Board of Governors, State University System of Florida

Request to Offer a New Degree Program

Florida International University	**Fall 2014**
University Submitting Proposal	**Proposed Implementation Term**
	School of Computing and Information Sciences (SCIS), and Department of Electrical and Computer Engineering (ECE)
College of Engineering & Computing	
Name of College(s) or School(s)	**Name of Department(s)/ Division(s)**
Cybersecurity	**Master of Science in Cybersecurity**
Academic Specialty or Field	**Complete Name of Degree**
11.1003	
Proposed CIP Code	

The submission of this proposal constitutes a commitment by the university that, if the proposal is approved, the necessary financial resources and the criteria for establishing new programs have been met prior to the initiation of the program.

Date Approved by the University Board of Trustees		**President**		**Date**
Signature of Chair, Board of Trustees	**Date**	**Vice President for Academic Affairs**		**Date**

Provide headcount (HC) and full-time equivalent (FTE) student estimates of majors for Years 1 through 5. HC and FTE estimates should be identical to those in Table 1 in Appendix A. Indicate the program costs for the first and the fifth years of implementation as shown in the appropriate columns in Table 2 in Appendix A. Calculate an Educational and General (E&G) cost per FTE for Years 1 and 5 (Total E&G divided by FTE).

Implementation Timeframe	Projected Enrollment (From Table 1)		Projected Program Costs (From Table 2)				
	HC	FTE	E&G Cost per FTE	E&G Funds	Contract & Grants Funds	Auxiliary Funds	Total Cost
Year 1	42	23.63	16,885	399,000	0	0	399,000
Year 2	46	25.88					
Year 3	53	29.81					
Year 4	57	32.06					
Year 5	63	35.44	11,258	399,000	0	0	399,000

Note: This outline and the questions pertaining to each section must be reproduced within the body of the proposal to ensure that all sections have been satisfactorily addressed. Tables 1 through 4 are to be included as Appendix A and not reproduced within the body of the proposals because this often causes errors in the automatic calculations.

INTRODUCTION

I. Program Description and Relationship to System-Level Goals

A. Briefly describe within a few paragraphs the degree program under consideration, including (a) level; (b) emphases, including concentrations, tracks, or specializations; (c) total number of credit hours; and (d) overall purpose, including examples of employment or education opportunities that may be available to program graduates.

The School of Computing and Information Sciences (SCIS) and the Department of Electrical and Computer Engineering (ECE) plan to offer a Master of Science degree in Cybersecurity (MS-Cybersecurity) to complement their current graduate offerings of MS and PhD in Computer Science (CS), MS in Information Technology (IT), MS in Telecommunications and Networking (TCN), MS and PhD in Electrical Engineering (EE), and MS in Computer Engineering (CpE). The goal is to provide broad and deep technical training in cybersecurity, enabling its graduates to address the critical security needs facing our nation today.

A growing number of universities are offering such programs in the US. Our program will be the first such program in the state of Florida, offering the students in a formal in-classroom education setting. The MS-Cybersecurity program is designed for students holding a Bachelor's degree in Computer Science, Computer Engineering, Information Technology, or a related discipline. These students will have solid skills in programming, analytical thinking, and mathematical maturity to allow the courses in the MS-Cybersecurity program to be taught at the deep technical level necessary for rigorous understanding of cybersecurity. At the same time, to address the broad security issues involving various dimensions, including social and political aspects, our MS-Cybersecurity program will also encompass courses allowing the study of computer security from a wide variety of perspectives.

The proposed MS-Cybersecurity program will be course based, requiring 30 credits from 10 courses. A required core of 5 courses is envisioned, together with 5 additional courses to be chosen from an approved set of electives. The core courses are carefully designed to include three complementary perspectives: (1) a practical, hands-on study of current "best practices" in cybersecurity, along with their limitations; (2) a study of the principles of the growing science of cybersecurity; and (3) a study of the broader human context of cybersecurity, including social, economic, and policy aspects. In addition, the students will elect five courses from a set of graduate-level courses to ensure a broad and in-depth exposure to various topics in cybersecurity.

