are training the future leaders of America, who in their future roles will rely daily on the integrity of information. The founders of the IA-SAGES conceived a Cyber Defense Exercise (CDE) in which participating academies would match information assurance wits against one another. Several hurdles had to be overcome to make this a reality; however, the concept was quickly accepted. This exercise serves as a real-world educational experience, and the inter-service rivalry generates interest in the growing field of IA.

This report describes how the CDE became a reality, the development of the Cyber Defense Network (CDN) to support the CDE, and the plans for its first execution. It describes the vital role that the IWAR Lab plays in teaching information assurance and preparing undergraduate students majoring in computer science to "defend the network" against professional security evaluators, known as Red Teams.

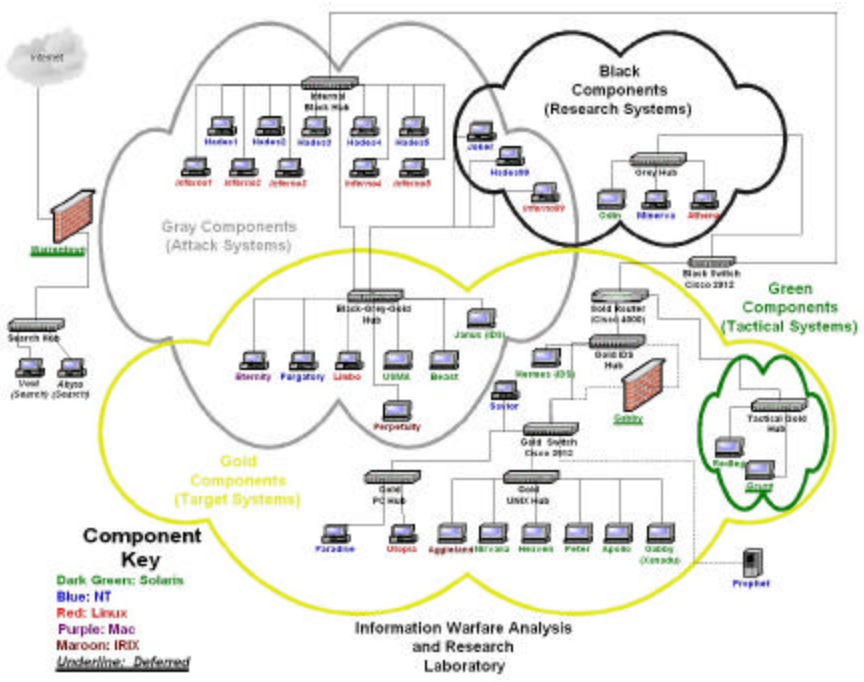

Figure 1: IWAR Laboratory

BACKGROUND

The nation that will insist upon drawing a broad line of demarcation between the fighting man and the thinking man is liable to find its fighting done by fools and its thinking by cowards. - Sir William Butler, 1874

The U.S. military is rapidly changing to take advantage of information technology from the Army's Advanced Warfighting Experiments to the Navy's Network-Centric Global Wargames. Tomes argues that we are so far ahead, no adversary will threaten us with information warfare for twenty years [1]. Carver counters that, although we have the tools to defend ourselves, we are not using them, and we are blundering toward another Pearl Harbor [2]. The fact that nearly half of the nations employed in U.S. Y2K remediation efforts have been identified as using offensive information warfare supports Carver's pessimism [3]. George Surdu, Global Director of Information Systems, Technology, and Services at Ford Motor Company, said that most of Ford's Y2K code was written in India and Israel [4]. The wide dissemination of hacker tools, lack of designed-in security in virtually all Department of Defense (DoD) information systems, and increasing DoD use of commercial communications infrastructures makes the prospect of asymmetrical threats horrifying. Each day it becomes increasingly plausible that young hackers working for a foreign power could cripple critical information systems. Recently the Army has placed as much emphasis on defending its information infrastructure as it had spent on Y2K remediation [5].

History teaches us that "technology permeates warfare," but the technological advances do not necessarily govern or even influence strategy and tactics immediately [6]. The mission of the U.S. Military Academy is to prepare future military leaders. A basic technical literacy is required of all cadets. For computer science majors, one of the most popular courses is the Information Assurance (IA) course. The goal of Information Assurance education at West Point is to improve awareness of security issues associated with information system. To this end, cadets get a broad appreciation for the policy and ethical considerations of Information Operations along with a strong grounding in the hands-on, technical aspects.

