

Cybersystems and Information Security: Master of Science Program at Auburn University Montgomery

Mehmet Sahinoglu, *Senior Member, IEEE*

Abstract— Auburn University at Montgomery (AUM) proposed a Master of Science in Cybersystems and Information Security (CSIS) degree program, which was approved by ACHE (Alabama Commission on Higher Education) on December 4, 2009. AUM will be the first university in Alabama and Southeast to offer a program classified as 11.1003 by the Classification of Instructional Programs (CIP) coding system. The implementation date for this program will be the Fall Semester 2011 since the accreditation by SACS (Southern Association of Schools and Colleges) has been officially notified on December 14, 2010. The initial target audience for this program will be Air Force uniformed and civilian personnel located at Maxwell/Gunter AFB and related defense industry personnel associated with information technology (IT) contractors. IT community located in the AUM service area is included in this audience. This group is composed of employees of state/local governments, businesses, as well in- and out-of State graduate and undergraduate students. These projections are based on statistical surveys conducted by AUM to gauge interest. Course requirements will be listed for each semester and what makes this program unique will be discussed including resources. A conclusive summary of challenges since 2008 is presented at the end.

Index Terms- Cybersystems; ACHE; Information Security, SACS

I. INTRODUCTION

The Master of Science in Cybersystems and Information Security (CSIS) program will be a newly established graduate degree program designed to meet the security needs of national defense, government, and business sectors now, and in the future. Instructional delivery methods will utilize the latest technology already in place at AUM, both in the classroom and online. As the program begins, approximately 80% of classes will be taught in a traditional in-class lecture and/or laboratory setting with both day and (mostly) evening classes. Approximately 20% of classes will be taught through distance education formats. Distance education technology will be used in the delivery of courses and special topics presentations by experts in the field from across the nation. According to the U.S. Computer Emergency Readiness Team (US-CERT), Cybersecurity refers to the prevention, detection, and response to attacks on personal information that is stored within information systems [1].

Manuscript received on October 7, 2010. Mehmet Sahinoglu is the Director of Informatics Institute with Auburn University Montgomery in Montgomery Alabama 36124 USA. Tel: 334-244-3769, Fax: 334-244-3127. E-Mail: msahinog@aum.edu, URL: www.aum.edu/csis. This work was supported in part by the Ida Belle Young endowment toward academic research publications conducted by the AUM's Informatics Institute.

Potential attackers include “unfriendly governments and militaries, intelligence agencies, organized criminals, and hactivists” [2]. In April 2009, for example, news that cyberspies from hostile nations had disrupted the U.S. electrical grid caused a stir among intelligence and information security officials [3]. International events, such as enemy hackers’ 2008 attack on the country of Georgia [4] and the 2007 attack on Estonia [5] suggest that cyberwarfare may in fact pose one of the greatest security threats to countries in the years to come.

Being located in the Alabama State capital, in close proximity to Maxwell/Gunter AFB (in particular the USAF 754th Electronic Systems Group), and centralized along the I-65 information technology corridor which is a hub to hundreds of technology-based contractual companies, the establishment of this program will fill a clearly identified societal need. The proposed program will not only prepare leaders who can implement, monitor, and respond to security issues, but will also train researchers who can develop original and innovative technologies to improve cybersystems security.

II. ASSESSMENT OF NEED AND PROGRAM PLANNING

There is an ever-increasing need in society for greater cyber systems and information security. This calls for the development of leaders who can implement, monitor, and respond to security issues, as well as researchers who can develop original and innovative technologies to improve cyber systems security. Within the last decade, cybersystems and information security have become increasingly significant priorities on the U.S. national political agenda. In the aftermath of September 11, and similar conflicts, and the subsequent political discourse on homeland security, this concern has been reflected in higher education, as colleges and universities began to introduce academic programs to provide specialized training in a brand new area.

