AC 2011-600: TEACHING COMPUTER SECURITY LITERACY TO STUDENTS FROM NON-COMPUTING DISCIPLINES

Joseph Idziorek, Iowa State University

Joseph Idziorek is a PhD candidate studying Computer Engineering at Iowa State University in Ames, IA, USA. His research interests broadly lie in the areas of cloud computing security, distributed denial of service attacks and stream computing. Joseph is also heavily involved in undergraduate education. He currently teaches Introduction to Computer Security Literacy and assists with a number of other undergraduate courses. He has earned a Bachelors of Science degree in Computer Engineering from St. Cloud State University in St. Cloud, Minnesota, USA.

Mark F. Tannian, Iowa State University

Mark Tannian is presently a PhD Candidate at Iowa State University in Computer Engineering with interests in information security education, cloud computing security and information security visualization. Mr. Tannian returned to pursue a PhD after 12 years of professional experience in information security and holds the CISSP credential. His professional experiences range from technical firewall support, consulting security engineer, technical product manager, senior operations security analyst, product trainer and technical sales engineer. He has earned a Bachelors of Electrical Engineering from the University of Delaware and a Master's of Electrical Engineering from George Washington University.

Douglas W. Jacobson, Iowa State University

Doug Jacobson is a University Professor in the Department of Electrical and Computer Engineering at Iowa State University. Dr. Jacobson joined the faculty in 1985 after receiving a PhD degree in Computer Engineering from Iowa State University in 1985. Dr. Jacobson is currently the director the Iowa State University Information Assurance Center. Dr. Jacobson teaches network security and information warfare and has written a textbook on network security. Dr. Jacobson has received two R&D 100 awards for his security technology and has two patents in the area of computer security. Dr. Jacobson has given over 50 presentations in the area of computer security and has testified in front of the U.S. Senate committee of the Judiciary on security issues associated with peer-to-peer networking.

Teaching Computer Security Literacy to Students from Non-Computing Disciplines

Abstract

Gone are the days when cyber security education was only a concern for computer and Internet experts. In today's world of pervasive computing, everyone is a target. The volume, sophistication, and effectiveness of cyber attacks continue to grow and show no signs of abating. At the center of this cyber epidemic are college students whom rely on their computing and communication devices and the Internet more than any previous generation for their educational, social, and entertainment needs. Yet these same students have little knowledge of the threats they face, the potential short-term and long-term consequences of their actions and the context to make informed security decisions.

The objective of this paper is to describe our approach to practical computer security education for students of non-computer disciplines at the university level. Our primary objective is not to delve into the technical workings of computer security, but instead bring security context to the common computing actions that students already perform on a daily or weekly basis. In this paper, we present our course in detail discussing topics of focus, approaches to engage students and our assessment of student learning.

1. Introduction

Educating students to thrive in a world that depends so heavily on computers and the Internet requires new pedagogical approaches to deal with the advances in technology and the resulting malicious side effects that continually plague students[1,2]. The dangers, both seen and unseen are not merely a concern for the security experts or technology gurus, but for all users of information technology (IT). By now, most college students are aware of at least some of the dangers lurking on the Internet. Yet there exists a gap between being aware of this knowledge and effectively protecting one's computer and personal privacy[3]. At Iowa State University, we have designed a one-credit half-semester course entitled "Introduction to Computer Security Literacy" to address this very shortcoming. The purpose of this course is to educate students of all backgrounds and IT experience levels about the inherent risks of using computers and the Internet. We introduce mitigation techniques and computer security best practices. The course is designed to help students avoid malware infections, steer clear of phishing attacks, and most importantly, learn how to become security-aware cyber citizens. It is our belief that the knowledge acquired by students in this course will be immediately applicable and serve students long after they leave the university. Beyond serving the students, we believe that society's collective security depends on every user being security-aware and exhibiting thoughtful discipline over their personal information and computing resources. It has long been recognized by security experts that the user is in fact the weakest link in the security chain and that technical measures alone cannot and will not solve current cyber security threats[1]. So why not target the weakest link and address it in a formal educational environment?

2. Computer Security for Non-Computing Majors

Educating students from non-computing disciplines (i.e. not Computer Science, Computer Engineering, Electrical Engineering, Management Information Systems, Software Engineering), at the university level addresses a need in computer security education. If offered at all, current security courses are often only accessible to junior or senior students and require many prerequisites of engineering, math, or computer science courses. For students from non-computing disciplines, computer security advice is often found in the form of Web-based top-ten lists of computer security best practices[4,5], which are incomplete and offer little context. It is our belief that computer security education must not be exclusive solely to audiences of computing disciplines. If abstracted correctly, practical computer security education can be made accessible to university students with non-computing backgrounds.

