Fostering E-Mail Security Awareness: The West Point Carronade

An e-mail security awareness proof-of-concept exercise conducted at West Point helped foster and strengthen online security practices among cadets

By **Aaron J. Ferguson**

Despite the damage the Melissa and Sasser worms and other embedded hyperlinks and e-mail–enabled viruses have caused to millions of computers and their data, the majority of users will undoubtedly continue to click on embedded hyperlinks and e-mail attachments they receive from people they do not know. As computers and networks become more ubiquitous in academia, the need to protect campus networks and the information on them becomes imperative.

Today's generation has access to a variety of "insta-technologies," such as cell phones, instant messaging, and two-way pagers, that exacerbate the demand for instant access and immediate gratification. This "I want it now!" attitude sometimes causes a person to make poor decisions regarding e-mail attachments or embedded links. Clicking on an embedded hyperlink (a hyperlink that is part of a document, such as an e-mail message) is easy and convenient, and the recipient rarely considers the potential negative consequences.

The United States Military Academy (USMA) at West Point had a problem with some cadets clicking on suspicious attachments and embedded links, significantly affecting network performance and resource availability. West Point information technology leadership needed a way to increase e-mail security awareness in hopes of maintaining a strong security posture. I designed and developed an e-mail security awareness exercise called the West Point Carronade as a proof-of-concept response to this need to make sure cadets were practicing good e-mail security. The hypothesis behind the Carronade was that even with healthy doses of security education awareness, training, and education, at least 75 percent of randomly selected cadets would click on an embedded hyperlink in what should be a suspect e-mail message. The exercise was designed to point out this security awareness deficiency.

This Good Ideas does four things:

- Characterizes the e-mail security-related problem at West Point and describes how West Point faculty and staff leadership sought to address it
- Describes the West Point Carronade e-mail security awareness proof-of-concept exercise
- Discusses challenges in getting West Point leadership buy-in for a proof-of-concept deployment
- Provides guidance for other educational institutions seeking to develop and launch effective security awareness exercises

The Carronade

The Carronade was a naval cannon used in the early 1770s. The inventors, Charles Gascoigne, Lieutenant General Robert Melville, and Patrick Miller, designed the cannon in 1759 while working at the Carron Iron Works Company on the Carron River in Stirlingshire, Scotland. The Carronade, although possessing limited range, was destructive at close quarters (less than 0.6 miles). This exercise was named the Carronade because

- while the e-mail had the potential to be destructive, the intent was to get the attention of cadets, not to cause damage to the academy network or to penalize the cadets; and
- the exercise was short range—conducted inside the USMA security perimeter—and only cadets with a usma.edu domain name could launch the embedded link.

Why West Point?

West Point is a four-year undergraduate institution where the average SAT

score is approximately 1300. Even the brightest students are vulnerable to e-mail deception, however—our cadets are among the millions who regularly click on suspicious attachments.

Like the Naval and Air Force Academies, West Point is both a Department of Defense (DoD) facility and an academic institution. Thus, when it comes to network protection, the academies always seek to balance the need to protect a DoD asset with the need to connect to the academic community at large.

West Point was chosen for this proof-of-concept security exercise for the following reasons:

- West Point is the only service academy with a Computer Emergency Response Team (CERT) that includes academic faculty and staff.
- The academy was the first undergraduate institution to be certified (since spring 2000) by the National Security Agency (NSA) as a Center of Academic Excellence in Information Assurance Education (CAEIAE). West Point is currently the only service academy with this certification. CAEIAE certification establishes West Point as a proactive institution of higher learning in the area of information assurance.
- At the beginning of each semester, the Corp of Cadets at West Point receives security awareness training. The freshmen spend four hours (four lessons) learning about information assurance and network security. The network security lesson includes discussions of viruses, worms, and other malicious code, or malware.

West Point leadership felt that providing awareness of potential e-mail security problems was the best path to prevention. The Carronade was purely a "proof-of-concept" exercise to achieve this goal.

Carronade Exercise Design Considerations

Four primary design and implementation considerations influenced deployment of the Carronade, even as a proof-of-concept:

- Establishing a relatively high degree of randomness in selecting cadets
- Socially engineering the cadets in a way that could not be deemed entrapment
- Deploying the Carronade at a strategic time of the semester
- Getting USMA stakeholder and leadership buy-in and approval for deployment

Randomness

Establishing a high degree of randomness involved selecting cadets who represented a cross-section of the Corps of Cadets while avoiding the "high-beam effect."[1] Cadets with a priori knowledge of the bogus e-mail would either deliberately click on the embedded link or totally ignore the message. Either way, the data would be skewed.