To assess the educational need for a specialized program in Cybersystems and Information Security in the Southeast, Auburn University at Montgomery employed the Hanover Research Council to develop a research report on *The Viability of a New Master's Degree Program in Cybersystems and Information Security* [6]. The Hanover Research Council utilized the Integrated Postsecondary Education Data System (IPEDS) to identify a group of 24 institutions that offer graduate degree programs in Computer and Information Systems Security.

An online survey was developed to gauge student interest in the field of Cybersystems and Information Security. The online survey required each respondent to log in using their e-mail address, which ensured that the survey was only completed once by each respondent. The link to the online survey was e-mailed to all upperclassmen in related majors at Auburn University at Montgomery. Each upperclassman was contacted three times, which yielded a 45% response rate. 56% of the respondents answered yes to the question, “Are you interested in pursuing a master’s degree in Cybersystems and Information Security?” Additionally, 77% of the respondents requested additional information about the program.

A separate online survey was used as an additional gauge of employment needs in the Montgomery region. The link to the online survey was e-mailed to these potential employers. The survey required each respondent to login using their e-mail address, which ensured that the survey was only completed once by each respondent. Each potential employer was contacted twice which yielded a 32% response rate. 72% of the respondents agreed or strongly agreed to the question, “If an advanced degree in this field were available at AUM, you would support your employees enrolling in the program.” Additionally, 78% of the respondents agreed or strongly agreed that, “The presence of employees with an advanced graduate degree in Cybersystems and Information Security in [their] organization would enhance efforts to promote and create a more secure computing environment.”

Several mechanisms were utilized to project job openings in the area of Cybersystems and Information Security. To generate the numbers for the Projected Job Openings, www.indeed.com was reviewed in detail as the most cohesive and extensive website to project job openings in Montgomery (local), State, southern region (as defined by the Southern Regional Education Board (SREB) member states), and national markets. The “Information Security and Network Security” search words were sought and the results obtained for 2010 are as follows: 9 projected job openings in the local Montgomery area; 63 projected job openings in the State; 6,079 job openings projected for the SREB; and 11,613 projected jobs nationwide.

The Bureau of Labor Statistics’ Occupational Handbook notes that “the need for computer security specialists has increased over the past few years as cyber attacks have become more common” and this trend is expected to continue [7]. Research showed that students graduating from this program can find jobs in Information Technology, Private Business, Armed Forces, Government and State Agencies, and Homeland Security [8].

The proposed program has also been approved the Auburn University Board of Trustees and the Alabama Commission on Higher Education (ACHE) and further accredited by SACS (the Southern Association for Colleges and Schools) [9].

III. PROGRAM REQUIREMENTS AND OUTCOMES

The proposed Cybersystems and Information Security program will provide specialized training in computer network and information security, secure software engineering, operating system security, secure network engineering, and applied cryptology. Upon completion of this program, graduates will be able but not limited to demonstrate an understanding of the technical, management, and policy aspects of Cybersystems and Information security, and assess information security risks faced by an organization and develop a response plan by mitigating system vulnerabilities and restore compromised services. The oversight of students’ success will be additionally monitored by the graduation percentage, and job employment and retention rate over five-year periods each. See Table I and Table II that complement each other for students’ outcome assessment.

TABLE I: The expected outcomes of the proposed program, numbered and matched with the courses in Table II.

<ol style="list-style-type: none"> 1. Demonstrate an understanding of the technical, management, and policy aspects of cybersystems and information security. 2. Identify and respond to information security challenges in distributed and embedded systems. 3. Recognize the impact of security issues related to software engineering on distributed information systems. 4. Assess information security risks faced by an organization and develop a response plan. 5. Demonstrate an understanding of technological and human engineering problems linked to security risks. 6. Assess the impact of information security policies, and market developments on complex systems and organizational objectives. 7. Evaluate and recommend technological tools and protocols to protect against risks. 8. Mitigate system vulnerabilities and restore compromised services. 9. Manage the development, acquisition and evolution of a secure information network. 10. Construct secure networked and distributed computer systems. 11. Troubleshoot large scale information networks and distributed systems. 12. Establish requirements for complex security applications and translate these requirements into a design architecture. 13. Integrate the use of encryption technology in non-secure and non-private computers and systems. 14. Design and conduct research in the area of cybersystems and information security. 15. Critically evaluate and apply research and reports of threats to computers and cybersystems. 16. Discuss the importance of life-long learning and professional development in information security disciplines.

