ASEE 2014 Zone I Conference, April 3-5, 2014, University of Bridgeport, Bridgeport, CT, USA.

Digital Freedom Fighting

An Interdisciplinary Science and Engineering Education Module

Nicholas S. Rosasco
Department of Computer and Information Sciences
Towson University
Towson, MD

Dane Brown
Department of Electrical and Computer Engineering
United States Naval Academy
Annapolis, MD

Abstract—**The STEM program at the U. S. Naval Academy is intended to enlighten and educate students, by presenting both applications and abstract concepts in an interactive, hands-on manner. Modules that teach a wide range of topics, some multidisciplinary, are presented in short, informative sessions. The module presented in this paper involved discussions of networking and communications technology, as well as the societal impacts caused by the evolution of these technologies, the variety of tools and techniques currently available and the tradeoffs they present. Specifically, IP based networking, symmetric and asymmetric encryption, onion routing, and secure deletion are all presented to the students. To assess comprehension and prior knowledge in these areas, a 3-question tool was used; the before and after scores from this mechanism illustrate improved understanding in these areas.**

Keywords—STEM; Networking; Encryption; Communications Systems in Society; cybersecurity.

I. Introduction

The ongoing evolution of communications technology has changed politics and society deeply, providing an array of tactical and strategic options that have rapidly accelerated the pace of change in opinion and behavior. That pace of change, and the discussion of risks of dependence on digital ways and means, provides a potent source of material for education and illustration. This dependence, as articulated widely by the cybersecurity scholarly and practitioner communities [4], is made more compelling as an outreach area because the tools, assets, and applications are familiar to and used by people in everyday life.

By embracing this reality and using it as a teaching tool, the science/technology/engineering/math (STEM) disciplines can be presented as impactful on the world as a whole, and as exciting and cutting edge. By offering these current and live challenges, it is hoped that the ongoing issues of recruitment and retaining specialists in the associated career fields can be mitigated to some degree. This module was constructed on the premise that education in this area can be a vehicle for development of future interest and curiosity, as has been shown for similar efforts [10].

II. Educational Justification

STEM outreach at the United States Naval Academy (USNA) entails a different approach to recruiting and retaining technologists. We engage elementary, middle, and high school students and teachers in a diverse range of science and engineering activities [14] using Navy relevant curriculum, our midshipmen as near-peer mentors and our Academy resources as a backdrop. To help achieve these objectives, the Academy's STEM Office hosts a series of summer events for students that expose them to a variety of hands-on modules which demonstrate various activities germane to STEM careers.

One of the key components of the USNA STEM effort is involvement of midshipmen, the undergraduate students of the U. S. Naval Academy. Involvement with the program is expected to prepare midshipmen "for intellectual challenges by creating opportunities for midshipmen to learn current STEM theory and application, as well as lead in the classroom" and "hone their ability to respond to spontaneous situations [13][14]." Additionally, there is a goal to "prepare midshipmen to interface with multiple technologies, expose midshipmen to the reality of the interdependence of different disciplines in STEM military technologies, and enhance the technical proficiency and communication skills of graduates [13][14]." Faculty and staff are encouraged to both train and educate these students so that they can go beyond simple assistance and actively run and teach the modules themselves.

III. Context

The current USNA Summer STEM program is "designed to encourage rising 8th – 11th graders to pursue a course of study in engineering and technology throughout high school and college. Students must demonstrate superior academic performance to include GPA, class standing, and/or strong PSAT, SAT or ACT results [15]." Additionally, since geographic diversity is a goal for the program as an extension of the national mission of the Naval Academy, a typical year for the STEM program will include participants drawn from all fifty U. S. states**.**

The module under discussion was used for sessions for those either entering the 8th/9th grade (June 3-8, 2013) and entering 10th grade (June 10-15, 2013). This module was also employed as an example of a typical first year classroom experience for the Academy's "Summer Seminar" program [12], which the Admissions Office supports to expose potential applicants, rising 11th grade students, with an overall experience of military and student life at a service academy, including classroom instruction.

IV. Logistics

To deliver the module effectively, a variety of components were required and a variety of considerations had to be taken into account. Both equipment and software require preparation, some of which must be done for each execution of the module.

A. *Equipment and Facilities*

A classroom was equipped with power-cabled furniture, laptops, a network switch, and a small router/access-point to create a stand-alone network. The classroom came with an Internet connected instructor-station PC linked to a projector with screen. The room was equipped with per-seat Ethernet wiring that allowed for the construction of a local, in-room-only network. To simplify configuration, a local router/access-point was connected to the same switch powering this network, and used to provide IP allocation via the dynamic host configuration protocol (DHCP) to both the laptops used by attendees and the laptop serving as a local webserver. Handouts illustrating the command sequences to be input by the attendees were also used as supplements to the presentation.

