POLYTECHNIC UNIVERSITY
PUERTO RICO

Cybersecurity Programs at a Premier HSI **Polytechnic University of Puerto Rico (PUPR)**

Master of Science in Computer Science (MS CS)

Master of Science in Computer Engineering (MS CpE)

Graduate Certificates in:

Information Assurance and Security (GCIAS)

Digital Forensics (GCDF)

Scholarship/Fellowship Opportunities

Cybersecurity Education at PUPR

- Polytechnic University of Puerto Rico is a key provider of cybersecurity education for students and local faculty and teachers in Puerto Rico.
- The institution is committed to increase cybersecurity education among mainly Hispanic Serving Universities and Community Colleges in Puerto Rico.

Cybersecurity Education at PUPR

- The Institution hosts a competitive graduate IA security program (MS CS ITMIA) and a track in Cybersecurity under the BS CS and BS CpE programs.
    - Two (2) graduate security certificates:
        - Graduate Certificate in Information Assurance and Security (GCIAS);
        - Graduate Certificate in Digital Forensics (GCDF).

All these programs service a large, mainly Hispanic, under-represented student population.

Master in Computer Science

Master in Computer Science has three areas of interest:

- ITMIA – Information Technology Management and Information Assurance
- KDDM - Knowledge Discovery and Data Mining
- CGGT – Computer Graphics and Game Technology

The Master of Science in Computer Science with a Specialization in Information Technology Management and Information Assurance (MS CS ITMIA) covers most of the aspects of Computer Science, IT Management, and focuses on Information Assurance to protect data and information at large organizations.

Master in Computer Science

- Related Jobs:
  - System and Network Administration
  - Database Management
  - Software Development
  - Data Mining and Warehousing
  - Gaming Technologies
  - Network Security
  - Database Security
  - Information Security
  - System Analysis and Design

Master in Computer Science

- PUPR has graduated more than 50 students from the Master of Science in Computer Science in the Information Technology Management and Information Assurance Track (ITMIA).
- Many are now working with the DoD, FBI, CIA, NSA, DHS, MITRE, MIT Lincoln Labs, Sandia Labs, Navy, Oak Ridge, LLNL, DoE, among others.
- This is proof that IA and cyber security education are in great demand in federal organizations, providing career opportunities that are well remunerated.

Master in Computer Engineering

- Master in Computer Engineering has three areas of interest:
  - Software Engineering - Students completing this area can provide consulting services, perform system programming, lead application development, and perform software testing and validation.
  - Internet Engineering - Seeks to develop broad technical skills necessary to develop Internet applications, and tackle issues associated with the internet such as security, e-business, and e-commerce systems.
  - Digital Signal Processing - This area emphasizes mathematical and software techniques to process signals derived from speech, images, natural and other man-made sources

Master in Computer Engineering

- Related Jobs:
  - System Software Engineers
  - Application Software Engineers
  - Computer Hardware Engineers
  - Network and System Administrators
  - Computer System Analysts
  - Computer Scientists
  - Computer Support Specialists
  - Project Leaders
  - Internet & Intranet Developers

Graduate Certificates in Cybersecurity

- The security certifications being offered at PUPR help to capacitate local students and faculty with the skills they need to apply and teach cyber security to IT security professionals from Computer Science, Engineering, Law, Criminal Justice, Business, and other related fields and/or communities of interest.
- These certificates serve as a magnet to attract students from a variety of disciplines to specialize and make them competent in the security job market.
- They also serve as an asset to teach in. Since the Certificates were developed, more than 35 students have received the certificates and 30 more students are currently enrolled in both certificates.

GCIAS and GCDF Courses

Courses in the Certificates cover multidisciplinary fields, such as:

- *CS and Engineering:*
  - Data Communication Networks
  - Network Security
  - Computer Security
  - Principles of Information Security
  - Computer Forensics
  - Advanced Computer Forensics
- *Law:*
  - Law, Investigation and Ethics
  - Electronic Discovery & Digital Evidence
- *Business School:*
  - Contingency Planning
  - IT Auditing and Secure Operations

Graduate Certificate in Information Assurance and Security (GCIAS)

- The GCIAS covers both technical and managerial aspects of IA and Security at the graduate level
- GCIAS Overview:
  - A total of 18 graduate credits (6 courses).
  - Can be completed in 1 year enrolling in two courses each trimester.
  - Can be completed while enrolled in MS CS, MS CpE, MS EE or as a non-degree.
  - Students enrolled in the Master in Computer Science can use these courses as electives to complete the Degree and the Certificate at the same time.

