GRADUATE CERTIFICATE PROGRAM
in
CYBERSECURITY

I. Basic Information

1. Institution: University of Georgia Date: September 21, 2016

2. School/College: Franklin College of Arts and Sciences

3. Department/Division: Department of Computer Science

4. Certificate Title (as it will appear in the *Bulletin*): Cybersecurity

5. Level (undergraduate or graduate): Graduate

6. Proposed starting date for program: Spring 2017

7. Abstract of the Certificate Program (for the University Council's agenda):

    Purpose: The Computer Science Department is proposing the following new graduate certificate program in Cybersecurity. This certificate would be useful primarily for graduate students in Computer Science, as well as some students in Mathematical Sciences and Engineering who aim to become experts in the growing field of Computer Security and Privacy.

    Eligibility: Admission is open to graduate students across the university, but is specifically targeted towards graduate students in Computer Science, as well as related mathematical and engineering disciplines.

8. Letters of support with signatures: See attached letters.

II. Response to the Criteria for All Programs

1. Purpose and educational objectives:

A) Purpose and objectives: The Computer Science Department is proposing a new graduate certificate program in Cybersecurity. This certificate program would be useful for students in Computer Science, as well some students in Mathematical Sciences and Engineering. The certificate program aims to develop expertise in various aspects of computer security and privacy, such as networking, operating systems, network and systems security, and data and communications privacy. The need for expertise in the broad field of Cybersecurity has grown tremendously in recent years. The Forbes Magazine reports “Some estimate that between $9 and $21 trillion of global economic value creation could be at risk if companies and governments are unable to successfully combat cyber threats" (http://www.forbes.com/sites/frontline/2015/07/13/why-cybersecurity-leadership-must-start-at-the-top/). In addition, the US government has initiatives to expand cybersecurity education and expand the professional workforce, e.g., as part of the Comprehensive National Security Initiative, the executive branch has/will "begin a campaign to promote cybersecurity awareness and digital literacy from our boardrooms to our classrooms and begin to build the digital workforce of the 21st century." The proposed certificate program is intended to help provide a well-trained workforce to meet the increasing demand for cybersecurity experts in the modern economy.

2. There must be a demonstrated and well-documented need for the program:

A) Why this certificate program is necessary: Students majoring Computer Science, as well as related Mathematical and Engineering disciplines, would benefit from the proposed certificate program as new courses will be designed and existing courses will be restructured to include material that will support the certificate program. This is very consistent with the "USG Cyber Security Initiative that will focus all of the cyber education and training resources across USG in order to meet the needs of the U.S. Army Cyber Command, the National Security Agency, the financial transaction processing industry and the health informatics/electronic medical records industry. The initiative aims to create a cybersecurity workforce of sufficient scale, quality, and capability to meet the needs of Georgia companies, military installations, government agencies and other institutions." For more information please refer to: http://gov.georgia.gov/press-releases/2014-12-10/deal-state-acts-high-demand-career-initiative-report. Also note the report from Information Systems Audit and Control Association, Inc. (ISACA): "Cybersecurity skills are in high demand, as threats continue to plague enterprises around the world. An overwhelming majority of students surveyed by ISACA recognizes this and plans to work in a position that requires cybersecurity knowledge. However, one in five report that their universities do not offer cybersecurity courses and less than half feel they will have the adequate skills and knowledge when they graduate" (http://www.isaca.org/cyber/pages/cybersecurity-fundamentals-certificate/aspx). This proposed certificate is in line with the UGA strategic plan. The University of Georgia President Jere W. Morehead and Provost Pamela Whitten have announced a new hiring initiative focused on recruiting faculty to enhance the University's instruction and scholarship in the rapidly growing field of informatics: http://news.uga.edu/releases/article/presidential-informatics-hiring-initiative Computer Science Department is one of the few Departments on campus to receive an authorization to hire a tenure track Assistant Professor in the area of Data and Communications Privacy and a joint tenure-track Assistant Professor with Engineering on Secure Big Data.

B) Describe the expected stage of development:

1. Semester/Year of Program Initiation: Fall 2016
2. Semester/Year Full Implementation of Program: Fall 2016
3. Semester/Year First Certificates will be awarded: Spring 2017
4. Annual Number of Graduates expected (once the program is established): 20

Projected Future Trends for the number of students enrolled in the program: Expect continued growth based on the growth of our undergraduate majors from 441 in Fall 2013 to 751 in Fall 2015 and the growth in our graduate program from 118 enrolled students in Spring 2015 to 141 in Fall 2015. In addition, the number of Engineering majors is increasing as well.