INFORMATION ASSURANCE COURSE OBJECTIVES

Upon graduation, all cadets are commissioned as officers in the U.S. Army. Many of them will be responsible for the security of critical Army information systems. The IA course, therefore, is designed to provide a firm foundation in the fundamentals of information assurance. With this foundation, recently commissioned lieutenants have in their toolbox the intellectual skills needed for continued self-education.

The protection and defense of physical locations is a notion with which all cadets are comfortable. All cadets have had the benefit of no less than three years of military training and education by the time they take the IA course. A tenant of military planning and operations from as long ago as Sun Tzu and Julius Caesar is that knowing the tools, tactics, vulnerabilities of ones opponent as well as oneself leads to victory [7]. To establish an effective defense you must have a good understanding of your own vulnerabilities. In addition, you must be aware of the techniques that your adversary

might employ to exploit those vulnerabilities. These ideas have direct applicability in the cyber domain.

In the IA course, cadets learn many offensive techniques. Cadets write malicious applets and viruses. They use port scanners, network sniffers, and vulnerability scanners to find the holes in a system's defenses. They use scripts, Trojan horses, and other tools to gain root-level access to target hosts. The purpose of all this familiarization, however, is not to make them hackers. The purpose is to give them an appreciation for the tools used by potential adversaries as well as the vulnerabilities of currently fielded or commercially dominant information systems and how those vulnerabilities might be exploited. Information ethics are emphasized throughout this learning process to strengthen moral character.

For the IA course to be successful, it is necessary to provide an environment that facilitates active learning and provides maximum opportunity for hands-on experiences for the cadets [8]. It was quickly determined, however, that nearly all of the tools and capabilities needed for this hands-on experience could not be installed in any of the general-purpose computer laboratories for both legal and practical reasons. This led to the creation of an Information Warfare Range, like those used for conventional weapons training.

Once the IWAR Range was developed, it was time to create the “sandbox” for actual wargames to be held. Since the goal from the onset of this IA course has been to educate in the context of defense, defense of a network would be the objective for the wargame. The sandbox needed to consist of a network that would mimic the function, form, and fit of an information infrastructure used to support a base or organization in which a future lieutenant might be assigned. After learning various offensive and defensive techniques throughout the semester, cadets would be assigned to defend the network, while professional Red Teams would remotely access, attack, and identify vulnerabilities associated with the system. This Cyber Defense Exercise would serve to not only test their defense skills but also to allow the faculty to evaluate the effectiveness of their education.

IWAR RANGE

As part of their training, cadets are taught the military concepts of offense and defense as well as tactics like reconnaissance and "defense in depth." Additionally, by the time they are eligible for the IA course they will have had significant basic classroom and field military training experiences. This training includes familiarization and/or qualification with various weapons systems on weapons ranges. These ranges provide a safe and authorized location to conduct training. Leveraging this knowledge, the IWAR Laboratory is introduced to the cadets as an IWAR range. While the IWAR Laboratory (Range) also facilitates faculty research, this paper focuses on the laboratory itself and how it supports the IA course.

By describing the IWAR as a range, instructors leverage several important concepts from conventional weapons training. First, the range is a special, isolated space. Just as one may fire automatic weapons on a rifle range at various targets and launch missiles at

other targets, so too can cadets launch cyber attacks from their firing position (cadet computer terminals) at the IWAR Range target computers (also within the isolated laboratory). Second, it is unthinkable to fire an automatic weapon at a crowd of people from one's barracks room; it should also be unthinkable to use any of the cyber attacks from one's barracks room - *or anywhere outside the IWAR laboratory*.

Recall that the IWAR is a completely isolated laboratory with no physical connection to the outside world.