The current state of computer security education falls short of providing opportunities for all those interested to learn. Recent educational trends focus on how to better educate students of computing disciplines in the concepts of security[6]. Recently progress has been made in introducing security concepts earlier in computing curriculums[7], yet these courses still possess significant barriers of entry and would generally not be accessible to, for example, a junior studying Agricultural Life Sciences who desires to better protect his/her security and privacy on the Internet. Others have attempted to provide security education at the university level in the form of a three-hour training session[8]. While arguably better than a Website, a single session is not a sufficient amount of time for students to comprehend, reflect and attempt to apply knowledge. From our experiences, students need repetition, time to reflect on course material, and the opportunity to write about and discuss presented material in order to assess and improve their own understanding. This type of learning simply cannot be achieved in a single three-hour training session. From the authors' collective experiences, a broad demographic of students do not have access to practical information about computer security that would improve their quality of life today and for many years to come.

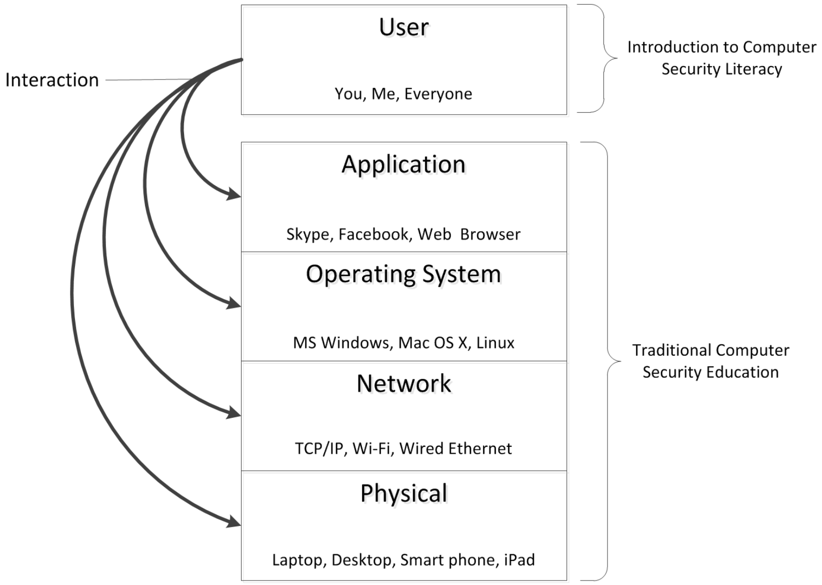
User
You, Me, Everyone
Introduction to Computer Security Literacy
Interaction
Application
Skype, Facebook, Web Browser
Operating System
MS Windows, Mac OS X, Linux
Network
TCP/IP, Wi-Fi, Wired Ethernet
Physical
Laptop, Desktop, Smart phone, iPad
Traditional Computer Security Education

Figure 1 – User-Focused Security Education

Traditional computer security courses typically focus on the theory or implementation of security controls and mechanisms at the application, operating system, network, or physical technology layers (Figure 1). Breaking this traditional model, Introduction to Computer Security Literacy instead seeks to educate students from the perspective of the user-layer – the interactions all users experience with technology on a daily basis regardless of technical prowess. Early indicators from using the user-layer approach have been very promising and initial results show that computer security education is effective with students from both computing and non-computing disciplines.

3. Course Details

From a curriculum perspective at Iowa State University, Introduction to Computer Security Literacy is isolated with no course progression prior to or following it. Although the course is dual-listed (i.e. CprE/InfAs 131) – it is shared between the Computer Engineering (CprE) and Information Assurance (InfAs) departments – it is not currently required for any curriculum nor does it count as a technical elective for any degree. In its current form, it is a course that allows students to explore a topic to which they would otherwise not gain a formal introduction without having to sort and assemble a series of disparate sources in the hopes of teaching themselves what it is they want to learn.

CprE/InfAs 131 is offered as a one-credit, satisfactory-fail course only. Class meets twice a week for eight weeks, and the course is taught twice in its entirety during Fall and Spring semesters. The decision to offer CprE/InfAs 131 as satisfactory-fail only course was made to relieve students from non-computing disciplines of potential fear or self-doubt regarding taking a Computer Engineering course. One of the advantages of satisfactory-fail course offerings in general is that they create an inviting environment in which students are willing to take a chance on a course outside of their comfort zone because there is minimal risk to their standing in their respective programs.

As an optional elective, we have found that the students that have enrolled in CprE/InfAs 131 have joined because they are genuinely interested in the course material for a variety of reasons. Some students have struggled with malware in the past; others have enrolled in the course to help themselves and their parents follow security-aware computing practices. Regardless of the students' initial motivation, the fact that they went out of their way to enroll in the course has certainly contributed significantly to student engagement in the course material, attendance, and quality of work produced.

