Lessons Learned in the Development of a Graduate Certificate in Information Assurance and Security (GCIAS)

Alfredo Cruz, PhD
Polytechnic University of Puerto Rico, Hato Rey, PR, alcruz@pupr.edu

Jeff Duffany, PhD
Universidad del Turabo, Gurabo, PR, jeduffany@suagm.edu

ABSTRACT

The Electrical and Computer Engineering and Computer Science (ECECS) Department at Polytechnic University of Puerto Rico (PUPR) developed a Graduate Certificate in Information Assurance and Security (GCIAS) in 2011. The Certificate is primarily for students who are pursuing a Master Degree in Computer Science or Computer Engineering and for professionals who are working in the area of Information Technology (IT) and wish to broaden their skills and knowledge base in information assurance and computer/network security. The GCIAS is and excellent opportunity for local and federal employees, as well as the private sector. The primary goal of the Graduate Certificate in Information Assurance and Security is to help meet the current and future needs of local and national industry and government by providing a talent pool of professionals with expertise in this area. This Certificate strengthens PUPR's role as a Center for Academic Excellence in Information Assurance Education (CAE/IAE) and the role of the Center of Information Assurance for Research and Education (CIARE) at PUPR. CIARE's main goal is to develop Information Assurance (IA) professionals in areas that are important to national security.

Keywords: Information Technology (IT), Graduate Certificate in Information Assurance and Security (GCIAS), Center of Academic Excellence in Information Assurance Education (CAE/IAE), Information Assurance (IA), Computer and Network Security

1. INTRODUCTION

The Polytechnic University of Puerto Rico (PUPR) currently has a Master in Science in Computer Science (MS CS-thesis option) and a Master in Computer Science (MCS-non-thesis option) in the Department of Electrical & Computer Engineering and Computer Science (ECECS). These Master Degrees are the first and only in Puerto Rico, and have a specialization in Information Technology Management and Information Assurance (ITMIA). Information Assurance is defined as the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. Technology changes rapidly, and computer specialists must continue to acquire the latest skills. IA professionals can enhance their skills and employment opportunities by earning certifications, which are offered through academic institutions, product vendors, computer associations, and other training institutions.

The Graduate Certificate in Information Assurance and Security (GCIAS) highlights the ITMIA specialization and other Master programs at the ECECS Department. It is also an excellent opportunity for other Information Technology Managers, Computer Scientists and Engineers, and other Information System professionals who are working in the development or maintenance of information and secure computer systems or products.

The graduate certificate program focuses on threats and vulnerabilities, cryptography, IT auditing, contingency planning, authentication and access control, security models, data communications, computer and network security, Internet security, trusted computer systems, distributed system security, applications security and security management policies, ethical and legal aspects, among others.

2. GOALS AND OBJECTIVES OF THE GCIAS

The main objective of this certificate is to prepare students in one of the most demanding fields in IT at this moment: Information Assurance and Security (IAS). The main goals of the GCIAS are to:

1. Develop a national/internationally-recognized quality Graduate Certificate Program in Information Assurance and Security (GCIAS).
2. Develop joint research projects in IA between university and industry partnerships.
3. Prepare IT professionals in computer and information security areas, which are of great demand, worldwide.
4. Attract more faculty members with specializations in these areas of great concern.
5. Increase the quality of IAS education, which will lead to strengthening our curriculum and augmenting the quantity and quality of research projects in the areas of information assurance and security.
6. Make PUPR an effective candidate pool for IT Security Managers, Computer Scientists, Engineers, and related positions in Puerto Rico and the Caribbean.

3. PROGRAM JUSTIFICATION

Information assurance and security has actually become an important area of interest in the Information Systems and Computer Science and Engineering fields due to the IT boom of the twenty-first century. The increase in the number of Internet applications and users, combined with the computerization of business processes, has made IAS professions of great demand. Studies have revealed that computer-based criminal activities are costing businesses and government organizations billions of dollars every year. Due to the shortage of information system security professionals there exists a need for comprehensive programs and certificates to educate more individuals in the field of Information Assurance and Security (IAS).

