Meeting the Criteria for a Center of Academic Excellence (CAE) in Information Assurance Education

Dino Schweitzer, Jeffrey Humphries, Leemon Baird
Academy Center for Information Security
United States Air Force Academy
acis@usafa.af.mil

ABSTRACT
Information assurance is a critical topic in computer science curricula. Several publications in the educational literature address the development of curriculum and integration of information assurance into existing computer science programs. One objective measure of a successful program is to be designated by the government as a National Center of Academic Excellence in Information Assurance Education. To receive this designation, the applicant must meet documented criteria about their program and institution. Meeting these criteria can be challenging, especially for undergraduate-only institutions. This paper describes our institution's approach and experience in successfully meeting the necessary criteria for receiving the Center of Academic Excellence designation.

Categories and Subject Descriptors
K.3.2 [**Computer and Information Science Education]**
Computer science education

General Terms
Security

Keywords
Information assurance, information security, curriculum

1. INTRODUCTION
There has been a great deal of emphasis in recent years on the importance of information assurance (IA) in higher education. This emphasis is a result of an increased awareness of security issues and vulnerabilities, expanded resources for IA research, an increasing number of highly publicized attacks on vulnerable systems, and an increasing awareness of computer-related privacy issues. As a result of this emphasis, much has been published on how to effectively integrate IA into existing curricula [13,15], how to set up new programs and concentrations in IA [2,3,4], and successful classroom and laboratory experiences in teaching specific IA topics [7,14,16]. The Colloquium for Information Systems Security Education (CISSE) was founded in 1997 to provide a forum for promoting information security in higher education (www.ncisse.org).

At the Air Force Academy, information security has been an integral part of our computer science curriculum for almost a decade. We have taught IA topics in several of our standard CS courses, and have created specific courses in cryptography, information warfare, and information security. Our motivation has been both the increased security emphasis within general computer science education, as well as preparing our students for their future role in protecting the nation. Part of the educational experience we provide cadets is based on current Air Force needs and issues. Information security has been one of the top priorities of the Air Force in recent years due to the critical role it plays in all aspects of every mission.

Measuring the effectiveness of integrating IA into a curriculum and determining whether it is receiving sufficient coverage is mostly subjective. There is no hard requirement for teaching IA in an ABET-accredited computer science program [1]. ACM's Computing Curricula 2005 lists security as a knowledge area for undergraduate computing programs without identifying specific topic areas [5]. One objective measure of success is receiving designation as a Center of Academic Excellence in Information Assurance Education (CAE) from the National Security Agency (NSA) and the Department of Homeland Security (DHS). The Air Force Academy applied for CAE designation in 2004 based on our IA curriculum and activities, and was awarded the designation for academic years 2005 – 2008. Our experience in going through the process highlighted requirements which were a challenge for us to meet, partly due to our status as a service academy, and partly as a result of being a strictly undergraduate institution. This paper addresses how we successfully met those challenges. This experience may be useful for other undergraduate institutions pursuing the CAE designation.

2. THE CAE PROGRAM
The National Centers of Academic Excellence in Information Assurance Education Program is jointly sponsored by NSA and the DHS in support of the President's National Strategy to Secure Cyberspace, February 2003 (http://www.whitehouse.gov/pcipb/). The designation is open to nationally or regionally-accredited four-year colleges and universities for their graduate and undergraduate programs. The benefits to the college or university include formal recognition from the United States government, associated prestige and publicity opportunities, and eligibility to apply for government Information Assurance Scholarship Programs (http://www.defenselink.mil/nii/iasp/). Although the designation of CAE does not carry a commitment of funding for IA research from NSA or DHS, it does serve as a measure of institutional credibility when applying for research funding. In addition, the designation serves as an objective third-party

measure of the quality of the IA program and activities in place. The motivation for the government to provide such recognition is to assist in meeting the national demand for professionals with IA expertise, and to encourage independent research in critical IA areas.