Given the growing and widely recognized importance of cybersecurity, our MS-Cybersecurity program will be attractive to a large body of students, including both new graduates in computing-related disciplines and skilled professionals in South Florida, including those in the FBI, CIA, Secret Service, and US Southern Command. The program will draw our faculty strong expertise in research and education related to cybersecurity. For example, the program will be fully supported by our faculty in the Florida Cyber Infrastructure Education and Research for Trust and Assurance (CIERTA) Center housed at the FIU School of Computing and Information Sciences, which aims at increasing FIU's presence in cybersecurity, making it more attractive to strong cybersecurity students and researchers, and increasing its competitiveness for large-scale cybersecurity research.

B. Describe how the proposed program is consistent with the current State University System (SUS) Strategic Planning Goals. Identify which specific goals the program will directly support and which goals the program will indirectly support. (See the SUS Strategic Plan at http://www.flbog.edu/pressroom/_doc/2011-11-28_Strategic_Plan_2012-2025_FINAL.PDF)

The MS-Cybersecurity program will directly support SUS Goals in **Teaching & Learning**, specifically advancing the strategic priority of increasing the number of graduate STEM degrees in the critical area of cybersecurity. It will also directly support **Community & Business Engagement** by increasing the community workforce in this area. (See II.A below for further discussion of the current workforce shortage in cybersecurity.)

The MS-Cybersecurity program will also indirectly support the SUS Goals in **Scholarship, Research, & Innovation** though its innovative curriculum which will focus both faculty and graduate students on the key concepts and technologies needed to address the deep challenges of cybersecurity. It is expected that a number of the MS-Cybersecurity graduates will go on to doctoral study in Computer Science or Electrical Engineering and will then have the skills needed for truly innovative research in cybersecurity.

C. *If the program is to be included in an Area of Programmatic Strategic Emphasis as described in the SUS Strategic Plan, please indicate the category and the justification for inclusion.*

The Areas of Programmatic Strategic Emphasis:

1. *Critical Needs:*
   - *Education*
   - *Health Professions*
   - *Security and Emergency Services*
2. *Economic Development:*
   - *Globalization*
   - *Regional Workforce Demand*
3. *Science, Technology, Engineering, and Math (STEM)*

The program is in the **Science, Technology, Engineering, and Math** (STEM) area of Programmatic Strategic Emphasis; it will develop the deep technical and mathematical skills allowing rigorous solutions to the challenging problems of cybersecurity. The program moreover addresses the Critical Needs area of **Security and Emergency Services**.

D. *Identify any established or planned educational sites at which the program is expected to be offered and indicate whether it will be offered only at sites other than the main campus.*

The MS-Cybersecurity Program will be offered exclusively at FIU's Modesto A. Maidique Campus and Engineering Center.

INSTITUTIONAL AND STATE LEVEL ACCOUNTABILITY

II. Need and Demand

A. *Need: Describe national, state, and/or local data that support the need for more people to be prepared in this program at this level. Reference national, state, and/or local plans or reports that support the need for this program and requests for the proposed program which have emanated from a perceived need by agencies or industries in your service area. Cite any specific need for research and service that the program would fulfill.*

The state of cybersecurity in today's world is poor, as demonstrated in a host of ways, such as

- the massive vulnerabilities of real systems, as demonstrated by recent news about Shanghai Unit 61398 and Stuxnet;
- the 2010 statement by Debora Plunkett, head of NSA's Information Assurance Directorate, that "we have to build our systems on the assumption that adversaries will get in";
- the continual stream of operating system security patches being issued, with unclear efficacy;
- unresolved social and legal questions about violations of privacy by NSA, Google, and many others;
- the non-usability of authentication nowadays, where users are expected to memorize and constantly change large numbers of non-memorable passwords; and
- the general unreliability (or "flakiness") of all interactions with computers.

