# *Meeting the CAE IA/CD Knowledge Units Requirements for the Polytechnic University of Puerto Rico*

*Diana M. Darabi*
*Master in Computer Science*
*Alfredo Cruz, Ph.D.*
*Electrical & Computer Engineering and Computer Science Department*
*Polytechnic University of Puerto Rico*

***Abstract*** *— The current information security field has gone through tremendous growth over the years and is continuously changing. Today the threats on information security systems are sophisticated, prevalent, have the potential to cause vast damage, and the attackers are not only more skilled and well-funded but the motives have also changed. Because of the current state of the field we must make sure that we have a workforce that is skilled to combat the current threats in order to protect our national information security infrastructure. In an effort to address the current shortage of information security professionals and protect our national information security infrastructure the Center of Academic Excellence in Information Assurance/Cyber Defense was created. In this paper we share our experiences in applying for the Center of Academic Excellence in Information Assurance/Cyber Defense re-designation at the Polytechnic University of Puerto Rico, focusing on meeting the courseware requirements by mapping our curriculum to the CAE IA/CD Knowledge Units. The information provided in this paper will be helpful for institutions applying for the Center of Academic Excellence in Information Assurance/Cyber Defense designation as well as for professionals to identify the knowledge and skills that are important to have to be in an IA profession.*

***Key Terms*** *— CAE IA/CD, Courseware Requirements, Knowledge Unit Mapping, IA Education.*

## INTRODUCTION

The information security field has been forced into rapid change thanks to the increasing security risks we face. When we speak of malware today, it is not just a simple worm or virus. Often times they are more complex and sophisticated types of malware and threats. Cyber criminals are relying more on stealth and encryption and making use of the anonymity afforded to them by anonymous areas of the internet called the "darknet". One threat that makes use of stealth and that prevailed in 2013 was the advanced persistent threat (APT) [1]. An advanced persistent threat (APT) is carried out over a long period of time as it works in multiple phases. The attacker must first break in, avoid detection, and continue to harvest valuable information to carry out the rest of the attack.

Attacks in 2013 were not only well organized and funded, but they came from skilled, highly-motivated, and technologically advanced adversaries [1]. This has caused high financial losses. In 2013, in the US alone, the cost of cybercrime totaled $113 billion [2].

Due to this evolution of the attackers, malware and threats, it has become more important than ever to protect ourselves and the national information infrastructure from these emerging security threats. In order to achieve this protection, we must have a highly skilled workforce that is equipped with the necessary skills and knowledge. However, the demand for skilled cyber security professionals is growing faster than we can train them, and are unable to meet the demand [3]. This, combined with the fact that the majority of the current federal, information security workforce is closer to the retirement age threshold creates a big workforce shortage in the area of cyber security [4].

As a result of the shortage of skilled cyber security professionals, it has become necessary to have more university, college and training programs offer a cyber security curriculum. However, we also

have to have a way of making sure that such programs are high quality and cover all the necessary material to prepare their students for the cyber security workforce.

The National Centers of Academic Excellence in Information Assurance/Cyber Defense (CAE IA/CD) Education Program helps distinguish universities that have a strong IA/CD curriculum. The CAE IA/CD program's goal is to promote higher education and research in the area of information assurance and cyber defense and help increase the number of IA/CD professionals, in order to reduce the vulnerabilities that our national information infrastructure faces [5]. When an educational institution is designated as a CAE IA/CD, it brings credibility to their IA/CD program.

The Polytechnic University of Puerto Rico (PUPR) earned the designation as a National Center of Academic Excellence in Information Assurance Education Program (CAE/IAE) in 2009. PUPR was the first university in the Caribbean and is one of the very few Hispanic Serving Institutions (HSI) to receive such designation. Since then, PUPR has contributed to the IA/CD area by producing IA professionals, promoting research and public awareness in IA, and maintaining collaboration with other universities in IA research and education. The CAE designation must be renewed every five years and PUPR is currently in the process of applying for re-designation as a CAE IA/CD.