4. Course Content

It is no surprise that the main challenge of designing this course is making the material accessible to students of all backgrounds. One must make the material not only engaging but also tangible to a diverse set of students in the classroom. Past student demographics have included a graduate student in Hospitality Management, a senior in Computer Engineering, a freshman in Journalism and a junior in Agriculture Studies. Achieving interest and engagement by all students is challenging; however, a key realization is that use of computers and the Internet is nearly ubiquitous among the student population. Students perform the same basic tasks on computers and the Internet each day. During an average day, students use passwords, connect to the Internet on unencrypted wireless connections, use public computers, share content via external storage devices, surf the Web, share information via social networking, and much, much more. Each of these actions involves potential risk of which the average student is unaware. Beyond common activity, many students have been exposed to terms such as "firewall" and "antivirus software" with variable understanding. We explore these issues among many in a way that is accessible to non-computing students and in a way that allows the students to learn the material within a personal context.

Computer security for this course is centered on the individual student's protection of their digital and non-digital assets. It is defined as the ability to control the release, change and availability of personal and financial information, thereby safeguarding the reputation and the financial standing of each student. This, in turn, is manifested in practices that improve availability, integrity and confidentiality of their data, computing platforms and communication systems they utilize. The selection of course topics is focused on common computing and Internet activities and relevant threats and defense mechanisms. The sequence of course topics are presented to the students in a progression starting with a foundational knowledge and comprehension of terminology and concepts that are added upon, and referenced as the course progresses. Although the high-level topics remain fairly constant, the supporting content that is presented in these modules is constantly adapting to the needs and interests of the students and to address the continually changing threats that they face.

Although the underpinnings of computer security are of a technical nature, a number of concepts are of a practical nature and can be abstracted to the user-layer (Figure 1). When security is presented in conjunction with tasks that students already perform every day and using well-recognized analogies, these concepts are more readily understood regardless of the students' educational interests. Below is a high-level breakdown of the concepts covered in the course:

- Introduction to cyber security
- National cyber security issues
- Computers and Internet architecture
- Passwords: threats and best practices
- Basic cryptography
- Malware: threats, prorogation techniques, function
- Defense-in-depth: firewalls, antivirus, software patches, user education, data backup
- Surfing the Internet safely
- Online shopping
- Wireless networks
- Public computers/removable storage media
- Security and privacy
- Social engineering: phishing
- Social networking

In addition to the topics above, raising current events topics throughout the course allows students to see how what they are learning in class is significant and relevant on a local, national or international level. During 2010, in Iowa alone, there were three major computer hacking incidents on government computer systems. These events clearly demonstrate to the students that geographic location has little bearing in the cyber world and that cyber criminals are thieves of opportunity, constantly searching for victims. Using well-documented news stories, such as the Stuxnet Worm[9], Google/China hacking incident[10], and the Gawker Media password breach[11] present very tangible examples that reinforces computer security topics, vocabulary, and best practices. Stories such as these can serve as excellent case studies and present themselves with enough regularity to provide compelling and timely accounts.

Although the course topics by no means constitute an exhaustive survey of computer security, they are the essential user-layer principles, tools, and terms that enable students to develop practical and applicable computer security knowledge. These topics are consistent with an established body of computer security literacy knowlege[12].

4.1 Defense

A point stressed early on in the course is that there is no such thing as absolute security. Despite all of the advances in technology, there does not exist a silver bullet to protect students from all potential threats. One of the students in the class asked the question, "If hackers are really good at being bad, why can't good guys be really good at protecting us?" This question raises two important points. First of all, the scenario requires that the "good guys" be right all of the time to provide protection, while the bad guys only have to be right once in order to be successful in their crime. Students learn that the cards (i.e. vulnerabilities) are stacked in favor of the attacker and because of this there will always be risk. Secondly, the student's question suggests that computer security is solely a responsibility of the "good guys." Breaking this perception is one of the central themes of the course. Despite the actions of good guys and bad guys alike, the student plays a significant role in the protecting of their own digital assets. A key point is that the user is a weak link in the security chain and that they can do a great deal to protect themselves from many security threats.

In this class, we stress a defense-in-depth or belt-and-suspenders approach to computer security as a means of self-protection (Figure 2). More specifically, one does not rely on any one security mechanism (i.e firewall or antivirus software) to prevent all potential threats. Instead, a number of security measures are put in place that together can protect the user against many threats. If one mechanism fails, another is in place to prevent, detect or recover from an attack. As part of this approach, students are taught the purpose, strengths and weaknesses, and the threats that software patches, antivirus software, user education, firewalls, and backups protect against. The synthesis of the security mechanisms and the students' comprehension and application of this knowledge creates a significant and practical knowledge base to protect their digital assets.