To successfully qualify for the CAE designation, institutions must:

a) possess current certification under the Information Assurance Courseware Evaluation Program, and
b) clearly demonstrate through documentation how they meet ten program criteria

Successful meeting of the criteria is based on a scoring system with points awarded for certain specific activities within the scope of the criterion. Each criterion has a minimum required score. The criteria for the CAE designation are:

1. Partnership in IA education with minority colleges and universities.
2. Evidence that IA is not treated as a separate discipline, but as a multidisciplinary science.
3. The academic program demonstrates how the university encourages the practice of IA.
4. The academic program encourages research in IA.
5. The IA curriculum reaches beyond the normal geographic borders of the university.
6. Faculty is active in current IA practice and research, and contributes to IA literature.
7. The university library or the IA Center maintain state-of-the-art IA resources.
8. The academic program has declared IA concentrations.
9. The university has a declared center for IA education or a center for IA research from which IA curriculum is emerging.
10. University IA faculty consists of more than one individual devoted full time to IA.

www.nsa.gov/ia/academia/caeCriteria.cfm?MenuID=10.1.1.2

It is important to note that these criteria are subject to change and that the following discussion is based on the criteria that were in place at the time of our application for the CAE designation. Application for the CAE designation is made online by December of each year. Applicants must clearly demonstrate how each of the ten program criteria are met with supporting documentation where required. As of the writing of this paper, 65 colleges and universities have received the CAE designation (www.ncisse.org).

3. MEETING THE CRITERIA

The Academy made the commitment to apply for the CAE designation in the summer of 2001 (three years prior to when the application was actually made). The motivation for doing so was based on several factors. Several faculty members had been engaged in IA research activities in their advanced degrees and Air Force duties, and had continued their pursuits as part of their faculty development. In addition, the academy, and specifically the Computer Science department, has been a long term partner in IA research with the NSA through a Visiting Professor program. Part of the purpose of this relationship is to strengthen IA awareness and education at the service academies. The department was also interested in growing their research capability and chose IA as an area that was an important research area for the Air Force, an area in which there was faculty expertise, and an area that was well-suited for research funding.

Some of the challenges in meeting the criteria resulted from the unique nature of service academies as being both academic and military installations. There were also a number of challenges as a result of being a strictly undergraduate institution. Although the criteria for the designation explicitly states that undergraduate institutions are eligible to apply, some of the requirements are better suited for a program that has an active graduate research program in place. The specific challenges and how they were addressed are described below.

3.1 IA Courseware Evaluation

The first requirement for being awarded the CAE designation is that the IA courseware being taught must be certified under the National IA Education and Training Program (NIETP). The NIETP serves as the National Manager for IA education and training related to national security systems. They develop IA training standards with the Committee on National Security Systems (CNSS) based on the National Training Standard for INFOSEC Professionals. These standards are documented in five publications [8,9,10,11,12].

The CAE certification process requires that a list be submitted that shows how each of a long list of learning objectives can be met by some course or courses offered by the applicant. The list of objectives comes from concatenating the NIETP certification standards plus additional requirements. In some cases, the objectives appeared to be more appropriate to a technical training and certification program than to an undergraduate Bachelor of Science program.

To meet this requirement, the Air Force Academy listed a number of computer science courses, especially those related to information assurance. However, the list also included a large number of courses outside our major. As an example, for an objective dealing with the laws relating to network monitoring, the list included two law courses. For objectives dealing with INFOSEC contingency plan preparation, it included several of our military training programs in which the cadets are engaged during the summers. For objectives such as good password selection, it included "LOCAL TRAINING", referring to training that the cadets receive outside the classroom related to use of their computers.

One of the challenges for any academic institution in this evaluation is that the standards were developed for INFOSEC training, not academic education. However, the Academy's focus on active learning helped alleviate this concern to a great extent. Activities can be chosen to support the overarching educational goal while providing practical training at the same time. This idea gave rise to the current instantiation of our Design of Secure Networks course. While the course has educational goals to instill critical thinking and formal consideration of secure network design, the students participate in the inter-academy competition known as the Cyber-Defense Exercise [6]. This exercise provides intense training in many of the areas covered by the CNSS

standards while coursework before and after the exercise can emphasize educational goals.

An additional course in which the technique was applied only by happenstance is found in the Academy's core civil engineering course covering the design of air bases. While the educational goals of the course are specific to civil engineering, the students are given very practical training in aspects of operational security unique to air base design. They consider and explore options to disguise the mission of a base.

The active learning approach seems to be the best fit in enhancing the information assurance curriculum. Using specific contexts to allow students to explore larger educational goals is promising. The most challenging area for the computer science curriculum has been in the area of formal models of access control – which are included in some of the standards and show a very good direction for future standards. We are still seeking effective active learning projects for formal access control models.