Table II: CSIS Semester-by-Semester Curriculum (36 credit hours) followed by students' outcome assessment match in Table I

1st year Fall Semester (9 credits)

CSIS 6003 – Introduction to Computer Security – 3 credits; {1,8,13,15}

CSIS 6010 – Introduction to Data Communications and Computer Networks – 3 credits; {2,3,15}

CSIS 6020 – Distributed Systems – 3 credits; {2,3,11,12}

1st year Spring Semester (9 credits)

CSIS 6013 – Network Security and Reliability-Quantitative Metrics – 3 credits; {7,8,10}

CSIS 6403 – Systems Modeling and Simulation – 3 credits; {4,6,7,12,14}

CSIS 6033 – Secure Software Systems – 3 credits; {3,8,9,12}

2nd year Fall Semester (9 credits)

CSIS 6053 – Information Security Management – 3 credits; {4,9,16}

CSIS 6040 – Applied Cryptology – 3 credits; {7,11,13}

ACCT 6180 – Financial Accounting Integrated Business Concepts - 3 credits; 4,9,12

2nd year Spring Semester (9 credits)**Non-thesis option*

QMTD 6750 – Operations Research – 3 credits; {1,6,12}

CSIS 6912 – Supervised Practicum with Cyber-Industry Experience – 3 credits; {1,4,5,14}

CSIS 6952 – Security Policy Seminar: Healthcare, Finance , Business or Government – 3 credits; {1,5,6,16}

**Thesis option*

CSIS 6992 – MS Research Thesis – 9 credits; {14,15,16}

A. Thesis Option Degree Requirements

Thirty-six semester hours of Cybersystems and Information Security courses in the AUM's Informatics Institute including a support course offered by the School of Business are required in this option along with one year in residence. Nine of the semester hours which are required in the thesis option are thesis research hours. The student will consult with faculty and establish a 3-member faculty committee, including the advisor, which will be responsible for working with the student in planning the program of study, administering the thesis research, and ensuring that the thesis is of high quality. All members of the committee must be members of the graduate faculty. Upon completion of the course requirements, the student will submit a written copy of the thesis to the faculty committee and present a public defense of the thesis. The thesis defense will consist of a formal presentation of the thesis research followed by a graduate studies. The faculty committee will determine if the defense of the thesis was successful (pass or fail).

B. Non-Thesis Degree Requirements

Thirty-six semester hours of Cybersystems and Information Security courses including two support courses successfully complete a comprehensive written and oral examination by the program faculty that will cover the student's graduate studies. All of the faculty that participates in these examinations must be members of the graduate faculty. The faculty participating in the examinations will determine if the student's performance

on the examinations was acceptable (pass or fail). The student must pass the examinations in order to complete the program.

C. Faculty

The program will be administered through the AUM School of Sciences. The dean of this school will be responsible for oversight of the program. Examples of evaluations/assessments that will be utilized by the dean in order to carry out this function include: annual program assessment, student evaluation of courses, academic program review, and survey results of graduates and their employers assessment, student evaluation of courses, academic program review, and survey results of graduates and their employers. In addition to the Informatics Institute's own director and adjunct faculty approved, the proposed program will draw from expertise that currently exists at AUM in the Department of Mathematics (Computer Science option) of the School of Sciences, the Department of Information Systems and Decision Science of the School of Business. One group of external experts with whom a partially collaborative arrangement has been developed is the Department of Computer Science and Software Engineering in the School of Engineering at Auburn University (in Auburn).

