UNIVERSITY SENATE

UNVERSITY AT ALBANY
STATE UNIVERSITY OF NEW YORK

Introduced by: GAC and UPPC

Date: February 14, 2011

Graduate Certificate in Information Security

IT IS HEREBY PROPOSED THAT THE FOLLOWING BE ADOPTED:

1. That the University Senate approves the attached proposal as approved by the Graduate Academic Council and the University Planning and Policy Council.

2. That this proposal be forwarded to President George M. Philip for approval.

UNIVERSITY AT ALBANY
State University of New York
School of Business (SOB)

GRADUATE CERTIFICATE IN INFORMATION SECURITY

Program Identity
- Graduate Certificate in Information Security

Proposed Starting Date
- Certificate will begin in Spring 2011

Introduction and Rationale

As the need to secure computers and networks as well as well as analyze security breaches and other crimes increases, education in information security (IS) becomes more and more essential. There is an acute shortage of skilled workforce in this area for both public sector organizations and private firms. The proposed certificate of advanced studies in the area of IS is designed to train the workforce in skills required for its practice. IS is a broad field that covers multiple disciplines and classes in the program provide the students the background knowledge and skills to actively work in the field. The University has strong collaboration in this area in multiple countries across the globe, includinge. Spain, Russia, Ireland, and Israel. This certificate program will help in building innovative collaborative programs with partner universities internationally. The University has established close connections with several New York State agencies in the area of research and education in information assurance. The proposed curriculum has been developed in consultation with these agencies and our collaborators in other universities.

We have developed expertise in creation and dissemination of information security curriculum. Based on grants received from National Science Foundation, Department of Education, and New York State, the NYS Center for Information Forensics and Assurance (CIFA) was created at the University at Albany with a mission to promote IS education. As a part of the mission at CIFA, an IS Teaching Hospital is being implemented, where real security cases are solved for agencies and abstracted into teaching cases for supplemental education. The students in the certificate program will benefit from the innovative teaching models that are being introduced and utilized.

Other universities offer similar programs such as: the University of Tulsa's Graduate Certificate in Information Security, the University of South Carolina's Graduate Certificate in Information Assurance and Security, the University of Alabama at Huntsville and the University of Washington's Graduate Certificates in Information Assurance and Cyber-security, Louisiana Tech University's Graduate Certificate in Information Assurance, Brandeis University's Graduate Certificate in Information Security and Compliance, and George Mason University's Graduate Certificate in Information Systems Security. These programs are a testament to the growing popularity of this field.

Certificate Learning Objective
- Develop skills for work and research in the information security industry.

Plan of Study/Curriculum (15 credits)

Core Courses:
1. ITM 640 - Information Security Risk Assessment (3)
2. ITM 641 – Information Security Policies (3)
3. ITM 642 - Computer Forensics (3) or ACC 553 – Digital Forensics

4. ITM 643 - Incident Handling (3)
5. ITM 691 – Field Project (or an elective course)

Elective Courses

ACC 522 Statistical Methods for Forensic Accounting and Assurance (3)
ACC 581 Internal Controls and Financial Information Systems (3)
ACC 661 Auditing of Advanced Accounting Systems (3)
ACC 695 Independent Study in Accounting (3)
ITM 692 Special Topics in Information Technology (3)
ITM 695 Independent Study in Information Systems or Information Technology (3)

Prerequisites

- ITM 640, 641, 642, 643 have a prerequisite of a basic information security course (e.g. ITM 604 or CSI 524).
- ACC 553 Digital Forensics pre-requires ACC 512.
- ITM 691 pre-requires ITM 522 or equivalent.
- ITM 692 has a co-requisite of ITM 601.
- ACC 522 pre-requires ITM 220 or MAT 108 or equivalent statistics background.
- ACC 661 pre-requires ACC 681 and ACC 512 or equivalent
- ACC 512 pre-requires 3 credits of Financial Accounting or equivalent.

Note: The elective courses are selected from the courses that are currently available for students and over time additional courses may be added to the list based on their availability.

