The IWAR Range: A Laboratory for Undergraduate Information Assurance Education

Major Joseph Schafer
U.S. Naval War College

Daniel J. Ragsdale, John R. Surdu
Information Technology and Operations Center, United States Military Academy

Curtis A. Carver
Texas A&M University

Abstract

This paper describes a unique resource at West Point, the Information Analysis and Research Laboratory, referred to as the IWAR range. The IWAR range is an isolated laboratory used by undergraduate students and faculty researchers. The IWAR is a production-system-like, heterogeneous environment. The IWAR has become a vital part of the Information Assurance curriculum at West Point. We use the military range analogy 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 also describes the process used to create the IWAR and how an IWAR might be built using limited resources. Finally this paper describes the future directions of the IWAR project.

1 Introduction

The USMA Information Technology and Operations Center (ITOC) developed the Information Warfare Analysis and Research (IWAR) laboratory to support undergraduate education and faculty research at West Point. This report describes the vital role that this isolated computer laboratory plays in teaching information assurance and security to undergraduate students majoring in computer science. First, the background will be explored. Then, the lab design considerations and capabilities will be described. Then the information assurance course will be outlined and pedagogical examples will be presented.

2 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 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 information system. To this end cadets get a broad appreciation for the policy and ethical considerations of Information Warfare along with a strong grounding in the hands-on, technical aspects.

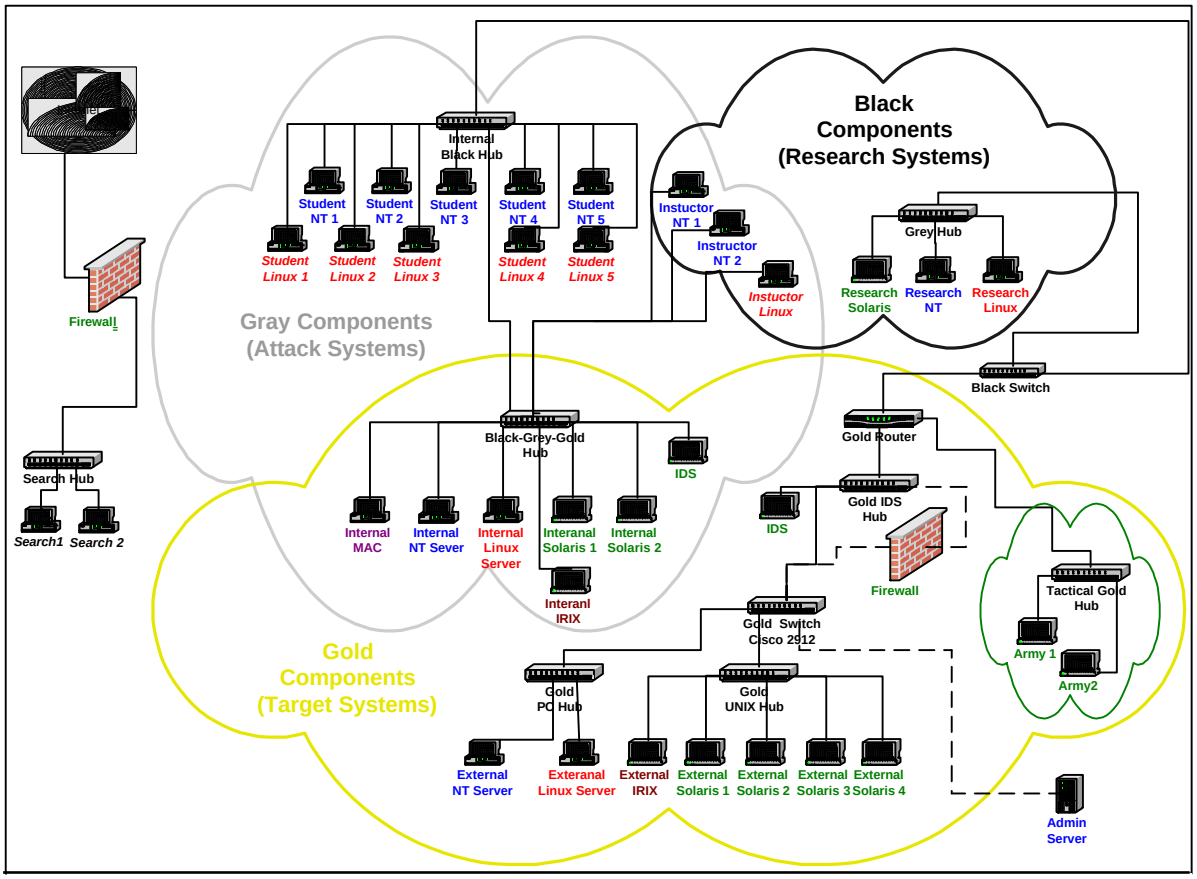

Figure 1: IWAR Range Schematic

3 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. 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 many offensive techniques are taught. 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 of 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.