This situation calls out for a certain amount of honest humility, as Purdue computer scientist Gene Spafford observes in his February 23, 2013 weblog,

> Calling someone in the 1600s a "medical professional" because he knew how to let blood, apply leeches, and hack off limbs with a carpenter's saw using assistants to hold down the unanesthetized patient creates a certain cognitive dissonance; today, calling someone a "cyber security professional" based on knowledge of how to configure Windows, deploy a firewall, and install anti-virus programs should probably be viewed as a similar oddity. We need to evolve to where the deployed base isn't so flawed, and we have some knowledge of what security really **is** — evolve from the equivalent of "sawbones" to infectious disease specialists.

To move from this poor status quo towards a cyber-infrastructure that is secure and trustworthy will require workers trained to understand security deeply in all its facets. This involves knowledge of both widely-deployed current technologies like firewalls and anti-virus software, with all their inadequacies, as well as new foundations for rigorous security, which are however often far from current practice. Knowledge of this depth and breadth cannot be gained in just a couple of classes; instead what is needed is the sort of coherent and comprehensive study that the MS-Cybersecurity program will aim to provide.

Specific evidence of the need for better-trained security professionals was found in a recent lecture by Marisa S. Viveros, IBM Vice President for Cyber Security Innovation, stating that 58% of chief information security officers report being unable to find people with the right skills. Also, MS programs in Cybersecurity are now being started at a number of universities, including Stevens, Johns Hopkins, and Drexel, making an MS-Cybersecurity program in the state of Florida very timely.

The critical need for such a program in South Florida was indicated at the September 13, 2013 SCIS Industrial Advisory Board meeting, where Christopher Fleck, Vice President of Community and Solutions Development at Citrix, stated that Citrix was unsuccessful at attracting local hires for security positions, forcing them to hire out-of- state security professionals. Further, these hires do not relocate, but work remotely from outside of Florida. Steven Reid, Vice President of Software Engineering at Ultimate Software, made similar statements and commented that these are very high-paying jobs. The consensus of the board is that jobs in cybersecurity are increasing and will continue to be a challenge to fill in the absence of MS-Cybersecurity programs to build a base of trained security professionals.

B. *Demand: Describe data that support the assumption that students will enroll in the proposed program. Include descriptions of surveys or other communications with prospective students.*

The need for cybersecurity is very much "in the air" nowadays, with constant stories in the press about the high demand for cybersecurity professionals and the high salaries they command. Numerous MS programs in cybersecurity are currently begin developed around the country, and current undergraduate students in SCIS and ECE have shown great interest in our proposed MS-Cybersecurity program, making many inquiries to our Graduate Program Director about its date of availability. Moreover, our existing undergraduate security courses show very strong enrollments: in Spring 2014, *EEL 4789 Ethical Hacking and Countermeasures* has an enrollment of 46 students and *CNT 4403 Computing and Network Security* has an enrollment of 89 students.

C. *If substantially similar programs (generally at the four-digit CIP Code or 60 percent similar in core courses), either private or public exist in the state, identify the institution(s) and geographic location(s). Summarize the outcome(s) of communication with such programs with regard to the potential impact on their enrollment and opportunities for possible collaboration (instruction and research). In Appendix B, provide data that support the need for an additional program as well as letters of support, or letters of concern, from the provosts of other state universities with substantially similar programs.*

Our MS-Cybersecurity program has CIP code 11.1003. There is no other state program under this CIP Code according to the published Academic Program Inventory at State University System of Florida (see https://prod.flbog.net:4445/pls/apex/f?p=136:13:6160765317133128). Note that USF is starting a new,

fully online, MS program in cybersecurity, but with CIP code 43.0303 and with a major focus on management. Our program is in contrast technical in its focus, and including hands-on experience in security laboratories; such technical experience cannot be provided by an online program.

