Trial-By-Fire in Information Assurance Education

Donald Welch, Daniel Ragsdale and Wayne Schepens
United States Military Academy
West Point, New York 10996

Abstract

During the spring of 2001, the United States Military Academy, the United States Air Force Academy, and the Naval Postgraduate School participated in the first ever Cyber Defense Exercise. Each school set up identical small networks running a typical suite of services. They then configured the network to be as secure as possible in advance of attacks by a NSA-led Red Team. After almost a week of attacks a winner was declared. This was the best educational experience any of the authors ever participated in and most students felt the same way. Although this exercise required a great deal of resources, the information assurance educational outcome was great. By following the principles of exercise design we suggest here a less ambitious exercise could become a standard feature of information assurance programs.

Introduction

The United States Military Academy (USMA) at West Point is striving to educate leaders of character who serve the nation. USMA has evolved throughout the last 200 years to create leaders who meet the needs of national security as those needs have evolved. When Thomas Jefferson created USMA in 1802 he saw the requirement for not only a professional officer corps, but also skilled engineers. At that time there were no engineering schools in the United States and West Point was the nation's first.

Since then West Point has produced leaders who built the nation's infrastructure and defended the nation's interests as the world has evolved. The world and the technology continue to evolve and West Point is keeping pace with the times. The newest threat to our national security comes not through just a new type of weapon or a new adversary, but through an entirely new environment, i.e., cyberspace.

The U.S. military is leveraging information technology to become more effective in everything it does. Many economists attribute the economic growth of the last decade to the effective integration of information technology. A disconcerting attribute of information technology today is that the more advanced a nation is in the use of information technology, the more vulnerable they are to the loss of that technology. [1] 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 against our national interests very likely. Each day it becomes increasingly plausible that cyberwarriors working for an adversary that in no other way could hurt the U.S. could cripple U.S. critical information systems. In response the Army has placed as much

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	7/14/2001	Research Paper 7/14/2001

4. TITLE AND SUBTITLE
Trial-By-Fire in Information Assurance Education

5. FUNDING NUMBERS

6. AUTHOR(S)
Welch, Donald; Ragsdale, Daniel; Schepens, Wayne

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

United States Military
Academy
West Point, NY 10996

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

IATAC
3190 Fairview Park Drive
Falls Church, VA 22042

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

During the spring of 2001, the United States Military Academy, the United States Air Force Academy, and the Naval Postgraduate School participated in the first ever Cyber Defense Exercise. Each school set up identical small networks running a typical suite of services. They then configured the network to be as secure as possible in advance of attacks by a NSA-led Red Team. After almost a week of attacks a winner was declared. This was the best educational experience any of the authors ever participated in and most students felt the same way. Although this exercise required a great deal of resources, the information assurance educational outcome was great. By following the principles of exercise design we suggest here a less ambitious exercise could become a standard feature of information assurance programs.

14. SUBJECT TERMS
IATAC Collection, information assurance

15. NUMBER OF PAGES
12

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

emphasis on defending its information infrastructure as it had spent on Y2K remediation [2].

West Point is meeting this new challenge through education. West Point has doubled the number of information technology courses in the core curriculum. The cadets learn leadership in a wired world; they run the activities of the Academy using a sophisticated information infrastructure. Last year West Point started an information assurance club that now has over 250 student members. USMA teaches two elective courses devoted to information assurance, one a multi-disciplinary course aimed at non-technical students and the other a highly technical course for computer science majors. Five academic departments (Computer Science, Math, English, Law and Social Science) offer a total of eighteen courses that cover information assurance topics. The result of all these efforts has been USMA's designation as the first undergraduate-only National Security Agency Center of Excellence in Information Assurance Education.

A key component of this effort is the technical information assurance course. The course is built around the Cyber Defense Exercise. This is a hands-on competitive experience allows the students to pull together their computer science and information assurance education and put it to the test by defending a network against an adversarial Red Team.