For our 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 install 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.

4 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 our course they will have had significant basic classroom and field military training experiences. This training includes familiarization with various weapons systems on weapons ranges. These ranges provide a safe and authorized location to conduct training. Leveraging this knowledge, we describe our IWAR lab 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 you can fire automatic weapons on a rifle range at various targets and launch missiles at other targets downrange, so too can you launch cyber attacks from your firing position (cadet computer terminal) in the IWAR lab at target computers (also within the isolated laboratory). Second, it is unthinkable to fire an automatic weapon at a crowd of people from your barracks room; it should also be unthinkable to use any of the cyber attacks from your 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 Lab is divided into four networks. The Gray network is the "hacker" or "attack" side of the network. Cadets have their workstations on the Gray sub network[1]. Each cadet team has one host workstation, but each workstation uses VMWare™ to run both Linux (*Inferno*) and Windows NT (*Hades*) simultaneously on the same physical machine. Cadets have NT Administrator Linux root accounts in both environments. The also have user accounts on all Gray sub network machines. An in-class exercise has the cadets use their NT machines to download a malicious applet from their Linux box on the same physical hardware. The malicious applet then does "bad things" to the NT machine. Also on the Gray network are servers on which the cadet teams have user-level accounts. These "low-hanging fruit" allow the cadets to launch "insider" attacks.

The Gold network hosts the target systems. These are a series of Unix (Solaris and SGI), Linux, Windows NT, and Macintosh workstations and servers. Several machines are Black-Gold meaning that they are targets, but they are on the Black subnet and thus "low-hanging fruit." Except for those machines that are also Black, 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.

In the lab are two machines that are not on 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 lab 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 should avoid having these systems serve as launching points for attacks against other Internet resources.

Together the sub networks that make up the IWAR provide an effective laboratory 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.

5 The "Making Of" IWAR

We constructed all four of the isolated and non-routable networks comprising the IWAR Range to form a realistic, production-like environment of heterogeneous systems. The range was also initially constrained by four design criteria. First, our design must allow minimal possibility of misuse for damage to other systems. Second, we had to make use of on-hand resources. Third, we had a very short time. Finally, we had to fit it 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

[1] The colors of West Point are the colors of the components of gunpowder: black (charcoal), gray (saltpeter), and gold (sulfur).

nightmares we envisioned a New York Times headline, "Network Attack Lab at West Point used to destroy XX," where XX is your favorite innocent, or not so innocent, external site.

We had to make use of on-hand resources because we had constraints on both time and money. Our 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.

Our Electrical Engineering and Computer Science Department maintained 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 setup. 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 allowed us to identify several "underutilized" machines with which to augment our Lab. These machines consisted of three old SGI boxes that had been early Web and graphics servers and two old dual processor Pentium servers that we used for domain controllers and file servers on the Gray and Gold NT domains. We were able also to locate some equipment that had been procured for old projects, such as networking components and an IMac that we were able to transfer into the lab.

Additionally, once we made the decision to establish a completely isolated IWAR Range, we wanted to also provide a more secure method for our students to access resources on the Internet. Our goals were that they should be able search for and download information from even the most untrusted of sites without risking damage to any other systems. We accomplished this by rescuing two old 90 MHz Gateway PCs and loading a very limited and secure version of Linux on them. Forcing the user shell to Netscape and requiring the presence of a Zip disk as the home directory further secured these boxes. In addition, we connected these two "Search boxes" connected to the Academy network through a production firewall donated by the Academy's Directorate of Information Management.

We were much more concerned that our network would be compromised and used to attack external sites than we were about the possibility that someone would hack these search boxes. We could easily recreate the search boxes from a ghost image since there were 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 were 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.

Importantly, our early enthusiasm and achievement garnered some scarce dollars that we used to upgrade some of the rescued machines and procure essential networking, upgrading, and space saving components. Networking components that we were unable to rescue or redirect included mostly inexpensive hubs. Also, primarily due to space considerations, we decided that each student team would get one hardware system and that we would provide both NT and Linux environments by using virtual machines.

After experimenting with various configurations, we learned that we needed to upgrade several rescued machines to achieve acceptable performance. We accomplished this by buying and installing new motherboards, memory, and Zip drives in the Gray machines.

The classroom where we set up the IWAR range 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 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 Mouse) switches for nearly all of the Gold target systems. In addition to space, heat and power proved to be huge constraints for the number of systems we were attempting to setup in one classroom. With KVM switches, we used four sets of Keyboards, Mice, and Monitors for all 25 gold systems, significantly reducing the space, power, heat, and clutter of our target systems.