Description

The certificate is designed to understand the genesis of vulnerabilities in information systems that stem from weaknesses in software. The students learn how these weaknesses are exploited to perpetrate attacks on computers and networks. Students also learn how to analyze weaknesses in systems, how to respond when incidents occur, and how to design systems to prevent them. The core courses are designed to ensure that students have a sufficient background in both managing risks and analyzing security incidents. They can specialize further by taking one of the elective courses. Potential (likely) Instructors for the core courses are listed below. Based on their availability different instructors will be chosen for the courses. Additional instructors will be added to the list as more become available. Care will be taken to provide students exposure to several instructors during their program.

1. ITM 640 - Information Security Risk Assessment (3)
   Sanjay Goel
   Ingrid Fisher
   Larry Lessner

2. ITM 641 – Information Security Policies (3)
   Sanjay Goel
   Ingrid Fisher

3. ITM 642 - Computer Forensics (3)
   Sanjay Goel
   Siwei Lyu

4. ITM 643 - Incident Handling (3)
   Sanjay Goel
   George Berg

Detailed Objectives:

- Understanding the vulnerabilities and threats to information systems, and techniques for preventing, detecting and correcting them
- Learn how malicious code (viruses, worms, etc.) is written, and ways to protect your infrastructure from this code.
- Understanding the ways internal controls are incorporated including writing and enforcing security policies
- Understanding the process of auditing of information systems and developing skills in the preparation of audit programs and implementing them

Expected Market and Demand

IS is a critical function for all organizations to ensure the protection of their assets. Security threats are constantly increasing and there is a dire shortage of people in the area of Information Security. We expect that people who would enroll in this certificate program would include students from Business, Computer Science, Information Science and Public Administration. We also anticipate creating additional programs in collaboration with our partner universities. In addition, based on our active collaboration with the New York State Office of Cyber Security and Critical Infrastructure Coordination as well as the New York State Police we also expect employees in New York State agencies in security-related areas to enroll in this certificate program. We expect 15-20 students in the certificate program during the academic year.

Delivery Format

There is a need for this certificate both in the public sector as well as our partner institutions abroad. To meet the varied requirements we plan on offering this certificate in different modes. In one of the models that we intend to pursue in the near future we will be using a blend of online and in-class instruction formats. This makes it easier for participation of students in locations away from UAlbany. Students will be required to take one or two classes of the certificate in Albany where they will be able to work with a cohort of students. This will also help the instructor assess the capabilities and needs of the students and help the students create teams and work interactively with other students. We also feel that having students complete one or two courses on campus almost eliminates the possibility of fraud, since their capabilities are evaluated in person at least for a part of the curriculum. An alternate model would be to offer all classes in-class on campus for local students both as a certificate for UAlbany students or to New York State employees. The choice of the mode will be determined by ~~on~~ the demand and resources available. As a part of our grant activity from the Department of Education, we plan to offer Computer Forensics (ITM 643) and a Field Study (ITM 691) in-class. This will be followed by three online courses, sequenced in the following order: risk analysis, security policies, and incident handling.

Financial Resource Requirements

Any of the core courses offered during the academic year will be supported by grants or external funding. Courses offered during the summer session will be fully funded through student tuition. Students will also be able to take equivalent substitute classes reducing burden on any specific course even further. No need for additional sections for any of the elective courses is envisaged. The core 3-credit classes will be offered online and a separate section of ITM 691 Field Project will be created to accommodate the students in the certificate program. Students will be spread through different elective courses given availability and interest or enroll in the ITM 691 Field Project course. Curriculum development for this program will be done via a grant from the Department of Education that we have been awarded.

Admissions

To be considered for admission into the Certificate in Information Security program, the applicant must submit the following materials:

- Proof of an earned baccalaureate degree;[1]
- Official transcripts from academic institution(s) of earned degrees;[1]
- A cover letter that describes the applicant's background and his or her reasons for pursuing the Certificate;
- Evidence of proficiency in English for international applicants, such as TOEFL or IELTS scores;
- A completed graduate application and fee (CANNOT be non-degree)[2]
- A resume, summarizing educational and employment history since the age of 18
- At least two letters of recommendation

Prerequisite Guidelines

- Students should realize that some of the courses in the certificate program have prerequisites that they will need to satisfied either through equivalent coursework or background.
- Students with a background, or experience, in information assurance or information security may not need to take prerequisites required in the core curriculum, but it will be assumed that a basic knowledge of these topics exists. They will need to demonstrate their expertise and request specific prerequisite waivers from the instructor of the class.
- Specific tracks may require that certain prerequisites be completed prior to taking the track specific courses. Prerequisite waivers may be requested as specified below.