The IWAR Laboratory is divided into four networks. The Gray network is the "attack" side of the network. Cadets have their workstations on the Gray sub network. Each cadet team has one host workstation, but each workstation uses VMware to run various operating systems on the same physical machine. These operating systems include Window 2000? , Windows NT? , Window 98? , and Redhat? Linux. Cadets have Administrator and root accounts in each of these environments. They also have user accounts on all other Gray sub network machines. An example of how these systems are used for instruction is this: for an in-class exercise cadet's use their Windows NT? virtual machines to download a malicious applet from their Linux virtual machine on the same physical hardware. The malicious applet then does "bad things" to the Windows NT? machine. Also, on the Gray network are servers on which the cadet teams have user-level accounts. These "low-hanging fruit," fruit that is easy to take off the tree, allow the cadets to launch "insider" attacks.

The Gold network hosts the target systems. These are a series of Unix (Solaris? and Irix?), Linux, Windows NT? , and Macintosh? workstations and servers. Several machines are Gray/Gold, meaning that they are targets, but they are on the Gray subnet and thus "low-hanging fruit." Except for those machines that are also Gray, users do not have accounts on Gold machines. This makes attacking these hosts harder. In addition, Gold machines are on the other side of routers, switches, and firewalls, again creating a realistic heterogeneous environment. The Gold network helps cadets appreciate the capabilities and vulnerabilities of firewalls and routers. Also wrapped in the Gold sub network is the Green sub network on which tactical command and control systems are attached.

Faculty members use the Black network for information assurance research. Due to the placement of the machines and the switch (shown in the topology), researchers can work on both offensive and defensive projects on the Black network.

Two machines in the laboratory are not connected to any of the IWAR networks. Cadets use these machines for hunting the Internet for offensive and defensive tools. They can then copy these tools to disks and hand-carry them to an IWAR Range machine. Cadets physically remove these Internet connected boxes from the network when not in use. This isolation, along with some other techniques, reduces the likelihood that external hackers will compromise these machines. In this way the IWAR Range should avoid having these systems serve as launching points for attacks against other Internet resources.

Together the sub networks that make up the IWAR Range provide a valuable resource for teaching cadets how to defend systems against attackers. The Gray network allows cadets to get an appreciation for insider attacks while the Gold network gives them an appreciation for outsider attacks. The Green network allows cadets to explore the vulnerabilities of Army tactical systems. Finally, the Black network allows faculty to conduct research in the same isolated facility.

THE "MAKING OF" IWAR

All four of the isolated and non-routable networks comprising the IWAR form a realistic, production-like environment of heterogeneous systems. Initially four criteria constrained the design of the range. First, the design must allow minimal possibility of misuse for damage to other systems. Second, on-hand resources should be used whenever possible. Third, time was limited. Finally, the laboratory needed to fit into one classroom.

After investigating several possible designs involving all manner of access controls and firewalls, we decided that the most expedient and least risky method of reducing the possibility of misuse would be to electrically and physically isolate the range from all other networks. In our worst nightmares we envisioned a New York Times headline, "Network Attack Lab at West Point used to destroy XX," where XX is your favorite external site.

On-hand resources were used because of constraints on both time and money. The primary means of achieving these goals was to use "rescued machines." These machines were those that were five to ten years old and that the administrators had removed from main production use after replacing them with newer models.

The West Point Department of Electrical Engineering and Computer Science maintains a "Tech Area" where many of these old machines awaited turn-in and donation to other organizations. We rescued several of these machines to form the core or our initial IWAR. Typical of these machines were a dozen generic, 60MHz Pentium boxes with old monitors and four SUN IPC and IPX boxes.

This rapid initial success helped identify several "underutilized" machines with which to augment the IWAR. These machines consisted of three old SGI computers that had been early Web and graphics servers and two old, dual-processor, Pentium servers that had been used for domain controllers and file servers on the Gray and Gold Windows NT? domains. Support personnel located some equipment that had been procured for old projects, such as networking components and an Imac, that were transferred into the lab.

Since the IWAR Range is completely isolated, a more secure method for the students to access resources on the Internet was needed. The goal was that the cadets should be able to search for and download information from even the most untrusted of sites without risking damage to any other systems. Two 90 MHz Gateway PCs, loaded with a very limited and secure version of Linux serve this purpose. Forcing the user shell to Netscape and requiring the presence of a Zip disk as the home directory further secured these computers. In addition, these two *Search boxes* are connected to the Academy network

through a production firewall donated by the Academy's Directorate of Information Management.