Information Assurance Course

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. This course 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 that is so important in rapidly evolving disciplines like information assurance.

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 and a half years of military training and education by the time they take the information assurance 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 an opponent as well as oneself leads to victory. 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. The course goals not only emphasize the technical aspects, but also require the students to understand the context of how these tools are used.

Information Assurance Course Objectives

1) Know the components of a comprehensive information assurance model and be able to place a new concept in the model.
2) Understand the legal, ethical, and moral issues associated with information assurance.
3) Understand the considerations taken into account by Information Operations (IO) planners at the strategic, operational, and tactical levels of war.
4) Know the enabling technologies that can be employed to assure information.

5) Understand the underlying principles pertaining to the conduct of offensive information operations.
6) Understand the underlying principles pertaining to the conduct of defensive information operations.

These objectives support the three goals we have for the course, all of which we want to have a defensive focus. The first goal is to produce students that can think critically about information warfare policy and strategy. A second goal is to give students a better understanding of the conduct of information warfare and the *terrain* on which it occurs, i.e. cyberspace. Students start the course towards the end of an accredited computer science major. They generally understand information systems, software development, network protocols and that ilk. What they do not understand is how all these fit together to make secure or insecure systems. Our goal is to provide them with the tools to supervise the construction of a cyberspace defense with both depth and breath. The final goal is the blending of the two above goals. Our graduates must make low-level security decisions that take into account the larger framework and the effects that will be felt far beyond their own span of control.

For the information assurance 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 students [3]. Major portions of the course included in-class laboratory exercises or out of class projects and homeworks that got the students using security tools.

Cyber Defense Exercise

We know from our own experience as well as that of others [4] that project-based learning is a effective tool for education. In addition, making the project competitive greatly enhances the educational value. [5] Since the goal from the onset of this information assurance course has been to educate in the context of defense, we decided that the defense of a network would be the ideal course project.

Cyber Defense Exercise Genesis

Since the early stages of information assurance education program development, West Point had thought of initiating an inter-academy Cyber Wargame. These thoughts began to take shape during the a meeting of educators from USMA, US Naval Academy (USNA), and US Air Force Academy (USAFA) during an information assurance conference. The representatives explored the idea of establishing a network to host a Cyber Wargame between the three schools. The wargame itself focused on the defensive aspect of information operations rather then an open-ended, attack and defend framework. We felt this better aligned with the institution's information assurance programs. Next we pursued the means to create the "battlefield" networks and begin to outline the logistics behind hosting such an event.

Around the same time, the DoD Public Key Infrastructure (PKI) Program Management Office (PMO) decided to supply West Point with a PKI lab to support research and education in Public Key Encryption. The PKI PMO offered to provide a laboratory consisting of ten Windows-based workstations and two Sun servers. In return USMA would educate future officers in a system that is to be deployed DoD-wide. The

Naval Postgraduate School (NPS) and USAFA also became interested in acquiring similar resources and the PKI PMO was quick to accommodate their requests.

Happily, the delivery of the PKI lab equipment provided a means of furnishing all the academies with the resources they would need not only to perform PKI education, but also to support a Cyber Defense Exercise. When approached with the dual use plan, the PKI PMO whole-heartedly endorsed the concept. After further investigation USMA, the NPS and USAFA would participate in the first Cyber Defense Exercise. The USNA and United States Merchant Marine Academy agreed to accept the equipment with the expectation that they would require a year to ramp up their information assurance programs prior to participating in future Cyber Defense Exercises. The computers were 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 "battlefield", identify and coordinate the Red Teams willing to participate, and establish the execution plan for the 2001 event.

