Building Tomorrow's Information Assurance Workforce through Experiential Learning

David Dellacca and Connie Justice
Department of Computer and Information Technology
Indiana University-Purdue University Indianapolis
ddellacc@iupui.edu cjustice@iupui.edu

Abstract

The Department of Computer and Information Technology (CIT) at Indiana University Purdue University Indianapolis (IUPUI) has built a comprehensive and experience-based learning environment. Students coming to the department seeking knowledge and skills in the areas of networking and security are exposed to traditional learning methodologies focusing on terms, concepts and history of the subject matter. In addition to this, students gain practical knowledge and capture experience-based lessons in the field of networking and security. Through class work and outside projects students are given opportunities to gain valuable and relevant hands-on experience designing, implementing, and managing live network environments for the department, other on-campus groups, and ultimately for groups outside of the university. This experience-based teaching methodology not only addresses the challenges of preparing future technologists in an ever-changing field, but also arms students with the experience that many employers are seeking. This article discusses the growth, benefits, challenges, and future goals of the networking and security tracks of classes offered at IUPUI in the CIT Department.

1. Introduction

Preparing the future technology workforce is a challenging undertaking. As technology shifts and changes, one skill set will not fit all environments. The debate over how students should gain the required skills in today's high-tech industries is at the forefront of many educational discussions. With a program that focuses on educating students in the ways of network security, our approach is to provide students with not only valuable theoretical knowledge, but also experiential lab and eventually live production network security experience. Melissa Dark, Associate Professor in the Computer and Information Technology Department and Assistant Dean of the School of Technology at Purdue University in West Lafayette, Indiana stated that "…there is a critical shortage of skilled information assurance professionals in the workforce - this is true across several industry sectors including government, education, telecommunications, finance, health care, energy, and so on." Because of this truth, we have created our networking and security courses to address the needs of students seeking networking and security education, businesses seeking qualified candidates, and the IT professional community looking for continuing education.

Through design, we provide more than training to our students. Students who receive only training along their educational journey are provided a tunnel-vision repository of knowledge that can not be easily expanded to address the quickly changing environment of the networking and security fields. Universities and colleges make it their mission to provide a well-rounded educational experience, providing students with opportunities outside of the students' major that expands their world views, traditional thought patterns, and helps to defeat the one-size fits all mindset. Universities, especially those with a strong liberal arts program, can come under scrutiny by the public at large when research points to the underachieving math and science scores of our nation's youth (http://www.educationnext.org/20032/39.html).

However, in programs like ours that are preparing future technologists, we avoid getting caught up in the

hype and understand that if we narrow the scope of the education students receive at the university level, it would do little more than send them down a dead end road with nowhere to turn. Through our degree and certificate programs we provide students the technical, worldly, and communication skills that employers are seeking today. (http://www.networkworld.com/newsletters/manage/2003/0915manage2.html).

The purpose of this paper is to focus on the design of the security curriculum, innovative approaches taken to teaching security courses, the experiential learning opportunities afforded to students through our program, the challenges to teaching a security curriculum, and finally future security curriculum development and emerging needs.

2. Security Curriculum Design

The design of the security curriculum started to form in the summer of 2003 when a faculty member attended an 8-week intensive Information Assurance Education Graduate Certificate (IAEGC) faculty development program at the Center for Education and Research in Information Assurance and Security (CERIAS). The IAEGC program is an 11-credit hour graduate certificate program for college and university educators who want to develop Information Assurance (IA) programs at their institutions thereby increasing the number of faculty to teach Information assurance and security and ultimately increase the number of professionals graduating from our nation's colleges and universities. This educational opportunity, the collaborative partnerships formed while attending classes and the addition of another security faculty member in the CIT Department led to a wealth of new additions and changes to the department's offerings. These additions and changes included new course offerings, a Network Security Certificate, the reorganization of the existing networking track of classes to create two independent networking and security tracks, and finally a joint degree program between two other departments on campus.