This paper will outline the process for applying for designation as a CAE IA/CD, focusing on the courseware requirements and our experiences in the process. In the rest of the paper we give you a justification for this project, information about PUPR and our current IA programs, the CAE IA/CD designation requirements, our experience in mapping the IA/CD Knowledge Units, the CAE IA/CD course of study path at PUPR, the challenges faced along the way, and our conclusions.

## PUPR INFORMATION AND IA PROGRAMS

The Polytechnic University of Puerto Rico (PUPR) is a private, nonprofit, HSI with its main campus located in San Juan, Puerto Rico. It is also the largest private HSI in Engineering in the US. PUPR offers the following four academic disciplines, Engineering, Computer Sciences, Geomatic Sciences, Architecture, and Business Administration. There are undergraduate and graduate programs in all four academic disciplines. PUPR is accredited by the Middle States Commission on Higher Education (MSCHE) of the USA and fully authorized by the Puerto Rico Education Council [6]. PUPR is on a trimester schedule and classes meet four contact hours per week for a three-credit course, for a total of 45 contact hours per trimester. PUPR has a Master's degree in Computer Science with an Information Technology Management and Information Assurance (ITMIA) specialization, and a Graduate Certificate in Information Assurance and Security (GCIAS).

The following two subsections give an overview of the current IA programs at PUPR.

### ITMIA Specialization

The Master's degree in Computer Science is housed in the department of Electrical & Computer Engineering and Computer Science (ECECS) and has three specializations. The ITMIA specialization is one of three specializations.

The Master's degree in Computer Science with the ITMIA specialization has five core courses, (Advanced Design and Analysis of Algorithms, Computational Theory, IT Operations, Advanced Software Architecture, and Software Testing), three area of interest courses (Network Security, Computer Forensics, and Computer Security), and fifteen electives with eight of them being IA courses. There is a thesis option and a project or non-thesis option. The Core and Area of Interest courses are required for both options. The thesis option requires one elective while the non-thesis option requires three electives.

The Master's degree in Computer Science with the ITMIA specialization gives the students the IA

knowledge and skills required to succeed in a career in IA.

### Graduate Certificates in IA

Employers in the Information Technology field are focusing heavily on ways to verify that the candidates have the necessary skills to fill the job openings. With this in mind, the Graduate Certificate in Information Assurance and Security (GCIAS) was introduced in 2010 at the PUPR. Students in the ITMIA specialization can take advantage of this certificate without the need to take additional courses if they choose the electives that are required for the certificate. The certificate is also very valuable for those in other related areas of study or professionals who want to gain IA skills such as Computer Engineers or IT Professionals [7].

The certification is composed of 6 key courses (18 credits) in information assurance and security topics that include technical as well as managerial aspects of IA. The courses required for the GCIAS are: Data Communication Networks; Computer Security; IT Auditing and Secure Operations; Principles of Information Security; Contingency Planning; and Law, Investigation and Ethics [7].

The high demand for IA education motivated the Graduate School at PUPR to propose another Graduate Certificate in IA. The Graduate Certificate in Computer Forensics (GCCF) is geared toward students in the Master of Computer Science or IT professionals who wish to gain knowledge and skills in computer forensics. The GCCF prepares students with skills in investigation techniques and forensics strategies. The certification is composed of the following 5 courses (15 credits) that students must take to earn the GCCF: Computer Security; Network Security; Computer Forensics; Advanced Computer Forensics; Law, Investigation, and Ethics [7].

## CAE IA/CD Designation Requirements

The Centers of Academic Excellence in Information Assurance Education (CAE/IAE) was started by the National Security Agency (NSA) in 1998 and in 2004 the Department of Homeland Security (DHS) joined as a partner. CAE/IAE came about in an effort to protect the national information infrastructure from vulnerabilities. It promotes information assurance in higher education in order to meet the nation's rising need for IA professionals. The Centers of Academic Excellence in Information Assurance Research (CAE-R) was introduced in 2008 and it aimed at promoting IA research at the doctoral level. In order to afford two year institutions, technical schools and government training centers the opportunity to participate in the CAE program, the Centers of Academic Excellence in Information Assurance 2-Year Education (CAE2Y) program was introduced in 2010 [5].

