

# EDUCATING STUDENTS ON INFORMATION ASSURANCE THROUGH IMMERSION AND OPERATIONAL LEADERSHIP

Curtis A. Carver, Jr.  
United States Military Academy

## Abstract

This paper presents the results an experiment to educate students on information assurance through immersion and student-led learning. As technology progresses, students face increasing attacks on their information systems. Rather than educate students solely in the classroom, we implemented two experiences to increase student understanding of modern information assurance using the students themselves: the student information security officers (SISOs) and the Carronade exercise.

The student information security officer program empowers students to address information assurance education of their fellow students. Students are organized into groups of approximately 120 and each group is assigned a SISO. The SISOs are organized in a hierarchy so that ultimately one SISO is responsible for all. The SISOs educate and mentor their students on safe computing through formal classes in their dorms, formal inspections of personal computers, security awareness exercises, and assisting students when they encounter a problem. The empowerment of students to operationally lead their student organization has resulted in marked improvements in student learning regarding information assurance and computer attacks. An indicator of this learning is the Carronade exercise.

The Carronade exercise is an immersive information security awareness exercise conducted very semester since September 2003. SISOs launch the exercise using an automated phishing tool that generates a phishing email attack against every student under the control of the SISO. If a student succumbs to the attack, the SISO is informed of the identity of student. No personal information is transmitted. The

SISO then has an opportunity to mentor the student and explain why the email was a phishing attack and what the telltale signs were that identified the email as an attack. Because the attack occurs in the normal work environment of the students, it is viewed as highly relevant to the students. Due to the low threat and personal mentoring approach employed to resolve mistakes, students are receptive to the exercise. This has led to a marked improvement in student performance against phishing attacks over the last three years. The empowering of students to teach and mentor their fellow students through the SISO and Carronade programs has proven to be very successful.

## Background

The number and sophistication of computer attacks has grown dramatically in the last twenty years. In terms of numbers, the growth has been exponential[1]. The sophistication of the attacks has likewise increased with the development of rootkits, patch reverse engineering, and the involvement of organized crime and nation states in launching the attacks. In the last five years, as perimeter defenses have stiffened, computer attacks has attempted to bypass perimeter defenses and manipulate individual users through a number of social engineering techniques and attack vectors. Phishing attacks, spear phishing attacks, malicious websites, and encrypted emails with embedded attacks are all indicative of these new attack vectors.

Attempts to make our students aware of the threat and train them through passive classroom experiences proved inadequate. In fact, our students became more susceptible to these types of attack the longer they were at the college. What was needed was active, immersive

educational experience outside the classroom that was relevant to the students and changed their behavior.

Given the preference of the current generation for coauthoring solutions and collaboration[2], and the effectiveness of active learning approaches, the Military Academy decided in 2003 to empower students and conduct active learning exercises. The empowerment of students was done through a Student Information Security Officer program. The active learning outside the classroom became the Carronade exercise. The rest of this paper explains these two programs and provides an analysis of the results.

### **Student Information Security Officers**

The student information security officer (SISO) program empowers students to address information assurance needs of their fellow students. This program focuses on safe computing in a university environment with support embedded in the student dormitories. Students are organized into groups of approximately 120 and each group selects a SISO. The SISOs are organized in a hierarchy so that ultimately one SISO is responsible for all students. The SISOs educate and mentor their students on safe computing through formal classes in their dorms, formal inspections of personal computers, assisting students when they encounter a problem, and a security awareness exercise. The formal training and embedded mentors (SISOs) provide a foundation for understanding. The formal inspections ensure periodic reestablishment of safe computing platforms, and the security awareness exercise maintains sensitivity to the importance of information assurance.

All freshmen attend formal classes that orient them to what normal computing is at West Point. These classes are conducted by the SISOs and scheduled at the beginning of the academic year. Attendance is mandatory. The classes cover everything from accessing the student information system to recognizing a phishing

attack. The class also identifies the SISO and their role to fellow students, and, establishes a reporting scheme for any incidents. While seemingly trivial, knowing who to report abnormal computer activity to at a university is essential and uncommon.

Once per semester, the SISOs conduct a formal inspection of their fellow student computers (see Figure 1). This inspection examines a number of personal computing criteria including: last time the computer hard drive was defragmented; the currency of the antivirus files; the results of the latest antivirus scan; the presence of an anti-spam tool; and, a number of other criteria. The institution provides rewards to student organizations that perform well during this inspection. Due to the nature of the rewards, there is significant peer pressure for everyone in the organization to perform well on the computer inspection. SISOs also perform a role in outrage reporting.