B. *Software*

A set of DVDs from the TAILS i386 version 0.18 ISO was produced for student-use laptops, as well as a version of Ubuntu built as a live boot DVD, specifically Ubuntu Live 11.20 [7]. A very simple, lightweight web server implementation was required for the distributed denial of service attack. It also proved a useful mechanism for distributing files to students. The source for this application was taken from Erickson's *Hacking* [1].

C. *Data files*

To create a consistent example for the file deletion example, a set of small files that were created as mountable file systems were downloaded by participants. These were built in advance, and demonstrate the difference between existing files, standard deletion, and secure deletion. Additionally, a very shallow mirror of the homepage of the U. S. Department of Justice website was created and placed alongside the example files for use during the denial of service exercise.

D. *General Preparation*

To provide general familiarity for the participating midshipmen, a rehearsal was held several days before the first participants would arrive. This also afforded the faculty and staff the opportunity to ensure overall smooth operation of the module and identify last minute concerns. This rehearsal also provided an opportunity to prepare the room by pre-staging the laptops with network and power connections.

V. Execution of the Module

Once the preparatory steps were complete, the room and participating faculty, staff, and midshipmen were ready to conduct the module itself for the Camp and Summer Seminar visitors. Midshipmen acting as escorts for groups of students brought the participants in accordance with the Summer Seminar or STEM Camp schedule.

A. *Module Startup*

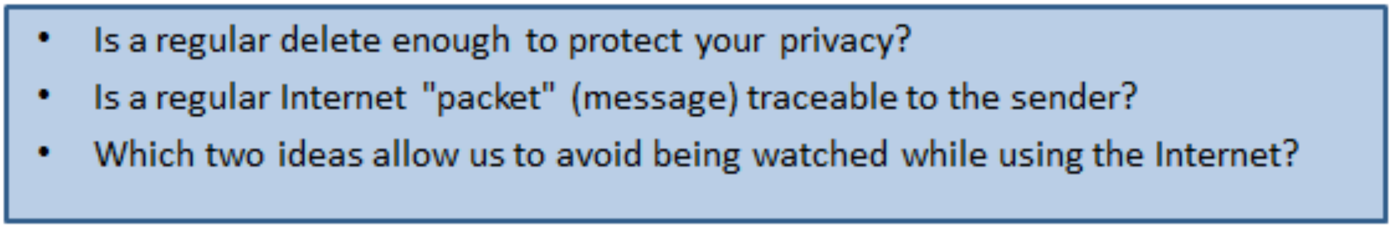
Prior to the arrival of each group of participants, the instructor workstation was checked to ensure the slides were ready. Following that, several websites were accessed to generate results to demonstrate the anonymity provided by TOR and provide input for the TOR mapping tool.

B. *Opening and Initial Assessment*

With the arrival of each set of STEM participants, an initial assessment comprised of three background questions was conducted to survey their overall awareness of the topics to be presented in the module (see Figure 1). With the Summer Seminar attendees, this step was omitted, in part to avoid confusion with other assessment exercises. This, which accompanied the initial greetings and welcome, was immediately followed by the opening part of the presentation that formed one of the components of the module. The initial phase of the presentation was intended to convey a broader social and interdisciplinary context to the module, and introduce the transformative effects of technological change, particularly that relating to speed of communication.

C. *Initial Presentation*

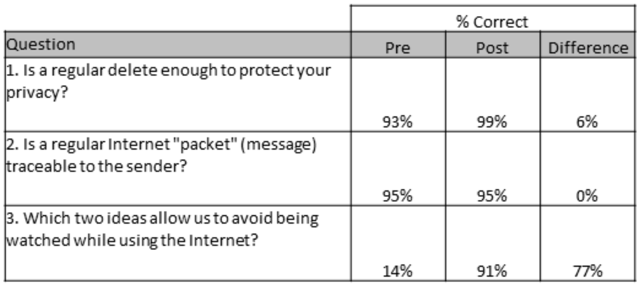
The opening discussion asked students to consider what is necessary for a successful popular revolution. Means of communication - both anonymous and attributable but secure - were offered as prerequisites to advancing a game-changing



- Is a regular delete enough to protect your privacy?
- Is a regular Internet "packet" (message) traceable to the sender?
- Which two ideas allow us to avoid being watched while using the Internet?

Fig. 1. Assessment Questions

TABLE 1. ASSESSMENT QUESTION COMPOSITE SCORES



	% Correct		
Question	Pre	Post	Difference
1. Is a regular delete enough to protect your privacy?	93%	99%	6%
2. Is a regular Internet "packet" (message) traceable to the sender?	95%	95%	0%
3. Which two ideas allow us to avoid being watched while using the Internet?	14%	91%	77%

agenda. As demonstration of this, several examples were offered. These include the "Committees of Correspondence" employed by the colonists during the American Revolution, as an alternative to the British-controlled postal and other systems [3], the fax machines employed to evade Eastern Bloc surveillance during the Solidarity period of Polish history [1]. The limitations and control of the available technologies (ships, horses, word of mouth, telephone, broadcasts) available in these eras was discussed usually with class participation. The inevitable delay in actually communicating, especially given the fact that not all of the participants in the former got the message concerning the end of hostilities for some time, is also briefly considered during the discussion.