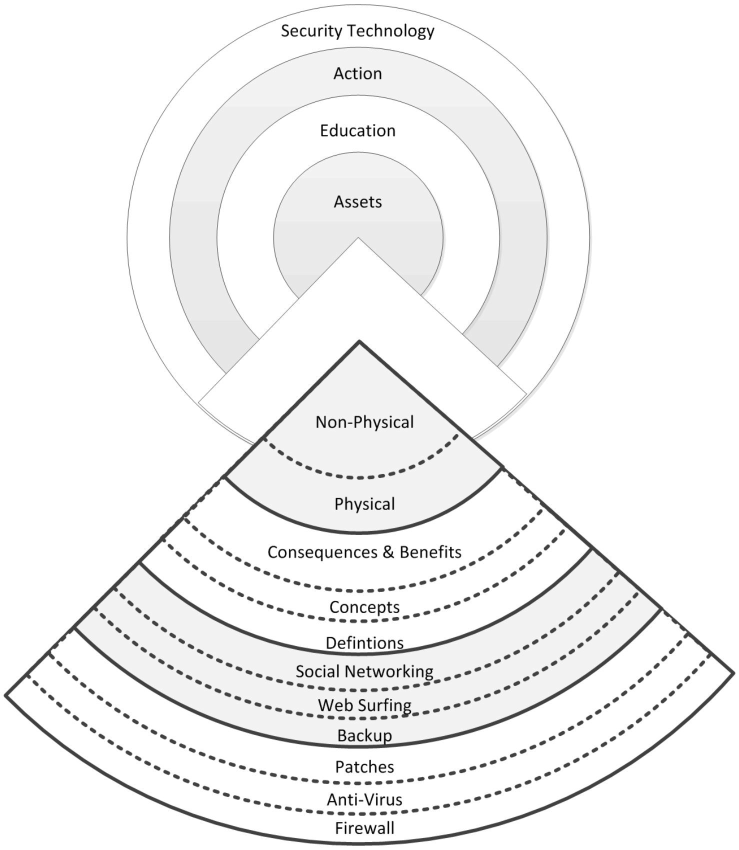

Figure 2 - Defense-in-Depth Approach

4.2 Offense

Imparting students with a basic knowledge of computer security means more than simply teaching defensive techniques. It is a long held belief that in order to defend against an adversary, one must understand how the adversary thinks and attacks. This is why courses in information warfare (i.e. hacking) are taught at the graduate-level and as part of a graduate curriculum[13,14]. Initially it may appear to be contradictory to teach computer security literacy students common straightforward offensive techniques, but it has been shown to be an effective way for students to evaluate their current defensive posture as well as the limitations and scope of common defensive mechanisms. Each security tool and practice in the defense-in-depth approach addresses a limited threat model. It is up to the defender (i.e. the student) to understand what threats security mechanisms can protect against and those threats they should do their best to avoid. An appreciation of the offensive mindset helps the student develop the wisdom necessary to be an effective last line of defense after their investments in mitigation like anti-virus software, firewalls and patching fails. Understanding that they are the target the attacker is trying to exploit improves their chances of thwarting social engineering attacks (e.g. phishing, spear phishing, Trojan horse, drive-by downloads, scareware, ransomware) that have been highly successful. As responsible educators, we ensure ethics discussions encapsulate the presentation of offensive methods in order to avoid encouraging malicious cyber behavior.

The means by which we introduce offensive measures and reflect on defensive approaches are key to effective pedagogy. Several approaches taken have been: 1) demonstrating threats to passwords as they are in transit or at rest (i.e. sniffing, key-logging, password cracking), 2) physical reenactment of firewall traffic filtering rules 3) case studies of common social engineering attacks. In the physical reenactment of firewall traffic filtering rules, students role-play firewall actions and the information flow through the firewall. Some students are assigned roles of Web and email content, while other play the roles of common types of malware such as viruses, worms, and Trojan horses. Under a simplifying assumption that the firewall is at the perimeter performing stateful inspection, the students come to realize that Web browser connections are a vector for threats the firewall is unable to mitigate. This realization reinforces the need for alternative defensive approaches. In addition to the limitations of firewalls over network-based threats, other non-networking threat such as malware infested USB drives are discussed as they bypass the network defenses altogether. Student participation and comments help us adjust our approaches, and so far we are encouraged by student feedback and assessment results.

4.3 Active Learning

In order to encourage interest and engagement, we incorporate student participation into the class session whenever possible. If the student cannot see how a particular topic directly applies to their immediate future or why it is meaningful to them, student engagement and learning effort will suffer. Furthermore, practical computer security is an applied field of study and how better to start the transfer of knowledge from the class into their daily lives than to actively participate in the class session.