D. *Use Table 1 in Appendix A (A for undergraduate and B for graduate) to categorize projected student headcount (HC) and Full Time Equivalents (FTE) according to primary sources. Generally undergraduate FTE will be calculated as 40 credit hours per year and graduate FTE will be calculated as 32 credit hours per year. Describe the rationale underlying enrollment projections. If, initially, students within the institution are expected to change majors to enroll in the proposed program, describe the shifts from disciplines that will likely occur.*

As seen in Table 1-B in Appendix A, a total headcount of 120 (FTE: 23.63) is projected in the first year, followed by steady growth in subsequent years, leading to a projected headcount of 63 students (FTE: 35.44) in the 5th year. The enrollment projections are realistic, given that the program will become known to more and more students over time, and given the number of stories in the news emphasizing of the critical need for improved cybersecurity and the very strong demand for cybersecurity professionals.

E. *Indicate what steps will be taken to achieve a diverse student body in this program. If the proposed program substantially duplicates a program at FAMU or FIU, provide, (in consultation with the affected university), an analysis of how the program might have an impact upon that university's ability to attract students of races different from that which is predominant on their campus in the subject program. The university's Equal Opportunity Officer shall review this section of the proposal and then sign and date in the area below to indicate that the analysis required by this subsection has been reviewed and approved.*

FIU is a minority-serving institution, with over 70% of the student body being minority. The MS-Cybersecurity program will directly enhance the capabilities, interests, and careers of our minority students. Both School of Computing and Information Sciences and the Department of Electrical and Computer Engineering are top producers of graduate degrees to Hispanics in Computer Science and Engineering. The program will be part of FIU's comprehensive industry and academic programs, and will take advantage of existing research, education, and workforce development activities.

Signature of Equal Opportunity Officer **Date**

III. Budget

A. *Use Table 2 in Appendix A to display projected costs and associated funding sources for Year 1 and Year 5 of program operation. Use Table 3 in Appendix A to show how existing Education & General funds will be shifted to support the new program in Year 1. In narrative form, summarize the contents of both tables, identifying the source of both current and new resources to be devoted to the proposed program. (Data for Year 1 and Year 5 reflect snapshots in time rather than cumulative costs.) If the university intends to operate the program through continuing education on a cost-recovery basis or market rate, provide a rationale for doing so and a timeline for seeking Board of Governors' approval, if appropriate.*

As detailed in Tables 2 and 3 in Appendix A, new recurring E&G funds are sought to support this new program in its first five years. We estimate that we will need to offer 12 course sections per year with an average enrollment of about 25 students, requiring 2 faculty FTE to provide that teaching effort. We also estimate a 0.75 FTE support personnel that will perform support and administrative duties related to the new program.

B. *If other programs will be impacted by a reallocation of resources for the proposed program, identify the program and provide a justification for reallocating resources. Specifically address the potential negative impacts that implementation of the proposed program will have on related undergraduate programs (i.e., shift in faculty effort, reallocation of instructional resources, reduced enrollment rates,*

greater use of adjunct faculty and teaching assistants). Explain what steps will be taken to mitigate any such impacts. Also, discuss the potential positive impacts that the proposed program might have on related undergraduate programs (i.e., increased undergraduate research opportunities, improved quality of instruction associated with cutting-edge research, improved labs and library resources).

The additional resources included in Table 2 will ensure that the MS-Cybersecurity program can be offered without negative impacts to existing programs. Moreover, it is anticipated that increasing FIU's capabilities in this area (e.g. richer graduate curriculum, improved cybersecurity laboratories) will eventually result in improved opportunities for undergraduate teaching and research in cybersecurity, potentially leading to large-scale external funding in the future.