Of greater concern was the risk that the IWAR network would be compromised and used to attack external sites than the possibility that someone would gain access to the limited resources on these search boxes. The search boxes are easily rebuilt from a *ghost* image since there are no home directories on the hard drive. The Zip disk was chosen since it would allow a relatively simple method of transferring files downloaded from hacker sites into the isolated IWAR range. Zip disks are also not in widespread use throughout the rest of the Academy, thus reducing somewhat the chance that someone would transfer these weapons to the main networks.

Early enthusiasm and achievements in the IWAR garnered some scarce dollars that were used to upgrade some of the rescued machines and procure essential networking, upgrading, and space-saving components. Rescued or redirected networking components included mostly inexpensive hubs. Primarily due to space considerations each cadet team uses a single hardware system, loaded with a variety of operating systems running in virtual machines.

Running many virtual machines on a single hardware platform significantly consumes memory and CPU cycles. New motherboards, memory, and Zip drives in the Gray machines helped to improve the performance of these machines from dismal to acceptable.

The classroom in which IWAR Range resides had been previously separated into two sides by a divider with a door to the hallway from each side. The *attack* machines were located on one side of the solid room divider and the target machines were located on the other side. This close proximity but isolation of the attack and target machines simplified administration and setup of the lab. Additional administrative simplification was achieved by *ghosting* most of the systems and using Sun Microsystems administrative servers and tape backups to allow rapid reconstruction of the systems.

The most important space, power, and heat saving components were the use of KVM (Key, Video, and Mouse) switches for nearly all of the Gold target systems. In addition to space, heat and power proved to be huge constraints on the number of systems that could be reasonably set up in one classroom. With KVM switches, four sets of Keyboards, Mice, and Monitors provide interfaces for all 25 gold systems, significantly reducing the space, power, heat, and clutter on the Gold network.

In addition to a heterogeneous hardware environment, the IWAR provides a wide variety of production quality network applications and services. These include Domain Name Service (DNS), WINS? , authentication and replication with Domain Controllers, Network Information Service (NIS), and NIS+. Also provided are web servers, mail servers, Network File System (NFS), Samba? , LanMan? , and additional services. Common production configurations were adopted. For example we ran Microsoft Internet Information Server? (IIS) and Exchange on the Windows NT? servers and Apache on the Linux and Sun servers.

The Gray/Gold servers were configured with old and unpatched versions of the operating systems (e.g., Redhat? 2.1 and Windows NT? 4 with no service packs applied) and applications. Additionally, these boxes were located on the Gray subnet on the same hub with the attack machines. The students also had user accounts on these servers. Thus, the students could log onto the Gary/Gold servers and easily sniff the network and attempt well-known exploits to upgrade their privileges from user to root or administrator. The Linux boxes and Linux virtual machines on the student's boxes participated in the Sun NIS Domain. The attack boxes were members of the Gray NT domain controlled by another Gray/Gold server.

Conversely, the main Gold boxes operated with the latest patches and versions of the operating systems (e.g., RedHat 7.0 and Windows NT? 4 SP6a), patches, and applications. After gaining some confidence in attacking the "low hanging fruit" of Gray/Gold, students could move onto the "treetop fruit" of the Gold domain. NIS+ was used on the Sun and Linux boxes in the Gold domain. One of the first requirements of the course was for the students to map the entire network.

Students used a wide variety of tools and a shared home directory environment for all of the systems with which they had privileges. The shared environment was achieved with Windows NT? , Linux, and Sun logon scripts and NFS and SMB mounts. The students could easily transfer exploits from among any of their environments and use development tools from Linux, Sun, and Microsoft to compile their code. Finally, recognizing the relative difficulty of using the search boxes and the time constraints for undergraduate students in a Computer Science elective, numerous "hacker tools" were cataloged on a Gray/Gold site.

A lab of enormous complexity and heterogeneity emerged in a matter of weeks. Despite the time and resource constraints the entire IWAR range was built in four weeks and cost less than $20,000.

Since this initial development and preliminary upgrade, interest in this local, unique resource has risen both in academia as well as industry. Government and military organizations have provided funding to support ITOC research efforts, enabling the ITOC to perform a complete upgrade of the Grey network. For instance, each cadet in the IA course has his or her own workstation on the Gray network now.

