Proceedings of the 13th Colloquium for Information Systems Security Education
University of Alaska, Fairbanks
Seattle, WA June 1 - 3, 2009

Integration of IA Research into an Undergraduate Capstone Class

Authors: Mark Bannister, Jason Zeller, and Keyu Jiang, Fort Hays State University

Abstract: The Department of Information Networking and Telecommunications has offered a capstone class for twelve years. 2008 was the first time that students from the two-year old Information Assurance Emphasis reached the course. With guidance of faculty and support from an industry partner, a team of IA students conducted valuable research studying wireless Wi-Fi 802.11 security deployment practices. This paper examines the purpose and design of the class and the results arrived at by undergraduate students. It describes the learning of both the students and faculty. This paper provides evidence that undergraduate students can conduct quality IA research within this type of class structure.

Index terms – IA Capstone Course, Undergraduate IA Research. Wireless Access Point Security

I. Introduction

Information Assurance education includes developing an understanding of important concepts and theory. Application and synthesis of concepts and theory may occur through a variety of means including laboratory exercises, case studies, or other experiential learning. One means is involving students in a "capstone" course that requires performance of a project or research that demonstrates understanding of theory and use of knowledge and related skills in an applied manner [1]. Integrating a project with private industry can add additional relevance, financial resources, and important information and feedback.

II. CAPSTONE Class

McLester and McIntire explored core findings of the "The Workforce Readiness Report Card" [2], a report released in September 2006 that summarizes the current state of the US workforce. Described as a crisis, the report clearly indicated that higher education is not fulfilling its role of preparing students for the knowledge economy. While students excel in technical skills, there is a considerable deficiency in the "must have" applied skills. These include professionalism, teamwork, oral communications, creativity, and perhaps most importantly, the ability to combine these skills with the knowledge within a specialized field. If higher education does not address this issue, the authors suggest the United States may lose its competitive edge in a global market. The two recommendations for higher education are:

1) Integrate applied skills into existing curriculum/program development
2) Develop stronger relations with industry to foster communications and provide opportunities for students [2].

Cox and King propose a skills set model that includes three layers 1) theory, 2) tools, and 3) application [3]. Students begin the program by developing a breadth of knowledge within the field (degree), exploring options, and developing a fundamental understanding of each area. Students then decide on a specific route to develop a depth of knowledge in one area of concentration. Each program is supported by a core set of classes that focus on "professional non-subject specific work skills." These include teamwork, communication, project management, analysis, design, ethics, and evaluation.

In designing and implementing an Information Assurance program at the under graduate level Fort Hays State University strategically sought to implement the type of "Must Have" workforce skills McLester and McIntire described [2]. The program was also influenced by the three layered model that Cox and King advocate [3].

The Information Assurance Emphasis at the undergraduate level resides in the Computer Networking and Telecommunications Concentration in the Bachelors of Arts or Science Degree in Information Networking and Telecommunications. A required course for this degree program is INT 430 Capstone in Information Networking and Telecommunications. The course is designed to add to student's general theoretical knowledge of information use as well as application of skills and knowledge. It links students with industry for research projects. The capstone class seeks to have students integrate the Cox and King [2] layers of: 1) theory, 2) tools, and 3) application through performance of a significant project. Demonstrating the knowledge and skills they have acquired during their undergraduate education, student groups of typically five students prepare and present a proposal reflecting their concentration area. Students may perform a project for a real client or may conduct more abstract research. Most chose to work with a client. In either case, the project must have defined goals, expectations, and evaluation. Each team must create a written proposal containing background research, a plan

for proceeding/methodology, a timeline, a statement of qualifications, and a budget. If the proposal is accepted by the professor, students develop a rubric for evaluating their work at the completion of the project. They embark into executing their project. Students are to seek out additional faculty mentors for advice and critique. At the project's completion, they provide a written report of their results, a 30-45 minute presentation in the Capstone class at which they are questioned by the professor and peers, and make an abbreviated ten minute ceremonial presentation of their project at the "Capstone Convocation" attended by the full departmental faculty, friends, family, and invited guests. The Capstone Convocation is held the evening before the university commencement and serves as the departmental graduate ceremony.