2.1. Network Security Certificate

Upon graduation from the IAEGC faculty development program the faculty in CIT developed the Network Security Certificate (NSC). The NSC provides information assurance and security education and training to students and professionals. Information assurance and security professionals are responsible for the policies and technologies used to safeguard the information systems infrastructure of a company. The NSC program is hands-on and requires students to have some networking and systems experience. Completion of the NSC provides students with a solid foundation in security techniques and prepares participants to work in the fields of information assurance and network security. The Network Security Certificate is an ideal mechanism for current systems and networking professionals to add to or update their knowledge related to Information Assurance. The certificate consists of six courses (five required and one selective) and is designed so that it can be completed within three semesters. Courses in the certificate also may be applied directly to a Bachelor's degree in Computer and Information Technology at IUPUI.

2.2. One Becomes Two – New Security Track and New Networking Track

The department originally started with a very limited number of courses that addressed the developing field of computer networking. These courses were being offered to supplement curricula in the Business, Standard, and Web Development tracks of courses in the department. Due to student enrollment increases, industry trends, and student interest in the networking field, a focused curriculum track in computer network design and administration was desired. This provided for more networking courses to be developed and the new Networking track to be finalized. After a couple of years of enjoying much success with the track, the desire to continue to grow the depth and coverage of the networking courses was realized. While planning for the networking track's growth, the field of network security was recognized as an important topic. While aspects of security were discussed in a few of the existing courses, nothing was offered at that point to allow students to focus solely on information assurance solutions and security administration.

In response to the growth of the networking track, industry changes, and the support from a National Science Foundation (NSF) grant as well as the resources brought back from the IAEGC program, the Network Security Certificate (NSC) was created. At the onset, the NSC security courses were add-on in nature for undergraduates; offering a handful of courses for those wishing to gain knowledge in and of the information assurance field. To better reflect our offerings, the Networking track was renamed the Networking and Security Track.

The demand and number of classes needed to adequately cover the topic of network security

demanded that another adjustment be made to the curriculum. The Network Security Certificate provided a complete core of information for professionals, but for undergraduate students seeking to learn of the security field we needed to provide more foundational courses. While trying to address the need for more courses, it was quickly realized that the degree would simply not allow many more credit hours to be added. Faced with running out of available credit hours, the separate Networking Track and Security Track were created to accommodate all of the courses now required to cover both topics, networking and security, adequately. This shift allows for students to specialize in either network administration or network security. A set of the same core courses are foundational to both tracks.

In the early Networking Track of classes, we focused on Local Area Networks, Wide Area Networks, Data Communications, Network Operating Systems, and Network Administration. There were made available a few slots for other "selective" technology courses held within the department and then others to take outside of the department to allow enrichment of the students. Trying to implement the security courses into the defined curriculum became difficult while trying to ensure a balanced education and avoiding leaving out important topics. We had begun to add the security courses that made up the Networking Security Certificate to the Networking and Security Track. As we got to the point of having no more room for credit hours, but lots more content to cover, we came up with the idea, after offering a survey to current students about their interests as well as talking with industry experts, of offering two tracks, instead of one.

The tracks as they will appear in the Fall 2006 course track sheets for the department are the Networking Track and the Security Track. Students will have the option, after declaring their major to pick between one of the five tracks available in the department. Their options are Standard track, Web Development track, Business track, and now the Networking track, and the Security track. We have shuffled our original set of networking and security courses and added a few more that were needed to better meet the goals of each track. The new set of Networking and Security tracks contain a core set courses detailing computer hardware, data communications, wireless communications, network design, and network administration. From this set of core courses, each of the two tracks branch off into its own specialty area.

We continue to offer the Network Security Certificate, which is continuing its growth and popularity with professionals coming to supplement or refresh their existing training and knowledge. Through the split of the Networking and Security track into two separate tracks, we can better groom students for a particular area of interest giving them detailed knowledge in a specific area of networking and security without sacrificing other aspects of each field while still providing for a well-rounded college education. The courses that comprise the networking and security tracks are listed in Table 1.