Figure 1: SISO Computer Inspection.

The SISOs have the contact information for the appropriate Dean's staff for providing IT services. Students contact their local SISO who in turn can contact the appropriate service personnel to fix any IT system outage. Due to the heavy reliance on student information systems, this approach has been very effective on weekends and holidays in restoring systems and allowing students to continue to learn. This system has significantly increased the speed at which outages are reported and resolved. This

improvement in service lead to increased student satisfaction.

Finally, the SISOs have limited system administration privileges on the student computers that they are responsible for. These privileges are implemented through Microsoft Active Directory using the ActiveRoles tool. SISOs can reset passwords, correct user information stored in Active Directory, rebuild the operating system and standard applications quickly, and address common problems that the students may encounter. Password resetting and Active Directory information correction is implemented through ActiveRoles. Rebuilding the operating system and standard applications is accomplished through a hidden partition that can be accessed through the computer BIOS. Finally, the SISO has working relationships with those organizations providing information technology support to the students and can intervene as necessary. The empowerment of students to operationally lead their student organization has also affected student learning. An indicator of this learning is the SISO-controlled Carronade exercise.

### **Carronade**

The Carronade exercise is an active learning, spear phishing exercise conducted every semester since 2003. The exercise is student controlled and initiated. Each SISO conducts the exercise for his or her organization. Once initiated, the Carronade system automatically sends one of four phishing attacks to each member of the SISO's organization (see Figure 2) in the form of an email. The student receives the attack in their normal work environment and not in the form of an artificial construct such as a classroom. This enhances the realism of the exercise and credibility of its results.

If a student succumbs to the attack, no personal information is transmitted but instead the SISO is notified so that they can mentor the student. This personal and non-threatening means of remediation reduces the negative aspects of the exercise and enhances the role of

the SISO. The Carronade system automatically collects statistics on each organization so that comparisons can be made and appropriate rewards provided to those organizations that excel.

**From:** sr1770@zzzz.edu[mailto:sr1770@zzzz.edu]  
**Sent:** Tuesday, June 22, 2006 4:57 PM  
**To:** smith@zzzz.edu  
**Subject:** Grade Report Problem

There was a problem with your last grade report. You need to:

Select this link [Grade Report](#) and follow the instructions to make sure that your information is correct; and report any problems to me.

Robert Melville  
Associate Dean  
sr1770@zzzz.edu  
Washington Hall, 7<sup>th</sup> Floor, Room 7416

Figure 2: Carronade Message

Academy leadership, the information technology service groups, and students are aware of the Carronade concept but not of the deployment date, deployment means, or the content of the spear phishing attack. Only the SISOs know when they initiate the exercise. Thus, the college's incident reporting mechanisms and leadership are tested every time that Carronade is run. While this effect has not been measured, it has had a positive effect on the ability of the college to respond to a computer attack as the institution practices one every semester under the leadership of the students. In an era of increasing zero-day attacks, the Carronade exercise has enhanced the college's ability to respond to attacks.

### **Analysis**

The SISO and Carronade programs have proven to be very successful. The empowerment of students to help other students with common computing problems and resolve system outages

has proven to be very popular. Student support is available from a convenient location all the time. Many students actively seek out the SISO positions as all students must serve in a leadership role prior to graduation and SISO is one of the institutionally approved roles. Exit interviews suggest the student perceive the positions as meaningful to the student organizations and beneficial to university. Anecdotal evidence suggests an increase in reporting system outages, increased system availability, and increased student satisfaction with the computing infrastructure in large part due to the SISOs.

The use of Active Directory and ActiveRoles provides only those permissions necessary for the SISOs to fulfill their responsibilities. The college has not detected a single attempt by a SISO to abuse their permissions.

When the Carronade program was first instituted in 2003, there was no correlation between time at the institution and student ability to detect a phishing attack (see Figure 3). In fact, the seniors were more susceptible to phishing attacks than the preceding classes. At this time, the student's only exposure to phishing attacks was in the form of classroom lecture. By 2005, the SISO and Carronade programs had had an impact and the longer the student spent at West Point, the more likely they were to identify a phishing attack (see Figure 4).

The improvement was significant as slightly more than half the freshman failed the exercise while slightly less than 20% of all seniors failed. The sample population for each year group is approximately 1,000 students. While a 20% failure rate is still too high, the decrease is movement in the right direction. As the sophistication of computer attacks increase, the sophistication of our users must likewise increase. Carronade is an active learning exercise that increases the ability of students to detect spear phishing attacks.