3.2 Partnership with Minority Institutions

The first of the ten criteria after getting the school's curriculum certified is the requirement for partnership with a minority college or university. As defined by the Department of Labor, this includes Historically Black Colleges, Hispanic Serving Institutions, and Tribal Colleges and Universities (www.dol.gov/osbp/programs/mcu.htm). The specific activities to demonstrate such a partnership include:

- Shared curriculum
- Shared faculty
- Reciprocity of credits

Meeting this requirement can be a challenge if the applying institution does not have an existing relationship with a minority-designated institution. While the shared curriculum is easy to meet by simply providing materials, it alone does not provide enough "award points" to meet the overall requirement. At the Air Force Academy, this requirement is especially challenging since shared faculty and reciprocity of credits cannot be done directly under the congressionally mandated mission of the academy. The way that we met this requirement was to establish "IA partners" with other academic institutions including minority ones. This partnership included sharing of curriculum, faculty visits with partner members to discuss IA related issues, and ongoing collaborative IA activities. These activities met the intent of the criterion in sharing ideas and resources in IA education with Historically Underrepresented Universities and Colleges.

3.3 IA in Other Disciplines

The second criterion is a requirement that IA be treated as a multidisciplinary science and that IA topics appear in various disciplines. The required evidence of this include:

- IA is taught to non-technical / non-IA students
- IA programs require non-technical courses of study

The second element of evidence is relatively easy for most institutions that have graduation requirements outside of the discipline. Once again, satisfying that requirement is not a sufficient number of "award points" to fully meet the criteria. The first evidence can be more challenging in institutions that have little influence in topics taught in other disciplines. For example, convincing the political science department to teach topics in information assurance may be difficult to achieve. On the positive side, IA topics are becoming common material across many disciplines, and there are likely several examples that can be found without explicit coercion. Since the criteria do not specify the exact topics that must be taught, a wide range of possibilities exist. For example, a mathematics department may be teaching a cryptology or cryptology-related course. Current issue classes are likely teaching topics in privacy and computer crime. To further encourage IA in other disciplines, it may be advantageous for the applying program to offer to provide topic-specific IA educational materials for other disciplines to use.

At the Air Force Academy several disciplines were already teaching IA-related topics as part of existing courses. We have also worked closely with other departments to provide IA material specific to their discipline. For example, we are currently working with the Law Department to assist in putting together a special topics course in computer forensics and cyber-law.

3.4 Practice of IA at the University Level

This criterion establishes the requirement that IA practices are not simply taught, but are in place in the institution. Specific evidence includes:

- University or department IA security plan
- IA Awareness Program for faculty and students
- University appointed Information Systems Security Officer

Once again, at a government institution with stringent security requirements, such as the Academy, these criteria are easy to meet. At other academic institutions, however, the amount of awareness and commitment to IA at the institutional level may be more challenging. To meet this requirement, the individual department can create its own security plan and create an online IA awareness program that is made available to all faculty and students in the institution. In fact, going through the CAE designation process provides an opportunity to raise institutional awareness of IA as a serious issue and encourage greater emphasis if necessary. It is likely that IT offices at most universities have some plan already in place regarding the security of the school's infrastructure. These plans may be sufficient or may need to be revised to meet the CAE criteria.

3.5 Research in IA

Two of the ten criteria (4 and 6) specifically address IA research for the CAE designation. The first of these require evidence of IA research or projects as part of the IA curriculum and evidence of courses outside of the IA program encouraging IA projects. This requirement can be easily met if the program is project-oriented, or if it is a graduate-level program with evidence of IA theses and dissertations. For a non-project oriented undergraduate institution, this criterion can be more challenging. At the Air Force Academy, our required IA courses have student projects

and we have encouraged other disciplines to promote IA-related topics for their required projects.

The second research criterion has to do with faculty currency in IA research and publishing. The evidence includes IA-related publications in refereed journals, grants, and presentations at national conferences. This requirement can be a challenge to meet in a teaching-centric undergraduate institution that does not have a research focus nor research grants. The level of research does not have to be solely "hard core" research topics in security, but can also include topics such as IA education, curriculum development, and experiences in the IA laboratory and classroom. The requirement for the number of publications or presentations is to collect enough points (two per paper/presentation) to meet the minimum point requirement for this criteria (20). The criterion does not explicitly state the time frame for this research, e.g., the publications do not have to all have appeared in the past year. In general, if a program cannot point to specific IA research results by faculty it will probably not be able to achieve a CAE designation.