Table 1. Networking track and security track core courses

These core courses are in addition to General Education, Associate Degree, and elective courses; all students take Data Communications, Hardware and Software Architecture, and beginning Operating Systems Administration courses. 121 credit hours are required for the bachelor's degree.
Networking Track
300 Level Programming
CIT 303 Communications Security & Network Controls
CIT 327 Wireless Networking
CIT 402 Design & Implementation of LAN
CIT 440 Comm. Network Design
CIT 415 Advanced Windows Systems Administration
CIT 499 Unix Programming and Administration
CIT 426 Enterprise Networks
CIT 490 IT Experience
CIT Selective
CIT Selective
CIT 310 Career Planning
Security Track
300 Level Programming
CIT 303 Communications Security & Network Controls
CIT 402 Design & Implementation of LAN
CIT 406 Advanced Network Security
CIT 420 Digital Forensics
CIT 415 Advanced Network Administration
CIT 499 Unix Programming and Administration
CIT 431 Applied Secure Protocols
CIT 460 Wireless Security
CIT 490 IT Experience
CIT Selective
CIT 310 Career Planning

2.3. Joint Degree Program

The Indiana University (IU) School of Informatics approached us to join with them in creating a joint bachelor's degree program. We used courses from Computer and Information Technology (CIT), Informatics (INFO), and Computer Science (CSCI) to create this degree. The degree is a Bachelor's of Science degree from IU. The courses that compose this degree are listed in Table 2.

Table 2. Joint degree courses

Information Technology Core Requirements
Courses:

CIT 140 Programming Constructs Laboratory[1]
CIT 212 Web Site Design
CIT 286 Operating Systems & Administration **or** CSCI 403 Introduction to Operating Systems
CIT 214 Web Data Management
CIT 307 Data Communications **or** CSCI 436 Data Communication and Computer Networks
CIT 303 Communications Security & Network Controls
CIT 356 Network Administration **or** CSCI N 321 System and Network Administration
CIT 406 Advanced Network Security
CIT 420 Digital Forensics
CIT 431 Secure Protocols
CSCI 432 Security in Computing
CIT 460 Wireless Security
Informatics Core Requirements
Courses:
INFO-I 101 Introduction to Informatics
INFO-I 201 Mathematical Foundations of Informatics **or** CIT 120 Qualitative Analysis I
INFO-I 202 Social Informatics
INFO-I 210 Information Infrastructure I
INFO-I 211 Information Infrastructure II **or** CIT 270 Intro to Java
INFO-I 308 Information Representation
INFO-I 330 Legal & Social Informatics of Security
INFO-N 480 Technology and Law
INFO-I 450/451 Design & Development of an Information System **or** INFO-I 460/461 Senior Thesis

2.4. Courses Developed

In order to create the NSC new courses had to be developed and current courses modified. CIT had one official course on the books for security. That course was CIT 303 Communications Security and Network Controls. The first task was to build out what was needed to map our courses to the Committee on National Security Systems (CNSS) standards, formerly known as the National Security Telecommunications and Information System Security (NSTISSI) standards [1]. CNSS and NSTISSI standards provide valuable standards to ensure consistency in curriculum content across institutions teaching information assurance and security [7].

Using the CNSS standards as a guide, we decided to modify CIT 303 Communication Security and Network Controls to provide students an overview of the field of information security and assurance, focusing on exploring current encryption, hardware, software, and managerial controls needed to operate networks and computer systems in a safe and secure manner. Then we decided to create Advanced Network Security, CIT 406, providing students with an in-depth study and practice of advanced concepts in applied systems and networking security, including security policies, access controls, IP security, authentication mechanisms, intrusion detection, and protection. We also added Digital Forensics, CIT 420, which provides an introduction to the fundamentals of computer forensics and cyber-crime scene analysis. The various laws and regulations dealing with computer forensic analysis are also discussed in this course. Students are introduced to the emerging international standards for computer forensic analysis, as well as a formal methodology for conducting computer forensic investigations. Another new course is Applied Secure Protocols, CIT 431, emphasizing the applied facets of cryptography for the information assurance and security professional. By the end of the course students are able to apply important cryptographic principles and tools to allow networks to communicate securely. We also addressed the field of Wireless Security, CIT 460, giving students the opportunity to focus on the risks and benefits associated with wireless local area network communications and how the industry defines a secure wireless network. In addition, students gain the skills needed to properly create, configure and maintain and a secure wireless network in the course. Most recently, an IT Security Risk Assessment course was created and is scheduled to be taught in the Fall Semester of 2006.