The Information Networking and Telecommunications academic degree that houses Information Assurance program has involved students in other areas of the degree program in its Capstone class and concomitant projects since 1996. In a twelve year time span, students have participated in more than 100 projects. 2008 was the first year that undergraduate students with significant Information Assurance coursework and career interest reached the course as seniors. This class has similar goals to those of the Capstone class at Walsh College described, by Livermore and Poulios [1], Both programs seek to require students to demonstrate knowledge of project management techniques and a mastery of the knowledge and skills taught across the program [1].

Despite having similar goals; the structure and implementation of the Fort Hays State University program differs. Due to the moderate size of the academic program, it uses one Capstone section to serve all Information Networking and Telecommunications concentrations Instead of students performing individual projects, they perform team projects. (In 2008, this course had 27 students who divided into five teams). The course differs from the course at Walsh College in that the class meets twice a week for full 90 minute class periods instead of three times during the semester. The students are encouraged to work with private industry, and present final projects in first a class setting and then a Capstone Convocation instead of at a Capstone Fair.

A 2008 Capstone project focusing on Information Assurance demonstrates the value of this type of project combining research on industry practices and field research testing and studying actual Information Assurance implementation. Students proposed to learn from identifying best practices, designing and building test equipment, gathering data and analyzing data, and presenting findings.

One of the authors of this paper is a student who was part of this Capstone team. He works full-time for an innovative Internet service provider (ISP). He realized from his work on the ISP's helpdesk that a significant share of customers use wireless access points and did not appear to be taking industry recommended steps to secure them. This author organized a team of students to undertake a study of wireless access point usage and security practices.

The students worked with the student's employer ISP in conducting their research project. The umbrella organization of the ISP has a very close relationship with the Department of Information Networking and Telecommunications and has been supportive of several Capstone projects over a number of years. The organization provides a variety of information technology and telecommunications services including competitive local exchange telephony, networking equipment and services, IT services, system integration, web hosting, software and equipment resale, and Internet service provision. The organization employs many graduates of the program and provides part-time employment for a number of current students in its ISP helpdesk and computer repair service operations. The partnership with the ISP for this project began with a formal proposal presented both through a presentation and in writing to the ISP's leadership team. The students' hypothesis was that a large share of wireless access points – including those serviced by the ISP, do not use wireless network security best practices. They offered to provide their data, analysis, and recommendations for protecting the ISP's customers. They also promised to coordinate with the ISP to assure that their research did not threaten its network or customers (or have the appearance of doing so). In return, the student team asked for funding of their detection equipment, technical information and feedback. The ISP readily agreed to the students' proposal.

III. LITERATURE REVIEW AND BEST PRACTICES

There is little academic research on home wireless network adoption or security. Nearly all of the available literature is industry based and security standards are industry driven. Before identifying security best practices, the students identified the attractiveness of wireless home networks. *The 2007 Wireless Network Industry Report* [4] describes Wi-Fi and 802.11 standard as "the primary wireless LAN standard world-wide. Wi-Fi offers relatively high performance for general mobile, stationary, portable devises."[4] The same report in describing the popularity of Wi-Fi estimated that there are approximately 40,000 such wireless access points in San Francisco.[4] Other cities are expected to have similar, if not less penetration.

The student literature review identified best practices for Wi-Fi best practices. Industry sources such as Microsoft [5] and a very limited number of academic/professional publications provided the information on this subject. [6 & 7]. The student team focused on best practices which could be readily measured from the street as they patrolled with their detection equipment. One of the recommended best practices is changing the Service Set Identifier (SSID) from its default setting [6]. Retaining the default SSID signals that the default password and other default settings may be in place. "It is standard practice for wireless equipment manufacturers to sell wireless equipment without any of the security features enabled [7]." Thus the default setting for wireless access points is unencrypted and the password may be simply "return." Users are warned not to create a SSID that is identifiable [6]. Instead they are encouraged to use "use long, nonmeaningful strings of characters, including letters, numbers and symbols [6]."