As the field has changed greatly since the original standards were first created, the program has been modified and has new requirements that better reflect the current IA discipline. The program also changed its name to NSA/DHS Center of Academic Excellence in Information Assurance/ Cyber Defense (CAE IA/CD) [5]. The new Knowledge Unit/core curriculum requirements model will make future requirement changes easier to update and to give recognition to those centers with focus areas such as Cyber Investigations, and Secure Mobile Technology, among others [8].

Being a CAE IA/CD-E and IA/CD-R brings recognition to the institutions holding the designation. The designation also makes these centers eligible to apply for scholarships and grants through the Federal Cyber Service Scholarship for Service Program (from NSF) and the Department of Defense Information Assurance Scholarship Program (DoD IASP) [8].

For an institution to be designated a NSA/DHS National Center of Academic Excellence for Information Assurance/Cyber Defense (CAE IA/CD) Education it must meet two sets of requirements:

- Program requirements
- Courseware requirements.

Another important eligibility requirement is that they must hold current regional accreditation as

outlined by the Department of Education. Four-year colleges and graduate-level universities must also be regionally accredited. Institutions must also give recognition to students that successfully complete the CAE IA/CD coursework by some type of formal method such as including it in the transcript or diploma, or providing a certificate [8].

### Program Requirements

The eight program criteria requirements that an institution must meet and demonstrate for the CAE IA/CD program requirements as stated in [8] is as follows:

1. IA/CD Outreach/Collaboration
2. Center for IA/CD Education
3. A robust and active IA/CD academic program
4. IA/CD is multidisciplinary within the institution
5. Practice of IA encouraged throughout the Institution
6. Student-based IA/CD/Cybersecurity research
7. Number of IA/CD/Cybersecurity faculty and course load is sufficient to meet the IA/CD curriculum needs
8. Faculty active in current IA/CD/Cybersecurity practice and research.

These eight criteria must be met and demonstrated in order to meet the program requirements. In addition to the program requirements the courseware requirements must also be met.

### Courseware Requirements

The courseware requirements are based on the new Knowledge Unit/core curriculum requirements model. To comply with the courseware requirements, a center must map to a set of knowledge units (KUs) as follows: a core set of KUs (2 years, 4 years); and for 4 year institutions, choose five KUs from a set of additional KUs. Each KU is composed of a list of required topics to be covered and one or more learning objectives [9].

The core KUs for two year institutions are composed of the following set of eleven KUs.

- Basic Data Analysis
- Basic Scripting or Introductory Programming
- Cyber Defense
- Cyber Threats
- Fundamental Security Design Principles
- IA Fundamentals
- Intro to Cryptography
- IT Systems Components
- Networking Concepts
- Policy, Legal, Ethics, and Compliance
- System Administration

The core KUs for four year institutions include the two year core KUs and the following additional six KUs.

- Databases
- Network Defense
- Networking Technology and Protocols
- Operating Systems Concepts
- Probability and Statistics
- Programming

In addition to the core KUs which are required for all institutions, four year institution must select five optional KUs from a list of forty seven KUs. Two year institutions are not required to map to optional KUs.

There are several ways to fulfill the mapping requirements and a combination of any of the following can be used to map the coursework to the KUs: Course Syllabus, Prerequisite Course(s), Prerequisite Degree, Student Assignments, Modules in a course/collection of courses, and Industry Certifications.

### Focus Areas

The Cyber Defense Focus Areas are an additional element of the CAE IA/CD program. Focus Areas are optional are composed of a set of Core and Optional KUs [9]. The focus areas give recognition to those centers with focus in a list of the following seventeen focus areas:

- Cyber Investigations
- Data Management Systems Security
- Data Security Analysis

- Digital Forensics
- Health Care Security
- Industrial Control Systems-SCADA Security
- Network Security Administration
- Network Security Engineering
- Secure Cloud Computing
- Secure Embedded Systems
- Secure Mobile Technology
- Secure Software Development
- Secure Telecommunications
- Security Incident Analysis and Response
- Security Policy Development and Compliance
- Systems Security Administration
- Systems Security Engineering

Applying for a Focus Area requires that an institution map to additional optional KUs, as each Focus Area requires additional optional KUs [9].