3. Experiential Learning

Traditional theoretical methods in teaching security give the student a solid understanding of the underlying principles. But what happens when students go out into the job market seeking non-research or technical types of jobs? It is accepted that students have excellent theoretical concepts but they also need to have practical experience. It is the combination of theory and practice that is at the pinnacle of our teaching. Approaches to security education through teaching theoretical concepts, experiential learning opportunities and collaborations have shaped a dynamic educational program. Researchers have stated that experiential learning is critical in the educational process [2,3,4,6]. While traditional methods for teaching theory occurs, we continue teaching foundational principles while moving into more advanced content by providing students the benefits of hands-on learning and the depth of knowledge gained through our educational partnerships. Experiential learning, the process of giving students hands-on learning opportunities beyond lab-created scenarios, provides tangible proof to students that learning the theory is more than academic rhetoric [5].

From the early beginnings of the program, emphasis has been place on the hands-on aspect of

learning as much as the desire for students to learn strong core fundamentals of networking and security theory. The result has been significantly rewarding for students and faculty, creating a diverse, engaging, challenging, and ever-changing learning environment.

Behind all of the opportunities that we present to students to broaden their knowledge, there is the desire to do good with the services that the students are performing. Many opportunities are growing within the department, school and university as well as around Indiana that will ultimately benefit the education of students. The students have the opportunity to see the positive impact their work can make on university departments and small businesses where previously no help or expensive help was the only solution. In the following subsections, we will highlight how these experiential learning opportunities have shaped student learning.

3.1. Dedicated and Functional Labs

We currently have two dedicated labs for the use of our networking and security classes. Our labs are cut off from the rest of the university network, using firewalls and other measures. Students have access to outside resources from within the lab for research and testing, while at the same time specific measures have been taken to "protect" the university network and the outside world from the services that may be running inside of the lab environment. In addition, the labs are housed on their own subnets, allowing only specific traffic out onto public networks. Inside the lab environment, students have access to individual workstations, network electronics including switches and routers, as well as various server and operating system platforms hosted on the workstations via VMWare to perform simulations and testing. The workstations are cabled so that each PC can connect to the rack mounted switches for Internet/network access and can also connect to a corresponding switch for console programming and configuration. The physical configuration of each lab also provides for us to be able to create a few smaller networks with in the labs for a variety of testing, simulation, and teaching experiences.

Through the decreasing prices of hard drive storage and associated components, we require students in a couple of courses to purchase an external USB hard drive. Using the drive in conjunction with labs resources, the students take the drive from being unformatted to running a couple of operating systems from the drive while performing a variety of tasks on them along the way. Sometimes these tasks purposefully create problems for the students, problems that they must then remedy on their drive to move on to the next step of the class.

Another example of how the lab's configuration is put to use is where students are learning about the process through which servers hand out Internet Protocol (IP) addresses. Students are able to boot one workstation into a server operating system, with another workstation running a client operating system. Utilizing the equipment in the room, students can network any two workstations together and utilize them to test configuration settings, working towards getting the server to hand out IP addresses to their partner's client workstation. Performing such a lab however, can not be completed with out making sure external access is cut off from the workstations and network that are completing the lab. This is a critical component to the overall success of the labs, ensuring the design is flexible enough for the tasks that are trying to be completed. Having measures in place to control traffic in and out of the network is paramount.