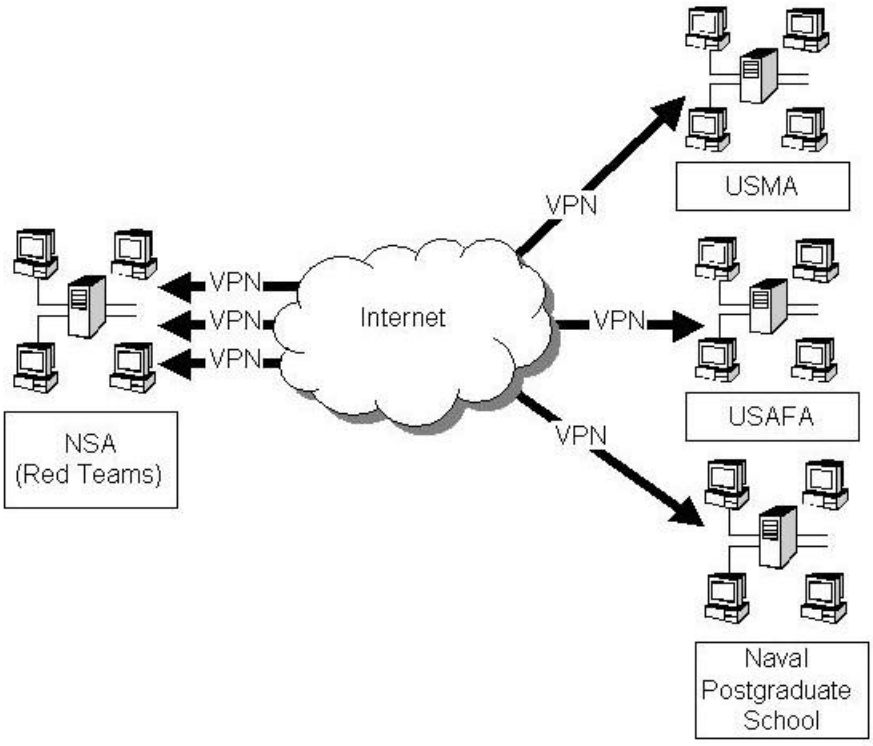

Figure 1: Cyber Defense Exercise Architecture. The Red Teams at NSA Headquarters were connected through VPNs to the Cyber Defend Network installed at each school. This architecture minimized the risk of collateral damage and allowed the attacks to take place without interference from the production security measures.

DESIGNING AND IMPLEMENTING THE "BATTLEFIELD"

The "battlefield" had to be a network that would resemble or even duplicate the kinds of networks that are part of the current infrastructure. To the greatest extent, the hardware and software should be the kind that officers encounter after graduation. the

work of defining parameters for such a battle field was an additional opportunity for student learning. Moreover, it was an opportunity for employing a multidisciplinary approach since the information infrastructure is a multidisciplinary space. The effort was suitable for an Information Systems Design Course capstone project. Cadets researched, designed, and constructed the "battlefield" which we called the Cyber Defense Network (CDN). A project team made up of four students majoring in Economics, Geography, and International Relations were assigned this task. USAFA volunteered to participate in the development as well. They assigned a Computer Science major enrolled in an independent study to join the USMA project team.

The project team was tasked to: (1) design a 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) provide installation instructions and CDs so the identical configuration could be copied at all the participating schools. The CDN as delivered to each academy would intentionally be weak in security safeguards. This would give participating students an opportunity to practice their newly acquired skills in defending the network. We used an Internet-hosted Virtual Private Network (VPN) to connect the Red Teams and the participating schools. The VPN provided a way for Red Teams to enter the battlefield without the danger of collateral damage to the production networks and without causing false alarms for the production network security monitors.

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 project review. The cadets delivered a briefing to the DoD PKI PMO, faculty involved with the Cyber Defense Exercise, and the US Air Force Red Team on their design and implementation plan. They gathered input to draft the Rules of Engagement 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: web servers, database servers, file servers, e-mail servers as well as the normal contingent of network utilities.