An unexpected side effect of the SISOs and the Carronade exercise was an increase in reporting (see Figure 5). The longer a student was at the institution, the more likely they were to report a phishing attack to their SISO. This was a rather substantial change in the behavior of our students. When Carronade first started, many students would simply follow the instructions claiming a person in authority had told them to do so or ignore the attack and not report it. Both student excuses are not acceptable and led to institutional strategies to properly respond to questionable instructions as well as how to respond to a suspected computer security incident. While the percentages are very low, they confirm a credible increase in reporting with approximately 4,000 students participating in the 2005 Carronade exercise. They also confirm the common belief that most attacks are not reported to an organization.

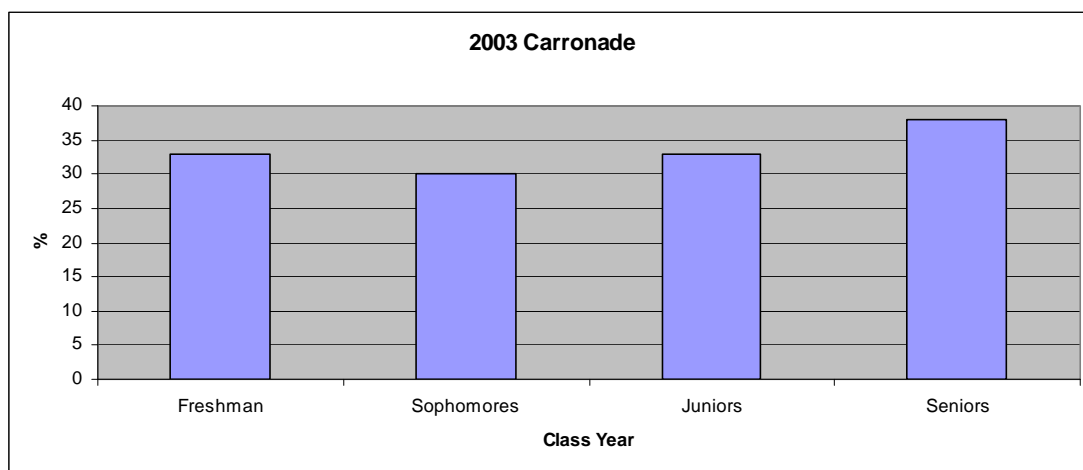


Figure 3: 2003 Carronade Results.

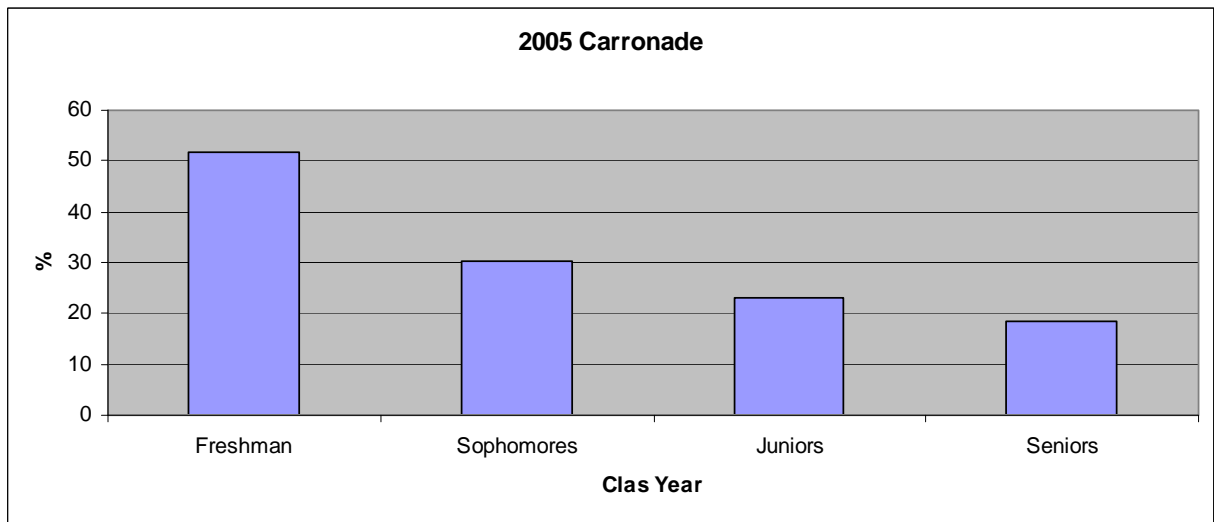
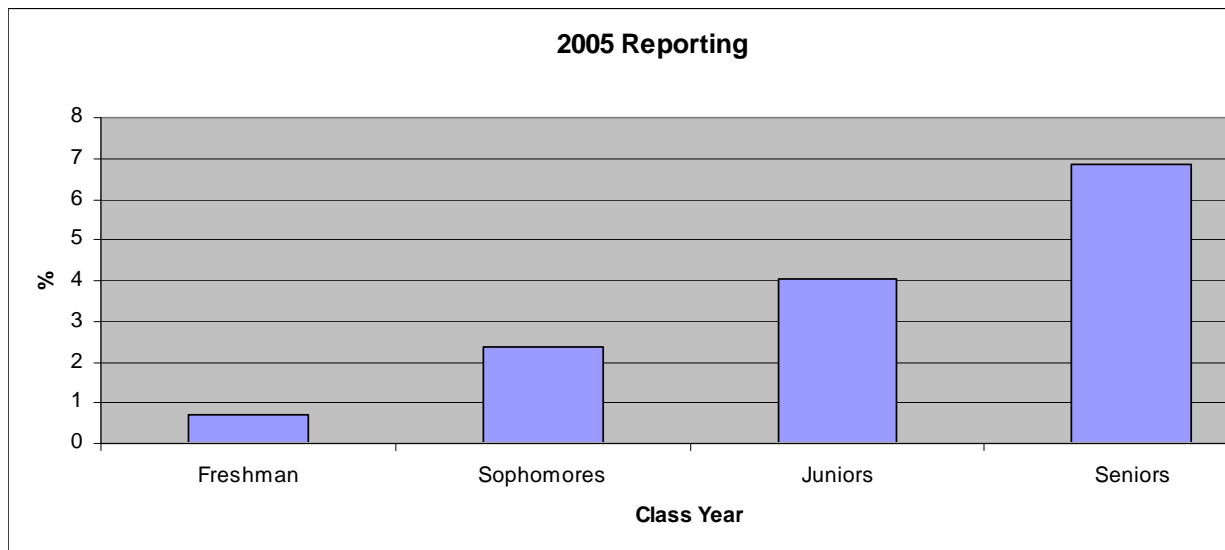