3. Evidence of student demand for program sufficient to sustain reasonable enrollments:

Student interest in the program: In the Department of Computer Science (with over 140 graduate students), the current courses related to the certificate program have experienced increasing enrollments. Nationally, a large number of universities have started programs in Cybersecurity. At a national level, Cybersecurity programs are experiencing an undiminished and sustained upward trend. We have completed a formal survey of the M.S. and Ph.D. students in Computer Science, 69 responded, and found that 28%, 23%, 9% “definitely would”, “might”, “would not” consider pursuing a certificate in Cybersecurity, respectively. And according to the survey, 22% are not sure and 18% will be graduating.

A) Diversity: The certificate program is expected to have diversity composition similar to those in the degree programs it draws from. Advertising and outreach to minorities will be included.

4. Design and curriculum of the program:

A) Detailed Curriculum:
Eligibility: Admission is open to currently enrolled graduate students across the university, but is specifically targeted towards graduate students in Computer Science, and related Mathematical and Engineering disciplines.

Curriculum: Cybersecurity spans all aspects of computer systems and networks, from hardware, to software, to systems' architecture and design. To complete the Graduate Certificate Program in Cybersecurity students must complete **18-20** hours of graduate coursework with **12** hours of core courses in Computer Science and **6-8** hours of elective coursework related to Cybersecurity.

The propose certificate requires students to first acquire the foundations of computer and network security, which will be achieved via three core courses. All three core courses are essential. As security threads focus on computer operating systems and computer networks, the first two classes are foundational computer science. The mainstream cybersecurity class for beginning graduate students is CSCI 6250.

CSCI 6730 Operating Systems
CSCI 6760 Computer Networks
CSCI 6250 Computer Security

While the Operating Systems and Computer Networks course do not embed "security" in the course title, they do include important security concepts. For instance, the Operating System course teaches concepts such as process isolation and access control. The Computer Networks course includes material related to the confidentiality, integrity, and authenticity of network communications. In addition, it teaches basic concepts related to Web security.

The course descriptions are listed below:

Core Courses (12 hours):

CSCI 6730 Operating Systems (4 hr)
Coverage of the key concepts in modern operating systems. Specific topics include process management, synchronization mechanisms, scheduling strategies, deadlock detection/avoidance, memory management, file systems, protection and security, and distributed systems. Concepts will be reinforced through programming projects using a realistic operating system.
Prereq: [(CSCI 4720 or CSEE 4280) and CSCI 2720] or CSCI 6720.

CSCI 6760 Computer Networks (4 hr)
In-depth coverage of computer networks, including: digital data transmission and encoding, layered protocol models, Internet protocol, Internet client-server software, and network design methodology.
Prereq: CSCI 2720 and (CSCI 2670 or CSEE 2220).

CSCI 6250 Computer Security (4 hr)
Basic concepts of computer security and the theory and current practices of authentication, authorization, and privacy mechanisms in modern operating systems and networks.
Prereq: CSCI 4730/6730 or CSCI 4760/6760.

Electives (6-8 hours):

CSCI 6050 Software Engineering (4 hr)
Full cycle of a software system development effort, including requirements definition, system analysis, design, implementation, and testing. Special emphasis is placed on system analysis and design. The design phase includes development of a user interface. A large term project incorporates the full software life cycle.
Prereq: CSCI 2720.

CSCI 6260 Data and Communications Privacy (4 hr) [new course offering]
This course focuses on privacy issues related to data collection and analysis, and on private communications. Specifically, it will cover the foundations of privacy-preserving data analysis as well privacy-enhancing technologies that have been so far proposed to provide private and anonymous communications over the Internet.
The course will include the following topics: Applied cryptography, Secure Multi-party computation, Privacy-preserving data analytics, Privacy-enhancing technologies Confidential and anonymous communications, internet censorship and anti-censorship technologies.

Prereq: CSCI 1730.

CSCI 6370 Database Management (4 hr)
The theory and practice of database management. Topics to be covered include efficient file access techniques, the relational data model as well as other data models, query languages, database design using entity-relationship diagrams and normalization theory, query optimization, and transaction processing.
Prereq: CSCI 2720.