D. Why This Program?

What makes this program unique is its first time introduction of a long-needed cyber-security educational degree program for both civilians and Maxwell AFB, a \$Billion economic dynamo in the region. Another primary

reason for offering the new program is to increase the information security presence of the greater Montgomery area, and develop urgency in responding to new threats and adversaries on a global scale. Nine of the semester hours required in the non-thesis option includes an additional business course, a seminar course, and an internship. Upon completion of the course requirements in this option, the student will utilize their information security skills to prepare them for more competitive and realistic challenging careers in information security, an invaluable career for the community and nation.

IV. CHALLENGES AND CONCLUSIONS

A initial review of the institutions offering information security-related graduate programs identified one graduate degree program offered via an on-campus format in the Southeast. This program is located at Nova Southeastern University in Florida. Virginia College (accredited by the Accrediting Council for Independent Colleges and Schools), with a branch campus in Birmingham, is the only institution in Alabama that offers a related program. This program, however, is offered exclusively online and it is unclear from which of the 12 Virginia College campuses in seven Southeastern states this online program originates. The vast majority of institutions offering programs similar to the proposed Cybersystems and Information Security program are located in the Northeast (DC, DE, IL, IN, MD, MI, NJ, NY, PA, WI). The lack of graduate degree offerings in Cybersystems and Information Security in the Southeast suggests exciting opportunities for the development of a degree program in this area at AUM.

At the federal level, this concern was partially addressed by the National Cyber Security Center (NCSC), which was set up within the Department of Homeland Security in January 2008. However, in recent months, a number of political leaders have called for greater federal oversight of cybersecurity. In April 2009, Senators Olympia Snowe (R-ME) and Jay Rockefeller (D-WV) introduced the "Cybersecurity Act of 2009," targeted at "reinforcing ongoing cybersecurity efforts within the government, while also ensuring that proper safeguards are implemented for critical infrastructure targets within the private sector, such as banking and power systems." The cybersecurity concerns raised within the proposed legislation were echoed later that same month by Melissa Hathaway, the federal official responsible for leading the 60-day review of the government's cybersecurity programs, who urged the White House to take on a greater role in coordinating cybersecurity efforts [8].

In light of recent events, these apprehensions are indeed timely. Within recent decade, and particularly in the last few years, cybersecurity has become a major priority on the national political agenda. In April 2009, the *Wall Street Journal* also reported that spies had broken into the U.S. Pentagon's \$300 billion Joint Strike Fighter project [10].

Domestic and international events suggest that cybersecurity will continue to be a national and global menace. Government officials further suggested that similar incidents had led to a breach in the Air Force's air-traffic-control system in recent months. Sources suggest that the threat of cyberattacks is becoming increasingly more prevalent [10]. According to a recent article, the Department of Homeland Security's US-CERT reported a grand total of 18,050 cyberattacks in 2008 in both private and government sectors at the local and national levels. This number represents a significant increase from reported attacks in previous years. In 2007, a total of 12,986 were reported, compared to 5,144 attacks in 2006 [11]. Given the political and social significance of cybersecurity, the need for individuals with specialized training in the area of Cybersystems and Information Security has become all the more urgent, hence its formal education through a new breed of books on Trustworthy Computing [12].

From the beginning when AUM's Informatics Institute was established in August 2008 to date, there were difficult phases, primarily owing to its CSIS (Cybersystems and Information Security) program ranking as a first such graduate degree program in the State of Alabama with a sizable Air Force contingency. Challenges were encountered when locating and surveying the area's IT people, and the pertinent college students. Preparing the budget schedules that ACHE required in order to approve the program was not easy. When the first-time program enrollees graduate, how lucrative the job market will be the next question. Studies have shown that there will be sufficient jobs for our future graduates in the target audience for this program, i.e., Air Force uniformed and civilian personnel, related defense industry personnel and associated information technology contractors. Aside from the tuition revenues, the major budget source will be the grant initiatives, cyber security certification programs with the local industry, and Air Force. NSF and NSA, DoD Homeland Security etc. possess programs to support students for tuition fees.