A more recent example was then presented, the Egyptian Revolution of 2011 [5]. The difference in time scales - 10 years for the War of Independence, approximately two to three years for Solidarity, down to 18 days for the Egyptian overthrow, is in large part attributable to faster means of communication and mobilization. The specifics of the technologies used in the Egyptian period, including YouTube, Twitter, and the speak-to-tweet workaround created by sympathetic technology firms in a matter of hours when standard Twitter services were shut down by the incumbent government, were then addressed [5].

A brief summary discussion followed about the key aspects of protecting oneself online, including that these are useful for the general individual, not merely the individual. This explanation transitions into a discussion of how the Internet, while posing obstacles to tapping or tracing, is not in and of itself built with protection in mind. This segued into the concept of encryption as a mechanism for protecting content.

D. *Encryption*

With the encryption exercises, the module transitioned to the hands-on portion. A succinct presentation of several cryptologic strategies, including the Caesar cipher and conventional digital symmetric implementation, was used to highlight the cumbersome need for an in person meeting prior to use. Then, the command line interface ("gpg –gen-key") for the SSL software suite was used to generate a public/private key pair [9], and the key-use-enabled editor bundled in the TAILS distribution was used by each student individually to encrypt and decrypt a message. The non-correspondence of message length between the clear and cipher text was identified, as well as the enhanced security of unique keys for every correspondent.

E. *Onion Routing*

The students were presented with an analogy likening the TCP/IP packet to a postcard, where everything is visible while in transit. The notion that encryption as described earlier normally only affords protection for the payload of the message, effectively obscuring only the content of the message, and the risks of leaving the addressing information - the "to" and "from" of the postcard - exposed were briefly discussed. An explanation of the behavior of The Onion Router (TOR) protocols [6], including a comparison to the strategy behind the game of "hot potato," was delivered. The TAILS-booted, Internet-connected workstation was used to show the map of TOR participant systems and the effect on various web services. Yahoo's location-aware start page proved particularly effective; the weather and local news functions quickly provided an illustration that the Annapolis based PC was perceived as being located variously in the American Midwest or one of several European states, including Germany, the Netherlands, and the Czech Republic.

F. *Secure Deletion*

The next interactive task demonstrated one aspect of the unintended permanence of digital information. A hypothetical situation involving the authorities breaking down the door was presented to the students as a potential scenario. The natural reaction, to delete the traces of activities, was suggested, but was then followed by questions asking how it would be possible to recover information once deleted. The expected answer, which it is possible to use the various undelete or "recycle bin" capabilities built into most modern operating systems, usually arrived fairly quickly in the resulting dialogue. The implementation of the standard delete feature, namely that it simply marks space available for reuse, was offered as an example of why care in data disposal is necessary; the behavior of the undelete capability, as an extension of this basic behavior, was also mentioned.

The discussion continued with a question, asking the participants if they have noticed that everything discussed up to this point has been inherently defensive, focused on securing their identity and data. The question posed bridges to the next exercise; if there is a defensive mode to things, what is the flip side of this? Further discussion was prompted by asking if anyone present has heard of the group "Anonymous." A brief introduction to the repercussions from the dispute over the shutdown of the U.S. Department of Justice, an event for which Anonymous [11] has taken responsibility, then followed. The definition of the term "distributed denial of service" was then offered as a rhetorical question, immediately followed by a question of how much technical expertise was needed to accomplish this.

With the terminology addressed, the discussion then moved into the area of execution simplicity – that it is easy to exploit the nature of the Internet's architecture and large number of hosts to generate a very large volume of traffic. Every participant in the room was then asked to prepare to do

Fig. 2. Student Participants, U. S. Navy Reservists, and Midshipmen executing the module

page reloads of the mirrored copy of the Department of Justice website, hosted in the back of the room, to illustrate this ease. For a typical session as shown in Figure 2, with 20 machines active on the closed network, the server software – chosen in part because of its brittleness – was overwhelmed within a minute or two. The students saw the lack of response after the application shuts down, and the similarity of this to a full Internet attack and response was briefly noted. The idea of unwilling and unwitting attacking hosts, commonly called zombies, was also mentioned at this point if time permitted.