IA research at the Air Force Academy has been a combination of basic research in the areas of cryptology, network security, and biometrics as well as more education-related IA research in course development and laboratory experience. Research is performed by faculty and students in support of IA courses, independent student research projects, and as part of individual faculty overall professional development.

3.6 IA Beyond the Borders

In addition to the internal program for IA education, there needs to be evidence of the IA curriculum extending beyond the university boundaries. Specific evidence of this include:

- IA curriculum web site
- Distance delivery of IA courses
- Sponsorship of regional or national IA workshops, etc

The first evidence is straightforward and would be a natural part of any IA program web presence. However, similar to other criteria, it alone does not suffice to meet the overall requirement. The second piece of evidence may also be straightforward if the institution has an existing distance education capability that IA courses would fall naturally within. However, if an institution, such as ours, does not have a charter to provide such capability, the efforts to create and manage an online set of IA courses could be prohibitive. In our situation, it was easier, and more effective, to focus on the third evidentiary element. We organized and hosted a day-long regional workshop on IA topics. By inviting local educational institutions in the surrounding region, this had the benefit of meeting other IA faculty and researchers, and awareness of their institutional efforts in this area. As a result, follow-on collaboration has been initiated.

3.7 IA Reference Material and Resources

This criterion is perhaps the simplest to meet. The specific requirements are for access to both current textbooks, monographs, reports and journals, as well as historical IA documents. Any fully established educational institution should have the necessary online access for faculty and students to IA reference material. There is no hard requirement for a local collection, either hard copy or electronic, although the applying institution may find it beneficial to have local IA reference material available to their students.

3.8 Declared IA Concentration and Center

There must be an official recognition of a declared IA concentration and there must be an official designation at the school or university level for a center of IA research or center of IA education. These are all-or-nothing requirements. The concentration requirement is at the BS, MS, or PhD level with an increasing number of "award points" at each level. For an undergraduate-only institution to satisfy this requirement, it must have the concentration in place and must have graduated students with the concentration over the previous two years. This requirement is significant if a program is just beginning and could delay CAE designation until students have graduated with the concentration. For institutions with graduate-level concentrations, it is possible to achieve the minimum required point total without having graduated students. At the Academy, we have had an IA concentration in place for our CS majors for several years.

The evidence for an IA center of research or center of education requires a charter signed by the appropriate approving body at the institution. Other than the existence of the center, the criteria does not specify the size, nature, or required activities of the center. As a result, there is a great deal of flexibility in how it is structured, what its charter is, and how it fits into the IA program.

At the Air Force Academy, the center requirement was met by forming an officially chartered Academy Center in Information Security (ACIS). The mission of the center is to promote faculty and student research in IA topics for national defense applications. The center recently hired a full-time Director and is in the process of investigating IA projects and funding opportunities. The primary research resource will initially be faculty with student involvement. Additional research staff may be added as projects and funding allow.

3.9 More than One IA Faculty

The final criterion for the CAE designation is that there be more than one individual responsible for IA education. Points are awarded for a faculty member working full-time in IA with overall responsibility for the IA program, as well as other full-time or part-time faculty working in IA. The criteria allow for shared and cross-departmental appointments as well as agreements for cooperative use and exchange of faculty between institutions. This criterion should be straightforward to meet in an institution with a commitment to an IA focus in their program.

4. SUMMARY

Information assurance is and will continue to be an important topic of computer science research and education for the foreseeable future. Well-rounded CS curricula will incorporate IA topics in existing courses as well as separate courses focused on specific IA areas. There is a lot of reference material available on how to effectively implement such integration. If a school chooses to focus on IA, either as a research or academic emphasis, there are advantages to receiving the designation of a Center of Academic Excellence in IA Education. It provides credibility of the program, opens up additional opportunities for funding and scholarships, and serves as an independent measure of the quality of the IA program within the institution. The criteria and

application process for a CAE designation is straightforward. However, depending on the circumstances of the institution, there may be challenges in successfully meeting the criteria.

Two overarching lessons stand out from our experience. First, to receive the CAE designation, a program must have institutional support and commitment. An individual department that teaches IA cannot receive the designation based strictly on their curriculum, faculty, and research. Several of the criteria specifically address requirements outside of the direct control of the applying program, such as university practices in IA, IA in other disciplines, and the official designations for an IA concentration and an IA center. In addition to the institution's commitment of resources to support an IA program in terms of sufficient faculty, it must be willing to demonstrate a university-wide commitment to IA.