A uniformly agreed upon "best practice" for Wi-Fi wireless local area networks (LANs) is encryption of all traffic [5]. The early wireless access point encryption standard was Wire Equivalent Protection (WEP). Contemporary industry publications and software companies including Microsoft caution users against relying on WEP as it be easily cracked [5]. Wi-Fi Protected Access (WPA) is encouraged instead [5].

The primary factors identified for data collection and measurement in this Capstone project were: 1) Whether SSIDs had been changed, and 2) whether encryption is deployed and what type of encryption – the weaker and older WEP standard, the newer more resilient WPA standard, or other encryption methods.

IV. METHOD

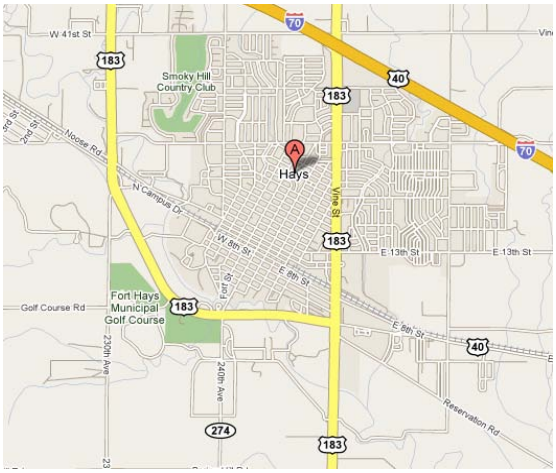
The students organized and named their "consulting group" "Innofish." They proposed to compile information on every wireless access point in the study city of Hays, Kansas. The students created a timeline with project milestones for their research.

Project Milestones

Milestone	Definition	Delivery Date
Build Team	Form a high performance team and develop a comprehensive plan for research study	1.24.08
Conceptual Agreement	Receive verbal commitment of project	1.31.08
Proposal Draft	Completed draft of the project proposal	2.14.08
Contractual Agreement	Completed release of the project proposal	2.21.08
Begin Research Study	Start mining the wireless data	3.22.08
Data Mining Completion	Finish mining the access points	4.12.08
Research Study Completion	Completed study, organized into an informational report	5.1.08
Final Report	Present findings to Nex-Tech	5.08.08

The students' goal was to gather and analyze data on every Wi-Fi wireless access point within the city broadcasting on the 802.11 a, b, g, and n wireless standards.

The study community population of the city of Hays, Kansas is just over 20,000 people with two dominant ISP's. It was expected to be a community with high wireless Internet penetration for multiple reasons: It is a regional center for higher education, health care, and professional services. The university has promoted use of laptop and tablet computers among its students. The public high school has a one-to-one laptop initiative which provides every high school student with a WI-FI 802.11 enabled laptop. The high school has a partnership with two local (and predominant) ISPs who offer discounted Internet service with a wireless router to families of high school students. Additionally, one of the ISPs has provided free public "hotspot" access at every hotel, the primary shopping areas, the public library, and at popular coffee shops and restaurants.



The students used the software suite below to plan their routes for data collection and for reporting information in a geographical manner.