C. *Describe other potential impacts on related programs or departments (e.g., increased need for general education or common prerequisite courses, or increased need for required or elective courses outside of the proposed major).*

The proposed MS-Cybersecurity program is very different from all of FIU's degree programs currently offered, and it can therefore be expected to have minimal impact on any of them. It does have some similarity with the existing Security Track in the MS-IT program, but the focus of the two programs is quite different:

- The MS-IT Security Track is part of the general MS-IT program, which aims at a general study of Information Technology and which includes core courses (*CEN 5087 Software and Data Modeling* and *CIS 5027 Computer Systems Fundamentals*) that are not directly relevant to cybersecurity.
- The MS-Cybersecurity program, in contrast, is totally focused on a deep and broad study of cybersecurity.

Furthermore, the MS-IT program also includes a Software Track and a Systems Administration Track, which are entirely distinct from the MS-Cybersecurity program. It is therefore expected that the MS-Cybersecurity program will have minimal impact on the MS-IT program.

D. *Describe what steps have been taken to obtain information regarding resources (financial and in-kind) available outside the institution (businesses, industrial organizations, governmental entities, etc.). Describe the external resources that appear to be available to support the proposed program.*

This program would be primarily supported by tuition revenue. Efforts are also being made to identify potential industrial sponsors who might send their employees to this program or even provide direct support, such as donations of equipment for use in our security laboratories.

IV. Projected Benefit of the Program to the University, Local Community, and State

Use information from Tables 1 and 2 in Appendix A, and the supporting narrative for "Need and Demand" to prepare a concise statement that describes the projected benefit to the university, local community, and the state if the program is implemented. The projected benefits can be both quantitative and qualitative in nature, but there needs to be a clear distinction made between the two in the narrative.

Implementing the proposed MS-Cybersecurity program will bring significant benefits to FIU, to the Miami community, and to the state of Florida. FIU will see increased graduate enrollment and, more importantly, will increase its presence in the critically-important area of cybersecurity, making it more attractive to students at all levels and increasing its competitiveness for large-scale research funding in this area. The Miami community will benefit from a steady supply of well-trained security professionals in the community who are able to fill the currently-unmet needs of local companies, as discussed in Section II.A above. Finally, the state of Florida and indeed the nation as a whole will benefit from knowledge and technologies that move us towards a secure cyber infrastructure, one capable of realizing the promises, while avoiding the perils, of the new Information Age.

V. Access and Articulation – Bachelor's Degrees Only

A. *If the total number of credit hours to earn a degree exceeds 120, provide a justification for an exception to the policy of a 120 maximum and submit a separate request to the Board of Governors for*

an exception along with notification of the program's approval. (See criteria in Board of Governors Regulation 6C-8.014)

Not applicable.

B. *List program prerequisites and provide assurance that they are the same as the approved common prerequisites for other such degree programs within the SUS (see the Common Prerequisite Manual at FACTS.org). The courses in the Common Prerequisite Counseling Manual are intended to be those that are required of both native and transfer students prior to entrance to the major program, not simply lower-level courses that are required prior to graduation. The common prerequisites and substitute courses are mandatory for all institution programs listed, and must be approved by the Articulation Coordinating Committee (ACC). This requirement includes those programs designated as "limited access."*

If the proposed prerequisites are not listed in the Manual, provide a rationale for a request for exception to the policy of common prerequisites. NOTE: Typically, all lower-division courses required for admission into the major will be considered prerequisites. The curriculum can require lower-division courses that are not prerequisites for admission into the major, as long as those courses are built into the curriculum for the upper-level 60 credit hours. If there are already common prerequisites for other degree programs with the same proposed CIP, every effort must be made to utilize the previously approved prerequisites instead of recommending an additional "track" of prerequisites for that CIP. Additional tracks may not be approved by the ACC, thereby holding up the full approval of the degree program. Programs will not be entered into the State University System Inventory until any exceptions to the approved common prerequisites are approved by the ACC.

Not applicable.