The second lesson learned was that the process can take a significant amount of time. The time to put a program in place and to graduate students with an IA concentration can be several years. In addition, the time to prepare the application for CAE designation was significant. We spent a great deal of time researching other disciplines for IA-related material, mapping the IA curriculum to the necessary standards, and working with the institutional administration to put the necessary concentration and center in place. It is not a process that can be achieved quickly.

The Air Force Academy was able to effectively address the challenges of receiving the CAE designation. We are excited about expanded opportunities in IA research with our newly formed center and we remain fully committed to education and research in information assurance topics.

5. ACKNOWLEDGEMENT

The process of applying for the CAE designation took a significant amount of time and effort on several individual parts. We are especially thankful for the contributions of Mr. Michael Collins, our NSA visiting faculty member.

6. REFERENCES

[1] ABET, Criteria for Accrediting Computing Programs found at: http://www.abet.org/Linked%20Documents-UPDATE/Criteria%20and%20PP/05-06-CAC%20Criteria.pdf.

[2] Azadegan, S., Lavine, M., O'Leary, M., Wijesinha, A., and Zimand, M. 2003. An undergraduate track in computer security. In *Proceedings of the 8th Annual Conference on innovation and Technology in Computer Science Education* (Thessaloniki, Greece, June 30 - July 02, 2003). D. Finkel, Ed. ITiCSE '03. ACM Press, New York, NY, 207-210.

[3] Bacon, T. and Tikekar, R. 2003. Experiences with developing a computer security information assurance curriculum. *J. Comput. Small Coll.* 18, 4 (Apr. 2003), 254-267.

[4] Crowley, E. 2003. Information system security curricula development. In *Proceeding of the 4th Conference on information Technology Curriculum* (Lafayette, Indiana, USA, October 16 - 18, 2003). CITC4 '03. ACM Press, New York, NY, 249-255.

[5] Computing Curricula 2005 found at campus.acm.org/public/comments/Draft_5-23-05.pdf

[6] Haynes, A. and Stratton, T. Cyber Defense 2003 & Information Assurance Education. In *Proceedings IEEE 2003 International Conference on Systems, man & Cybernetics*. Oct 2003.

[7] Mattord, H. J. and Whitman, M. E. 2004. Planning, building and operating the information security and assurance laboratory. In *Proceedings of the 1st Annual Conference on information Security Curriculum Development* (Kennesaw, Georgia, October 08 - 08, 2004). InfoSecCD '04. ACM Press, New York, NY, 8-14.

[8] NSTISSI-4011 - INFOSEC Professionals, National Training Standard. Jun. 1994.

[9] NSTISSI-4012 - Designated Approving Authority, National Training Standard. Jun. 2004.

[10] NSTISSI-4013 - System Administrators in Information Systems Security, National Training Standard. Mar. 2004.

[11] NSTISSI-4014 - Information Systems Security Officers (ISSO), National Training Standard. Apr. 2004.

[12] NSTISSI-4015 - System Certifiers, National Training Standard. Dec. 2000.

[13] Petrova, K., Philpott, A., Kaskenpalo, P., and Buchan, J. 2004. Embedding information security curricula in existing programmes. In *Proceedings of the 1st Annual Conference on information Security Curriculum Development* (Kennesaw, Georgia, October 08 - 08, 2004). InfoSecCD '04. ACM Press, New York, NY, 20-29.

[14] Schafer, J., Ragsdale, D. J., Surdu, J. R., and Carver, C. A. 2001. The IWAR range: a laboratory for undergraduate information assurance education. In *Proceedings of the Sixth Annual CCSC Northeastern Conference on the Journal of Computing in Small Colleges* (Middlebury, Vermont, United States). Consortium for Computing Sciences in Colleges. Consortium for Computing Sciences in Colleges, 223-232.

[15] Vaughn, R. B., Dampier, D. A., and Warkentin, M. B. 2004. Building an information security education program. In *Proceedings of the 1st Annual Conference on information Security Curriculum Development* (Kennesaw, Georgia, October 08 - 08, 2004). InfoSecCD '04. ACM Press, New York, NY, 41-45.

[16] Walden, J. 2005. A real-time information warfare exercise on a virtual network. In *Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education* (St. Louis, Missouri, USA, February 23 - 27, 2005). SIGCSE '05. ACM Press, New York, NY, 86-90.