As the US government in general, and the Department of Defense (DoD) in particular, become more dependent on computer networks, systems and software, we become more vulnerable to hostile intelligence gathering as well as computer network attacks. The need for graduate computer scientists specialized in IAS is pervasive in industry, scientific research, academic institutions, business, commerce, appliance manufacturing, and the government (Bishop, 1997; Dark, et al., 2005).

Through formal education and certified training, organizations and Information Assurance (IA) professionals have the opportunity to learn about the many options for improving the cyber protection of intellectual property. As society at large becomes more dependent on technology, the vulnerability to data-driven theft and corruption is greater than ever. We operate in a world where cyber criminals constantly invent sophisticated techniques to threaten and defeat the security of organizations; making it important to track threats as they change and evolve. Organizations need to be informed and prepared to minimize current risks and increase their capacity to recover from incidents that threaten and affect information assets.

PUPR was designated a National Center of Academic Excellence in Information Assurance Education (CAE/IAE) by the National Security Agency and Department of Homeland Security (NSA/DHS) in June, 2009. PUPR is proud to be the first CAE/IAE in Puerto Rico. The partnership between the NSA and DHS was formed in April 2004 and responds to Priority III of the President's National Strategy to Secure Cyberspace, (http://www.whitehouse.gov/pcipb/), February 14, 2003, which directs the federal Government to foster training and education programs to support the nation's cyber security needs, and to increase the efficiency of existing federal cyber security programs. As stated in the Federal Cyber Services Training and Education Initiative Fact Sheet (White House Office of the Press Secretary): "The demand for information technologists and information security specialists has grown faster than the supply. In both the public and private sectors, there is a dearth of qualified new professionals in information security."

With the Master in Computer Science with the ITMIA specialization, the GCIAS, and a Graduate Certificate in Computer Forensics (GCCF) that is under evaluation by the Academic Council at PUPR, there is no doubt that PUPR is strengthening its role as a Center for Academic Excellence in Information Assurance Education

(CAE/IAE). We are also working towards the main goal of the Center of Information Assurance for Research and Education (CIARE) at PUPR; that is to develop IA professionals in areas that are important to national security. The field of information assurance and security is growing at a fast pace; PUPR 's mission is to keep up with the most in-demand academic offerings in science and engineering and make them available to students here in Puerto Rico and the Caribbean. The Center for Information Assurance Research and Education (CIARE) at PUPR considers the GCIAS an important asset for IA education, and will continue to propose new degrees and certificates in related fields of study.

3.1 STUDENT SURVEY

Before implementation, a student survey was done to measure the acceptance of the GCIAS in the campus among students, and to obtain a profile of the students that are actually studying at Polytechnic University in related areas. The main purpose of the survey was to conclude if students who were enrolled in related Bachelors' or Masters' programs at the PUPR were interested in obtaining a Graduate Certificate in Information Assurance and Security (GCIAS) to complement undergraduate or graduate studies.

The student survey questionnaire was administered to 80 students at Polytechnic University, Hato Rey Campus. Gender, age, academic background, status, program enrollment, and employment statistics were obtained from the sample of students. The sample was randomly selected from the ECECS Department program, mainly from the Computer Engineering and Computer Science programs. The questionnaire addressed the student's general opinion and acceptance of the GCIAS and students' consciousness of the need for IAS skills. Of the sample, a total of 85 percent of the students were male and 15 percent female. The feminine sector is a great opportunity for recruitment in IA fields due to the growing participation of this genre in the Island's workforce and academic institutions. There is a need for more feminine participation in computer related fields of study. We at PUPR are committed to produce more feminine role models in related areas of study.