The director for the program will be a SUNY employee.

Retention Standards
Students enrolled in the certificate program should maintain a 3.0 GPA or higher to stay in the certificate program. If a student does not receive a GPA of 3.0 or higher, a meeting with the Director of the program will occur to discuss individual student progress. The maximum amount of time to complete the certificate program courses upon admission is 5 years.

Course Waivers / Transfers / Replacement
Course waivers will not be granted. However, course transfers and replacement of courses with other higher-level courses based on previously taken courses and/or experiential knowledge will be considered on a case by case basis. The pre-requisites required for some of the courses may be waived based on instructor discretion. Transfers are limited to one class since the certificate program is short in duration. Each request for course transfers / replacements will be evaluated on a case-by-case basis. Required courses may be substituted for other courses (and independent studies) at the discretion of the director of the program (faculty) based on availability of course offerings and pedagogic reasons. If the director of the program is not a member of the faculty then a faculty mentor would be assigned to the certificate program by the director to make course substitution decisions.

Using Certificate Courses Towards a Graduate Degree
Since all classes are at the graduate level, they can be used towards the completion of a graduate degree (depending on the specific program enrolled). At the University at Albany, State University of New York, these classes can be used to satisfy course requirements for graduate programs in the Business School. However, individual assessment and advisement will vary in terms of the courses taken, and the specific degree requirements upon enrollment.

Program Management
The following core faculty will be responsible for admission and both core and affiliated faculty will serve as advisors based on the track chosen by the individual student. In addition, consultation with

---

[1] Please provide official English translations if the original is not in English
[2] To apply, visit the Graduate Studies Admissions Office web site at http://www.albany.edu/graduate/

affiliated professionals will be used for recommendations for program modification / improvement. Sanjay Goel will serve as the initial Director of the Certificate Program (with the directorship able to change to another core faculty). If a non-faculty director is assigned to manage the program, a faculty mentor will be designated to make academic decisions such as course substitutions and addition of new tracks.

Core Faculty

Ingrid Fisher	Accounting (SOB)
Sanjay Goel	Information Technology Management (SOB)

Affiliated Faculty

Kinsum Tam	Accounting (SOB)
Andrew Chang	Accounting (SOB)
Shobha Chengalur-Smith	Information Technology Management (SOB)
Eliot Rich	Information Technology Management (SOB)

Affiliated Professionals

Fabio Auffant II (New York State Police)
Joseph Donohue (New York State Police)
Laura Iwan (New York State, Information Security Officer, CSCIC)
Damira Pon, Omniseer Inc.
Michael Smith, Symantec Corporation

Resources and Support
Computing and Laboratory Facilities
The Cyber Security Research Laboratory is a dedicated facility where multidisciplinary researchers, practitioners, and students can collaborate to investigate and demonstrate real world problems related to information security and computer forensics. The solutions and best practices developed in the lab will become the basis for rapidly developed educational modules. The Information Security Academy supports a hands-on classroom laboratory. This is a dedicated information security classroom where students and employee participants from the public and private sectors can receive instruction, engage in learning exercises, and develop and test new courseware.

Centers
The University at Albany is actively involved in research associated with information security and computer forensics. Center for Information Forensics and Assurance was created in collaboration between University at Albany, New York State Police, and New York State Office of Cyber Security and Critical Infrastructure. It has received funding from Department of Justice, National Science Foundation, Department of Education, and NY State. Several online and in class courses were developed at the center through the use of these grants for training NY State Employees.