The students designed their own tools for measuring and gathering access point data. The equipment used included:

HP Pavilion ZD7269CL Laptop Computer
Delorme Earthmate USB GPS

Delorme Earthmate Serial GPS
Apple MacBook Core 2 Duo
Atheros AR5008 Internal Wireless Card ABGN
Holux GPSlim 236
GlobalSat GPS
WISP Router - Mini ITX VIA 533mhz
Linksys WRT54GL v1.1 Wireless Router

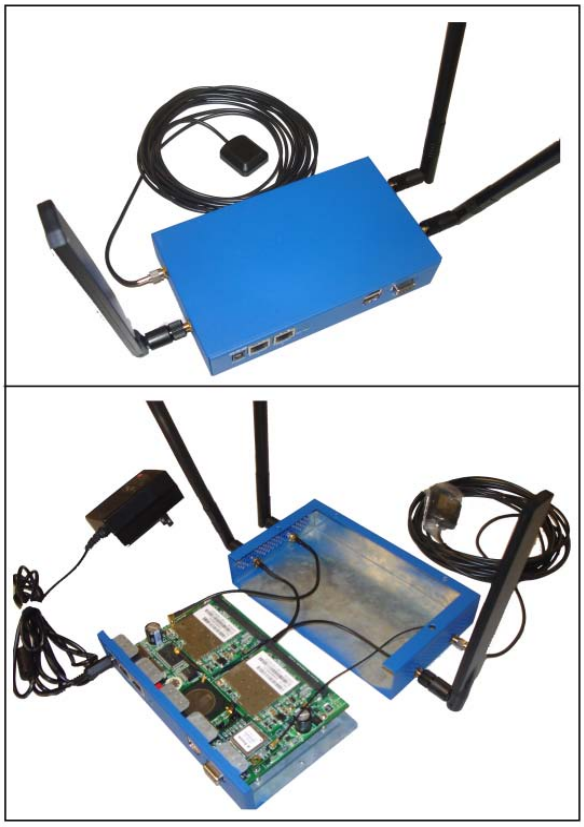
The software used included:

Windows XP Professional, Mac OSX Leopard Desktop, Linux Ubuntu 7.10 Desktop, OpenWRT,
Data Gathering: Kismet Developer's Build, KisWIN, Street Atlas 2007 mapping software
Data Analysis: KNSGem v. 2, Google Earth, Google Microsoft Excel, http://www.gpsvisualizer.com

The students' initial approach was to try to gather access point information using the Netstumbler software in connection with GPS and laptop computers. After a few trials they quickly learned that this type of software was simply not generating enough data for their needs. It also appeared to pose a liability threat as the software actively connected equipment to the wireless access points. Through research, the students found a program called Kismet which is designed to provide a multitude of data by passively listening to radio waves and interpreting the data in the waves. By analyzing the packet headers, the students were able to obtain the information for the statistics and filters they were seeking.

Kismet was originally designed to run on a Linux platform. Through testing the students used several variations of Kismet including KisMAC and KisWin. Unfortunately, they found these programs were either unstable or required the use of a drone in order to make them operate. They also found in testing and research that the amount of data generated from the original Kismet far outweighed the variations.

During testing, the students used several versions of the Kismet software in order to obtain a solid working sample environment. After this they began to solve equipment issues, testing and tuning to find the correct calibration. Initially they used Linksys WRT54G as a Kismet drone. While they were able to obtain data, they realized that the Broadcom chipset did not allow them to get accurate signal readings. They then turned to an Apple MacBook Pro laptop, based on the Atheros chipset in order to scan the channels of the 802.11 a/b/g/n networks. This allowed the team to obtain better signal information for mapping in Google Earth. They also setup an additional WISP Router as a drone to help get better results with the Apple MacBook Pro. After sampling the data they realized that in the car setup, it was easy to miss networks and potential data. Soon there after, they developed a self-contained system that included three wireless radios and onboard GPS. This included a custom built router designed by the student author that allowed more accurate data to be obtained.



The student team established filters and additional information for analyzing data in Google Earth.

