Using Phishing for User Email Security Awareness

Ronald C. Dodge and Aaron J. Ferguson

Department of Electrical Engineering and Computer Science
United States Military Academy, West Point, NY, USA
{ronald.dodge, aaron.ferguson}@usma.edu

Abstract. User security education and training is one of the most important aspects of an organizations security posture. Using security exercises to reinforce this aspect is frequently done by education and industry alike; however these exercises usually enlist willing participants. We have taken the concept of using an exercise and modified it somewhat to evaluate a users propensity to respond to email phishing attacks.

1 Introduction

The quest for information systems security has a significant, almost self cancelling facet—the user. User information assurance (IA) awareness is a random variable that is very difficult to characterize due to user's individual nature. Users create an open back door into our corporate networks through their internet and third party application use. This vulnerability is increased from mobile systems that join home and other commercial networks. While the application of host and network based security applications can provide some mitigation of this threat, one well timed or lucky random shot can provide a malicious user unauthorized access to the intranet. Security training and awareness programs have done a good job of mitigating this risk – but just how good? What measures exist to verify that users understand and consistently apply the best practices they are exposed to during periodic training?

The use of exercises to reinforce concepts in an educational setting has been written about frequently [1]. Typically, these exercises involve participation by knowing participants and involve a network attack/defense scenario. The United States Military Academy (USMA) took the concept of a hands-on exercise and developed an email phishing exercise with the intent of evaluating the efficacy of our user IA training. The exercise first ran as a prototype in the spring of 2004 and has since been run two additional times. The most recent exercise (at the time of this writing) ended in November 2005.

The phishing exercise at USMA was developed under the name of "Carronade". As described in [3], a Carronade is a Navy cannon used in the early 1770 and seemed an appropriate name.

> "The Carronade although possessing limited range, was destructive at close quarters (less than 0.6 miles). It is important to note that in offensive operations

Please use the following format when citing this chapter:
Author(s) [insert Last name, First-name initial(s)], 2006, in IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, eds. Fischer-Hubner, S., Rannenberg, K., Yngstrom, L., Lindskog, S., (Boston: Springer), pp. [insert page numbers].

during the 1700s, the objective was not to sink an enemy vessel but rather to avoid damaging the hull so as to capture it as intact as possible, so it would be retained as a 'prize.'
In keeping with this military theme, this exercise was named the Carronade because: (a) while the emails 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 (b) the exercise was short range--conducted inside the USMA security perimeter--only cadets with a usma.edu domain name could launch the embedded link."

In this paper, we will present a background discussion on the exercise, describing its origin and planning considerations. We will further describe the evolution of the exercise from a prototype to a multi-email exercise designed to evaluate different forms of phishing and the efficacy of training. We will provide results from each exercise and offer some assessment of our awareness and training program. We then conclude with a look toward future exercises.

2 Background and Previous Work

We begin explaining the exercise by first addressing the specific considerations common to each phishing exercise and then later describe the evolution of implementation.

We first must recognize that USMA is a very "connected" campus. Each student has a computer with a specific suite of software. While they are allowed to install third party applications that are not part of the official suite, they must purchase them on their own and the computer staff at USMA will not support them. Given these limitations virtually all students have the same basic configuration. In addition, email is a very heavily relied upon management and information dissemination tool.

Our first consideration was devising an email that a student would definitely be interested in opening and reading. One of our design decisions was to avoid common phishing email content such as financial or services emails. We decided for our final email prototype that the student would be instructed to visit a website (hyperlink) to validate course grades. The second specific consideration, timing, fit nicely with the email content. For the prototype we constructed the email near the end of the semester when students would be most concerned about grade correctness. The third specific consideration focused on the target. Prior to the exercise, a target population needs to be identified. For our prototype a very small sample population across all classes was selected. Lastly, our fifth consideration, post event notification and follow-up mechanism, needed to be defined. In the prototype, immediate notification via an automated email was selected.