Library Resources
The Minerva online catalog at the University at Albany Libraries lists the following journals:
1) ACM transactions on information and system security
2) Aviation Week's homeland security & defense
3) Computer fraud & security
4) Computer law & security report (Online)
5) Computers & security (Online)
6) Defense & security analysis
7) European foreign policy bulletin
8) European security (London, England)
9) IEEE security & privacy (Online)

> **Formatted:** Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

10) IOMA's security director's report

11) Industrial security

12) Information management & computer security

13) Information security technical report (Online)

14) Mershon international studies review

15) Network security (Online)

16) Perspectives in defense management

17) Science & global security: the technical basis for arms control & environmental policy initiatives Security (Newton, Mass.)

18) Security & safety

19) Security gazette

20) Security letter

21) Security systems digest

22) Security watch: protecting people, property & assets

23) Security world

24) 152 Government documents

25) Homeland Security digital archives

UAlbany libraries also provides the following resources:

a) -EBSCO database called the Military & Government Collection. Designed to offer current news pertaining to all branches of the military, this database offers a thorough collection of periodicals, academic journals and other content pertinent to these organizations. The Military & Government collection provides cover-to-cover full text for nearly 400 journals and periodicals. The database also includes full text for 245 pamphlets and offers indexing and abstracts for more than 500 titles. Some publications covered in this database include Air Force Comptroller, Army Reserve Magazine, Defense Studies, Global Security Review, JFQ: Joint Force Quarterly, Military Technology, National Review, Combat Edge, FBI Law Enforcement Bulletin, Foreign Affairs, Naval Forces, and many more. Many full text titles are available in native (searchable) PDF, or scanned-in-color.

b) **Criminal Justice Periodicals Index.** This database covers the journal literature of criminal justice. Emphasis is on criminal justice and criminology generally, law enforcement, corrections, law and the courts. Over 200 journals are covered, with 75 titles offered full-text.   Some of the titles relevant to information security are: Bank Security Report, Computers & Security, Defense & Security Analysis, Information & Security, International Journal of Cyber Criminology, International Journal of Information Security, Journal of Applied Security Research, The Journal of Digital Forensics, Security and Law: JDFSL, Journal of Homeland Security and Emergency Management, Proceedings of the Conference on Digital Forensics, Security and Law, Security, Security Journal, Security Law Newsletter, Security Letter, Security Management, Security Systems News, and Security Technology Executive.

c) **ACM Digital Library:** The ACM Digital Library is a full text archive of the Association for Computing Machinery, journals, magazines, and transactions. It also includes a significant collection of proceedings from ACM conferences and workshops along with newsletters from special interest groups, and journals and conference proceedings from affiliated organizations and publishers. Titles include ACM Computing Surveys, ACM Journal of Computer Documentation, ACM Journal on Emerging Technologies in Computing Systems, Journal of Data and Information Quality, Journal of Experimental Algorithmics, and Journal of the ACM.

d) **IEEE Computer Society Digital Library:** The IEEE Computer Society Digital Library provides online access to 22 society magazines, transactions, and letters, and a collection of conference proceedings and workshops. Of particular relevance to information security are IEEE Security and Privacy, IEEE Pervasive Computing, IEEE Distributed Systems Online, IEEE Transactions on Dependable and Secure Computing.

e) **INSPEC:** INSPEC is the world's largest bibliographic database in the field of physics, electrical engineering and electronics, computers and control engineering, and information technology. Over 330,000 new records from 4,000 journals and 2,000 conference proceedings are added each year.

f) **Springer Computer Science eBook Collection:** This electronic book collection contains most computer science books published by Springer from 2005 forward. The collection includes conference and workshop proceedings, research monographs, surveys, tutorials, textbooks, professional treatments, and encyclopedias. Subjects covered include computer forensics and data encryption.

Appendix I

Core Course Descriptions

ITM 640 Information Security Risk Assessment (1-3)

This course provides students with an introduction to the field of information security risk assessment. Initially, the students will be introduced to basic definitions and nomenclature in the area of security assessment. Thereafter they will be taught different approaches for assessment of risk. The course will incorporate cases in risk analysis derived from state and law enforcement agencies. Students will learn how to use a risk analysis matrix for performing both quantitative and qualitative risk analysis. As part of the course the students learn of the different threats that they need to incorporate in their risk analysis matrices.