There is no hiding that by committing to teaching networking and security courses through a hands-on approach requires resources, resources beyond the human factor. We have procured a lot of equipment from local businesses, others on campus, and even the campus surplus actions. A key element to lab and equipment acquisition is to not turn anything down and discover how it could be used, in some way, to benefit students. That being said, any equipment whether bought or donated, must eventually be figured into the overall design. Creating too much of a Frankenstein-ish environment may be inviting more problems that it could solve. Overall, through careful planning and purposeful designs, labs and networked environments can be created that are built specifically for learning.

3.2. Student Journals

In an effort to make students more accountable to lab experiences and topics discussed in the classroom, we require students to complete a journal for each networking and security class. Students are assigned to reflect on the experiences of each lab or specified class experience. The writing process gives students an opportunity to reflect on what they are learning and provide us their thoughts and opinions about certain topics discussed or experiences associated with the assignment. Finally, it provides us valuable feedback for improving particular elements of the course material. In the beginning, we had students do journals like they would in at home such as a diary. Now, we have developed a format in which students list daily class activities as well as the procedures, processes and fixes to certain tasks or

labs. An example of student journals for the living lab reflects the experience the students acquire. "Linux was updated and is running correctly. The problem we have encountered at this point is getting the OS to recognize the RAID card. Installing the correct drivers for it is proving frustrating. In the documentation, it only mentions Red Hat drivers so I'm hoping I don't have to revert back to that OS. On the plus side, I think we figured out why we were getting errors on Red Hat 7 so I think the install will be ok this time." Another student expresses some of his experiences with imaging and installing Macintosh operating system, OS X. "check the lab, for any a bused Macs, and for cleanliness, started all Macs, lodged in and logged out and shut them down to make sure the systems are working properly, every thing is at a 100%. Researching the OS X, and disk utilities, and how to build or create and image…. issue has been resolved for now, I had to check on the Mac lab (Wed., Sat., Mon.) and everything is running, researching firewall software (shorewall), OS, and hardware." This basic approach showed that students were able to think through the steps of the issue or problem they may encounter and research the issue and figure out the resolution. We discovered that this was helping the student to learn to systematically look at problems, organize information, and anticipate the next required steps. While this type of information can be lectured on, we believe the students have shown a much deeper understanding and acceptance due to these exercises. Students do at first complain about what they perceive to be extra work, but by the first or second project, they begin to appreciate the value in the journal, not only for deeper understanding, but also to use the journal as a reference for future projects.

3.3. Lab Write-ups

Students are provided a template to follow for each lab write-up. The lab template is the same for each lab, giving uniformity to the way the students summarize their lab experiences. Interestingly, as the semester progresses, students seem to look deeper at each lab, beyond the necessary steps to complete a task. We believe this begins the process of a stronger understanding of the big picture, avoiding the rushed approached of just completing an assignment and moving on to the next. Being able to look at cause, effect, specific steps taken to complete a task, and ways to improve for a future similar situation provide a well-rounded lab experience for each student.

This business-orientated approach to network administration documentation processes creates a sense of accountability and understanding for each lab experience, beyond the technical skills learned in the lab. Through the lab write-up process students learn how particular scenarios affects them as a future employee, as well as encourages and emphasizes the ever-important documentation process for work performed.

3.4. Living Lab

The Living Lab provides real world experience in networking and security to students by having them support portions of the computing infrastructure for various departments. Currently students support 8 servers providing a variety of services for the CIT department and 2 servers for the School of Journalism used for The Sagamore and Jag Radio (the student newspaper and web radio, respectively).

The mission of the Living Lab is to serve as the beginning of an experiential pipeline in which students apply their knowledge and develop their skills in networking and security. Students who have completed the introductory networking courses are eligible for the Living Lab. No experience in a production environment is required. The beginning student works with more experienced students in the Living Lab supporting CIT's security and networking labs. This creates a situation in which the experienced students become mentors to the students who do not have any experience.