In the survey a high percent of the undergraduate students revealed their interest in continuing additional certificate studies and strongly consider the GCIAS as a promising means for obtaining additional know-how and technical skills that could enhance their IT careers. All of the females interviewed (100%), as well as 98.75 percent of the males revealed a pronounced interest in enhancing their professional skills with additional certificate programs. Please see Figure 1 below:

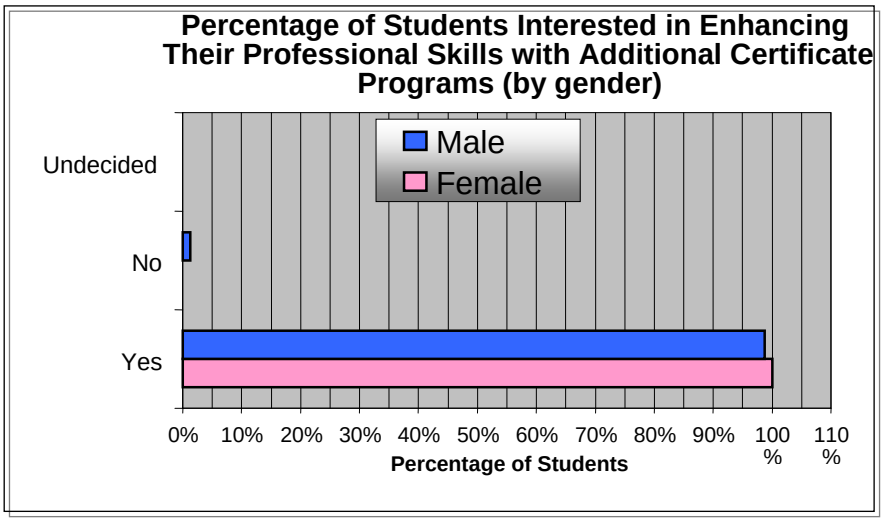

Figure 1: Percentage of Students Interested in Enhancing Their Professional Skills with Additional Certificate Programs

Four key questions were the core of the student survey questionnaire, related to the need for IAS skills and the Certificates' acceptance among students. Question A asked students if they consider information assurance and security an important IT issue. A total of 95 percent of the sample answered yes. Question B asked students if

there are workers specialized in IAS in the company where they work. A total of 46.25 percent answered yes to the question and 35 percent answered no. Question C asks students if they consider that obtaining additional skills in IAS would help them excel in their professional careers. A total of 97.25 percent of the students answered yes to this question. It is clear that most of the students understand the need for obtaining additional IAS skills. Question D asked students if they are willing to enroll in the GCIAS to acquire the additional skills in IAS. A total of 78.75 percent answered affirmatively to this question. This means we already had at least 63 students from the sample that expect to enroll in the GCIAS. This gives us a very positive feedback from students on the enrollment we can expect from our current ECECS students. Results for key questions (A, B, C, and D) can be observed in the Figure 2 below.

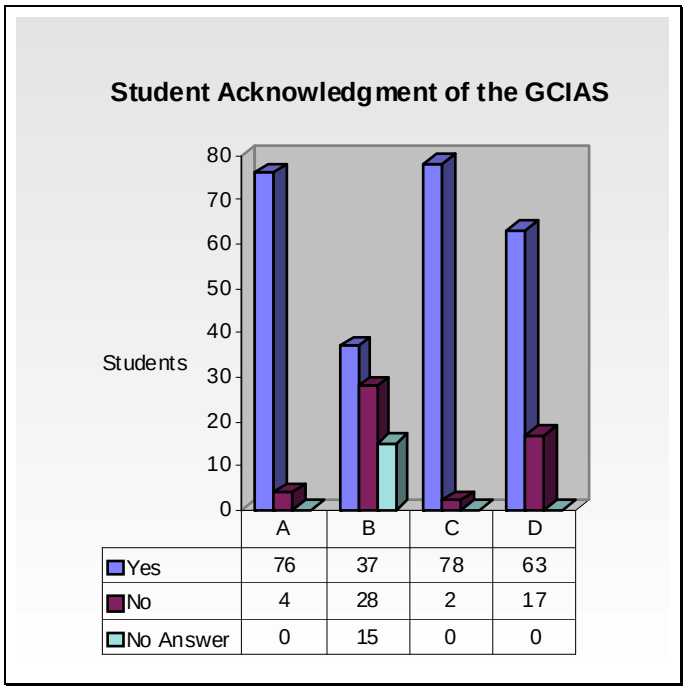

Figure 2: Student Acknowledgement of GCIAS

The students sampled revealed an overall interest in obtaining IAS skills, acknowledging that these skills will give them a competitive edge in their fields of study which are of great demand. The study clearly reflects that most of the students acknowledge the importance of IAS and have the intention of obtaining additional certification and IAS skills. In conclusion, students in related fields of study accept the need to obtain IAS skills to excel in their professions, and they consider the GCIAS an excellent way of acquiring them.