Google Earth Filters

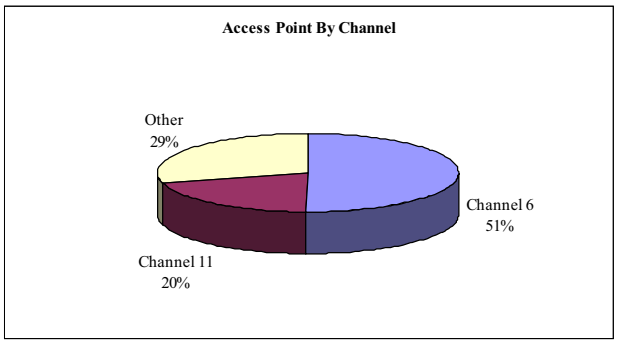
Filter	Description
AP's	This shows where average recorded location of an access point is located
Signal Points	Signal points are each individual point in time in which we saw a particular AP. The more of these that are present, the better the data for the Circles, Averages, and Hulls
Circles	Circles are based off the farthest signal point plotted to the center location of the AP. This gives an approximate range of coverage to any given AP. These are fairly inaccurate since they could be based on AP's that might be picked up from far away but do not have a data coverage near that size. The signal points it uses to createthese are beacon signals, not true data transfer

Averages	Averages are based on the density of the access points, using spherical trigonometry to determine the average shape of what the coverage area looks like. This gives by far the best representation of what the coverage area looks like. By using averages, it drops outliers that would otherwise misrepresent the data.
Hulls	Hulls are simply a connect-the-dot representation of the Signal Points that were plotted. They give a better idea than the Circles, but less accurate than the Averages.

IV. FINDINGS AND RESULTS

The students slowly (approx 10mph) drove every street in the study community gathering data and created a very rich dataset. The students logged over 100 miles of streets. The students found a total of 5423 wireless access points. The access point to person ratio based on the *United States 2000 Census* population figures [8] was 3.69 people per Wi-Fi access point.

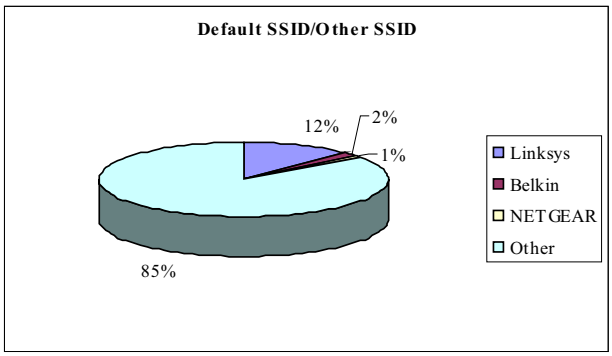
The researchers collected a variety of information on access points. One variable was the channel used by the access point. Over saturation of a channel can cause signal interference. A planned wireless system might alternate channels to reduce signal interference and improve quality. The default channel in most access points is Channel 6. The researchers found that 51% of the access points were still set on this channel.



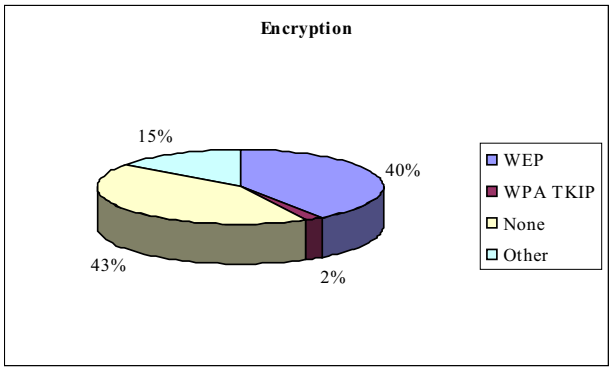
The wireless signals collected allowed the researchers to identify the vendor. They found Cisco/Linksys to be the dominant access point.

