AC 2008-2372: INFORMATION TECHNOLOGY LITERACY FOR NON-ENGINEERS

William Suchan, United States Military Academy
Will Suchan has a Ph.D. in Computer Science from Arizona State University. He is the Information Technology Core Program Director in the Department of Electrical Engineering and Computer Science at the United States Military Academy. He can be reached at william.suchan@usma.edu.

Susan Schwartz, United States Military Academy
Susan Schwartz has an M.S. in Computer Science from Old Dominion University. She is currently an Assistant Professor and Deputy Director of the Information Technology Core Program in the Department of Electrical Engineering and Computer Science at the United States Military Academy. She can be reached at susan.schwartz@usma.edu.

Edward Sobiesk, United States Military Academy
Edward Sobiesk has a Ph.D. in Computer and Information Sciences from the University of Minnesota. He is an Assistant Professor and Course Director for the course IT305-Theory and Practice of Military IT Systems in the Department of Electrical Engineering and Computer Science at the United States Military Academy. He can be reached at edward.sobiesk@us.army.mil.

Information Technology Literacy for Non-Engineers

Introduction

This paper describes the concepts and methodologies used in an undergraduate general education information technology (IT) course designed specifically for non-engineers. The semester-long course is required for all of our students who are not engineering majors, and is taken by about 750 juniors and seniors each year. The course builds upon a freshmen-level introductory course that covers microcomputer competencies, as well as basic programming techniques in both Java and Extensible HyperText Markup Language (XHTML). An immersive computing environment, in which all our students have a laptop and ubiquitous network access, also contributes to our students' technical foundation.

The primary objective of our course is to significantly contribute to the accomplishment of our institution's IT literacy goal, which states that "Graduates understand and apply information technology concepts to acquire, manage, communicate and defend information, solve problems, and adapt to technological change."[1] The course accomplishes this by emphasizing both the *theory* and the *practice* of information technology. From a theoretical perspective, it is critical that our students understand the general concepts involved with acquiring, communicating, managing, and defending information. From a more pragmatic viewpoint, though, we strive to also produce students who have the skills necessary to apply various IT tools in finding practical solutions to diverse problems in often unpredictable problem domains. Ideally, we want students who embrace and believe in IT, and who are confident from their current experiences that they will have the ability to successfully employ future, not-yet-developed IT tools throughout their professional career. We accomplish this goal by emphasizing hands-on learning, with students completing numerous in-class exercises and labs as well as several team projects, all of which are designed to help them learn how to learn IT.

Even though this course is for non-engineers, we receive an abundance of anecdotal evidence from our former students that the technological literacy gained in this course has made a significant difference in their chosen fields.

A Foundation Based on Cyberspace

The concepts of the World Wide Web (WWW) and electronic media permeate the entire course. In an introductory module, students are exposed to advanced XHTML and Cascading Style Sheet (CSS) techniques that significantly extend those they received in their freshman-level IT course. The homework for our course consists of four team projects,[2] and the first of these is to build a web portal that will be used as the submission vehicle for the remaining course projects. All projects in the course are submitted electronically by publishing them to a course web server.

Besides XHTML and CSS concepts, we also empower our students to properly exploit the immense resources of the WWW. One way we accomplish this is by introducing them to the concept of code reuse. We encourage students to use web designs from such sites as Open Source Web Design (www.oswd.org)[3] as a starting point for their work. By customizing an open

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Military Academy or the United States Army.

source design and integrating their own content, our students produce truly amazing web portals in a reasonable amount of time.

Another central issue that we address in the introductory module is intellectual property rights in cyberspace. Before our students begin work on their web portals, they participate in a lesson with an adjunct professor who is a lawyer specializing in electronic media copyrights and the concept of Fair Use.[4] Then, throughout the process of constructing their web portals, explicit attention is paid by both the students and the instructor to the variety of permission types that are required in the completion of the project. Examples of these permission types include permission given on the web site from which the media was obtained, permission successfully granted via correspondence, open source license agreements, use of non-copyrighted materials, and use of materials personally owned (or optimally, created) by the student. The overall effect is to create a strong awareness in the students that electronic intellectual property is generally owned by someone, and to give students confidence that they can still ethically succeed in this environment.

One final aspect of the introductory module is a small networking lab. This one hour experience presents a global overview of key IT concepts by having students build a small client-server network. Almost every concept in the course can be touched upon through this exercise. During this initial lab, the idea is to preview the course. At the end of the course the exact same lab is conducted, and then the goal is to tie together all the course concepts.

Acquiring Information

The next section of the course covers the digitization process for images, sound, and video. Both digital capture and analog-to-digital conversion are explored, along with data compression techniques. The topic of sensors is covered, letting students experience the connection between the physical and digital worlds.