CSCI 6570 Compilers (4 hr)
Design and implementation of compilers for high-level programming languages. Topics include all phases of a typical compiler, including scanning, parsing, semantic analysis, intermediate code generation, code optimization, and code generation. Students design and develop a compiler for a small programming language. Emphasis is placed on using compiler development tools. Prereq: CSCI 4720 or CSCI 6720.

CSCI 6720 Computer Systems Architecture (4 hr)
Functional components and structure of computing systems. Topics include principles of combinational and sequential logic, number systems and computer arithmetic, hardware subsystem design and test, I/O and memory subsystem principles and techniques, instruction set architecture and implementation, pipelining and system-level parallelism, interconnection networks, trends. Prereq: CSCI 4720.

CSCI 6780 Distributed Computing Systems (4 hr)
The fundamental concepts in distributed computing and the practical techniques for building distributed systems. Topics include distributed computing models, naming, synchronization, replication and consistency, fault tolerance, and security. Widely deployed distributed systems are used as case studies. Students design, implement, and analyze prototype systems.
Prereq: (CSCI 2720 and CSCI 1730) or CSCI 7010.

CSCI 8060 Advanced Software Engineering (4 hr)
Analysis of advanced methods in software engineering. Emphasis is placed on formal specification methods, advanced software testing, software reuse, distributed software design, and communication protocol specification. Studies include advanced software development tools and systems. Prereq: CSCI 4050/6050 and CSCI 4370/6370.

CSCI 8240 Software Security and Cyber Forensics (4 hr)
Exploration of both the foundation and recent advances in software security and cyber forensics. Topics will include software vulnerability analysis, advanced attack and defense techniques, cybercrime investigation and forensics, and security and forensics in different platforms (e.g., mobile, cloud computing, web application). Prereq: CSCI 4730/6730 or CSCI 4250/6250 or permission of department.

CSCI 8250 Advanced Network and Security Systems (4 hr)
Recent advances in computer networks and system security. Fast and secure network systems, secure storage systems, high performance intrusion detection systems, and efficient anti-abuse systems. Prereq: CSCI 4250/6250 or CSCI 4760/6760.

CSCI 8260 Computer Network Attacks and Defenses (4 hr)
This is an advanced course on computer and network security. The course will mainly focus on reading and analyzing recent top- tier research publications in the field of computer security and privacy and on the research and development of systems that can enforce security and privacy in the real world. Prereq: CSCI 4760/6760 or CSCI 4250/6250 or permission of department.

CSCI 8730 Advanced Topics in Operating Systems (4 hr)
Software systems geared at supporting parallel and distributed computing. Programming language support will focus on simple and efficient ways to express parallel programs. Compiler and operating system support will focus on new optimizations to make parallel programs execute more efficiently. Prereq: CSCI 4730/6730.

MATH 6450 Cryptology and Computational Number Theory (3 hr)
Recognizing prime numbers, factoring composite numbers, finite fields, elliptic curves, discrete logarithms, private key cryptology, key exchange systems, signature authentication, public key cryptology. Prereq: MATH 4000/6000.

STAT 6510 Mathematical Statistics I (3 hr)
Concepts and basic properties of some special probability distributions, independence, moment generating functions, sampling distributions of statistics, limiting distributions.
Prereq: MATH 2270 or MATH 2500.

These elective courses are related to Cybersecurity as follows:

- Compilers, Software Engineering, and Advanced Software Engineering provide the necessary knowledge to study software security (secure software development, automatically finding software vulnerabilities, etc.).

- Database Management includes concepts related to access control.

- Computer Systems Architecture is necessary to understand trusted computing platforms.

- Distributed Computing Systems includes fundamental concepts such as fault tolerance and the security of geographically distributed and complex systems.

- Advanced Topics in Operating Systems includes advanced concepts related to systems security, including OS kernel security.

- Mathematical Statistics I introduces fundamental concepts required for instance to develop statistical malware detectors, and in general to design anomaly-based attack detection systems.

- MATH 6450 is relevant due to the importance of encryption for Computer Security.

- Software Security and Cyber Forensics, Data and Communications Privacy, Advanced Network and Security Systems, Computer Network Attacks and Defenses, and Cryptology and Computational Number Theory are all directly related to cybersecurity.

Note: all the courses, except CSCI 6260, currently exist. This new course will be particularly useful in that it will deal with privacy issues in depth.