Social Engineering

The strategy employed was to convince the cadets that the e-mail message was legitimate and get the cadets to perform a certain action in response to the bogus e-mail. There is a culture at West Point that any e-mail with a "COL" (abbreviation for Colonel) salutation has an action to be executed. To a cadet, the action/request is to be executed regardless of its nature or rationale. The e-mail sought to exploit this culture. The e-mail message, shown in Figure 1, informed cadets of a problem with their current grade report and instructed them to click on the embedded hyperlink to make sure their grade report information was correct. The e-mail was sent from a fictitious Colonel Robert Melville (co-inventor of the Carronade cannon) in the United States Corps of Cadets (USCC) office on the 7th floor of Washington Hall.

The Carronade exercise took place in spring 2004. At that time in the academic year, most cadets, even freshmen (in the second semester of their college experience), should have realized that this e-mail was bogus for two reasons:

1. There is no COL Robert Melville in the USMA global address book.
2. There is no seventh floor of Washington Hall, a place they visit somewhat frequently.

Timing

The timing of this deployment was a critical factor in the design. The Carronade had to reach cadets at a time when they would be most likely to read

Figure 1

Bogus E-Mail Message

From: sr1770@usma.edu [mailto:sr1770@usma.edu]
Sent: Tuesday, June 22, 2004 4:57 PM
To: cadet@usma.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
COL, USCC
sr1770@usma.edu
Washington Hall, 7th Floor, Room 7206

it and act. Three weeks before the end of the semester seemed reasonable, as e-mails regarding final exams and end-of-semester grades always seem to get cadets' attention as the semester draws to a close.

Stakeholder Buy-In: West Point Community of Practice

Like most colleges and universities diligent in the area of information security, West Point seeks to accomplish two primary goals:

1. Balance the information technology needs of cadets, staff, and faculty with the need to maintain a secure and robust network.
2. Provide a forum that would foster development of educated leaders who understand information security.

These two goals were accomplished by having a USMA-level "community of practice" in place called the USMA Computer Emergency Response Team (USMA CERT).

The Carronade was explained at a weekly USMA CERT meeting held six weeks before the end of the semester. The initial exercise was intended to be somewhat punitive in nature—every cadet who clicked on the embedded link received a form e-mail scolding similar to a "gotcha."

Initially, USMA CERT agreed that the Carronade was a good way to test the e-mail security posture of the institution and capture, at a glance, the effectiveness of current security awareness, education, and training. However, the USMA chief information officer objected to implementing the exercise in its suggested form. He felt that implementing the Carronade in a "gotcha" way would undermine the trust relationship between the cadets and his office that he and his staff had established. He suggested that to get the cadets to develop a positive attitude about security, we should implement initiatives like this in a nonadversarial way that promoted awareness without punishment. He suggested letting the cadets assigned to oversee computer security in the barracks—the regimental Information Security Officers (ISOs)—take ownership of and implement the exercise. Since the ISOs were cadets, the perception of USMA leadership coming down on cadets would be, to some degree, dissipated.

The CIO pointed out several benefits of an ISO-owned and operated exercise. First, giving the ISOs ownership of an important component of the academy's security posture had the potential to institutionalize the exercise over time. Second, allowing the ISOs to enhance or modify the implementation would take the "care and feeding" away from the academy network administrators and give the ISOs immediate stakeholder status. Last, the exercise would give the ISOs visibility, allowing them to focus security awareness, training, and education efforts across the Corp of Cadets (more than 4,000 cadets). This, in turn, would enable the regimental ISOs to provide incentives and recognition to cadets practicing good e-mail security.

Carronade Exercise Design

The Corps of Cadets at West Point follows the traditional structure of the United States military—there are four regiments (1 through 4), with each regiment comprised of eight companies (A through H). Each company has approximately 130 cadets. The goal of the Carronade was to obtain results down to the company level.

Within each of the eight companies in each of the four regiments, four cadets were randomly selected from each class (four freshman, four sophomores, four juniors, and four seniors) for a total of 512 cadets out of approximately 4,200 cadets making up the Corps of Cadets (about 12 percent).

Using publicly available software found on the Internet, the Carronade consisted of a bogus e-mail message with an embedded hyperlink that linked to a "bad" URL. The message was sent to the randomly selected group of 512 cadets. When cadets clicked on the embedded hyperlink URL, they received a modified "HTTP 404 - Page Not Found" Web page. The HTML traffic viewed by the cadet clicking on the URL activated a "beacon" that gathered the browser attribute data and stored it in a central, secure database (available only to the database administrator within the usma.edu domain). This browser attribute data included computer name, IP address, operating system specifics, Web browser specifics, time the Web page was viewed, whether the cadet opened the e-mail, and, of those who opened the e-mail, who clicked on the embedded hyperlink.

Results

Because this exercise was a proof-of-concept with a small sample size, extrapolating the results to the general population is ambitious at best. Nonetheless, 80 percent (more than 400) of the cadets in the sample clicked on the embedded link. Even with four hours of computer security instruction, 90 percent of the freshmen clicked on the embedded link.