Because of the immersive IT environment that exists on our campus, students are already familiar with numerous basic input devices. The central concept of this module is the process of capturing an analog world and converting it into a digital format that can then be processed and shared using computers. To apply these concepts, we cover what is involved in the acquisition of images, sound, and video, including the theoretic limits described in the Nyquist Sampling Theorem.

A natural follow-on to the digitization process is the topic of compression. Digitized data in an uncompressed format is often expensive to store and transmit (movies are an excellent example of this). We cover the concepts of lossy and lossless compression, and then look at instances of each with compression techniques such as JPEG, MPEG, and MP3. We additionally emphasize how file size can be reduced during the digitization process by modifying either the sampling or quantization parameters. Exploring how these various techniques can compress or reduce the file size truly reinforces what is taking place during the digitization process and what is stored upon completion of it. The implications of the choices and techniques selected are also addressed.

For the practice aspect of acquiring information, we briefly survey a number of sensors including cameras, microphones, ground and aerial radars, aerial and satellite imagery, and other sensors that use the same general digitization process to sense various parts of the electromagnetic spectrum. These concepts are tied together using a hands-on exploration of biometrics, including facial recognition, fingerprint scanners, and retinal scanners.

Communicating Information

The middle section of the course covers local area networking and introduces global information grid concepts as well as general communication principles. Student teams design a local area network for a small building complex, which forces them to explore the tradeoffs involved in the engineering design process. They ultimately have to make recommendations about the best course of action to use based on the available resources.

Although our students have been using the West Point network for over two years, most are completely unfamiliar with the components within a network or how they work together to allow access to web and file servers, electronic mail, or the Internet. This module of lessons is designed to familiarize students with these concepts and to challenge them to put the components together in network designs.

We start by looking at the different hardware found in a network such as routers, switches, network interface cards, and wireless access points. We explore the functionality and roles of this equipment, as well as what type of connectivity is used between them (i.e., logical ports, physical ports, and various media used to connect the devices). Tradeoffs on data transmission rates, control of routing, and network security are emphasized. The TCP/IP protocol layers are covered in great detail so that the students understand why data is divided and encapsulated into packets. To simplify the concepts for non-engineering students, IP addresses are used without extensive subnetting.

Attention is also given to what services a network provides to its users. Familiar services such as email and web services are presented, along with specific services such as Dynamic Host Configuration Protocol and the Domain Name System. Comparisons of wired and wireless networks and the challenges of network security are considered.

To bring together these concepts, a scenario of network requirements between several multi-room buildings is presented in class. Over two class periods, the students are led through the design of both the physical layout of the network and the logical addressing used between the network components. The physical design includes analyzing where routers and switches will be placed, how computers will be connected (wired or wireless), how buildings will be connected, distances between major components, and bandwidth requirements. The physical network is drawn on a schematic of the buildings' layout.

Network equipment must be "bought" for the network. We have created a notional "store" which lists real equipment and some of its specifications (such as number of ports, transmission rates of the ports, wireless transmission standards, cable lengths, and cost per item). Students must choose which components meet the needs of the actual requirements to ensure that they

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Military Academy or the United States Army.

have the correct numbers of ports and can handle the types of cabling they want to use. This is where they begin to see the need to make tradeoffs based on desired results and cost. The graded event for this portion of the course requires the student teams to create three different designs for a provided scenario and to compare and contrast the designs based on criteria they develop. Criteria may include cost, security, expandability, redundancy, flexibility, etc.

Near the completion of this module, students are brought into a lab where they construct a network that includes routers, switches, a server, multiple laptops, and voice-over-IP phones. They see the network principles they have just learned in a live environment. Additionally, they have a guest lecture on real-world network and communication infrastructures.

Managing Information

The next part of the course covers the design and implementation of relational databases using Microsoft Access. Relational databases have become ubiquitous in society and Microsoft Access is frequently the database tool available in the workplace. As such, we have placed an emphasis on the skills required to design, implement, and extend a relational database in Microsoft Access.

Because most of the students have never created a database, the implementation part of the course begins with four extensive, self-paced exercises designed to have the students teach themselves many of the features of databases and in particular, how they are implemented in Microsoft Access: Databases and Tables, Relationships and Queries, Reports, and Forms. Three lessons are devoted to students working on these exercises. The exercises are centered around a small database that has a few tables already created and leads the student to develop additional functionality for the database, based on a provided design. The project for this module is based on a much expanded version of the exercise database in which students must provide a design for new functionality requirements, implement that design, and create specific queries and reports.

An implementation project requiring creation of a small information system follows the database section of the course. Students use Microsoft FrontPage-generated Active Server Pages (ASP) code and web forms and reports in conjunction with an Access database to create a front-end application that interacts with the database they have just completed.

The success of this part of the course has been tremendous. Almost two hundred students have requested server space (on a web server maintained in our department) to create information systems for their student clubs or other organizations. They have taken the new skills learned and applied them to other areas of their lives.