The prototype (Carronade I) was limited in nature. The emails were sent 512 students at USMA (roughly 12% of the student body). The student body at USMA (called the corps of cadets) is broken down into four regiments, each with eight companies. Each company has approximately 130 cadets. Four cadets were randomly selected from each class (i.e., four freshman, four sophomores, four juniors, and four

seniors) for a total of 512 cadets out of a total of approximately 4200 cadets. A detailed analysis of the exercise background can be found in [2].

2.1 Carronade Evolution

We conducted an assessment of the prototype and determined that the exercise could provide useful insights into the efficacy of our awareness and training program. Our focus for Carronade II was to develop a repeatable exercise that over time would serve as a yard stick to measure our programs. To that end, the exercise was conducted in September, 2004. The timing of the exercise was set to ensure the new freshman class had an opportunity to become familiar with their computer and the email system at USMA. The exercise was conducted prior to any regularly scheduled IA training. A detailed discussion of the technical implementation of Carronade II can be found in [3].

To validate that the email content was consistent with current training foci, we decided to seek input using a survey of information technology instructors. The survey asked the instructors to identify the top information assurance-related negative behaviors of their students. Using the survey, we developed the following requirements for Carronade II, incorporating four different styles of emails:

- The system must be able to deliver an email to all students.
- The first email type asks the student to click on an embedded link in an HTML encoded questionable email to fix a problem with a fictitious grade report; clicking on the link records information readily available from the browser.
- The second email type is identical to the first email except that the email asks the student to open the corresponding .html attachment.
- The third email type asks the student to click on a link that takes them to a web form that asks for sensitive information (i.e., their social security number).
- The fourth email type asks the students to click on a link, download an application and run the application. (This was implemented, however due to technical problems, the results were not valid).
- Each of the emails should be questionable enough to raise the suspicions of the end user.
- None of the emails, if opened outside of the USMA domain, would collect, track, or transmit any user data.

As noted, a significant difference in Carronade II was the number of cadets targeted with the emails. This time the scope increased to the entire student body (minus those involved in the planning and execution). Of the total number of 4155 in the student body, 4118 received the emails. The email breakdown by type was: 1010 embedded link emails, 1014 attachment emails, 999 sensitive information emails, and 1095 download emails were sent out. (As stated, in the final results these emails are discounted due to technical problems.)

Carronade III was implemented functionally with very few changes from Carronade II. A similar sample population was used (everyone minus the exercise coordinators), however the timing was changed to more closely follow the required IA training that each student receives. The date was selected to assess whether the

recently received training produced lower "violations". The exercise was implemented in November 2005.

We chose a very similar email package – embedded link, attachment, sensitive information, and download emails. Unfortunately, different but similar problems plagued the download email and the results from this set are not included in the final analysis. The total emails sent 4136; were broken down as follows: 1006 embedded link, 1013 attachment emails, 1058 sensitive information emails, and 1059 download emails. (As stated, in the final results these emails are discounted due to technical problems.)

3 Results

We elected to examine the results of the exercises in three facets. First, by overall percentage, by year, of the number of students that succumbed to the phishing email. Second, we look at the distribution of failures by class for each exercise. Then finally, we look at the performance of a specific class over the two years.

3.1 Failure Percentage by Exercise

As seen in Figure 1, the failure rate in the prototype is very high. This is more than likely explained by the very small sample size (512). The results for 2004 and 2005 suggest minimal impact due to the recently conducted training. This however will require further data points to accurately draw this conclusion. It should be noted that in post exercise discussion with the students, the majority that did "fail" said they found the emails odd, however responded anyways.

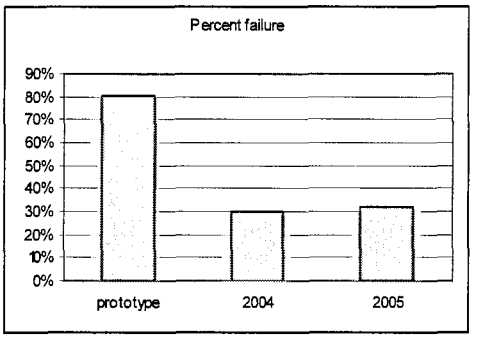

Fig. 1. Percentage of Failure by Exercise.