## MAPPING THE IA/CD KNOWLEDGE UNITS

The Polytechnic University of Puerto Rico currently holds the CAE/IAE designation and has a strong IA curriculum. With the support of the administration and the department of Electrical and Computer Engineering and Computer Science we decided to apply for the CAE IA/CD re-designation. We began the process of applying for re-designation in November 2013 (about six months ago) and took on the two sets of requirements separately. The team that worked on the program requirements was composed of Dr. Alfredo Cruz, Associate Director for the department of Electrical & Computer Engineering and Computer Science (ECECS), and Mr. Alexander Lopez, external resource. The team that took on the KU mapping is composed of Dr. Alfredo Cruz, Diana Darabi, Master Student of Computer Science, and Jose Ramon de la Cruz, Adjunct Faculty.

The CAE team provided a set of documents that outlined the requirements for becoming a CAE IA/CD and also gave some guidance. We started working with these documents and asked the CAE team for clarification as we went. We met twice weekly for several hours to work on the course mapping. Having a team which combined has extensive knowledge in the IA field of study and knows about the university curriculum was very important to identify which courses should be used for each KU.

When we started mapping the KUs, we did not have the submission platform available yet and while the requirements documents specifically outlined the topics that should be covered in each KU, they did not give us a specific format in which the information was to be submitted. Hence, our initial mapping was a document with the KU requirements, a list of courses that mapped the KU, and a narrative that explained which topics were covered by what courses. We had one core course but mentioned additional courses that also covered each topic in a KU as to strengthen the mapping. We ended up with a total of sixty two courses that mapped the twenty three knowledge units. We felt that having the number of courses that we do to map and reinforce the KU mapping attested to our strong curriculum.

Once the mapping was complete and the submission platform was ready, we realized that there were additional details required for each course such as a description for each major topic in the syllabus/course outline, where each major topic was covered in the book, among other details and there was no place to simply put our narrative. Therefore, we decided to minimize the number of courses that we used to map the KUs. Also thinking about meeting the program criteria requirement that states that a student must be given recognition for completing the CAE IA/CD course of study, we reduced the courses that we used to map the KUs to twenty.

### Courses Used for KU Mapping

The courses that we used to map the KUs are a combination of undergraduate and graduate courses in the Electrical and Computer Engineering and Computer Science (ECECS) Department as well as the Business Administration Department. The set of courses makes it easy for any graduate student in

Computer Science to obtain the certification of completion of the CAE IA/CD course of study, as most of the undergraduate courses selected are prerequisites for the Master's Degree in Computer Science. The list of courses that we used for mapping the KUs as well as how many KUs each course mapped is detailed in Table 1. The "# of KUs mapped" column is the number of KUs that each course was used to map. For example, the Computer Security course was used in the mapping of six different KUs.

**Table 1**

**Courses used for mapping**

| | Course | # of KUs mapped |
|---|---|---|
| Undergraduate | Computer Networks | 2 |
| | Communication Systems, Simulation & Design | 1 |
| | Probability & Statistic for Engineers | 2 |
| | Computer Programming Fundamentals | 3 |
| | Computer Programming I | 1 |
| | Data Structures | 1 |
| | Network Security | 1 |
| | Operating Systems | 1 |
| | UNIX Administration | 2 |
| Graduate | Advanced Database Systems | 2 |
| | Advanced Design & Analysis of Algorithms | 1 |
| | Computational Theory | 1 |
| | Computer Forensics | 1 |
| | Computer Security | 6 |
| | Data Communication Networks | 4 |
| | IT Auditing and Secure Operations | 2 |
| | IT Operations | 1 |
| | Law, Investigation, and Ethics | 1 |
| | Network Security | 1 |
| | Principles of Information Security | 9 |

As mentioned in the previous section, there are several ways to map to the KUs; we mostly used modules in courses and student assignments to do our mapping. In the next two subsections we outline how we did the mapping for both the core and optional KUs.