Vendor Count	
2Wire, Inc	3
Belkin Corpo	82
Cisco	1050
Enterasys	120
Netgear Inc.	56
Other	767
Trapeze Networks	239

One of the fundamental best practices is changing the SSID [6]. The researchers found that 85% of the users have changed the SSID. It appears that the ISP's have routinely advised users to change the SSID. Another best practice is to use a SSID that does not identify the user [6]. The researchers found that a substantial number named the family, business, or governmental organization operating the access point. The actual number cannot be determined as names could be inaccurate or even decoys, but names like: "311 Ash," "315 W. 6th," "3Chechs," "ABC Seamless," "Andersons," ""Brooks Home Network," etc. appear to identify the location or owners of the network.



A key factor the researchers sought was encryption. Each access point was tested to determine 1) whether it was encrypted; and 2) the type of encryption.

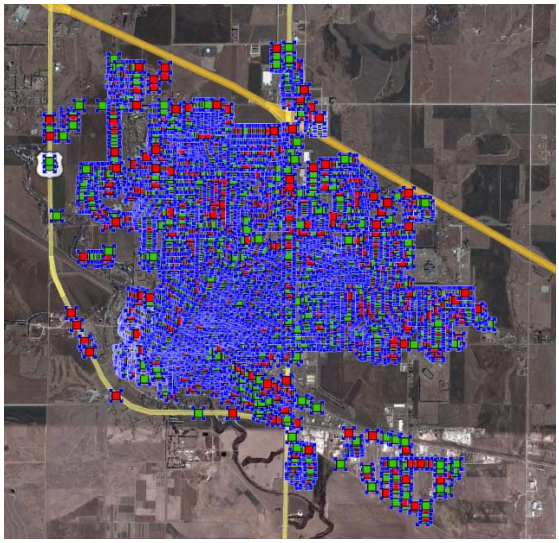


The students found that 43% (2017) of the access point had no encryption. Some access points were intentionally "open access" including wireless "hotspots" in restaurants, coffee shops, the public library, and guest access points at the university. The majority were home access points owned by home owners who were unaware of security vulnerabilities.

They found that 40% of the access points were encrypted using WEP. The students used one of their group member's homes to experiment and to see how quickly they could break the WEP encryption. They utilized open

source tools including Kismet to locate the access point and to obtain generic information. Once they gathered the target information, they captured packets to crack the WEP key. Using the default WEP setting of 64 bit encryption, they cracked the network's encryption in approximately 8 minutes from a car sitting outside the home.

Illustrated Broadcast Signals



Only 2% (111) of the access points were encrypted with WPA and 15% (805) with a method other than WEP or WPA. In all over 80% of the access points were either unencrypted or vulnerable due to their WEP encryption.

In studying two easily identifiable wireless network "best practices," – changing of the default SSID and used of an effective means of encryption -- the students' research clearly showed that a substantial portion of the wireless networks in the study community exhibited vulnerabilities. The most significant of these was the lack of encryption or reliance upon WEP encryption. The students formulated recommendations for their sponsor ISP for carefully communicating this vulnerability to customers and for changing deployment practices when the ISP helps customers set up wireless networks. Key recommendations included:
- Help new customers and upgrading customers change SSID and establish WPA encryption when setting up wireless networks.
- Start a public awareness campaign to inform consumers – particularly those providing their own routers – of basic best practices for wireless security.
- The students provided recommendations to the ISP on how to communicate vulnerabilities to users.

A. Student Lessons Learned

Students, faculty, and the private sector partner all termed this Capstone project a success. From the student and faculty standpoint, this project was primarily valuable because students learned a great deal. They learned about the theory and practice of wireless security, research tools, application of research methods, analyzing data, developing recommendations for a client, and presenting research. It provided a valuable work product that received accolades from the Internet service provider as the research exposed a significant potential problem for consumers. The Internet service provider responded to the information and recommendations of the student research team by proactively helping consumers adopt wireless Internet security best practices, establishing a ticketing database to help alert the ISP's helpdesk of known vulnerabilities, and initiated an educational campaign for customers. These responses have led to changes in processes that will provide greater protection to consumers.