Performing demonstrations during the lecture allows the students to see first-hand the applications of security. Students were particularly interested in password cracking and wireless sniffing demonstrations. For example, witnessing first-hand how a password on the NYtimes.com Webpage is transmitted in clear text and observing that it can be sniffed out of the air raises the students' awareness. It further shows that information that they themselves choose to disclose when surfing the Internet on an unencrypted WI-FI connection in public places such as a coffee shop or the library is vulnerable to such sniffing attacks.

During the defense-in-depth section of the course, we ask the students to physically act out scenarios that test the rules of a firewall. The objective of this exercise was to help students understand how a basic software firewall works and to show them what a firewall does and does not protect against. Physically acting out a phishing attack, malicious software download, and normal Web activity in the context of a firewall truly brought the concept of a firewall to life for the students. One student remarked that it was "a fun activity that clearly showed how a firewall protects or doesn't protect a computer."

5. Experiences

Enrollment for the first four offerings of CprE/InfAs 131 has been encouraging. Within the first year, 100 students representing 31 different majors have completed the course. The popularity of CprE/InfAs 131 grew so quickly that during the second offering of the course there were not enough chairs in the assigned classroom to accommodate all interested students. Although the volume of students is encouraging, the more telling outcome is the diversity of students that have gravitated towards the first offerings of CprE/InfAs 131 with nearly half the students enrolled from a non-computing focused disciplines (Figure 3). The coupling of this statistic with the breakdown of students by their home college (Figure 4) supports the hypothesis that students with a non-computing educational focus are interested in acquiring practical computer security knowledge.

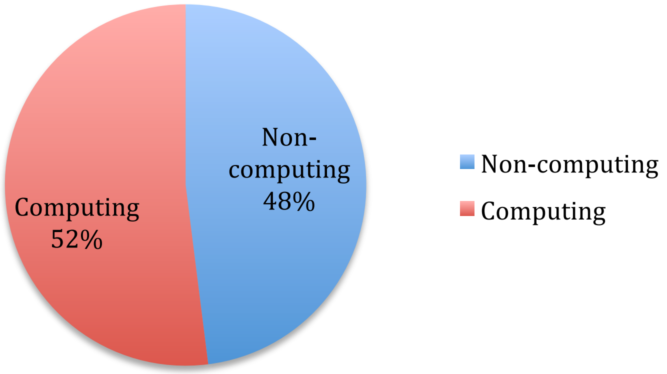

Figure 3 – CprE/InfAs 131 Student Breakdown by Computing and Non-Computing Disciplines

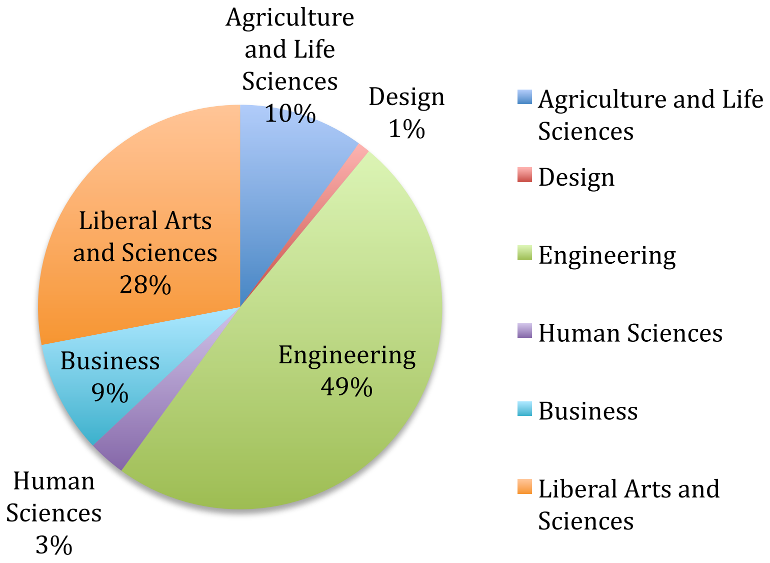

Figure 4 – CprE/InfAs 131 Student Breakdown by College

The initial expectations of students during the first few lectures coincide with their educational background. In the first homework assignment when asked "What do you expect to learn in this course?" non-computing students are generally open-minded and are more concerned with being able to understand the technical aspects of security. The computing students often state that their expectations are low because many already consider themselves quite knowledgeable in computer security topics. Despite this attitude, students from computing disciplines still have a great deal to learn. In one particular case, a Computer Engineering (CprE) student mentioned the following in a post-class evaluation:

> I came into this course expecting to not learn anything due to my background in CprE. I honestly thought I could teach the class with the knowledge that I had before I signed up for the class. Thus, I'm truly glad to have been proven wrong in that I learned quite a bit of interesting things. It was truly great to look forward to Monday and Wednesdays to attend class.