C. *If the university intends to seek formal Limited Access status for the proposed program, provide a rationale that includes an analysis of diversity issues with respect to such a designation. Explain how the university will ensure that community college transfer students are not disadvantaged by the Limited Access status. NOTE: The policy and criteria for Limited Access are identified in Board of Governors Regulation 6C-8.013. Submit the Limited Access Program Request form along with this document.*

Not applicable.

D. *If the proposed program is an AS-to-BS capstone, ensure that it adheres to the guidelines approved by the Articulation Coordinating Committee for such programs, as set forth in Rule 6A-10.024 (see Statewide Articulation Manual at FACTS.org). List the prerequisites, if any, including the specific AS degrees which may transfer into the program.*

Not applicable.

INSTITUTIONAL READINESS

VI. Related Institutional Mission and Strength

A. *Describe how the goals of the proposed program relate to the institutional mission statement as contained in the SUS Strategic Plan and the University Strategic Plan.*

As noted in Section I.B, the goals of the proposed program relate to the SUS Strategic Plan's emphasis on STEM education and the Critical Needs area of Security and Emergency Services. Moreover, the SUS Commission on Higher Education Access and Educational Attainment report, *Aligning Workforce and Higher Education for Florida's Future* http://www.flbog.edu/about/_doc/commission-materials/Access-and-Attainment-Comm-FINAL-REPORT-10_29_13_rev.docx projects an annual undersupply of 2,361 in

Computer Occupations (Table 1) and specifically mentions CIP code 11.1003 (Computer and Information Systems Security/Information Assurance) among the college majors needed to fill this undersupply (Table 3).

B. *Describe how the proposed program specifically relates to existing institutional strengths, such as programs of emphasis, other academic programs, and/or institutes and centers.*

Florida's status as a major gateway for international banking, trade, and tourism makes cybersecurity critical for the economic development and welfare of the state. An innovative MS-Cybersecurity program at FIU will therefore be of great value, contributing a supply of well-trained professionals who are able to address the security needs of our state. The MS-Cybersecurity program also aligns perfectly with the new Florida *Cyber Infrastructure Education and Research for Trust and Assurance (CIERTA)* Center, which aims to provide an environment for synergistic multidisciplinary research and education in broad areas of cyber innovation, to facilitate collaboration among academic, government and industry institutions, and to increase community awareness of cyber-related issues and technologies. We envision that our MS-cybersecurity program will inspire a new generation of cyber research warriors, educate cyber savvy intelligence agents and workforce, and advance technologies specifically in cybersecurity and privacy of information, communication, and cyber-physical system, all with the goal of building a safer society.

C. *Provide a narrative of the planning process leading up to submission of this proposal. Include a chronology (table) of activities, listing both university personnel directly involved and external individuals who participated in planning. Provide a timetable of events necessary for the implementation of the proposed program.*

In Spring 2013, as part of the development of the Florida *CIERTA* Center (*Cyber Infrastructure Education and Research for Trust and Assurance*, http://cyber.cs.fiu.edu) discussions about a new MS-Cybersecurity program were begun. In Fall 2013, it was decided that the program should be a joint effort between the School of Computing and Information Sciences (SCIS) and the Department of Electrical and Computer Engineering (ECE). Discussions between these two departments led to the design of the proposed curriculum and its new core courses.

Planning Process

Date	Participants	Planning Activity
February 2013	Ram Iyengar, Giri Narasimhan, Niki Pissinou	Initial discussion of MS-Cybersecurity program
April 2013	Geoffrey Smith	First draft of program structure
October 2013	Geoffrey Smith, Mark Weiss, Malek Adjouadi, Alexander Perez-Pons	Preparation of Feasibility Study
November 2013	Geoffrey Smith, Bogdan Carbunar, Jinpeng Wei, Alexander Perez-Pons	Designing of core courses

Events Leading to Implementation

Date	Implementation Activity
January 2014	Preparation of New Course Proposals for core courses.
January 2014	Writing of this Request to Offer a New Degree Program

VII. Program Quality Indicators - Reviews and Accreditation

Identify program reviews, accreditation visits, or internal reviews for any university degree programs related to the proposed program, especially any within the same academic unit. List all recommendations and summarize the institution's progress in implementing the recommendations.