### Core KUs Mapping

The cores KUs for 4 Year institutions are composed of the 2 year core KUs and an additional six KUs. The 2 year core KUs seem to be more basic than the additional 4 Year core KUs. Table 2 shows the 2 year KUs and the courses that we used to map each KU. The first column is the KU and the subsequent columns are the courses that we used to map the KUs. To indicate whether a course was undergraduate or graduate, we put the letter U for undergraduate or the letter G for graduate in parenthesis after each course. To indicate that a course was used in the mapping of a KU, we marked the intersection with an "x". As Table 2 shows, one KU could use more than one course for mapping to its topics. An example is the Systems Administration KU which uses five courses for its mapping.

**Table 2**

**2 Year Core Mapping**

| Knowledge Unit | Computer Networks (U) | Probability & Statistic for Engineers (U) | Computer Programming Fundamentals (U) | UNIX Administration (U) | Principles of Information Security (G) | IT Auditing and Secure Operations (G) | Law, Investigation, and Ethics (G) | Data Communication Networks (G) | IT Operations (G) | Network Security (G) | Computer Security (G) |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Basic Data Analysis** | | x | | | | | | | | | |
| **Basic Scripting** | | | x | x | | | | | | | |
| **Cyber Defense** | | | | | x | | | | | | |
| **Cyber Threats** | | | | | x | | | | | | x |
| **Fundamental Security Design Principles** | | | | | x | | | | | | x |
| **IA Fundamentals** | | | | | x | | | | | | x |
| **Intro to Cryptography** | | | | | | | | | | x | |
| **IT System Components** | | | | | x | | | x | | | |
| **Networking Concepts** | x | | | | | | | x | | | |
| **Policy, Legal, Ethics & Compliance** | | | | | x | x | x | | | | |
| **Systems Administration** | | | | x | x | x | | | x | | x |

(U) = undergraduate course, (G) = graduate course

Similar to Table 2, Table 3 shows the courses that we used to map the additional core KUs for the 4 year programs. For each KU there is a list of topics that must be mapped as well as a set of objectives. We must identify where each topic and objective are

covered in our curriculum. The objectives can be mapped to one of the course objectives or a topic covered in the course.

**Table 3**

**Additional 4 Year Core Mapping**

| Knowledge Unit | Computer Networks (U) | Probability & Statistic for Engineers (U) | Computer Programming Fundamentals | Network Security (undergraduate) (U) | Operating Systems (U) | Principles of Information Security (G) | Data Communication Networks (G) | Advanced Database Systems (G) | Computer Security (G) |
|---|---|---|---|---|---|---|---|---|---|
| **Databases** | | | | | | | | x | |
| **Network Defense** | | | | x | | x | | | x |
| **Network Technology & Protocols** | x | | | | | x | x | | |
| **OS Concepts** | | | | | x | | | | x |
| **Probability & Statistics** | | x | | | | | | | |
| **Programming** | | | x | | | | | | |

(U) = undergraduate course, (G) = graduate course

We will use the Introduction to Cryptography KU (2 year core) as an example of a KU mapping. The Introduction to Cryptography KU was mapped to the CECS 7230 Network Security graduate course based on the course outline. Table 4 shows the outline of the Network Security course and it shows a list of topics covered in the course by week and the chapter(s) of the book where the topic is found.