Regardless of initial expectations stemming from the students' backgrounds, post-course responses have shown that both groups of students have had positive learning experiences. Unless students have a prior understanding of human-technology challenges within computer security, they are more or less at the same level of understanding when the course starts despite their area of study.

After completing the course, students have come to recognize the importance of the knowledge that they have learned. A student from a non-computing major stated "This course made me feel confident in using the skills I learned even though I had minimal prior knowledge of the subject." Furthermore, a common remark in post-course evaluations follows along the same lines as the following "This should be a mandatory course for incoming freshmen." and "[I] learned a lot of important, helpful and useful information." While these statements show positive progress, the real measure of success in this course is how students react when they are presented with a situation in which they are able to successfully apply the knowledge that they have learned.

6. Assessment

Assessment of learning is derived directly from the established learning objectives of the course. The learning objectives were formed based on the premise that this course is a true introductory course and that the intended audience – university students that regularly use information technology – have little to no knowledge of practical computer security topics. At the conclusion of the course, students will be able to:

- Define computer security terms and mechanisms
- Describe fundamental security concepts
- State computer security best practices
- Describe the strengths, weaknesses and limitations of security mechanisms and concepts
- Give examples of common security threats, threat sources and threat motivations
- Explain their role in protecting their own physical and non-physical computing assets
- Discuss current event topics and read security articles in the popular press
- Assess computing actions in the context of security

In order to begin to have meaningful conversations related to security, ask informed questions, and read articles in the popular press, students must be familiar with and recall the terms of the field. From a Bloom's Taxonomy perspective, the foremost course objective is for all the students to exhibit *knowledge* in the subject of practical computer security. In this context, knowledge is defined as student's ability to recall definitions of specific keywords (e.g virus, phishing, keylogger), describe fundamental concepts (e.g. defense-in-depth, social engineering, security vs. privacy) and state computer security best practices. To assess such knowledge, during each class meeting students are given either an individual quiz or group quiz in which they are asked to demonstrate knowledge of previously discussed topics by way of multiple-choice, matching, short answer, or fill-in-the-blank type questions.

In a more formal and quantifiable type of assessment, pre- and post-tests are also given to students on the first and last days of the course. The test, which is the same for both assessments, consists of 20 multiple-choice questions that represent the core terms and concepts brought forth in the course. Although student enrollment over the past four course offerings has totaled 100, examination oriented assessment of computer security literacy before the class started and at the end did not start until recently. Thirty-eight students have taken a pre- and post-test. This preliminary data is very encouraging (summarized in Figure 5) and when broken down to compare computing and non-computing students, it raises a somewhat counter-intuitive observation. Figure 6 presents the statistical plots for all students assessed. Results show that the mean scores among all students increased between pre- and post-assessments and the difference was statistically significant.

	All Students		**Computing**		**Non-computing**	
	Pre-test	**Post-test**	**Pre-Test**	**Post-Test**	**Pre-Test**	**Post-Test**
Mean	13.89	18.45	14.52	18.22	12.93	18.80
Std Dev	3.32	1.31	2.84	1.48	3.84	0.94
Maximum	19	20	19	20	19	20
Minimum	6	15	15	15	6	17
N	38	38	23	23	15	15

Figure 5 – Pre- and Post-Test Statistical Summary

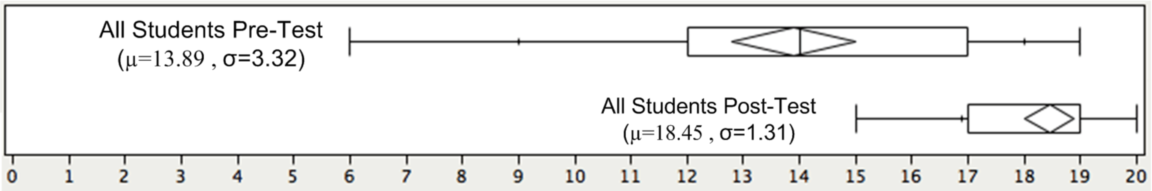

Figure 6 – All Student Pre- and Post-Test Statistics

When focusing on the non-computer student group (Figure 7), one sees that the teaching approach appears to have been effective in both moving the mean score higher and reducing the variability of understanding within the group. Although computer students have a perceived advantage in this course due to their affinity to computer related subjects and prior knowledge, the difference in pre-test means and variance are not statistically significant for this group of students as compared to non-computer students. In other words, the computing and non-computer students on average start at the same place and show they all end up improved in the same place, statistically speaking. The small sample available to us prevents from making generalizations about these results, but we are very encouraged and are a little more skeptical about advantages declared computer majors may have in this course.