Feedback from the cadets who clicked on the embedded link included comments such as, "The e-mail looked suspicious but it was from an Army colonel, so I figured it must be legitimate" and "Any e-mail that contains the word 'grade' in it gets my immediate attention and action!"

The 80 percent click rate might seem surprising. However, this proof-of-concept launched at a time of the semester when the cadets were very sensitive to issues regarding grades. In addition, unbeknownst to the Carronade deployment team, three days before the Carronade started, the commandant[2] notified seniors via a legitimate e-mail message to come into his office, look over their academic grade reports, verify that the information was correct, and sign the reports. Then the Carronade e-mail came. Immediately, the cadets assumed that the two e-mails were related and clicked on the embedded link. As a result, some of the data might have been skewed. Nevertheless, the commandant's e-mail went only to seniors. With the exception of the freshman class response rate (90 percent), all classes responded at approximately 80 percent, suggesting that the commandant's e-mail had little, if any, effect on response to the Carronade.

Moreover, the cadets' comments about always responding to anything related to "grades" suggests an obvious vulnerability that extends to any college or university.

Implementations in Other Academic Environments

Many civilian colleges and universities consider practicing good e-mail security a personal choice rather than an institutional responsibility. However, by developing and implementing exercises like this, colleges and universities can get a good reading of the e-mail security awareness of their students and the security posture of their networks.

Those considering launching their own Carronade should consider the following issues:

- Stakeholder identification and buy-in
- Network security posture and exercise maintenance
- Timing
- Awareness versus punishment
- Follow-up

Stakeholder Identification and Buy-in

Before you can have stakeholder buy-in, you have to identify the relevant stakeholders. They should include the person(s) responsible for network operations, relevant system administrators, the dean of students, and others responsible for network resources.

Network Security Posture and Exercise Maintenance

A critical element in planning is to make sure that the exercise does not either introduce vulnerabilities into the network or allow entities external to the organization to use the exercise as an entry point into the network.

Another issue to consider is exercise maintenance. The exercise should not add responsibilities to the network system administrators unless it falls within the scope of their normal duties.

Timing

Planning is the key to success. Making sure that the exercise is deployed during a time that maximizes coverage but minimizes collisions with other activities (such as exams or class projects) will prove critical.

Awareness Versus Punishment

It is highly recommended that institutions deploy the exercise for awareness only. The goal is to make students aware of the dangers of clicking on embedded links and attachments that look suspicious or come from people they do not know. Making the exercise punitive increases the risk that a student may try to retaliate.

Follow-Up

It is extremely important to reinforce the e-mail security awareness message after the exercise has been deployed. Giving the students immediate feedback will make them more cautious in the future and help enhance the network security posture in general.

Future Work

The West Point Carronade was deemed a success as a proof-of-concept exercise. The CIO was so pleased that he authorized launching the Carronade to the entire 4,400 Corps of Cadets. The West Point Carronade II will consist of four variants, each deployed from three to four weeks apart. In addition to the original West Point Carronade, they include the following modifications.

Social Security Number

Cadets receive an e-mail informing them of a problem with their Social Security number and telling them to click on an embedded link to verify their number. Due to privacy concerns, even if they enter their Social Security number, no data is actually collected or transmitted.

Attachment

This version is essentially the same as West Point Carronade I. Instead of requesting the cadets to click on an embedded link, however, they the message asks them to click on an attachment that acts as a beacon that reports (back to a secure database) their student identification numbers and various attributes of their computers.

Download

Cadets receive an e-mail asking them if they want free music. They are asked to "Select this link: Songs You Know Offer" and follow the instructions. When they click on the embedded hyperlink, an application is installed on their computer that obtains complete access to their data. This innocuous application collects the number of files in their "My Computer" folder, not the actual files, and sends this file list back to an access control list-protected database. The Carronade managers view the database looking for file lists to identify transgressors.

Conclusion

While imperfect at best, the West Point Carronade exercise proved that the traditional classroom instruction model is necessary but not sufficient when it comes to learning. Students have to touch, feel, and experience the content in order to learn. The goal of any security awareness exercise should be to make security an attitude within the organization, campus, or university. Periodic launching of these types of awareness exercises will help minimize network downtime and maximize network performance as students become more judicious about handling e-mails. *e*

Endnotes

1. The "high-beam effect" refers to the situation where drivers on one side of the highway spot a law enforcement officer at the side of the road looking to catch speeders. These drivers flash their high-beam headlights to warn oncoming drivers that a law enforcement officer is targeting speeders, encouraging them to slow down.
2. The commandant is the civilian school equivalent of a dean of students.

Aaron J. Ferguson (Aaron.Ferguson@usma.edu) is National Security Agency Visiting Professor in the Department of Electrical Engineering & Computer Science at the United States Military Academy at West Point in West Point, New York.