3.2 GCIAS CAREER SKILLS AND OCCUPATIONAL OUTLOOK

Since there is not a common curriculum for teaching IA at universities and colleges, graduates do not have the same skills across different levels of graduate and undergraduate education. IA graduates who come from business backgrounds are more prepared to work on IA policies and procedures, while those with engineering backgrounds could tend to approach IA from a technical design perspective. To help business and industry when hiring security professionals, many job search and research companies such as TechTarget.com offer a more generic classification of levels of IAS professionals:

1. Information Technology (IT) security technicians: These focus on the application of technology to provide security needs at the everyday level. These are mainly IA graduates produced by community colleges and four-year institutions. They support IT and implement policies and procedures.
2. Information Technology (IT) security professionals: Produced by four-year and research schools, these IA graduates have skills in areas such as computer science or computer engineering and also IA training or

certificates. They technically work on computer and network systems, as well as understand and develop the theoretical and/or policy level of security.

3. Security professionals: These include IT security professionals and IA graduates produced by four-year and research schools with broader, and less technical, backgrounds equipped to write or enforce security policies (such as auditors) . They are able to see how security needs to be addressed at a corporate level.
4. Security researchers/engineers: These often earn an advanced degree (i.e. MS or Ph.D) and are produced by research schools. They develop the newest technologies for future product development. They could be the design engineers integrating the security technologies into products, or the mathematicians developing the newest cryptographic algorithm. They are usually hired to perform basic security research, or to enter an academic career.

Employment of information security analysts, web developers, and computer network architects is projected to grow 22 percent from 2010 to 2020, faster than the average for all occupations. As reported by the Bureau of Labor Statistics, U.S. Department of Labor, Occupational Outlook Handbook, 2012-13 Edition (BLS-OOH 2012-13), the Salaries and Growth Outlook expects an increase of 14% for some of the IT careers that require knowledge in Information Assurance and Information Security. According to the BLS-OOH, the IT security workforce had an increase of 27 percent in six months in 2011, as the number of IT security analysts continues to grow steadily; but definitely, not as fast as employers need them. Industry, government, law enforcement, FBI, and Secret Service are among the organizations actually in high demand of IA professionals. Many of these occupations are listed below in Table 1:

Table 1. Expected Growth and Salaries for IA Occupations 2010-2018

Occupation	Percentage of Growth	Salaries
Security Architect	+23.23%	$115,000
Security Engineer	+23.23%	$110,000
Infrastructure Architect	+13.14%	$110,000
Network Security Engineer	+23.23%	$103,210
Infrastructure Engineer	+13.14%	$98,800
Telecommunications Engineer	+53.36%	$82,000
Infrastructure Manager	+16.90%	$80,000
Network Analyst	+53.36%	$72,000
Software Quality Assurance Analyst	+13.14%	$70,000
Infrastructure Analyst	+20.31%	$66,000
Firewall Engineer	+23.23%	$65,000
Software Quality Assurance Tester	+13.14%	$65,000
Telecommunications Analyst	+53.36%	$65,000
Server Manager	+23.23%	$62,920
Telecom Analyst	+53.36%	$62,400
Server Administrator	+23.23%	$60,000
Telecommunications Specialist	+53.36%	$55,000

(Sources: Career Igniter 2011; Bureau of Labor Statistics, U.S. Department of Labor, Occupational Outlook Handbook, 2012-13 Edition)

Due to this progressive growth, there is an urgent need to supply the demand for IA professionals at the local and national level. As stated by the BLS-OOH 2012-13: “The growing emphasis on information security will lead to new jobs.” Another significant fact is that many occupations associated to IA such as Information Security Analysts and others have an unemployment rate of zero percent. Eric Chabrow, Executive Editor of GovInfoSecurity.com shares this information in the article written on July 9, 2011: “Infosec Joblessness Remains

Steady, at 0%". It acknowledges that none of the Information Security Analysts interviewed by the BLS in the United States were out of a job!