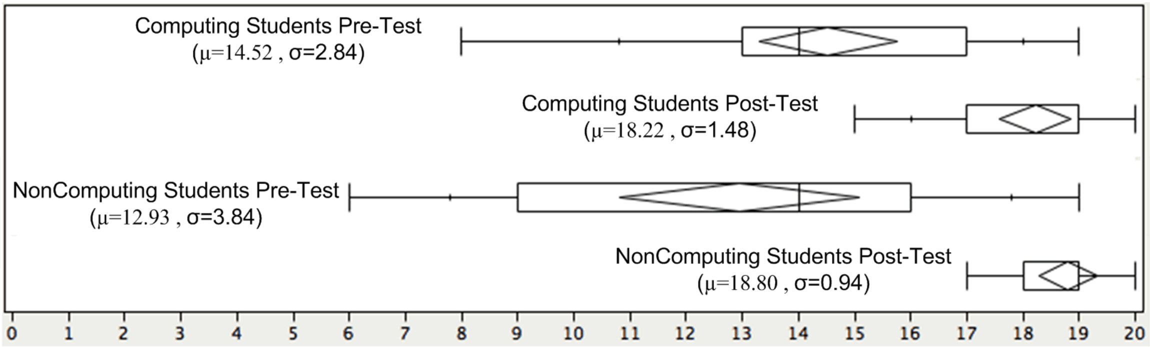

Figure 7 – Computing vs. Non-Computing Test Statistics

The second course objective is for the students to demonstrate *comprehension* of the material. Not only should students know the definitions of key terms in practical computer security vernacular but also they should be able to make connections and relationships between the terms and concepts. To assess comprehension, weekly writing assignments are given in which students are to read popular press articles - selected by the instructor - on a topics recently discussed in class. Students are asked to write a response to the article and answer questions that are crafted to evaluate comprehension of the learned material. Formulating such responses in a written form allows the students to not only reflect upon the lecture content but also to express their interpretation of the articles in their own words. In evaluation of such work, the instructor has the ability: to correct the student's comprehension of a concept or a group of concepts, to reinforce comprehension through positive feedback or by providing additional articles to encourage the student to explore a topic further.

The third and end goal for the students is to be able to apply their new knowledge to their everyday actions with information technology. Currently, assessment of application is done either through the presentation of hypothetical situations in class in which the students are asked to analyze a situation and make an informed decision or are asked to evaluate real examples such as a phishing email or a malicious Skype message. The real and perhaps the most meaningful test of such knowledge in this particular subject happens outside the classroom, which is challenging to assess. While hypothetical and real examples can be presented in class, the students are in an artificial environment in which answers to the questions are biased by their situation. It is one thing to identify a suspicious Skype message when sitting in a classroom for the course entitled "Introduction to Computer Security Literacy" in which the students associate everything that is presented by the instructor in the context of security. It is another matter for the transfer of knowledge to be sufficient for a student in the realistic context of being in a hurry, distracted, lackadaisical, or in routine settings and for them to act appropriately to actual challenges. This is when the real application of knowledge occurs. Initial assessment of application has only been done informally by way of students voluntarily sharing anecdotal accounts. As the course matures, we plan to provide more thorough and valid assessment of this particular course objective.

7. Future Work and Conclusion

Computer security education is key to combating the risks and vulnerabilities intrinsic to the Information Age. Each day, students are inundated with alerts and pop-ups informing them about patch updates, antivirus signatures, firewalls exceptions, Facebook friend requests, and offers for free items, but lack the proper knowledge and comprehension to evaluate the benefits and consequences of taking specific action on these items.

As educators and computer security practitioners, we feel that the task of providing university students with the opportunity to become knowledgeable about the malicious side of the Internet falls squarely upon our shoulders. It has long been recognized that there exists an urgent need to improve security education[1]. Although this is clearly true in computing technology curriculums, the direct benefits of security-focused courses at the undergraduate level are not presently accessible to non-computing majors. Realistically, computer security involves much more than secure programming, protocols, and algorithms. It also encompasses everyday decisions that students make about whether or not to open email attachments, understanding why clicking on inviting hyperlinks can have negative results, maintaining virus definitions and much more. It has become apparent that the security community needs to begin educating about all aspects of computer use and needs to focus its efforts at the broader audience beyond those who design, implement and maintain information technology[1,12,15].