3.2 Distribution Summary

The breakout of failures by exercise, type of email, and class is interesting and should shed interesting insight as additional data is gathered through future exercises. Figure 2 shows to major groups (left to right), the first full Carronade exercise and the second full exercise. With in each group the data is further broken down by class (freshman, sophomore, junior, and senior), then again, by email type.

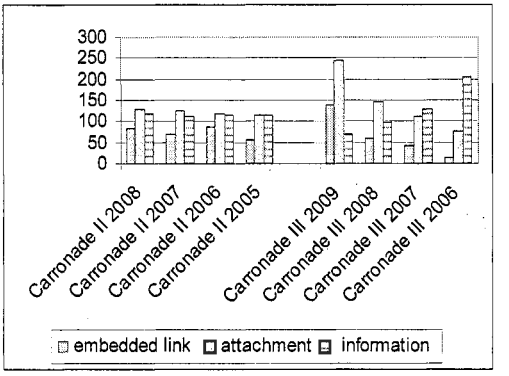

Fig. 2. Failure Breakout.

The primary difference between the two major exercises was the timing in relation to training. In Carronade II, training had not yet been conducted when the exercise was conducted. In Carronade III, training had been conducted within the previous 2 weeks. The first exercise produced results that are not very interesting. The second exercise produced results that are quite interesting. The "younger" the class, the more likely they were to fall victim to the email using an embedded link or an attachment. The opposite however is true for the email requesting sensitive personal information.

3.3 Distribution by Class

The final observation on the student performance can be gained by examining the students who participated in each exercise, as shown in Figure 3. The results show a positive increase in the user awareness across all classes on clicking embedded links and opening attachments. Our students continue to disclose information that should not be disclosed to an unauthorized user. For the United States Military, this is an important distinction given the future requirement for operational security once the students graduate and enter the Army. This information will help us not only modify the IA awareness program, but also provide input to the other areas where operational security is important.

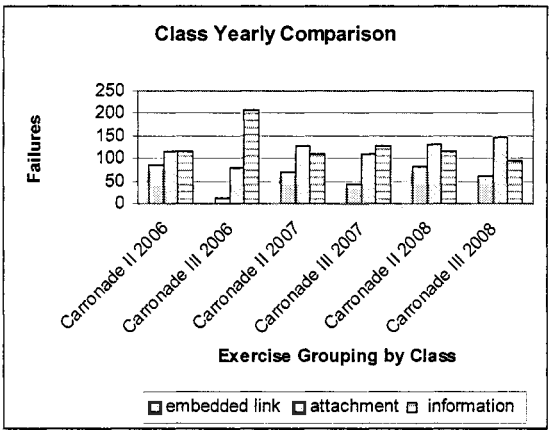

Fig. 3. Comparison of Class Performance over two Exercises.

4 Conclusions and Future Work

The phishing exercises served to provide an insight into the awareness levels of our students and help us better focus our IA and awareness training. The results are still very immature; however they provide an opportunity to look at the effectiveness of our programs. One might look at the assessment of the programs using an exercise as "poisoning the well", given the very fact that the exercises themselves may raise awareness, making it difficult to separate out any increased awareness due solely to the annual training. While this is true, when looking at the exercise from a bottom line – if our user's awareness is increased, providing enhanced network security whatever the cause is a worthwhile cause.

We intend to continue the phishing email exercises, increasing the frequency to once every semester. One exercise will follow closely existing training; the second will be used to assess longer term retention.

References

1 Dodge, R., Hoffman, L., Rosenberg, T., Ragsdale, D., "Exploring a National Cyber Security Exercise for Universities," IEEE Security and Privacy, September/October 2005, pp 52-58.
2 Ferguson, A., "Duty, Honor, Country and Email Attachments: The West Point Carronade" Educause Quarterly, Number 1 2005, pp 54-57.
3 Jackson, J., Ferguson, A., Cobb, M., "Building a University-wide Automated IAAwareness Exercise: The West Point Carronade", Frontiers in Education Conference, 19-22 October 2005, pp T2E7-10.