In August 2013, SCIS's BS in Computer Science program received re-accreditation until 2017 from ABET, with "no deficiencies, weaknesses, or concerns". ECE's BS in Electrical Engineering and in Computer Engineering are also accredited by ABET.

VIII. Curriculum

A. Describe the specific expected student learning outcomes associated with the proposed program. If a bachelor's degree program, include a web link to the Academic Learning Compact or include the document itself as an appendix.

The MS-Cybersecurity program will include student learning outcomes that address cybersecurity from several complementary perspectives:

1. Students will gain practical, hands-on skills in current "best practices" in cybersecurity, such as configuring firewalls and writing secure web applications, while also understanding their limitations.
2. Students will gain deep knowledge of the principles of the emerging science of cybersecurity, enabling them to understand and even design solutions with rigorously-provable security guarantees.
3. Students will gain understanding of the broader human context of cybersecurity, enabling them to consider and address its social, economic, political, and psychological implications.
4. Students will gain deeper knowledge of specific areas in cybersecurity through their selection of elective courses.

B. Describe the admission standards and graduation requirements for the program.

Current standards of admission into the College of Engineering and Computing will be used as parameters for admission into the MS-Cybersecurity program. Specific requirements for the program will be a Bachelor's degree in Computer Science, Computer Engineering, Information Technology, or a similar discipline, along with acceptable scores on the TOEFL (if relevant).
For graduation, the students are required to earn 30 credit hours from 10 courses, including 5 core courses and 5 elective courses chosen from an approved set of electives.

C. Describe the curricular framework for the proposed program, including number of credit hours and composition of required core courses, restricted electives, unrestricted electives, thesis requirements, and dissertation requirements. Identify the total numbers of semester credit hours for the degree.

The proposed MS-Cybersecurity program will be course based, requiring 30 credits from 10 courses. A required core of 5 courses is envisioned, together with 5 additional courses to be chosen from an approved set of electives. The core courses are carefully designed to include three complementary perspectives: (1) a practical, hands-on study of current "best practices" in cybersecurity, along with their limitations; (2) a study of the principles of the growing science of cybersecurity; and (3) a study of the broader human context of cybersecurity, including social, economic, and policy aspects. In addition, the students will elect five courses from a set of graduate-level courses to ensure a broad and in-depth exposure to various topics in cybersecurity.

D. Provide a sequenced course of study for all majors, concentrations, or areas of emphasis within the proposed program.

Students will be able to complete the MS-Cybersecurity program in 3 or 4 semesters of study. The first two semesters will ordinarily focus on the completion of the 5 core courses, and the last one or two semesters on the completion of the electives. But there will be flexibility to take courses in other orders if appropriate.

E. Provide a one- or two-sentence description of each required or elective course.

Note that the precise core course prefixes and numbers for the new courses will be determined later; the new course proposals are attached with this proposal.

Core Courses:

EEE 5xxx Practical Applied Security (3)
Hands-on training in practical installation and maintenance of secure systems, including such topics as security configuration, DMZs, firewalls, anti-virus software, hardware security modules (HSMs). Study of common attacks and how to protect against them. Class to be held in a security lab.

CIS 5xxx Secure Application Programming (3)
Development of applications that are free from common security vulnerabilities, such as buffer overflow, SQL injection, and cross-site scripting attacks. Emphasis is on the development of distributed web applications in Java.

CIS 5xxx Principles of Cybersecurity (3)
Cybersecurity algorithms and techniques. Mathematical foundations. Symmetric and public key encryption. Authentication, key infrastructure and certificates. Covert channels. Access control. Security vulnerabilities.