Graduate Certificate in Digital Forensics (GCDF)

- The GCDF covers the highly technical aspects of Digital Forensics including knowledge and skills to protect, detect, recover and mitigate data loss and theft. also has managerial approach to digital and computer forensics.
- CGDF Overview:
  - A total of 18 graduate credits (6 courses)
  - Can be completed in 1 year enrolling in two courses each trimester.
  - Can be completed while enrolled in MS CS, MS CpE, MS EE or as a non-degree.
  - Use these courses as electives to complete the Degree and the Certificate at the same time.

GCIAS and GCDF Course Descriptions

Both GCIAS/GCDF

- *Data Communication Networks* – Knowledge of the fundamentals of data communication networks, including architecture, principles of operations, and performance analyses. Understand multi-layered network architecture, data link layer, protocols, high-speed packet switching, queuing theory, LAN's and WAN issues, among others.
- *Computer Security* – Identify the fundamental tools and techniques for computer security. Impact computer technology has over the individual, the enterprise, and society at large. General models of computer security and intrusion detection techniques are also covered.

GCIAS and GCDF Course Descriptions

GCIAS

- *Principles of Information Security (IS)* – Knowledge in various technical aspects of IS and assurance to understand computer data and communication security issues. Key issues: protecting information assets, determining levels of protection, the design of IS systems with intrusion detection and reporting features, SecSDLC.
- *Contingency Planning* – Secure current information systems and networks, recognizing and planning for threats and vulnerabilities present in the existing systems. Managerial issues associated with planning for, and reacting to events, incidents, disasters and crises. A module to complete a Risk Management Plan will be included in the course.

GCIAS and GCDF Course Descriptions

GCIAS cont..

- *Law, Investigation and Ethics* - Knowledge on the laws and regulations that address most of the underlying issues related to computer security, management, the use of information systems, the Internet, business to business, and e-commerce. Topics include: IT social and ethical issues; computer crime laws and regulations; measures and technologies used to investigate computer crime incidents.
- *IT Auditing and Secure Operations* - Implement an effective Information Technology (IT) audit. Principles and practices related to the evaluation of secure operations in existing and new information technologies. Core concepts related to security auditing and accountability using the standard IT audit approach and contemporary information system auditing concepts.

GCIAS and GCDF Course Descriptions

GCDF

- *Network Security* – Fundamental tools and techniques for network security in the context of the pervasive role and impact that the internet has over the individual, the enterprise, and our society at large. A module in cybersecurity competitions will be included in the course.
- *Electronic Discovery & Digital Evidence* – Upon completion participant will have advanced knowledge on the principles and methodologies of the e-discovery process, understanding the increasing importance of digital evidence in litigation. How corporate computer data and electronic business records can be used as digital evidence in civil and criminal proceedings.

GCIAS and GCDF Course Descriptions

GCDF cont..

- *Computer Forensics* – How to use investigative tools and techniques, and the hardware and software required for computer forensics. Learn how to acquire data and preserve digital evidence for presentation in a U.S. Court of Law.
- *Advanced Computer Forensics* – Forensic knowledge on file system forensics, hard drives, USB drives, removable media, CD-ROMs and flash drives. Learn to access data from cell phones and PDA's, recover deleted data from DOS, NTFS, MAC, and other widely used file systems. Data carving techniques will also be observed. Evidence that previously may have been determined as "unrecoverable" can now be recovered, analyzed and interpreted. Case studies and open source tools will be used.

Scholarship/Fellowship Opportunities from NRC and NSF-SFS at PUPR

- Internships and placement are a critical component of the **NRC** and **NSF-SFS** fellowship and scholarship programs.
- Candidates must pass screening from the ECECS Department
- Required to be an American citizen or permanent resident, 18 years or older.
- GPA of 3.3 minimum at the graduate/undergraduate for NRC
- GPA of 3.0 at undergraduate and 3.30 graduate for NSF-SFS
- Be enrolled in a Bachelor or Master Degree in Electrical Engineering, Computer Engineering, or Computer Science.
- Have to work a paid summer internship at a federal agency
- Students will be provided with work space and state-of-the-art equipment available at the ECECS laboratories.

Scholarship/Fellowship Opportunities

- National Science Foundation CyberCorps Scholarship for Service (NSF-SFS)
  - PUPR was awarded a grant for 2.7 million for a five-year period
  - This federal program aims to strengthen the workforce charged with protecting the nation's critical information infrastructure.
  - The main goal of the program is to build information assurance capacity and provide "an educated cadre of information technology professionals who can help ensure the protection of the US Government information".
  - Increases research, education, and activities in technology areas relevant to information assurance and cyber security.