3.5. School of Journalism

As they become more experienced, students move through the pipeline into mentoring positions and on to more complex internal projects such as working on The Sagamore/Jag Radio (http://www.sagamore.iupui.edu) project. CIT supports two student laboratories in the School of Journalism as well as a web server and a streaming server. Students under the mentoring of faculty and the department systems engineer, implement, support and maintain the systems in a production mode. The students are responsible for creating and pushing network images out to Microsoft Windows (Windows) and Apple Macintosh (Mac) desktop environments. Students are responsible for the security of all the machines and must keep up with the patches and hardening the machines. Students are also responsible for the Mac server that supports the Mac lab cluster and the Windows server that support the Windows cluster. Students are also responsible for the Sagamore web server and the Jag Radio streaming server. Again, the students must secure and harden all systems. There is a firewall for the Journalism and

Sagamore/Jag Radio servers that are maintained by students as well.

3.6. Wireless Survey

In the spring 2006 Wireless Security course, students conducted an unofficial survey of IUPUI Engineering and Technology students on their use of security solutions on their home wireless network. This fairly simple task provided the class some very interesting talking points. We were able to discuss, what a secure wireless network looks like, to what degree or solution is good enough for the consumer market, how that differs from a corporate solution, and a variety of other topics. This discussion took the students' newly learned technical understanding of wireless security to a new level by being able to converse using the appropriate terminology, comparing strengths and weaknesses of approaches, as well as critically analyzing the usefulness of Small Office Home Office (SOHO) wireless security solutions. By being immersed in the topic through discussion and research, the students gained a much broader understanding of the solutions, issues, challenges, and techniques of wireless security.

3.7. Local Government

An opportunity arose for Wireless Security students to become involved in the political process here in the Indianapolis area in the Fall 2005 semester. A student and a faculty member met with State Senator David Ford to discuss his proposed Senate Bill 381 that encouraged a statewide network be established, helping the growth of broadband access in rural areas. Notes from this meeting gave the class an opportunity to see they way the State and particularly the senator viewed the wide deployment of wireless network solutions to increase broadband access and the role the State of Indiana should/might have in its deployment.

During the same semester, five students attended a committee meeting at the State House regarding House Bill 1148. The bill died on the floor as a vote was not taken. However, the bill proposed placing high amount of restrictions on municipalities in constructing local broadband / wireless networks for public use, so again during the course of the semester students had the opportunity to see and experience the government at work providing plenty of discussion material on whether or not the state, cities, or municipalities belong in the wireless internet service provider business and what security concerns exist with each of these proposed deployments. The class was also able to discuss corporate viewpoints on the topic by looking at the business gains of mass wireless deployment and then comparing certain companies lobbying efforts to their position on that particular senate bill.

3.8. Wireless Presentations

A second group of students, not involved directly with the aforementioned wireless survey, developed a presentation on how to secure a SOHO wireless network. Once completed, students presented the presentation to several civic groups, free of charge. The benefit for students was incredible. While they learned a lot from the presentation creation process, they learned even more by giving the presentation and becoming expert in answering more complex questions from presentation attendees. By teaching the subject matter, they gained a deep understanding of this aspect of wireless security.

3.9. IT Risk Assessments

The Technical Assistance Program (TAP) from Purdue University and the Purdue School of Engineering and Technology at IUPUI, of which CIT is a part, have partnered to provide an IT Risk Assessment service for small to medium-size businesses. Students are directly involved with the research and implementation of IT risk assessments which can be used as a projects for class credit or paid internships. The IT Assessment Center has completed 4 projects and has made a civic contribution to educate and make a difference for these small businesses.

Companies often lack the in-house expertise or have the time to assess and secure their IT infrastructure. IT staff are usually stretched beyond their limits and must find a way to update their security skills on their own time. These companies and staff members need a cost-effective and objective appraisal of their IT security needs. Through the service provided, students identify critical security needs and prioritize those needs for appropriate action. The students selected for these assessments will have progressed through the experiential pipeline and have the experience required to perform a quality assessment, while being mentored by a faculty member. Overall, the services offered not only addresses the immediate IT security needs for a company but also provides a roadmap for a cost-effective, long-term security strategy. The outline used for each project is shown below in bulleted form.