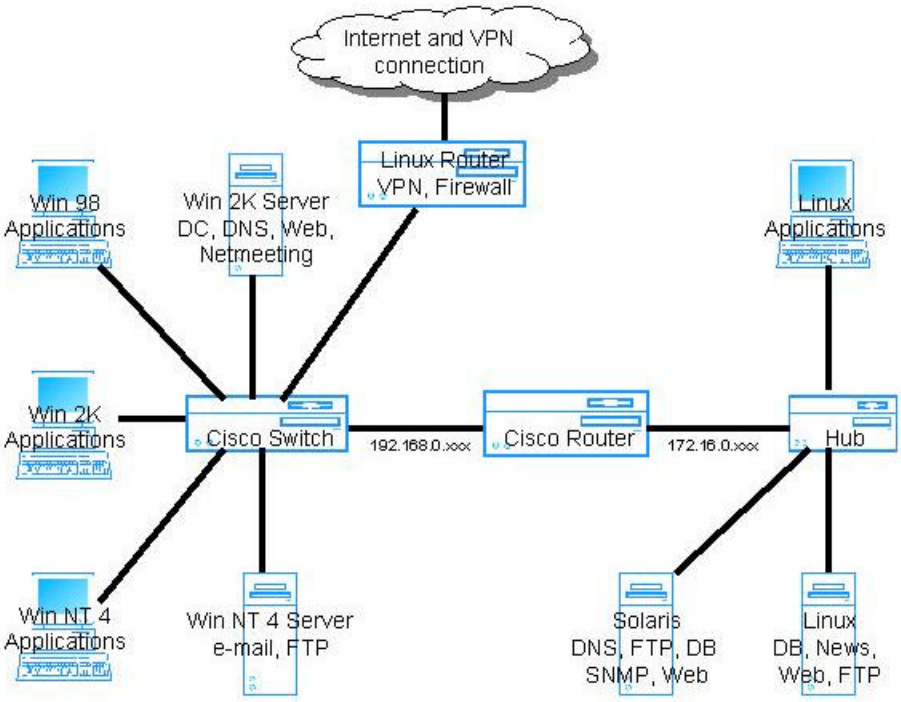

Figure 2: The Cyber Defense Network. This is a diagram of the simple network installed at all the participating schools. It balances the need for broad representation of different operating systems, networking equipment, and services against size and simplicity.

THE ATTACKERS

The Cyber Defense Exercise concept involves competition in two ways. The most obvious is the competition between the service academies for the best defense. The second is the adversarial competition between the Red Team and the students. The Red Team did double duty, serving as the student-team evaluators. As early as September 2000, the 92nd Aggressor Squadron, US Air Force IWAR Center, Kelly Air Force Base, learned about the Cyber Defense Exercise through a chance meeting with a West Point faculty member at an information assurance conference. They immediately expressed interest in supporting as a Red Team. The 92nd Aggressor Squadron briefed their organization and mission at the Cyber Defense Exercise summit, and were subsequently accepted as a Red Team. They also agreed to provide the evaluation criteria used to objectively determine a student-team winner.

After a briefing to the NSA Executive Command in January of 2001, the NSA also offered to provide a Red Team to support the exercise. The third and final Red Team to join the exercise was from the Land Information Warfare Activity, US Army. The three Red Teams gathered at the NSA headquarters to plan and conduct the attack under the leadership of the NSA. It was up to the Red Teams themselves to insure fairness throughout the exercise. They provided an independent final report and recommendation to the Cyber Defense Exercise Board. The Board was made up of

representatives from each service academy, the Red Teams, and an additional member from the NSA. It decided the winner of the competition based on the outcome of the Red Team attacks.

The exercise generated so much excitement in the information assurance community that on top of all the personnel, equipment, and financial resources generously donated; the NSA also donated a trophy. The trophy is called the NSA Information Assurance Director's Trophy and is kept by the winning academy for the year.