B) Model Programs and Curricula:

Georgia Institute of Technology:
https://pe.gatech.edu/certificates/cyber-security-certificate.
This certificate has only one core course (Cyber Security: A Systems Approach) and the rest are electives. This certificate is designed for technical professionals who seek to develop deeper and broader knowledge as they take on growing responsibilities for securing organizational assets.

University of Maryland University College:
http://www.umuc.edu/cybersecurity/academics/certificates.cfm
This is an online certificate.

The Central Michigan University:
www.cmich.edu/Cybersecurity
Required Courses *(15 hours)*
Network & Systems Security Fundamentals, Governance, Risk, & Compliance in Cybersecurity, Cybercrime Forensics, Managing Security & Privacy in the Cloud, and Cybersecurity, Systems and Network Certification.

The proposed certificate program has 2 core courses and electives from Computer Science, Mathematics and Statistics. The proposed certificate is more rigorous than the above mentioned certificates.

There are a number of other universities offering graduate certificates in Cybersecurity as well as full degree programs at the Master's and Doctoral levels.

C) Program Accreditation: The undergraduate Computer Science Degree program is accredited by the Accreditation Board for Engineering and Technology (ABET), but the Computer Science graduate programs do not need to be accredited.

5. Faculty resources:

A) Full-time faculty: The current full-time faculty within the Department of Computer Science are sufficient to initiate the proposed certificate program. More than half of the department's faculty have taught the required and/or the elective courses for the certificate.

B) List of involved faculty:

- Hamid Arabnia, Professor, Ph.D., University of Kent, U.K.
- Ismailcem Budak Arpinar, Associate Professor, Ph.D., Middle East Technical University, Turkey
- Brad Barnes, Lecturer, Ph.D., The University of Georgia
- Suchi Bhandarkar, Professor, Ph.D., Syracuse University
- Daniel M. Everett, Assistant Professor, Ph.D., University of Wisconsin
- Maria Hybinette, Associate Professor, Ph.D, Georgia Institute of Technology
- Krzysztof J. Kochut, Professor, Ph.D., Louisiana State University
- Kyu Hyung Lee, Assistant Professor, Ph.D., Purdue University
- Kang Li, Professor, Ph.D., Oregon Graduate Institute
- John A. Miller, Professor, Ph.D., Georgia Institute of Technology
- Roberto Perdisci, Associate Professor, Ph.D. University of Cagliari, Italy
- Lakshmish Ramaswamy, Associate Professor, Ph.D., Georgia Institute of Technology
- Thiab Taha, Professor and Head, Ph.D., Clarkson University

Note: More detailed information about the listed Faculty above can be found at: http://www.cs.uga.edu/directory/front

Most of the above courses are taught by one or two of the above listed faculty and therefore, there will be no need to adjust their assignments unless the program expands by admitting a considerable number of students.

C) Additional faculty: The department was authorized in August 2015 to hire a Tenure-track Assistant Professor in Data and Communications Privacy as part of the President’s Informatics Hiring Initiative. The new hire will start in August 2016 and will teach courses relevant to this certificate such as the Privacy course. Please see the formal job Ad for more information on the position (http://www.cs.uga.edu/news-and-events/tenure-track-assistant-professor-position-computer-science-0).

6. Resources needed to support the program:

A) Library resources: There is no need for additional library resources.

B) Equipment: There is no need for additional equipment.

7. Physical facilities:

There is no need for additional physical facilities.

8. Expense to the institution:

A) Funding to initiate the program (first three years): No amount of funding is needed for Years 1-3.

B) Support for students: The program will not be providing assistantships.

9. Commitments of financial support:

A) Sources of additional funds: Current funding through the Department of Computer Science will be sufficient to initiate and maintain the certificate program.

B) Long-range plans: The Department was authorized in August 2015 to hire a Tenure-track Assistant Professor in Data and Communications Privacy as part of the President's Informatics Hiring Initiative. This new hire will teach courses relevant to this certificate.

10. Administration of the program:

The proposed graduate certificate in Cybersecurity will be administered by the Graduate Coordinator of the Computer Science Department. Students will be admitted to the certificate program by submitting an application to the Graduate Coordinator. The administrator in conjunction with the Department Head will be responsible for admitting students to the certificate program, coordinating course offerings, maintaining student records, promoting activities, securing additional funding, and consulting with the department's graduate program and curriculum committees regarding courses in the certificate program.

The semester before completing the certificate, students will be required to fill out a certificate completion form. The graduate certificate will be awarded to the student upon the completion of her/his graduate degree.