In addition to a heterogeneous hardware environment, we wanted to provide 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+. We also provided web servers, mail servers, Network File System (NFS), Samba, LanMan, and additional services. We strove to configure these in the most common production configurations. Thus, for example we ran Microsoft Internet Information Server (IIS) and Exchange on the 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 (i.e. RedHat 2.1 and NT4 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 know 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 also were members of the Gray NT domain controlled by another Gray/Gold server.

On the other hand, the main Gold boxes operated with the latest patches and versions of the operating systems (i.e. RedHat 6.0 and NT4 SP6a), patches, and applications. After gaining some confidence in attacking the "low hanging fruit" of Gray/Gold, students could move onto the "tree top 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.

We also wanted to provide a wide variety of tools for students to use and a shared home directory environment for all of the systems with which they had privileges. The shared environment was achieved with 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, we provided a veritable mountain of cataloged "hacker tools" from a Gray/Gold site.

Finally, we engineered a lab of enormous complexity and heterogeneity in a matter of weeks because we sought to provide a high fidelity production-like environment. Despite the time and resource constraints the entire IWAR range was built in four weeks and cost less than $20,000.

6 IWAR Lite

Because we enjoyed the challenge and we did not know precisely which direction this initial course would take, we created an environment that was more complex than it needed to be. We created a quarter million dollar lab with less than ten percent of that cost resulting from new procurements. In hindsight, we could have achieved much of our educational goals with a less complex lab.

Many organizations have old machines that may be rescued for use in a lab such as we describe. A bare minimum

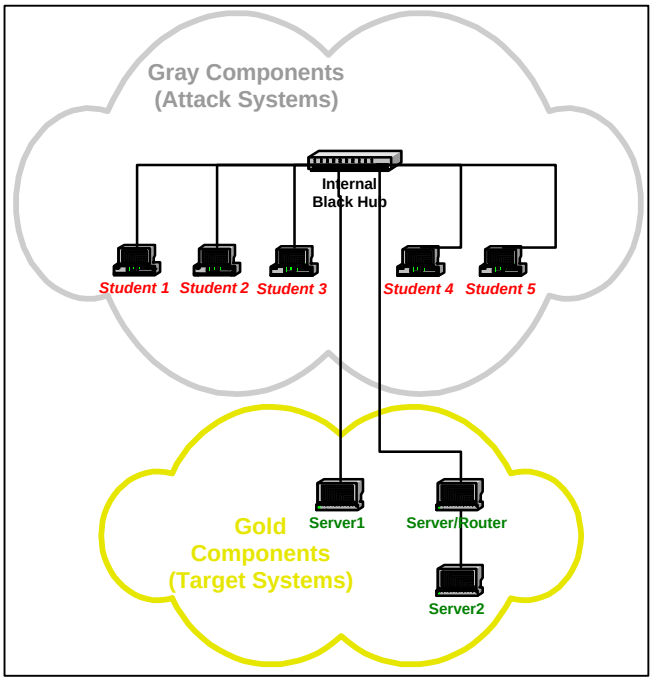

Figure 2: IWAR Lite Schematic

configuration would be for one attack box for each student team of 2-5 students and three target boxes. None of these systems would need to loaded with the latest versions of operating systems and application software. A valuable single semester course could do well to concentrate on a single operating system. For the purposes of this lab, Linux represents a cost-effective and robust environment with which to demonstrate a wide variety of offensive and defensive techniques.

Thus each of the student attack systems could be configured with a full development version of Linux. One of the target systems could serve as a Gray/Gold system upon which the students have user level accounts. The second system could be a file server and act as a router to the third system. The third system would be the hardened Gold system on a separate network with all the latest patches and applications. This approach could then be expanded as resources and time permits to add additional servers and networking components can be located and procured.

7 Is it 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 we 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. We plan to conduct experiments to conclusively demonstrate this efficacy as future work.

8 Conclusion and Future Challenges (a.k.a. "Son of IWAR")

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. We envision more and more classes at West Point making use of the IWAR range in the future – even if that use is only for one or two class periods.

The success of the IWAR range has attracted a great deal of attention – and increased resources. As a result, we were able to completely rebuild the IWAR with new equipment. The older equipment, described in this paper, will be used to see the new Cyber Defense Committee of our local Association of Computing Machinery (ACM) chapter at West Point. Cadets in the club will have an opportunity to defend their hosts (Gray boxes) from other cadets, to try to replicate exploits that appear in popular news media, and experiment with a variety of defensive software products and firewalls. This provides cadets on their unstructured time to tinker with this technology in a fun, unthreatening, un-graded manner. This free play will be supplemented with demonstrations by external consultants, faculty doing research in this area, and other cadets.

As mentioned previously, we have some interest in demonstrating conclusively that the increased educational efficacy of the IWAR actually exists. Secondly we intend to try to determine a value of the IWAR as an educational tool – a return on investment, so to speak. To this end, we are conducting literature reviews and designing experiments to support these claims.

9 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.