EXECUTION OF THE 2001 EXERCISE

The mission of the students during the Cyber Defense Exercise is to minimize the risk of a security breach while ensuring necessary operational services remain functional. This includes reacting appropriately to any penetrations of the network. The supervising faculty assigned subordinate missions to each student team. Those teams first developed plans without touching the CDN. Then they had ten days to configure and secure the network. During the Red Team attacks, the cadets were required to electronically transmit the "Order of the Day" to all workstations within the CDN while maintaining the confidentiality and integrity of the message. This message included a system status and indication and evaluation of any known intrusions and/or attacks. Because of the rigid cadet schedule, the students were not required to detect and react immediately. Normally, they would do this in the evenings when they did not have conflicting obligations.

Student reactions were limited to reconfiguring their own network to make it more secure. We did not allow any operations against the Red Team or other participants. We also ruled out social engineering by either the attackers or defenders. We understand this is the biggest threat that we face in information assurance, but allowing social engineering would have introduced a lot of complexity without corresponding benefits due to the constrained nature of the exercise.

As you might imagine in an undertaking of this complexity, the execution of the Cyber Defend Exercise did not go off without a hitch. The problems were many and each problem presented an educational opportunity. The cadets participating in the exercise were all computer science majors and as such understood much of the theory of operating a network but had very little experience doing so. Most of the cadets thought that the challenge would be securing the network, not keeping it functional. To the contrary, numerous times they found to their surprise that changing a configuration setting, installing a patch or other security measure had consequences far beyond what the students expected.

From the USMA perspective the exercise started very poorly. The Red Team made several serious penetrations and effectively owned the network. Slowly, but surely the cadets battled back. They removed one vulnerability after another, discovering the security measures they should have taken during the initial configuration the hard way. But they did figure out how to defend the network. The Red Team attacks gave them real-time feedback that meant more than a professor's red pen ever did.

After the exercise the Red Teams gave the students feedback in a teleconference. This was very valuable because the cadets were very interested to find out exactly what went on. We were pleased that they detected and understood many of the attacks, but it

was also very informative to find out what they did not know about. A good example involves the administrator password on the Solaris server. One cadet noticed a compromise and to be safe changed the administrator password on the server. He put a note so that the follow on shift would know the new password. When the new shift arrived, they could not get access using the new password. After much frustration they found the old password still worked. This happened numerous times and finally stopped after they completely reinstalled the operating system. The rest of the students were very angry with the cadet who kept claiming that he had changed the password and correctly noted the change. During the after action review the Red Team revealed that they had installed backdoor accounts and made a copy of the password file. To preclude the loss of their backdoor every 30 minutes the copy of the old file was automatically copied over the live password file, overwriting the changes. This incident left an indelible impression on the students. What's more, the effect of this lesson is not one that can be achieved without experiencing it first hand and with out effective feedback.

In order to encourage student reflection we had the students then put together a final briefing to discuss the things that they did correctly and incorrectly during the exercise. While preparing for this briefing, the students were made to understand what exactly happened during the exercise and the causal relationships between their actions. They thought collectively for the first time, and carefully clarified their own actions as well as the red team's actions. This was necessary in order to produce a coherent briefing on the exercise. We cannot emphasize enough the importance of the after action review and the exercise presentation. Students absolutely learned the most during this period of reflection and writing.

Results of the Cyber Defense Exercise

The United States Military Academy at West Point is the first owner of the NSA Information Assurance Director's Trophy. The trophy competition this year only included USMA and USAFA, as the NPS is a graduate school. The decision was a close one, but based on USMA's ability to keep the required services running as well as their prevention and detection of penetrations they were declared the winners. There were no losers in this competition. This may sound trite, but all participants learned so much during this exercise it was a win-win competition.

Figure 3: The winning Cyber Defense Exercise Team posing with NSA and USMA leadership after the presentation of the NSA Director's Trophy.