Figure 4: 2005 Carronade Results.



## Summary and Future Work

This paper presents the results of experiments to educate students on information assurance through immersion and student-led learning. Both experiments have been successful with positive results in terms of student satisfaction, incident detection, and incident reporting. The use of SISOs appears to be novel. We are unaware of any other university using unpaid students as a component of the technical governance of the institution. Our experiment with SISOs suggests that this approach may be appropriate for other institutions of higher

learning as a form of service education. It is particularly appropriate for those selecting information technologies as their major. The initial use of Carronade to address spear phishing attacks in an active learning environment is novel. The Carronade exercise has received some publicity in the popular press and a similar exercise was run by the State of New York in 2005 after they became aware of Carronade[3]. The Department of Veterans Affairs is likewise planning a similar exercise for 2007[4].

We are exploring expanding Carronade to other delivery means such as instant messenger and community of practice discussion boards. Due to requests, we are also considering a publicly releasable version of Carronade that can be installed at other institutions. Our experiences with Carronade suggest additional experimentation is warranted to explore its effect on organizational culture. Coupled together, SISOs and the Carronade exercise can significantly improve student learning of modern information assurance concepts.

### References

1. CERT Statistics. HYPERLINK "<http://www.cert.org/stats/>". Assessed on 7 January 2007.
2. Frand, Jason L., "The Information Age Mindset, Changes in Students and Implications for Higher Education", September/October 2000, Educause Review, P.15 – 24.
3. Pelgrin, William, "Cyber Security - An Ever Changing Landscape" Federal Information Systems Security Education and Awareness Conference, 20-21 March 2006. Washington, DC.
4. Email traffic dated January 3, 2007 between Curtis A. Carver and Ken MacGarrigle, Department of Veteran Affairs announcing the CARVER Facility Vulnerability Assessment Training, 6-8 February, 2007.

### Biographical Information

Curtis Carver is a career active duty Army Colonel and the Vice Dean for Resources at the United State Military Academy where he is responsible for personnel, budget, strategic planning, research, and international affairs. In addition to his administrative responsibilities, he is a Professor in the Department of Computer Science and typically teaches courses associated with information technology or web-based computing. He has lived in all sorts of interesting places including a short combat tour in both Afghanistan and Iraq where he mentored the academic leadership of their respective National Military Academies. Outside the office, he is active in the church, with the West Point Women's Soccer team, and as a mentor for the 30 cadets for whom he serves as their foster parents while they are attending West Point. Dr. Carver enjoys computer games, reading, writing, traveling, and most sports for which his enthusiasm should not be confused with any real skill.