Defending Information

With the rapid escalation of computer crime and identity theft, it is imperative that college graduates have some understanding of how to protect both their own digital assets and the cyber resources that their organizations depend upon. The final section of the course is designed to arm students with the knowledge they need to accomplish this. In a sense, the protection of information can be seen as the overarching goal of the course. This module is positioned at the end of the course precisely because students cannot truly understand how to protect information until they understand networking, databases, and the other topics covered earlier in the course.

To teach students how to defend information, we begin by explaining the application of a multidimensional information assurance model.[5] The use of a model is critical in that it allows students to create a realistic mental model of the risks and vulnerabilities involved in defending information. Armed with this knowledge, the students explore information security from both the attackers' and defenders' points of view. A key component of this module is a multi-lesson, hands-on experience in which students conduct attacks and establish defenses in an isolated virtual environment. This "hacking" experience, using VMware software to manage the environment, allows the students to experience first hand the ease with which attackers can compromise a system, and also the protection that simple but integrated security measures can provide.

Assessment

Each year, the two semesters of our course are assessed using about 40 embedded indicators (graded events such as projects and exam questions) that evaluate performance on the four main components of our course goal. When examining student performance, an indicator average above 90% exceeded course expectations, an average below 80% did not meet course expectations, and all remaining averages (in the range 80-90%) met course expectations. Table 1 summarizes student performance for the 2006-2007 academic year based on these embedded indicators.

Component / Standard	Acquire Information	Communicate Information	Manage Information	Defend Information
Exceeded Expectations	**1**		**1**	
Met Expectations	**5**	**8**	**17**	**3**
Did Not Meet Expectations		**2**	**2**	**1**

Table 1. Student performance for the 2006-2007 academic year based on embedded indicators.

As can been seen from Table 1, our course is consistently meeting our goal. The five indicators for which we did not do so involved (1) the TCP/IP Protocol Stack, (2) creating web forms and reports that are connected to a back end database, and (3) applying an Information Assurance Model. These results do not indicate that our course fails to successfully teach these topics (there are "met expectations" indicators for each of them as well), but rather reflect areas of the course in which students sometimes struggle. When one looks at these three topics and remembers that our students are not engineers, the challenges involved become obvious. To mitigate these challenges, we are relooking both the content for these topic areas as well as the method of delivery.

Another interesting aspect of Table 1 is that it portrays how much weight is placed on the different key components of the course. The selection of graded events for a course isn't accidental and the allocation in Table 1 accurately reflects our philosophy.

Replicating the Course

Our colleagues at other schools sometimes ask us how to import this course to their own institution. Without a doubt, the key to the hands-on component of the course is "the equipment cabinet." Our classes are limited to 18 students per section, and each section uses a stack of equipment housed in a rolling cabinet to execute labs. Each cabinet holds 18 laptop computers, a multifunction server, two routers, five switches, nine hubs, a wireless access point, and adequate cabling, both copper and fiber optic. Additional components include an iris scanner and a fingerprint reader per cabinet. For the most part, this equipment doesn't have to be new to be effective. Almost all of the components we use (we have seven cabinets) are five years old. If anything, having slightly older equipment allows us to focus on concepts without having to navigate through the latest bells and whistles.

With the exception of the VMware and "hacker" tools, the cabinet laptops have a standard Microsoft Windows/Office environment installed. (A Microsoft site license is nice to have.) Other critical infrastructure components needed for the course are file and web servers. All teams of students have file space allocated on department-owned servers to work on their projects, and all teams have space on the department web server to publish their results.

One of the most challenging aspects of teaching this course to non-engineers is that they have a great range of capabilities. A technique we have used successfully to handle this variation is to cluster students by their Grade Point Average. While all of the benefits of doing this are beyond the scope of this paper, we have found that it truly enhances the learning for all of the students.

Conclusion

To its credit, our school's administration realized in 2001 that it needed to add an IT literacy goal that was well beyond the typical freshman-level computer course. To its greater credit, it also realized that a course to fulfill this goal did not exist. The course described above has evolved over the past six years as a means to provide non-engineers the IT literacy they need to ensure professional success.

Bibliography

1. *Educating Future Army Officers for a Changing World*, Office of the Dean, United States Military Academy, 2002.
2. Sobiesk, E. and Suchan, W. "Starting in the Middle: Design and Implementation in the Information Age," *Proceedings of the American Society for Engineering Education New England Section Conference*, March, 2006.
3. "Open Source Web Design," http://www.oswd.org, 2008.

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Military Academy or the United States Army.

4. Sobiesk, E., Suchan, W., and Trope, R., "Overcoming the Ethical Dangers of Academic Fair Use in the High Technology Classroom," *Proceedings of the American Society for Engineering Education Annual Conference*, June, 2007.
5. Suchan, W. and Sobiesk, E., "Strengthening the Weakest Link in Digital Protection," *IEEE Security and Privacy*, vol. 4, no. 6, pp. 78-80, Nov/Dec, 2006.