**Table 4**

**Network Security Course Outline**

| Week | Chapter | Topic |
|---|---|---|
| 1 | 1,2 | Introduction/Classical Encryption |
| 2 | 3 | Data Encryption Standard (DES) |
| 3 | 5 | Advanced Encryption Standard (AES) |
| 4 | 6 | Block and Stream Ciphers |
| 5 | 8 | Number Theory - Prime Numbers |
| 6 | 8 | Number Theory – Discrete Logarithms |
| 7 | 9,10 | Public Key Cryptography (RSA) |
| 8 | 11,12 | Message Authentication and Hash Functions |
| 9 | 13,18 | Electronic Mail Security |
| 10 | 19 | IP Security |
| 11 | 16 | Web Security |

After finding where the KU topics aligned with the topics in the syllabus, we prepared the mapping as shows in Table 5 to enter into the platform. Table 5 shows the KU topics and where they were covered in the syllabus. The second column is the topic/week from the course outline where the KU topic is covered.

**Table 5**

**Introduction to Cryptography KU Mapping**

| KU Topics | Where it was covered |
|---|---|
| Symmetric Cryptography | Weeks 1 & 2 – Network Sec |
| Public Key Cryptography | Week 7 – Network Sec |
| Hash Functions | Week 8 – Network Sec |
| Digital Signatures | Week 9 – Network Sec |
| Key Management | Weeks 7 & 8 – Network Sec |
| Cryptographic Modes | Week 4 – Network Sec |
| Types of Attacks | Week 1 – Network Sec |
| Common Cryptographic Protocols | Weeks 10 & 11 – Network Sec |
| DES -> AES | Weeks 2 & 3 – Network Sec |
| Security Functions | Week 8 – Network Sec |

For example, the Symmetric Cryptography topic of the Introduction to Cryptography KU was covered in Weeks 1 and 2 of CECS 7230 Network Security graduate course. In this example, the CECS 7230 Network Security graduate course covered all the topics of the Introduction to Cryptography KU.

### Optional KUs Mapping

As mentioned previously, 4 year institutions must select additional Optional KUs. We chose the optional KUs based on the KU topics that we felt we had a strong curriculum for. We chose the following six Optional KUs: Algorithms; Data Structures; Digital Communications; Digital Forensics; DB Management Systems; and Theory of Computation.

The following are the nine courses that we used to map the Optional KUs requirements: CECS 6605 Advanced Database Systems; CECS 6010 Advanced Design and Analysis of Algorithms; EE 4718 Communication Systems, Simulation and Design; CECS 2200 Computer Programming Fundamentals; CECS 6030 Computational Theory; CECS 2202 Computer Programming I; CECS 7235 Computer Forensics; CECS 3212 Data Structures; and CECS 6130 Data Communication Networks.

Similar to Table 2, Table 6 demonstrates which courses were used to map each of the Optional KUs.

**Table 6**

**Optional KU Mapping**

| Knowledge Unit | Communication Systems, Simulation & Design | Computer Programming Fundamentals (U) | Computer Programming I (U) | Data Structures (U) | Advanced Design and Analysis of Algorithms (G) | Computational Theory (G) | Data Communication Networks (G) | Advanced Database Systems (G) | Computer Forensics (G) |
|---|---|---|---|---|---|---|---|---|---|
| **Algorithms** | | | | | x | | | | |
| **Data Structures** | | x | x | x | | | | | |
| **Digital Communications** | x | | | | | | x | | |
| **Digital Forensics** | | | | | | | | | x |
| **DB Management Systems** | | | | | | | | x | |
| **Theory of Computation** | | | | | | x | | | |

(U) = undergraduate course, (G) = graduate course

As an example of an Optional KU mapping, the Data Structures KU was mapped with the CECS 2200 Computer Programming Fundamentals, CECS 2202 Computer Programming I, and CECS 3212 Data Structures courses.

### Submission Platform

The application to become a CAE IA/CD is submitted through a web based submission platform. The submission platform contains all the instructions and supporting documents that an institution needs to apply for the CAE IA/CD designation. The link titled Apply CAE IA/CD is where the optional KUs are selected, an institution enters the program criteria requirements, the courses are mapped to the KUs and the final application is submitted. Before being able to do the course mapping, we must first enter all the details for the courses that will be used for mapping. This is done in the Add New Courses link.