The BLS-OOH 2012-13 also states: "Cyber- attacks have grown in frequency and sophistication over the last few years, and many organizations are behind in their ability to detect these attacks. Analysts will be needed to come up with innovative ways to prevent hackers from stealing critical information or creating havoc on computer networks."

The federal government is increasing the hiring of information security analysts to protect the nation's critical information technology (IT) systems. In the healthcare industry, the efficient and secure use of electronic medical records, ensuring patients' privacy and protecting personal data, are exponentially becoming more important. It is likely that more information security analysts will be needed to satisfy client and organizational concerns on laws, privacy, and other ethical issues; as well as to analyze security issues and establish system security and controls. Information security analysts plan and carry out security measures to protect an organization's computer networks and systems. Their responsibilities are continually expanding as the number of cyber-attacks increase. According to the BLS_OOH 2012-13, information security analysts:

- Research the latest information technology security trends
- Monitor their organization's networks for security breaches and investigate a violation when one occurs
- Help plan and carry out an organization's way of handling security
- Develop security standards and best practices for their organization
- Install and use software, such as firewalls and data encryption programs, to protect sensitive information
- Recommend security enhancements to management or senior IT staff Help computer users when they need to install or learn about new security products and procedures

Information security analysts must stay up-to-date on IT security and the latest methods attackers use to penetrate computer systems. They need to research new security technology to decide what methods will be used to effectively protect their organization. This may involve attending cyber-security conferences and seminars to hear other professionals' experiences on new forms of attack.

IT security analysts should also create the organizational disaster recovery plan (DRP), for IT employees to follow in case of an emergency to help the IT department continue functioning. Preventative measures include: regularly copying and transferring data to an offsite location; plans to restore proper IT functioning after a disaster; continually testing the steps in their recovery plans. Because of the critical responsibilities they have to undertake, security analysts usually report directly to upper management. Many work hand-in-hand with the Chief Technology Officer (CTO) to design and test security or disaster recovery systems (Knapp, 2009).

There is also an urgent need to promote information assurance and security skills among women, minorities, and other underrepresented groups. As stated by Eric Chabrow, Executive Editor, GovInfoSecurity.com in his article "Women, Minorities Scarce in IT Security Field Profession Does Not Mirror Rest of American Workforce" (October 11, 2011): "Despite virtually no unemployment among IT security pros, the scarcity of women, African Americans, Latinos and women is highly evident." Information reported by the BLS-OOH 20012-13 states "Whites make up 70 percent of the IT security workforce. Latinos make up about 5 percent of the IT security labor force and women also are underrepresented in the IT security workforce representing about 8 percent". PUPR considers there is an urgent need for academia, the government, and private industries to promote academic programs and certificates in IA such as the GCIAS and the GCCF, for underrepresented groups and minorities.

4. GCIAS CURRICULUM, GRADUATE PROFILE AND FACULTY

4.1 CURRICULUM

The GCIAS provides students and IT security professionals with theoretical components and hands-on-practice in a curriculum that is specially designed to cover the managerial and technical aspects of IAS (Nelson, 2009;

Stallings, 2011; Whitman & Mattord, 2007; Pfleeger, 2006). The certification is composed of 6 key courses (18 credits):

- Data Communication Networks
- Computer Security
- Principles of Information Security
- Contingency Planning
- IT Auditing and Secure Operations
- Law, Investigation and Ethics

4.1.1 COURSE DESCRIPTIONS

Courses descriptions for the Graduate Certificate in Information Assurance and Security (GCIAS) courses:

- **CECS 6005: Principles of Information Security**: This course is an introduction to the various technical aspects of information security and assurance to understand computer, data, and communications security issues. It provides the foundation for understanding the key issues associated with protecting information assets, determining the levels of protection and response to security incidents, and designing a consistent, reasonable information security system, with appropriate intrusion detection and reporting features.
- **EE 6130: Data Communication Networks**: The course covers the fundamentals of data communication networks, including architecture, principles of operations, and performance analyses. It provides a rationale from the engineering standpoint that justifies the way networks are currently structured, and facilitate understanding the issues and tradeoffs faced by designers of future networks. Strong emphasis is provided to understanding algorithms used in networking and their performance impact. Some of the topics included are: multi-layered network architecture, data link layer protocols, high-speed packet switching, queuing theory, LANs, and WANs issues.
- **CECS 7570: Computer Security**: The fundamental tools and techniques for computer security are discussed in the context of the pervasive role and impact that computer technology has over the individual, the enterprise and on society-at-large. Mathematical cryptography fundamentals are covered followed by a set of services built on these techniques, which are then used to provide security at the system and network levels. General models of computer security and intrusion detection techniques are also covered.
- **CECS 6035: Contingency Planning**: This course addresses the managerial issues associated with planning for, and reacting to events, incidents, disasters and crises. It covers organizational awareness, incident response, contingency strategies, disaster recovery, business continuity operations planning, and crisis management. Students will learn the skills to secure current information systems and networks, recognizing and planning for threats and vulnerabilities present in the existing systems.
- **CIS 6015: IT Auditing and Secure Operations**: The course will give students the know-how they need to implement an effective Information Technology (IT) audit. The course covers principles and practice related to the evaluation of secure operations in existing and new information technologies. Core concepts related to security auditing and accountability will be discussed using the standard IT audit approach and contemporary information system auditing concepts. Internet and e-commerce security auditing issues will also be addressed.
- **CECS 6045: Law, Investigation, and Ethics**: This course is intended for students of computer science and other related fields of study who are interested in the IT social and ethical issues that arise from computationally intense environments in the workplace and in society. It addresses computer crime laws and regulations, the measures and technologies used to investigate computer crime incidents and the ethics involved in the use of computers, information systems and technology. Controversies and alternate points of view are addressed on social, legal, philosophical, political, constitutional and economic issues related to computers.

4.2 GRADUATE PROFILE

Students taking the GCIAS courses will learn how to use many of the tools and technologies used in these security related occupations including: Network analyzers or LAN analyzers, Protocol analyzers, authentication server software, identity management and password management software, remote authentication dial-in user service software, Internet directory services software, Network monitoring software, hardware and software auditing software, system testing software, network security or Virtual Private Network (VPN) management software, Intrusion Detection System IDS software; Intrusion Prevention System IPS software; network and system vulnerability assessment software; snort intrusion detection technology, transaction security and virus protection software; stack smashing protection SSP software; and virus scanning software.

On completion of the Certificate students should be able to recognize the physical and logical threats that can affect information assets, and have enough technical knowledge of cryptography and cryptanalysis skills to secure the transmission of critical information and to decrypt coded information. They need to test these systems periodically to ensure the efficient use of these techniques; and identify controls, processes or procedures that can endanger information assets and affect system security, and the actions needed to improve these, relative to the goals of the system. Critical thinking using logic and reasoning is a must to identify the strengths and weaknesses of IT systems and develop alternative solutions, conclusions or approaches to problems related to the security of information assets.