The creation of this course marks only the first step of a much larger plan to provide practical computer security education to this broader audience. To support audience expansion that includes other universities, community colleges, high schools, and community groups, work is underway to create a textbook and make course materials (lecture slides, case studies, homework assignments) accessible on an accompanying Website. Beyond course content, the most significant impediment to a larger dissemination of security knowledge is the limited supply of educators that are able to effectively teach such a class. Understanding the audience and the material in context of the audience is crucial to the success of not just this course, but for all introductory courses. However, unlike other disciplines such as accounting and medicine, which offer introductory courses in personal finance and nutrition respectively, teaching methodologies that support computer security instruction is not as mature within the computer security community[12]. As a result, we have received grant money for the purpose of instructing educators on how to teach computer security to non-computing audiences. The end goal is being able to affect change in the security community where it is needed the most – user oriented computer security literacy.

Educating students at the university is an initial step to address the larger societal problem that exists of educating all users of information technology about computer security. It is widely accepted that purely technical solutions are not sufficient to combat cyber criminals or avoid costly mistakes[1,15] (e.g. MI6 wife revealing her husband's cover on Facebook[16], social media enabled home invasions[17]). Instead a comprehensive effort is needed, educating all users of information technology from the young to the old, technically savvy to the inexperienced. While this paper was written in the context of university students, it is our belief our user-focused approach can be adapted to a wider range of audiences including high school students and community groups to name a few. As educators, we feel this course fulfills in part our duty to prepare students to be constructive contributors as virtual residents of cyber space.

Bibliography

1. B. Schneier, *Secrets & Lies: Digital Security in a Networked World*. John Wiley & Sons, Inc., New York, NY, USA, 2000.
2. J. Ryoo, A. Techatassanasoontorn, L. Dongwon. "Security Education Using Second Life," *IEEE Security & Privacy*. vol.7, no.2, pp. 71-74, March-April 2009.
3. J. Hage, "Human Relationships: A Never-Ending Security Education Challenge?," *IEEE Security & Privacy*, vol.7, no.4, pp.65-67, July-Aug. 2009.
4. Stop. Think. Connect., "Tips & Advice," 2010. [Online] Available: http://www.stopthinkconnect.org/tips.html. [Accessed: Feb. 23, 2011].
5. Iowa State University Information Technology, "Security Tips," 2008. [Online] Available: http://www.it.iastate.edu/security/tips/. [Accessed: Feb 23, 2011].
6. M. Bishop, "Education in information security," , *IEEE Concurrency*, vol.8, no.4, pp.4-8, Oct-Dec 2000.
7. K. Nance, "Teach Them When They Aren't Looking: Introducing Security in CS1," *IEEE Security & Privacy*, vol.7, no.5, pp.53-55, Sept.-Oct. 2009.
8. Y.Y. Chan and V.K. Wei, "Teaching for Conceptual Change in Security Awareness: A Case Study in Higher Education," , *IEEE Security & Privacy*, vol.7, no.1, pp.68-71, Jan.-Feb. 2009.
9. J. Markoff, "A Silent Attack, but Not a Subtle One," *New York Times*. Sept. 2010. [Online] Available: http://www.nytimes.com/2010/09/27/technology/27virus.html. [Accessed: Feb 23, 2011].
10. K. Zetter, "Google Hack Attack Was Ultra Sophisticated," *Wired*. Jan. 2010. [Online] Available: http://www.wired.com/threatlevel/2010/01/operation-aurora/. [Accessed: Feb 23, 2011].
11. S. Gustin, "Gawker Media Websites Hacked, Staff and User Passwords Leaked," *Wired*. Dec. 2010. [Online] Available: http://www.wired.com/threatlevel/2010/12/gawker-hacked/. [Accessed: Feb 23, 2011].
12. M. Wilson, K. Stine, and P. Bowen, "Information Security Training Requirements: A Role- and Performance-Based Model (Draft)." NIST Special Publication 800-16 Revision 1 (Draft). 2009.
13. D. Jacobson. "Teaching Information Warfare with Lab Experimentations via the Internet." In *Frontiers in Education*, 2004. T3C/7-T3C12 Vol. 11 (2004).
14. J.A. Whittaker and R. Ford, "How to think about security," *IEEE Security & Privacy*, vol.4, no.2, pp.68-71, March-April 2006.
15. J. Viega, *The Myths of Security*, O'Reilly Media, Inc. Sebastopol, CA, 2009.
16. N. Gilani. "Wife Blows MI6 Chief's Cover on Facebook." *The Times Online*. July. 2009. [Online] Available: http://www.timesonline.co.uk/tol/news/uk/article6639521.ece. [Accessed: Feb 23, 2011].
17. CBS. "Facebook 'Friend' Suspected in Burglary." *CBS News*. Mar. 2010. [Online] Available: http://www.cbsnews.com/stories/2010/03/25/earlyshow/main6331796.shtml. [Accessed: Feb 23, 2011].