The general course information that is required for each course is the following:

- Course Designator/ Course Number
- Course Title
- Course Create Date
- Course Review Date
- Course Link
- Course Link Login, if needed
- Course Description (from catalog)
- Is the course currently being taught?
- Course Length (weeks, hours, number of meetings)
- Evaluation Methods
- Instruction Methods
- Current Enrollment
- Past Enrollment
- Course Syllabus
- Course Outline (if different from Syllabus)

Once the general course information is entered, one must also enter each major topic that is covered in the course and the objectives of the course. For each major topic in the course, the following details have to be provided:

- Topic description
- Is the topic material covered in a textbook?
- Is the topic material covered in Supplemental Reading?
- Book name
- Chapter where the material is covered
- Author of the book

Once all the required information for each course is entered, the KU mapping can be done. The KU mapping is done through the Apply CAE IA/CD link. Each KU subtopic can be mapped by selecting from the list of courses entered and from the list of major topics and objectives for each course. Multiple major topics or objectives can be selected for a course and multiple courses can be used. If the KU subtopic is not mapped to a course, a justification must be entered. Once each of the subtopics and objectives of a KU are mapped, a green check mark next to the KU shows that it is complete. When the Program Criteria, Knowledge Units, and Focus Areas (if applying for a Focus Area) are marked as complete, the application can be submitted.

## CAE IA/CD COURSE OF STUDY PATH

As an added benefit for both the CAE IA/CD center and the students taking IA/CD courses, recognition will be given to those students that complete the CAE IA/CD course of study. In order to complete the CAE IA/CD course of study a student must successfully complete the courses that mapped to the entire core KUs and at least five optional KUs. For PUPR, this means completing all the courses outlined in Table 7 or equivalent courses.

**Table 7**
**CAE IA/CD Course of Study**

| | Course | Requirement Met |
|---|---|---|
| **Computer Science/ Engineering Undergraduate** | Computer Networks | Core |
| | Network Security | Core |
| | UNIX Administration | Elective |
| | Computer Programming Fundamentals | Core |
| | Computer Programming I | Core |
| | Data Structures | Core |
| | Operating Systems | Core |
| | Probability & Statistic for Engineers | Core |
| **Computer Science, ITMIA Graduate** | Data Communication Networks | GCIAS/ITMIA Elective |
| | IT Auditing and Secure Operations | GCIAS/ITMIA Elective |
| | Law, Investigation, and Ethics | GCIAS/ITMIA Elective |
| | Principles of Information Security | GCIAS/ITMIA Elective |
| | Advanced Design & Analysis of Algorithms | ITMIA Core |
| | Computational Theory | ITMIA Core |
| | Computer Forensics | ITMIA Core |
| | Computer Security | ITMIA Core |
| | IT Operations | ITMIA Core |
| | Network Security | ITMIA Core |
| | Advanced Database Systems | ITMIA Elective |

Students pursuing the Master's degree in Computer Science and have an undergraduate degree in Computer Engineering or Computer Science will already have most of the undergraduate courses needed for the path such as Computer Programming Fundamentals, Computer Programming I, Computer Networks, Data Structures, Operating Systems, and Probability & Statistic for Engineers. The two other undergraduate courses are electives for the Computer Science and Computer Engineering undergraduate degrees. The remaining courses are part of the curriculum of the ITMIA specialization. Those who wish to get the ITMIA specialization along with the GCIAS would only need to take one additional graduate course.

## CHALLENGES

Applying for the CAE IA/CD designation is a lengthy process and as Bishop points out in [10] the process is time consuming and requires many resources. Having to get more people involved in the process made it a bit more challenging.

One challenge we came across was with the terminology used for some of the KU subtopics. The terminology used was not necessarily the most broadly used. After looking at our text books and materials, we had to research the topics further to determine where they would fit in our curriculum. Therefore, it took longer to map some subtopics. As an example, in the Cyber Threats core KU, one of the subtopics that we needed to map to was Attack Trees. After looking up the topic, we concluded that this material is covered in Risk Management but not specifically using Attack Trees.