The initial plans for network defense by the West Point Teams in the Cyber Defend Exercise were not very mature. Even though the students were required to develop attack trees [6], the plans did not exhibit good breadth or depth. The second iteration of the plans were much better but if completely implemented still would not form a coherent defense. Clearly abstract discussions of computer network defense did not develop clear understanding of a coherent defense in cyberspace in the students. During the configuration of the network the teams finally began to understand what securing a network entailed. We think that this experience is similar to teaching design in software engineering. Students generally only understand what is required in a complete, consistent design when they have to implement a design.

All teams had difficulty just keeping all services running on the network as they made changes to secure it. In fact, the West Point team was a day late in having an operational network for the Red Team to attack. Teams from other schools had roughly the same amount of trouble. Once the attack started they constantly battled to keep the required services running. The West Point teams discovered the hard way to plan and coordinate reactions to attacks.

From a pedagogical point of view we were very pleased to see constant improvement throughout the exercise. In fact, by the end of the week the USMA

network was essentially secure from attack. The cadets were exposed to situations they had never seen or even expected to see. They had to understand what was happening, determine how to fix it, and then actually implement the corrective action. Their ability to do this of their own accord later in the exercise is evidence that the students received an education that transcended the normal classroom experience. The first reaction of the students was that they would have preferred that we teach them exactly how to defend the network. Of course shortcuts diminish the chance for students to absorb the information in a meaningful way. We hope that even if they did not understand the difference between education and training right away, they will realize it when they first take responsibility for a computer network.

The students all realized that they were making tremendous strides during the exercise. The things they learned ranged from the obvious to the profound. We are satisfied that they developed a deeper understanding of what a defense in depth and breadth means in cyberspace.

Each group had to list what, if anything do they think they will remember about this exercise in five years. One group said that they would remember, "how insecure default systems installations are." If this point alone is the only thing that sunk in, the networks these cadets will be responsible for in the future should be better off. This concept coincides closely with the comments of another group. This second group felt the thought "never assume anything" would stay with them for years. Although it is unrealistic to not use assumptions when managing complexity, having a healthy mistrust and retesting assumptions is good leadership in both the cyberworld and the physical world. A common impression on students was, "how difficult it is to administer a network, and how little a computer science education prepared them to do so." Members of the computer science faculty might want to remind these students again of how education differs from training, and that they did do a credible job of learning how to run the network on the fly. The lack of resources for network administration certainly creates a security risk. Even if these cadets never install another patch, they will understand the struggle the administrators have to keep the network both functional and secure. Another group said they would remember, "the importance of teamwork in defending a network." This is a good lesson for any leader, who should recognize that these concepts apply in cyberdefense as well as in kinetic defense. The final group said they would remember, "that you can always make the network more secure." What more can we ask from the leaders responsible for running our information infrastructure? These comments indicate a depth of understanding in information assurance that is rarely encountered among the leaders and managers currently responsible for our nation's critical information infrastructure.

What the students did not say is also encouraging. They were engrossed in the minutiae of network configuration and security for weeks. During this time they discovered that one of the most effective tools in the arsenal was the host-based firewall. Even so, they understood that the technology will change very rapidly and the key to their success will be an understanding of context an ability to understand how technologies and policies interact. This fact underlies the difference between an education and training.

An educational aspect that cannot be discounted is the benefit to the Red Teams. The Red Teams involved in the Cyber Defense Exercise are professionals. They

normally go into an organization and do security audits. In some cases, they are tasked to conduct penetration exercises, but usually these are very limited in scope and take place over extended periods of time. In the Cyber Defense Exercise they greater freedom and the entire exercise took place in a short period of time. Due to the compressed schedule the Red Team got a different perspective of computer network attack. According to the Red Team leader they felt they might have learned almost as much as the cadets did during the exercise.

CONCLUSIONS AND FUTURE EXPECTATIONS

The US Military Academy, US Air Force Academy, and the Naval Postgraduate School successfully competed 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 next year. The NSA Information Assurance 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 to learn about information assurance.