As consultants or service providers, graduates should have knowledge of: principles, standards, ethical and legal aspects, processes, auditing and controls for providing secure operations and IT security services, law and government, legal codes, court procedures, precedents, government regulations, executive orders, agency rules, and the democratic political process. Also could be required to develop customer need assessments, meeting quality standards for services, and the evaluation of customer satisfaction. IA professionals should understand the implications of information assurance and security for both current and future problem solving and decision-making in the development of IT systems and secure IT operations. The GCIAS provides know-how on:

1. IT security management. The knowledge of business and management principles involved in strategic planning, resource allocation, human resources modeling, leadership techniques, production methods, and coordination of people and resources, in order to plan and evaluate secure business operations throughout the organization.
2. Change Management. The knowledge to determine how, when and why a system requires change to improve its effectiveness, and provide its' secure operations. This includes the judgment and decision-making required to consider the relative costs and benefits of the potential actions that are implicated in the changes; to be able choose the most appropriate one. Ability to manage the resistance of employees, managers, and even administrators to changes in both logical and physical controls.
3. Risk Management. The ability to identify and control the risks facing an organization. This includes risk identification to document the security posture of an organizations IT and the risks it faces; and risk control to apply the controls to reduce the risks to data and information systems.
4. Knowledge of IT Auditing. The review of a system; the observation, evaluation, and action taken to ensure secure operations; effective controls for physical and logical security in IT systems. Determine if misuse or malfeasance has occurred.
5. Engineering and technology knowledge of the practical application of engineering science and technology to administer and evaluate security systems. This includes applying principles, techniques, procedures, and equipment to the design and production of various goods and services for secure IT operations and for the evaluation of these systems and products.
6. Telecommunications knowledge of transmission, broadcasting, switching, control, and operation of telecommunications systems.
7. Public safety and security knowledge of relevant equipment, policies, procedures, and strategies to promote effective local, state, or national security operations for the protection of people, data, property, and institutions.
8. Contingency planning, and be able to develop and execute business continuity, disaster recovery, and strategic security plans, and their applications, without affecting business performance.

9. Effective writing and communication skills to disseminate security policies and practices, including awareness on new company policies. Ability to read and understand information and ideas presented in writing, arranging things or actions in a certain order or pattern.
10. Ability toward inductive reasoning in order to combine pieces of information to sense when something is wrong or is likely to go wrong with a system. This does not necessarily involve solving the problem in its initial stage, but recognizing there is a problem and taking actions to correct it.

5. FACILITIES FOR GCIAS STUDENTS

PUPR has modern equipment for research and education currently available for students from the Electrical & Computer Engineering and Computer Science (ECECS) Department programs and certificates. These laboratories have been established in the last six years with grants from the DoD, NSF, NSA, DHS, DE, and local PRIDCO. Some are used for classroom activities and others for graduate research and studying.

The established laboratories are:

- The Data Communication Laboratory and Advanced Network Laboratory
- The High Performance Computing Laboratory (HPC) that includes three PC Clusters and an Altix 350 Supercomputer
- The Windows to the Caribbean Laboratory
- The Turing Laboratory for Graduate Studies
- The Cyber Information Assurance Wireless Lab (CIAW)
- The Cyber Digital Forensics Investigation Laboratory (CDFIL)

All the mentioned laboratories also support research in other basic sciences requiring sophisticated computing facilities. These resources are key components in PUPR's goal to provide IA students and faculty with state-of-the-art infrastructure for their academic endeavors in research and education.

Polytechnic University of Puerto Rico, through various grants for over $150,000.00 from the DOD, DHS, DE, and NSA increased their infrastructure in information assurance and computer forensics by establishing the Cyber Digital Forensics Investigation Laboratory (CDFIL). The Cyber Digital Forensics Investigation Laboratory (CDFIL) is used for analyzing financial frauds, telecommunication frauds, cyber crime, and terrorism investigation, among other activities. This laboratory encourages other institutions to adopt similar models that provide high quality training and further increase the available supply of practitioners prepared in this critical discipline. The laboratory provides real and simulated analysis by gathering digital evidence from computer systems using legally established procedures of computer forensic science. The activities done include: ensuring evidence is not altered, impacting learning of how investigations in forensically sterile environments can be conducted, documenting chains of custody, and logging investigative actions. In addition, this equipment stimulates students to develop new research in IA.