It was important to make sure that the courses used indeed covered the material that we thought they should cover. We had more access to the graduate program faculty and material, therefore this was more a concern for undergraduate courses in which some of the KU subtopics were not listed in the syllabus. We had to speak to the instructors that taught the courses and also asked to borrow the text books in order to identify where in the book the material was covered. For some of the courses, we had to meet with the curriculum committee to make sure that the topics we needed were covered in the courses we identified. If the topics were covered and it was a simple change, we asked that they added the topic to the syllabus. The Unix Administration course which we used to map the Systems Administration KU is an example of this. After speaking with the course instructor we learned that the OS security concepts were taught in

the course, but they were not specified in the syllabus. After evaluating our request, the committee agreed to include the information in the syllabus.

A challenge that we foresee some institutions will face will be meeting the courseware requirements if they do not have a Computer Science or Computer Engineering program as many of the KUs focus on Computer Science/Engineering topics. This might leave out some institutions that are eligible to apply but are not able to meet the criteria. This might yield more developer type professionals but might leave out the IT professional with the soft skills such as leadership, and communication skills that are also of great need in IA/CD.

Overall, the challenges we faced were all worked out and the only way they affected the process was that it slowed down our progress.

## SUMMARY

This paper presented the process for applying for the CAE IA/CD designation and our experiences in the application process at the Polytechnic University of Puerto Rico. In applying for re-designation as a CAE IA/CD we gained great insights into the current state of the information assurance field. Along the way we learned which skills the government sector is in need of and finds important to have in a skilled cyber security professional. In the process, we also got to assess our own curriculum and identify where our IA/CD curriculum strengths are and where we need further improvement. Although it was a very lengthy process, applying for the re-designation as a CAE IA/CD was straight forward and a great learning experience. We hope that this information will be of use to those who wish to apply for the CAE IA/CD designation.

## ACKNOWLEDGMENTS

This material is based upon work supported by the Department of Defense, Information Assurance Scholarship Program. The present work benefited from the input of Dr. Alfredo Cruz, PhD, Associate Director for the ECECS Department, and Jose Ramon De la Cruz, Adjunct Faculty, who provided valuable assistance and ideas to the undertaking of this project.

## REFERENCES

[1] Sophos, Ltd, "Security Threat Report 2014", 2014. Retrieved from: www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf.

[2] Symantec Corporation, "2013 Norton Report", 2013. Retrieved from: www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013.

[3] "2013 (ISC)² Global Information Security Workforce Study", (ISC)² Foundation, 2013. Retrieved from: www.isc2cares.org/IndustryResearch/GISWS/.

[4] National Initiative for Cybersecurity Education, "2012 Information Technology Workforce Assessment for Cybersecurity (ITWAC) Summary Report", 2013. Retrieved from: www.niccs.us-cert.gov/sites/default/files/documents/files/2012%20ITWAC%20Summary%20Report_Final.pdf.

[5] National Security Agency, "2013 National Centers of Academic Excellence in Information Assurance Designees Announced", 2013. Retrieved from: www.nsa.gov/public_info/press_room/2013/academic_excellence_designees.shtml.

[6] Polytechnic University of Puerto Rico, "About PUPR", 2014. Retrieved from: www.pupr.edu/about/.

[7] Cruz, A. & Bonilla, S., "Experience Learned in Obtaining the CNSS IA Course Certification and the CAE/IAE designation at Polytechnic University of Puerto Rico (PUPR)", *in Proc. 10Th Latin American And Caribbean Conference For Engineering And Technology*, Panama City, Panama, 2012.

[8] *National Centers of Academic Excellence in Information Assurance/Cyber Defense (IA/CD) Education Program Criteria for Measurement*, CAE Program, 2013.

[9] *National NSA/DHS Centers of Academic Excellence in Information Assurance/Cyber Defense Knowledge Units*, CAE Program, 2013.

[10] Bishop, M. & Taylor, C., "Critical Analysis of the Centers of Academic Excellence Program", *in Proc. 13Th Colloquium for Information Systems Security Education*, Seattle, WA, 2009.