Scholarship/Fellowship Opportunities

- NSF-SFS cont..
  - Financial Support
    - **Annual Stipends** – Combined or joint Bachelor/Masters program (up to three years) or two year Masters.
      - $22,500 as an undergraduate (one year)
      - $34,000 as a graduate scholar (two years)
    - **Student Travel and Professional Development Allowance** – $4,000.00 per student.
    - **Health Insurance** –Reimbursement allowance of $3,000.00 for each student.
    - **Tuition and Fees Costs** – Yearly tuition support and fees at the rate of 18 credits per year.
    - **Books** - $2,000 for the purchase of text books.

Scholarship/Fellowship Opportunities

- NSF-SFS cont..
  - This program helps to meet the needs of national security (U.S. Government, Federal Civil Service) and an increasing technological society.
  - Increases the intellectual capital of the Federal IA workforce.
  - Contributes to the successful placement of SFS graduates into the U.S. Civil Service to help alleviate the acute shortage of information assurance and cyber security qualified workers.
  - Students have to serve one full year in federal employment for each full or partial year of support.

Scholarship/Fellowship Opportunities

- Nuclear Regulatory Commission (NRC)
  - Provides graduate and undergraduate students with Fellowships and Scholarships:
    - Adequate academic guidance to obtain their degree
    - Involvement of students in research in the area of nuclear engineering or related areas provides new ideas, research directions, and momentum that would other-wise not be possible.
    - For each full or partial year of academic support students have to serve six months in a related employment with: NRC, other Federal Agencies, State Agencies, Department of Energy Laboratories, nuclear-related industries, or academia in the recipient's field of study.

Scholarship/Fellowship Opportunities

- NRC cont..
  - Financial support
    - **Annual Stipends -** The stipend per year for each graduate fellowship is $12,000 and $10,000 for undergraduates.
    - **Tuition and Fees Costs** –Yearly tuition support and fees is provided at a rate of 24 credits per year for graduates and 36 credits per year for undergraduates.
    - **Travel -** is available for students to attend and present at annual IEEE/ACM refereed conferences.

NSA CNAP
Increasing Faculty in Cybersecurity

Through this proposal PUPR will support a total of eight (8) faculty and teachers with tuition, fees, stipends, and books to complete the GCIAS or the GCDF during the one year period.

Program Outcomes of One-Year Project

- By the end of the third trimester eight (8) participants from the selected academic environments are expected to complete the cybersecurity Certificates.
- Five (5) participants will complete the GCIAS,
- Three (3) will complete the GCDF, as initially planned and according to their academic background.

NSA CNAP
Increasing Faculty in Cybersecurity

- These eight (8) educators will increase the candidate pool in cybersecurity education.
- They will be ready to offer in-demand cybersecurity consulting, and education through seminars, workshops, K-12 modules, courses at universities and Community Colleges, among other educational activities where they can share the lessons-learned and their experiences.

NSA CNAP
Increasing Faculty in Cybersecurity

- As a module of the Network Security course, a cyber competition will be planned and hosted by the participants taking the course.
- The competition will bring together at least five different universities/collaborators from Puerto Rico and 30 students/faculty.
- These competitions promote a teaching-learning environment that brings invaluable experiences to the participants. These experiences would not be available through traditional course lectures or laboratory environments.

NSA CNAP
Increasing Faculty in Cybersecurity

- As a module of the Contingency Planning participants will develop a Risk Management Plan.
- By providing cybersecurity education to these participants, we are helping to create the domino effect that empowers the educator to disseminate cybersecurity knowledge and skills to a broader audience. This is key in effective cybersecurity education.
- During and after the year the project is expected to continue impacting hundreds of students from different disciplines through the dissemination of the knowledge acquired by the educators.

CAE IA/CD Designation

- PUPR is one of the few Hispanic Serving Institutions in the Nation recently re-designated as a Center of Academic Excellence in Information Assurance and Cyber Defense CAE IA/CD until the year 2020. This designation is made by the Department of Homeland Security (DHS) and National Security Agency (NSA)
- In the School of Engineering the Department of Electrical and Computer Engineering and Computer Science (ECECS) also teaches information security related courses at the undergraduate level

Polytechnic University of Puerto Rico
Graduate School

Thank you

Dr. Alfredo Cruz
Graduate Program Director