G. Leaving No Trace/Amnesia

One final technical component completed the overall presentation for this module. While it could more logically accompany the secure deletion component, demonstration of the TAILS distribution's [7] amnesia capabilities was done as part of the conclusion of the exercise. Since the demonstration included the rebooting of the computers used for all other exercises, placement of this step at the end was more convenient. This capability also allows the turnaround for the next session to be reduced to simply powering off the laptops and rebooting them from the DVD copy of TAILS, easily accommodating the approximately fifteen minute breaks between each of the two morning and two afternoon sessions called for in the camp schedule.

H. Second Assessment

To conclude the exercise, the participants were again presented with the same assessment questions. These responses were collected and scored the same way the initial assessments were evaluated. The results from both sets of scoring are found in Table 1, and showed a strong starting knowledge of basic computer safeguards but showed substantial improvement in the overall comprehension of the methodology required to assure security.

VI. Conclusions

This module was created to educate participants about the importance of STEM topics to both society and the individual. It was executed to further the goals of the United States Naval Academy's STEM programs, including increasing STEM exposure for the pre-collegiate participants, and improving the technical and presentation skills of the involved midshipmen. Based on the Table 1 results, which present the before and after scores from the assessment tool, it is evident that increased awareness of technical realities resulted for the participants. The anecdotal reactions of the midshipmen, as well as the general observations of the participating faculty, also reflect the overall success of the goals.

By presenting the advantages, disadvantages, and repercussions of the evolution of communications systems, alongside the technologies that provide various attributes and capabilities, a compelling picture of the impacts of STEM upon history as a whole is offered by this module. In presenting this, a wider context for the power of mathematics and the sciences and engineering discipline is offered, hopefully inspiring others to utilize a similar holistic approach to the inspire interest.

ACKNOWLEDGMENTS

The authors would like to thank Professor Richard T. O'Brien, Jr. of the United States Naval Academy's Weapons and Systems Engineering Department for his help in the classroom and the USNA STEM program for funding and managing the camps. The support of the STEM office faculty and staff, particularly Professor Angela Moran and Raphaela Cassandra, was integral to successful delivery of the module. The Engineering and Weapons Division's Computer Support Branch staff - Sandra Erb, John Wilcox and Jeremy Bryson - were very helpful in identifying what assets were available and for supporting a broad range of administrative needs. Lastly, our thanks to the US Naval Reserve participants, and the midshipmen who supported all aspects of the camp, whose enthusiasm and energy helped make the experience positive for all involved.

REFERENCES

[1] C. Bernstein, "The Holy Alliance," Time, 24 June 2001, [Online]. Available: http://content.time.com/time/magazine/article/0,9171,159069,00.html

[2] J. Erickson, *Hacking: The Art of Exploitation*, 2nd ed. San Francisco, CA: No Starch Press, 2008.

[3] A. B. Hart, Formation of the Union. 1892, p. 49. [Online]. Available: http://books.google.com/books/about/Formation_of_the_Union_1750_1829.html?id=ophFAAAAIAAJ

[4] A. T. Phillips, "The Asymmetric Nature of Cyber Warfare," *Procedings* Magazine US Naval Institute, vol. 139, no. 10, p. 1316, 2012.

[5] National Public Radio (NPR), "Wael Ghonim: Creating A 'Revolution 2.0' In Egypt," 09-Feb-2012. [Online]. Available: http://www.npr.org/2012/02/09/146636605/wael-ghonim-creating-a-revolution-2-0-in-egypt

[6] TOR Project Team, "The Onion Router." [Online]. Available: https://www.torproject.org/.

[7] TAILS Project Team, "The Amnesiac Incognito Live System." [Online]. Available: https://tails.boum.org/.

[8] GPG Project Team, "Gnu Privacy Guard Tools." [Online]. Available: http://www.gnupg.org/.

[9] GNU/Linux Project, "GENKEY man page." [Online]. Available: http://www.linuxcommand.org/man_pages/genkey1.html.

[10] S. Russell, M. P. Hancock, J. McCullough. "The Pipeline: benefits of undergraduate research experiences," *Science*, vol. 316, p. 316, 2007.

[11] L. Segall, "Anonymous strikes back after feds shut down piracy hub Megaupload," CNN Money, 20 January 2012, [Online]. Available: http://money.cnn.com/2012/01/19/technology/megaupload_shutdown/

[12] USNA Admissions, "Naval Academy Summer Seminar," 2014. [Online]. Available: http://www.usna.edu/Admissions/NASS/index.php

[13] USNA-STEM, "US Naval Academy STEM Mission," 2014. [Online]. Available: http://www.usna.edu/STEM/STEM_Mission.php.

[14] USNA-STEM, "USNA Stem Office Vision," 2014. [Online]. Available: http://www.usna.edu/STEM/_files/documents/STEM Mission 2020.pdf.

[15] USNA-STEM, "USNA STEM Summer Program Brochure," 2013. [Online].Available: http://www.usna.edu/Admissions/STEM/STEM2014.pdf.