- Pre-Assessment
- Assessment

  - Template
  - Non-penetrating tools
  - Hardware and software
- Post Assessment Analysis and Reporting
- Post Assessment Meeting
- Follow-up Opportunities

3.10 Dissemination and Collaboration

All teaching methods and materials are generously disseminated to other educational institutions. We strongly believe that through involvement with the educational community, our program and other university programs will become stronger and contribute to the overall quality of education for the next generation of security professionals. Our students take an active role in providing feedback to us on the curriculum and consequently see changes in the curriculum due to their comments and suggestions for improvement. These ideas along with the existing curriculum are what we pass along to others. We believe that through curriculum improvement and consequent information sharing with other information security professionals, students will see the benefits of dissemination and collaboration. Our goal is to foster a mindset in them to do the same among their peers in the workforce; working collaboratively with each other as security professionals. Our ultimate goal is to promote disclosing security concerns within professional security communities urging solutions and not tolerance of or apathy to information assurance administrative, political, and application concerns.

4. Conclusions and Future Work

As the tide of technology changes there is an ever growing need for educational institutions to be able to adapt and change with it. Educators need to uphold the strongest values of university education but at the same time give today's students the tools they need to survive and succeed as IT professionals. By merging traditional theoretical-based education with experiential learning students get the best of both worlds.

We must continue to evaluate and improve the curriculum in order to continue to meet the needs of our students as well as keep course material up-to-date. Security in IT is the new landscape and it is not going away. Recognizing the importance of relevant and up-to-date curriculum is the first step. Next, we must find ways to break down the barriers that tempt some to hoard knowledge, thinking it is only for a few to possess. It is not the knowledge that makes one powerful, but what is done with that knowledge that is the equalizer. We need to look at what has been learned from our experiential scholarship and report the findings to the educational community.

Having quality collaborations with other universities and like-minded educational institutions is paramount. Through educational and local business partnerships, we can create a cornerstone in the foundation of solid curriculum development and experiential opportunities for students.

Finally, taking our newly formed curriculum, partnerships and research we won't truly succeed until it is actually passed on to the students. This benefit should be evident in not only classroom instruction, but also in experiential learning opportunities, providing students the knowledge, tools, and experience to be a productive and contributing member of the IT community.

As our networking and security tracks continue to grow and evolve, we look towards the future of making new friends, finding more partnerships, and looking for funds to support the education of tomorrow's information assurance workforce.

5. References

[1] The Committee on National Security Systems. (Accessed September 1, 2006). http://www.cnss.gov/.

[2] Heng, S, "Combining Theory and Practice in the Right Proportions", CDTL Brief: Combining Theory and Practice in the Right Proportions. July 2005, Vol. 8, No. 4. http://www.cdtl.nus.edu.sg/brief/V8n4/default.htm.

[3] Kolb, D. A. (1976). Management and learning process". *California Management Review*, 15(3): 20-31.

[4] Kolb, D. A. (1984). Chapter 2. In D. Kolb, The experiential learning: Experience as the source of learning and development. NJ: Prentice-Hall.

[5] Kolb, D. A., Boyatzis, R., & Mainemelis, C. (2000). "Experiential learning theory: previous research and new directions". Prepared for R. J. Sternberg and and L. F. Zhang (Eds.), Perspectives on cognitive learning, and thinking styles.

[6] McCarthy, P.R. & McCarthy, H.M. (2006). "When case studies are not enough: integrating experiential learning into business curricula". *Journal of Education for Business*, 201-204.

[7] Why are CNSS Standards Important? (Accessed September 1, 2006). http://www.nsa.gov/ia/academia/iacefaq.cfm?MenuID=10.2.1.4#3.