The Cyber Defense Exercise took a great deal of time and effort on the part of many organizations. Yet it resulted in a tremendous payoff, and although the resources to duplicate the Cyber Defense Exercise may be out of reach for many programs the educational benefits are available in smaller exercises. Having observed this first iteration here are our list of principles for designing a similar exercise.

1. **Culminating experience**. This exercise took place near the very end of the student's undergraduate study of computer science. By its nature, information assurance pulls together many different fields from inside and outside of the computer science discipline. It served as a way for students to draw on their entire education and apply it in a practical way. Any exercise should strive draw upon the breadth of a student's education.
2. **Student ownership**. The students must have the responsibility for running and securing the network. Moreover they must have the authority to control most aspects of the exercise. These two requirements go hand-in-hand. Giving the students this kind of control is high-risk. However, without a sense of ownership the students will tend to quit when faced with a very difficult problem. Keeping the instructors in a facilitating role is essential leverage in student motivation and learning.
3. **An adversary**. Being able to match wits against other minds at work is a great incentive as well as great experience. It is one thing to be told that you did something you did was wrong and why. It is another to discover that you have been outwitted and have to clean up the mess that results. There is tremendous learning that goes on when you have to work just to determine what is going on in your network.
4. **Competition**. Competition is the irreplaceable motivator. An exercise like this is difficult and frustrating for the students. Something other than a grade is necessary to keep most students in a hot stuffy laboratory on beautiful spring weekends. Our competition plays on the well-established athletic rivalry between the service academies. Although this is the ultimate motivator, the competition can be much lower key and still effective. Even a competition between two teams from the same school can be a tremendous motivator.

5. **Isolated Laboratory**. Restrictions on what students can and cannot do as part of the exercise should be limited. Otherwise, collateral damage to a production network or the Internet will cause real problems for everyone involved. Having a network *sandbox* where the students and Red Team can safely operate is critical to maintaining student ownership of the network. We had help from the NSA in establishing identical, first-class networks. However, an effective exercise does not require top of the line equipment. We built our first isolated laboratory using leftover and obsolete equipment. So the funds required can be minimal even if the time requirements are great.

All those involved with the 2001 Cyber Defense Exercise felt that it was a huge success. The 2002 competition will be even better with the participation of two more service academies. We learned a lot this year with respect to running the exercise and as a result we expect the 2002 Cyber Defense Exercise to run more smoothly than it did this year. We understand that this is a very complex operation and it is impossible to preclude all problems, so the key is to be able to react quickly any unforeseen problems.

Information assurance is a topic that is vital to the national security of our nation. Unlike the past, we can no longer rely solely on our Armed Forces to defend the nation. Professionals in the commercial sector, the government sector as well as the military must be able to defend our critical information infrastructures from cyberattack. A competitive exercise such as we have described is a tremendous educational opportunity. We strongly encourage educators of information assurance professionals to use similar exercises in their information assurance programs.

REFERENCES

[1] "Critical Foundations: Protecting America's Infrastructures." [web page online], last accessed 15 June 2001, Washington, D. C.: Government Printing Office, October 1997. available from http://www.info-sec.com/pccip/pccip2/report_index.html

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

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

[4] Shankar, P. M. and B.A. Eisenstein, "Project-Based Instruction in Wireless Communications at the Junior Level." IEEE Transactions on Education, Vol 43, No. 3, August 2000, pp 245-249.

[5] Paulik, Mark J. and Mohan Krishnan, "A Competition-Motivated Capstone Design Course: The Result of a Fifteen-Year Evolution." IEEE Transactions on Education, Vol 44, No. 1, February 2001, pp 67-75.

[6] Schneier, Bruce, Attack Trees: Modeling Security Threats. Dr. Dobb's Journal, CMP Media, Inc. December 1999.