The students who completed this Information Assurance based Capstone project were asked to reflect and to identify what they had learned from the project. Interestingly, the first items identified were learning to work together as a team and to organize and manage their joint efforts. They described learning significant information about Wi-Fi 802.11 wireless networks, network security, the methods used to attack and exploit such networks, the tools used to detect, identify, and measure network data.

The students carefully considered methods of measurement and weighed their ethical and legal responsibilities as they discovered vulnerabilities. They weighed a series of decisions on the type of tools to use for their research. Factors included time efficiency, a limited budget, protection of the public (themselves, their sponsor and the university), ability to gather the types of data sought and their own abilities to design and construct tools that they would use.

The students were pleased that their partner ISP was very interested in their findings and recommendations and immediately took steps to change its practices in order better protect its customers.

B. Faculty Lessons Learned

The faculty involved in the Information Assurance program learned a number of things themselves:
- There are viable student Capstone opportunities in which students can apply knowledge and skills within a semester and complete a meaningful project. Studying best practices and actual application appears to be a very viable type of project. Other projects may include examining equipment or software for vulnerabilities and

effective remediation or protocols, or performing audits of organizations.
- Information Assurance projects may involve more ethical and legal questions than most other Information Networking and Telecommunications Capstone projects.
- Due to technical and legal issues, Information Assurance projects may require more faculty support and interaction than other Information Networking and Telecommunications projects.
- Students benefit from experience in working with a team, self and group-reflective activities, proposal development and report writing, using formal research methods, presentation experiences, and from delving deeper into a and Information Assurance technical subject matter.
- Students justifiably felt significant pride in developing technical solutions and process recommendations for a real client.
- Private sector entities such as Internet service providers may be willing to work in partnership with Information Assurance students on Capstone projects. An established relationship with the academic program, a clear proposal from students, and open line of communication with both the faculty member teaching the class and students appear to have been very important for this successful project. This project appears to exemplify the type of partnerships with private industry that McLester and McIntire [2] advocate.

III. References

[1] Livermore, J, & Poulios, N. (2008). "Integrating a Capstone Project into an Information Assurance Program." *12th Colloquium for Information Systems Security Education*, Dallas, TX, 2-4 Jun. 2008. CISSE/Texas Univ. at Dallas. Dallas, TX. ISBN: 1-933510-96-8, 2008.

[2] McLester, S., & McIntire, T. (2008). The Workforce Readiness Crisis. (Retrieved February 7, 2009) from http://www.techlearning.com/shared/printableArticle.php?articleID=193700630

[3] Cox, S., & King, D. (2006). Skills set: an approach to embed employability in course design. *Education & Training, 48*(4), 262-274.

[4] Geier, J. (2007) *Wireless Network Industry Report 2007* http://www.wireless-nets.com/resources/downloads/wireless_industry_report_2007.pdf (Retrieved January 20, 2008).

[5] Microsoft Website, http://www.microsoft.com/windowsxp/using/networking/security/wireless.mspx (Retrieved February 6, 2008)

[6] Kennedy, S. (2004). Best practices for wireless network security. *Information Systems Control Journal*, 3. http://www.isaca.org/Content/ContentGroups/Journal1/20044/Best_Practices_for_Wireless_Network_Security.htm (Retrieved February 7, 2008)

[7] Ashley, M. (2004). A guide to wireless network security. *Information Systems Control Journal*, 3. http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=19733 (Retrieved February 7, 2008)

[8] United States Census Bureau http://factfinder.census.gov/servlet/SAFFFacts?_event=&geo_id=16000US2031100&_geoContext=01000US%7C04000US20%7C16000US2031100&_street=&_county=hays&_cityTown=hays&_state=04000US20&_zip=&_lang=en&_sse=on&ActiveGeoDiv=&_useEV=&pctxt=fph&pgsl=160&_submenuId=factsheet_1&ds_name=ACS_2007_3YR_SAFF&_ci_nbr=null&qr_name=null&reg=&_keyword=&_industry= (Retrieved February 7, 2008)