ITM 641 Security Policies (1-3)

This course provides students with an introduction to information security policies. Students will be introduced to sociological and psychological issues in policy implementation in general and then provided with a focused dialogue on information security specific policies. The class discusses the entire lifecycle of policy creation and enactment and presents students with issue specific policies in different domains of security. The structure of the policy is also discussed to assist the students in design and modification of policies. Several examples from different domains are incorporated in the curriculum to assist students to learn in context of real life situations.

ITM 642 Computer Forensics (1-3)

Computer forensics is a relatively new field focused on solving computer crime that is an amalgamation of forensics investigative techniques, computer security, and law. Computer forensics is the study of cyber attack reporting, detection, and response by logging malicious activity and gathering court-admissible chains-of-evidence using various forensic tools able to trace back the activity of hackers. The course provides students with training in collection and preserving evidence from computers and networks.

ITM 643 Incident Handling (1-3)

The course primarily involves management of computer security incidents, including detailing different types of incidents, identification, preparation, and analysis of incidents; as well as gathering of evidence, recovery and follow-up to computer security incidents.

ITM 691 Field Study in Information Technology Management (3)

Field projects are conducted by students under faculty supervision in a variety of business and not-for-profit organizations. The projects provide students with an opportunity to apply and further develop their skills in information technology management. May be repeated for a total of 3 credits. ~~Must be repeated for 3 credits.~~ Prerequisites: ITM~~tm~~ 522 and permission of the department chairperson.

Appendix II

Elective Course Descriptions

ACC 522 Statistical Methods for Forensic Accounting and Assurance (3)
Exploratory descriptive data analysis using Data Analysis & Mining Software. Basic graphics commands in S-Plus including trellis graphics. Descriptive data exploration and statistical modeling. Data processing for Datamining. Classification: Induction of Decision trees, Association Rules in Large Databases. Multivariate Methods; Clustering and other multivariate statistical methods. Anomaly detection. Prerequisites: ITMitm 220 or MATat 108 or equivalent.

ACC 581 Internal Controls and Financial Information Systems (3)
This course addresses the design and evaluation of computer-based accounting information systems with a focus on the recognition and identification of information technology risks. General and application internal controls for information systems environments are examined across client/server, end-user computing, and service bureau internal control environments. Both computerized auditing techniques as well as techniques for auditing computerized systems are analyzed. Risks of emerging technologies and computer-based business models for planning and control are considered.

ACC 661 Auditing of Advanced Accounting Systems (3)
Auditing of modern complex accounting information systems. General & application controls and the design & development of generalized audit software. Auditing of operating systems and database management systems. Privacy & security of data in accounting systems. Audit of on-line systems, management systems. Prerequisite: ACCcc 681 and ACCcc 512 or equivalent.

ACC 695 Independent Study in Accounting (3)
The student and instructor jointly develop a plan of independent study on an advanced topic in accounting. The student is usually required to prepare a report or paper. May be repeated for a total of 3 credits. Prerequisite: Permission of instructor and department chairperson.

ITM 692 Special Topics in Information Technology (3)
This course covers programming concepts using the Java language and business intelligence using data mining. In the first half of the class students learn the concepts of programming. From this class, students are not expected to become expert programmers, but will gain an understanding of basic programming concepts that will enable them to think through and solve business problems in a logical and structured fashion. Understanding of programming will also help students in making decisions regarding technology acquisition and development as they mature into management roles. The second part of the class focuses on learning data mining techniques, including: clustering (e.g. k-means, hierarchical), classification (e.g. decision trees), and association rule mining (e.g. market basket analysis). This part of the class will teach students to efficiently filter through large volumes of data to gain intelligence for business decision making. The lectures in the class will be complemented by hands-on workshops and tutorials.

ITM 695 Independent Study in Information Systems or Information Technology (3)
The student and instructor jointly develop a plan of independent study on an advanced topic in information systems or operations management. The student is usually required to prepare a report or paper. May be repeated for a total of 3 credits. Prerequisites: Itm 522 and permission of instructor and department chairperson