Evidence provided above clearly indicates the importance of cybersecurity on society and the need for greater Cybersystems and Information Security. The proposed program has received all necessary approvals and authorizations including approval by the Alabama Commission on Higher Education (ACHE) and accreditation by SACS (Southern Association of Colleges and Schools). The Department of Computer Science and Software Engineering (CSSE) at Auburn University – Auburn offers computer-related programs in Computer Systems, Computer Applications, Theory and Programming Languages, Computer and Wireless Networks, Human Computer Interactive Systems, Artificial Intelligence, and Software Engineering. The primary difference between these programs and the proposed graduate degree program at Auburn University at Montgomery is that the proposed program at the Montgomery campus is primarily focused on Cybersystems and Information Security. See Appendix for the CSIS flyer which can be found at www.aum.edu/csisis.

APPENDIX

auburn montgomery school of sciences

School of Sciences

Master of Science in Cybersystems and Information Security

Description:

The Master of Science degree program in Cybersystems and Information Security (CSIS) prepares students to become leaders in the field of information and network security, offering instruction and research opportunities that provide graduates with the necessary knowledge and skills to effectively assess, develop, and manage secure information networks and to respond to newly developed threats. This program offers a unique opportunity for students to learn to:

- ◆ Identify and respond to information security challenges in distributed and embedded systems.
- ◆ Evaluate and recommend technological tools and protocols to protect against risks.
- ◆ Integrate the use of encryption technology in non-secure and non-private computers and systems.
- ◆ Design and conduct research in the area of cybersystems and information security.
- ◆ Critically evaluate and apply research to computer and cybersystems threats.

Why a master's degree in CSIS is important:

There is an ever-increasing need in society for greater cybersystems and information security. This calls for the development of leaders who can implement, monitor, and respond to security issues, as well as researchers who can develop original and innovative technologies to improve cybersystems security. The Cybersystems and Information Security master's program will provide specialized training in computer network and information security, secure software engineering, operating system security, secure network engineering, and applied cryptology.

www.aum.edu/csis

Program Director: Mehmet Sahinoglu, Ph.D. 334-244-3769, msahinog@aum.edu



ACKNOWLEDGMENT

The author dutifully acknowledges his gratitude for many at AUM from Chancellor Dr. Veres with a clear “cyber vision” to its past and current Provost and Associate Provost as well its Dean of School of Science. Special thanks go to distinguished scientists and Informatics Institute Board Members who remotely supported, and/or assembled in November 2009 at Montgomery. They ranged from the University of California at Berkeley to Carnegie Melon University, and from the University of Pittsburgh, Purdue, and Integrated Computer Solutions, a local IT company and Maxwell AFB to the AUM’s local Faculty and Staff. The author is also grateful to the Auburn University President Dr. Gouge, and Board of Trustees, as well as ACHE and SACS specialists during the course of 2009-2010 to elevate this program to its current completion in 2011. AUM Informatics Institute Board deserves a special recognition:

- 1) Prof. C.V. Ramamoorthy, CSE, Univ. of Cal., Berkeley, CA
- 2) Prof. Eugene H. Spafford, Dir., CERIAS-Purdue Univ., IN
- 3) Prof. James Joshi, Dir., LERSAIS- Univ. of Pittsburgh, PA
- 4) Prof. Kai Chang, Chair, CSSE, Auburn Univ., Auburn, AL
- 5) Stephen Goldsby, CEO, ICS, Montgomery, AL
- 6) Prof. Murat Tanik, ECE, UAB, Birmingham, AL
- 7) Col. Mary Griswold, HQ 754th ELSG, Maxwell AFB, AL
- 8) Dr. Karen Stine, Dean, School of Sciences, AUM, AL
- 9) Dr. Luis Cueva-Parra, School of Sciences, AUM, AL
- 10) Dr. Jeff Barksdale, Associate Provost, AUM, AL
- 11) Dr. Yaw-Chin Ho, Special Assistant to the Chancellor, AUM, AL
- 12) Dr. Bob Gehling, School of Business, AUM, AL
- 13) Dr. Jane Goodson, Dean, School of Business, AUM, AL
- 14) Dr. Jeffrey Elwell, Provost, AUM, AL
- 15) Dr. John Veres III, Chancellor, AUM, AL

REFERENCES

[1] US-CERT, “National Cyber Alert System,” <http://www.us-cert.gov/cas/tips/ST04-001.html>. January 17, 2007.

[2] Jaikumar Vijayan, “Internet Warfare: Are We Focusing on the Wrong Things? A lack of vision and leadership have left the U.S. woefully unprepared for a cybercatastrophe,” *ComputerWorld*, April 27, 2009.

[3] Siobhan Gorman, “Electricity Grid in U.S. Penetrated by Spies,” *The Wall Street Journal*, April 8, 2009
<http://online.wsj.com/article/SB123914805204099085.html>.
<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9131050>.

[4] Brandon Griggs, “U.S. at Risk of Cyberattacks, Experts Say,” *CNN*.
<http://www.cnn.com/2008/TECH/08/18/cyber.warfare/index.html>.

[5] Joshua Davis, “Hackers Take Down the Most Wired Country in Europe,” *Wired Magazine: Issue 15.09*, August 21, 2007.
http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=1.

[6] The Hanover Research Council, *The Viability of a New Master’s Degree Program in Cybersystems and Information Security*. Washington DC: 2009.

[7] The US Department of Labor Bureau of Labor Statistics. The Occupational Outlook Handbook, 2008 – 09 Edition.
<http://www.bls.gov/oco/ocos268.htm>. April 14, 2007.

[8] Jaikumar Vijayan, “Cybersecurity Official Says White House Should Lead,” *Computer World*, April 27, 2009.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=338289>.

[9] M. Sahinoglu, “A Case Study in Cyber Risk Education: Cybersystems and Information Security Graduate Degree Program at Auburn University Montgomery,” Accepted for Presentation at CSEIT 2010, Hilton Phuket Arcadia Resort & Spa, Thailand, 6 - 7 December 2010.

[10] Siobhan Gorman, August Cole, and Yochi Dreazan, “Computer Spies Breach Fighter-Jet Project,” *Wall Street Journal*. April 21, 2009.
<http://online.wsj.com/article/SB124027491029837401.html>.

[11] Ben Bain, “Number of Reported Cyber Incidents Jumps,” *Federal Computer Week*. February 17, 2009.
<http://www.fcw.com/Articles/2009/02/17/CERT-cyber-incidents.aspx>.

[12] M. Sahinoglu, *Trustworthy Computing: Analytical and Quantitative Engineering Evaluation*. John Wiley & Sons, Hoboken, NJ. 2007.



Mehmet Sahinoglu (M’78–SM’93) is the founder Director of Informatics Institute in Auburn University at Montgomery. He obtained his Ph.D. from Texas A&M (1981) and his MS from UMIST, England (1975) both in EE. Following his 20 year-long tenure at METU (his alma mater, BS-ECE 1969-73) in Ankara as an Assistant-Associate-Full Professor, he served as the founding dean, and department chair in the College of Sciences at DEU in Izmir (1992-97). He taught at TAMU (1978-81) and Purdue (1989-90, 1997-98) and Case Western Reserve University (1998-99), as Fulbright fellow, and NATO research scholar respectively. He is a Fellow of Society of Design and Process Science www.sdpsnet.org and an elected member of International Statistical Institute.