IS IWAR WORTH THE EFFORT?

The creation of the IWAR involved significant time and resources. Weeks went into the design of the IWAR Range, and four more weeks were devoted to its construction. While the IWAR made extensive use of rescued hardware, it still cost $20,000 to get started. The question that should be asked is "does this expenditure of resources result in greater educational efficacy?"

There is great intuitive appeal to the notion that the hands-on experience provided by the IWAR Range is more effective than PowerPoint? slides and white boards. When the cadets actually implement an attack or exploit they must also describe how they would

defend against such an attack. Later in the course they must implement these defensive measures in securing a network against external attack. This not only provides practical experience as both an attacker and a defender but it exercises their ability to think critically, analyze, and synthesize.

The comments received in end-of-course critiques were statements like "A great course that will be very applicable to my future career. I am very grateful for the experience. Learning and experimenting was [sic] the best thing," [our emphasis] "Best course I have taken, hands down," and "[I learned] that nothing is secure [you need to be] careful of everything and anything you do." This end-of-course feedback provided anecdotal evidence of the efficacy of the course. The ITOC plans to conduct experiments to conclusively demonstrate this efficacy as future work.

Almost as soon as the IWAR was built and used to teach the Information Assurance class, other departments became interested in it. One semester after it's completion, the Department of Social Sciences began teaching a course in the IWAR focusing on policy of cyber warfare. Because many cyber warfare policy makers are ignorant of the technology for which they are decreeing policy, a large component of this course at West Point involves hands-on orientation to a number of exploits, attacks, and defensive measures. Several times the Fundamentals of Information Technology course, a mandatory course for all Plebes (freshmen) has used the IWAR to emphasize a topic. More and more classes at West Point are considering making use of the IWAR Range in the future even if that use is only for one or two class periods.

HOW DID THE CYBER DEFENSE EXERCISE COME ABOUT?

Since the early stages of IWAR development, USMA had thought of initiating an inter-academy Cyber Wargame. These thoughts began to take shape during the first meeting of the Information Assurance – Service Academy Group for Education Superiority (IA-SAGES) in June 2000. Representatives from the US Military Academy (USMA), US Naval Academy (USNA), and US Air Force Academy (USAFA) explored the idea of establishing a network to host a Cyber Defense Exercise. It was agreed to focus on the defensive aspect of information operations as it aligned well with the goals of the IA programs being developed at the academies. It also directly related to the goals employed by the National Information Security (INFOSEC) Education and Training Program, which had instituted NSA Visiting Fellows within the USMA and USNA. It was, therefore, decided to pursue the means to create the “sandbox” and begin to outline the logistics behind hosting such an event.

Shortly after this meeting, an unrelated request to the DoD Public Key Infrastructure (PKI) Program Management Office (PMO) for resources to support research and education in Public Key Encryption resulted in a landfall of acquisitions. The PKI PMO offered to provide funding to supply USMA with a PKI lab to consist of ten Windows-based workstations and two Sun Servers. In return USMA would educate future officers in a system that is currently be deployed DoD-wide. Once the word was out the Naval Postgraduate School (NPS) and USAFA became interested in acquiring similar resources and the PKI PMO was quick to accommodate the request.

The delivery of the PKI lab equipment provide a means of furnishing all the members of the IA-SAGES with the resources they would need not only to perform PKI education, but also to support a Cyber Defense Exercise. The minimum computers, networking components, and software required at each of the five US service academies and NPS to support a PKI-enabled Cyber Defense Exercise were determined. This plan was proposed and the PKI PMO whole-heartedly endorsed the concept.

The Chairman of IA-SAGES then set out to convince the USNA, US Merchant Marine Academy (USMMA), and US Coast Guard Academy (USCGA) to participate in the exercise. USNA and USMMA agreed to accept the equipment with the expectation that they would require a year to ramp up their IA programs prior to participating in the Cyber Defense Exercise.

Funding was in place and the stage was set for the USMA, USAFA, and NPS to participate in the first Cyber Defense Exercise in the spring of 2001. The remaining tasks were to design and build the "sandbox", identify and coordinate the Red Teams willing to participate, and establish the execution plan for the 2001 event.