6. FURTHER ENRICHMENT OPPORTUNITIES BEYOND THE CORE CURRICULUM

Students are encouraged to take courses outside of the core curriculum and participate in other activities to enhance their academic experience. Polytechnic offers courses in Network Security and Computer Forensics and special topics courses in Cloud Computing Security and Privacy that students can take towards their Master's degree. The GCIAS program at Polytechnic University also has been designed to prepare students for third party computer security related certifications such as the CISSP (Certified Information System Security Professional) and CEH (Certified Ethical Hacker). Both of these are widely recognized by industry and endorsed by the NSA and the DOD. Polytechnic has faculty that hold both of these certifications who teach in the core curriculum and also teach special topics courses that focus in these areas. The core curriculum for GCIAS program at Polytechnic has been designed to cover all 10 domains in the common body of knowledge required to pass the CISSP exam. Students are encouraged to enrich their academic experience by seeking security-related certifications, attending conferences and seminars and participating in internship programs. Every year Polytechnic has students that participate in summer internship programs at Lawrence Livermore and Oak Ridge National Laboratories.

7. SUMMARY AND CONCLUSIONS

Colleges and universities are beginning to produce more students with degrees in IA. The first schools to teach security courses began in the 1990s, and in 2000 they started offering degree programs in 2000 (SearchSecurity.com, 2012). In 1999 the National Security Agency created the Centers of Academic Excellence (CAE) program as a way to entice a larger number of universities to produce security professionals. Seven schools met the government's criteria the first year, and were designated as charter CAE schools. Since then the number of CAE schools has grown to more than 150, ranging from two-year colleges to graduate degree and research-focused institutions. PUPR is proud to be one of the very few HSI's that has the CAE/IAE designation; actually the first and only CAE/IAE in Puerto Rico and the Caribbean at this moment. But we need more schools in Puerto Rico with this designation to assure that the Island becomes a cadre of IA professionals with state-of-the-art skills in IAS to feed both local and national needs.

The student survey had revealed that a very good percent of the students were interested in continuing additional certificate studies and strongly consider the GCIAS as a promising means for obtaining additional know-how and technical skills in IA. Graduate and undergraduate students acknowledged that IA is a field of great demand in today's workplace in both industry and government. The survey reflected that PUPR students acknowledge the importance and have the intention of obtaining additional certification and skills. Student awareness in IA was noticeable among those interviewed.

The GCIAS is actually attracting people from local and national law enforcement agencies who need the background in this area to enhance their job skills and overall performance. It is providing the necessary exposure to current problems and giving participants firsthand innovative ideas and approaches to troubleshoot them.

ACKNOWLEDGEMENT

This material is based upon work supported by, or in part by, the U. S. Army Research Laboratory and the U. S. Army Research Office under contract/grant number W911NF1110174."

REFERENCES

Bishop, M. (1997). "The State of INFOSEC Education In Academia: Present and Future Directions". *Proceedings of the National Colloquium on Information Security Education.*

Bureau of Labor Statistics (2013). U.S. Department of Labor, Occupational Outlook Handbook, 2012-13 Edition, http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts-web-developers-and-computer-network-architects.htm, 03/03/13. (date accessed)

Dark M., Ekstrom J. & Lunt B, (2005). "Integration of Information Assurance and Security into the IT2005 Model Curriculum". From ACM Database. Retrieved June 2, 2009.

Knapp, K. J. (2009). *Cyber-Security and Global Information Assurance: Threat Analysis and Response Solutions: Advances in Information Security and Privacy Series IT Pro*, IGI Global Snippet, ISBN 9781605663272.

Nelson, B. (2009). *Guide to Computer Forensics and Investigations*. Thomson Course Technology, ISBN 1-43-549883-6.

Stallings, W. (2011). *Cryptography and Network Security*, 5th edition, Prentice Hall, ISBN 0-13-609704-9.

Whitman, M. E. & Mattord, H. J. (2007). *Principles of Information Security*, 2nd edition, Thomson Learning, Inc.

Pfleeger, C. (2006). *Security in Computing*, 4th edition, Prentice Hall, ISBN 0-13-2390779.

Authorization and Disclaimer

Authors authorize LACCEI to publish the paper in the conference proceedings. Neither LACCEI nor the editors are responsible either for the content or for the implications of what is expressed in the paper.