DESIGNING AND IMPLEMENTING THE "SANDBOX"

With continuing focus on educating cadets in the area of Information Assurance while employing a multi-disciplinary approach, the ITOC decided it was important to capture the learning experience associated with the gathering of requirements, design, and construction of the Cyber Defense Network (CDN). The effort was perfect for a non-Computer Science major Information Systems Design course capstone project. A project team made up of four students majoring in Economics, Geography, and International Relations were assigned this task. USAFA wished to participate in the development as well. As a result, they assigned a cadet majoring in Computer Science and enrolled in an independent study to join the USMA project team.

The USMA project team was tasked to: (1) design a network (Cyber Defense Network) include various operating systems, network services, databases, and applications typical of military and commercial information infrastructures; (2) provide secure, remote connectivity to the CDN for Red Teams; (3) ensure the CDN is electronically separated from the academy backbone; (4) and provide installation instructions and ghost CDs so the identical configuration could be copied at all the participating schools. The CDN as delivered to each academy would be intentionally weak in IA safeguards. This would give students enrolled in the Information Assurance course and opportunity to practice their newly acquired skills in "defending the network". Cadets will have about two weeks to implement IA measures using what they have learned in their respective courses. An Internet-hosted Virtual Private Network, PKI-enabled and off-limits to the students during the exercise, would provide a way for Red Teams to evaluate the security posture each academy team achieved.

It is important to note that cadets developing the CDN will not participate in the Cyber Defense Exercise.

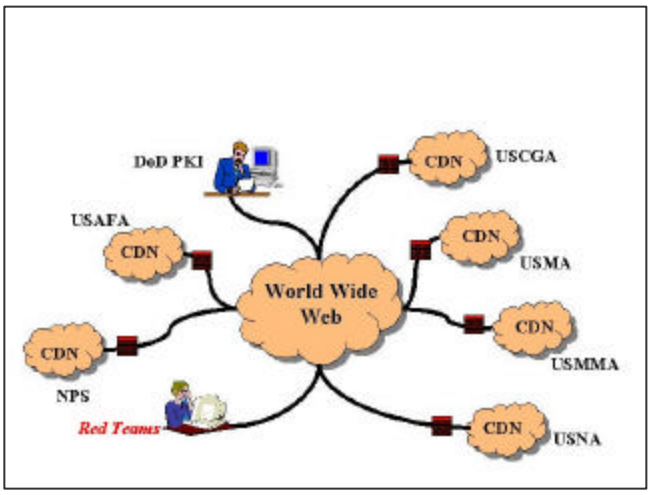

Figure 2: Inter-Academy Cyber Defense Exercise Conceptual Diagram

The cadet project team enthusiastically accepted ownership of this effort and went above and beyond what was normally required of capstone project teams. A Cyber Defense Exercise summit was held at the USAFA in January 2001, which served as a program review. The cadets delivered a briefing to the DoD PKI PMO, faculty involved with the CDE, and the US Air Force Red Team on their design and implementation plan. They gathered input to create a draft Rules of Engagement (ROE) and outline the milestones associated with conducting the 2001 Cyber Defense Exercise.

The final Cyber Defense Network design consists of platforms running Sun Solaris? , Linux, Windows 2000? , Windows 98? , and Windows NT? operating systems. Internet access is provided to allow for downloading the latest patches and software updates. These systems are configured to provide various services such as: IIS, ColdFusion? , database servers, Web servers, file servers, and application servers. The final design for the VPN is still under development. The long-term solution is to use V-One Smartgate? software in conjunction with a Gauntlet? firewall hosted on a Sun Solaris? platform. This will allow the DoD PKI to provide authentication and encryption between the CDN and the Red Teams; however, the current design relies on a series of CISCO routers to provide point-to-point encryption and authentication between each CDN and Red Team.

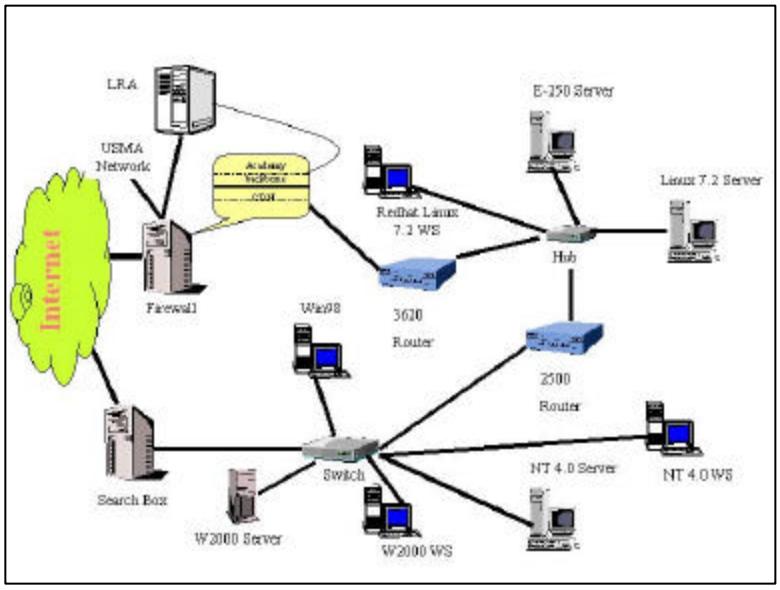

Figure 3: Cyber Defense Network Architecture

WHO WILL ATTACK?

The CDE concept involves independent parties to evaluate the performance of the cadets in securing the network. As early as September 2000, the 92nd Aggressor Squadron, US Air Force IWAR Center, Kelly Air Force Base, learned about the CDE through a chance meeting with an ITOC member at an IA conference. They immediately expressed interest in supporting as a Red Team. They briefed their organization and mission at the Cyber Defense Exercise summit, and they were accepted as a Red Team for the CDE. After a bit more coordination, they agreed to provide evaluation criteria that will be used to objectively determine a winner. They also indicated even if remote connectivity were not provided, they would be willing and able to support an on-site Red Team effort for each school.

After a briefing to the NSA Executive Command in January of 2001, the Defense Information Operations Group offered to provide a Red Team to support the exercise. This relationship has already proven to be of immense value. Due to problems each school encountered configuring the VPN, the NSA Red Team has taken the lead in establishing remote connectivity and has agreed to review and comment on the evaluation criteria provided by the 92nd Aggressor Squadron.

The third and final Red Team to join the exercise is from the Land Information Warfare Activity, US Army. In order to ensure the exercise is fair, each Red Team will attack each of the three participating schools during different time periods. They will each provide an independent final report and recommendation to the Cyber Defense Exercise Board. The Cyber Defense Exercise Board, made up of representatives from each US service academy, Red Team, and the NSA will decide the winner of the IA trophy.

EXECUTION OF THE 2001 EXERCISE

The overall mission of the CDE is to minimize the risk of a security breach while ensuring necessary operational services are maintained. It is also imperative, should a security breach take place, it does not go undetected. Cadet teams participating in the exercise are assigned to subordinate missions and will have four weeks to develop security implementation plans and ten days to work hands-on to secure the network.

During the Red Team attacks, the cadets will be required to electronically transmit the "Order of the Day" to all workstations within the Cyber Defense Network while maintaining confidentiality and integrity. This transmission must provide a system status and indication and evaluation of any known intrusion and/or attack. It is possible that the Red Teams may introduce vulnerabilities while entering the CDN. Since the CDNs will not be manned by cadets 24 hours a day, any vulnerabilities introduced will be left for a period of time to give cadets the opportunity to search and record intrusions. Once this time expires the Red Teams will return the CDN to its original state for the next Red Team.

The cadets will be provided with system documentation including network diagrams, hardware and software resources, operating systems, and services included within the CDN. They will be encouraged to use this information, all they have learned in their

studies, and any other ethical means at their disposal to immediately commence planning for the secure configuration of the CDN. In addition, they will be provided with the Rules of Engagement (ROE), which outlines the necessary operational services and limitations imposed to ensure fair competition.

No social engineering or attempts to introduce vulnerabilities into an opposing academy's infrastructure are authorized. This had to be addressed as the question arose from cadets, "…can we have insiders introduce malicious code to our opponents systems?"

Upon completion of the one-week attack period, the Red Teams will provide their independent After Action Reports (AAR) and recommendation to the Cyber Defense Exercise Board. The board will have one week to review and select a winner. The winning academy will be presented the NSA Information Assurance Director Trophy (currently under contract for procurement).

CONCLUSIONS AND FUTURE EXPECTATIONS

The US Military Academy, US Air Force Academy, and the Naval Postgraduate School will compete in the 2001 Cyber Defense Exercise. There is strong interest among faculty at the US Merchant Marine Academy and the US Naval Academy to compete in the future. Because NPS is a graduate program, it will not compete for the NSA IA Director's Trophy; however, since word has spread, there is interest in expanding the exercise to include graduate programs that are certified as Centers of Excellence in Information Assurance.

The NSA IA Director's trophy will be a traveling award and will reside with the winning academy for the academic year. This award will serve to advertise and generate interest among students nation-wide to learn about Information Assurance.

The results of the exercise will be out briefed by the Red Teams and discussed with each cadet team through a planned video teleconference. Results will also be evaluated to determine how well prepared the cadets were for the exercise. This information will serve as feedback to make future improvements to the IA course. It will also be valuable to see how the cadets perform as compared to real-life operational organizations undergoing similar Red Team evaluations.

Upon completion of the exercise, the expectation is for the CDN at USMA to be disconnected from the Internet and used by a newly formed student organization that is focused on information assurance topics. This group will be a Special Interest Group (SIG) of the student Association of Computing Machinery (ACM) chapter at West Point. The group's full name will be the Special Interest Group for Security, Audit, and Control (SIGSAC). Cadets in the group will have an opportunity to reconfigure the network into Red and Blue teams. They will then try to replicate exploits that appear in popular news media, and experiment with a variety of defensive software products and firewalls. This will provide a healthy outlet for cadets' interested in this topic. It provides an unstructured, but supervised, environment for them to learn about these technologies in a fun, unthreatening, and un-graded manner. This free play will be supplemented with

demonstrations by external consultants, faculty, and other cadets experimenting in this area.

The CDN will revert back to its original purpose, providing a facility for the conduct of the Cyber Defense Exercise, each spring so that it may be used in conjunction with the IA course. The CDN will be returned to its baseline configuration using the Ghost CDs and installation procedures provided by the PKI-Enabled VPN CDE Rapid Set-up cadet development team. It should be noted that the workload for cadets at USMA does not allow for cadets to branch out into many different areas. Fortunately, the resources provided in the Cyber Defense Network and by the SIGSAC give cadets, especially those who are not majoring in Computer Science, an opportunity to experience Information Assurance exercises throughout their cadet careers. These cadets could be thought of as participating in intramural or junior varsity athletics. Through their involvement in SIGSAC and by taking prerequisites courses they are preparing themselves for playing at the varsity level during their senior year when they participate in the CDE exercise. More importantly, they are preparing themselves for the time when all of them, as commissioned officers will be responsible to protect and defend the many critical information system upon which our Army depends.

REFERENCES

[1] Robert R. Tomes, "Boon or Threat? The Information Revolution and U.S. National Security," *Naval War College Review*, vol. LIII, pp. 21-38, 2000.

[2] Curtis A. Jr. Carver, "Information Warfare: Our Next Task Force Smith," Unpublished Research Paper. Fort Leavenworth: U.S. Army Command and General Staff College, 1997.

[3] Terrill D. Maynard, "International Implications and the NIPC," in Proc. *InfowarCon 99*, Washington, September 6-9 1999.

[4] Surdu, George, Global Directory of Information Systems, Technology, and Services, Ford Motor Company, personal conversation, October 2000.

[5] Robert Turk and Shawn Hollingsworth, "Information Assurance: Army prepares for next generation of warfare," *Army Communicator*, vol. 25, pp. 34-35, 2000.

[6] John Arquilla and Don Ronfeldt, "In Athena's Camp: Preparing for Conflict in the Information Age," Santa Monica: RAND, 1997.

[7] Michael I. Handel, *Masters of War: Classical Strategic Thought*, Second Revised and Expanded ed. London: Frank Cass, 1996.

[8] Richard M. Felder, "Reaching the Second Tier -- Learning and Teaching Styles in College Science Education," *Journal of College Science Teaching*, vol. 23, pp. 286-290, 1993.