CIS 5xxx Formal Foundations for Cybersecurity (3)
Formal models and methods for achieving rigorous security guarantees. Cryptographic indistinguishability properties (such as IND-CPA) and their reduction proofs. Formal analyses of security APIs. Secure information flow and quantitative information flow.

CIS 5xxx Social, Economic, and Policy Aspects of Cybersecurity (3)
The broader human context of cybersecurity, from the perspective of society, economics and policy.

Elective courses at SCIS:

CIS 5373 Systems Security (3)
Risk, Trust, and Threat models; Types of Attacks; Safe Programming Techniques; Operating System Mechanisms, Virtual Machine Systems; Hardware Security Enforces; Application Security; Personal Security.

CIS 5374 Information Security and Privacy (3)
Information Security Planning, Planning for Contingencies, Policy, Security Program, Security Management Models, Database Security, Privacy, Information Security Analysis, Protection Mechanism.

TCN 5080 Secure Telecommunications Transactions (3)
Telecom and information security issues such as: digital signatures, cryptography as applied to telecom transactions, network policing, nested authentication, and improving system trust.

TCN 5455 Information Theory (3)
Entropy and measure of information. Proof and interpretation of Shannon's fundamental theorem for various channels, including noiseless, discrete, time-discrete and time-continuous channels.

TCN 6880 Telecommunications Public Policy Development and Standards (3)
A concept-oriented examination of the domestic and international telecommunications policy processes and standards setting environment.

CAP 6778 Advanced Topics in Data Mining (3)
Web, stream data, and relational data mining, graph mining, spatiotemporal data mining, privacy-preserving data mining, high-dimensional data clustering, social network, and linkage analysis.

Elective Courses at ECE:

TCN 5271 Ubiquitous and Embedded Sensor Network- Centric Telecommunications (3) Techniques impacting ubiquitous, embedded sensor network-centric telecommunications, context-awareness,

autonomy, data quality, uncertainty, privacy, trustworthiness and wearable computing.

EEL 6787 Network Security (3)
Network Security Requirements, Number Theory, Steganography, Encryption Design Principles and Algorithms, Message Authentication and Digital Signature Principle and Designs, Network System Security Design.

EEE 6xxx Advanced Malware Reverse Engineering (3)
Tools and techniques to perform reverse engineering of suspicious files and firmware present of various devices (computers, DVD players, etc.) to analyze their impact.

EEL 5xxx Advanced Ethical Hacking (3)
Gives individuals an exposure to the latest hacking tools and techniques to understand and analyze the anatomy of computer attacks, and countermeasures to protect valuable data.

EEL 6xxx Advanced Digital Forensics Engineering (3)
Provides advanced skills in the area of computer and network forensics and media exploitation, including techniques to identify, contain, and remediate sophisticated threats including corporate espionage, 'hacktivism', financial crime syndication, and Advanced Persistent Threats (APT) groups.

F. *For degree programs in the science and technology disciplines, discuss how industry-driven competencies were identified and incorporated into the curriculum and indicate whether any industry advisory council exists to provide input for curriculum development and student assessment.*

The *SCIS Industrial Advisory Board (IAB)* meets quarterly to discuss program development activities with the SCIS director and FIU administrators, and to interact with faculty and students. It provides valuable industry feedback and insights on the direction, design, and execution of our research and education programs. As described in Section II.A above, *IAB* members have already shared their perspectives on the importance to their companies of the proposed MS-Cybersecurity program. Going forward, their feedback will be sought to guide us in implementing the program most effectively.

The *JPMorgan Chase Information Innovation Center at FIU* is another important industrial partnership that will foster collaboration, in both education and research, in cybersecurity areas such as network security, privacy and authentication, and cyber-physical systems.

G. *For all programs, list the specialized accreditation agencies and learned societies that would be concerned with the proposed program. Will the university seek accreditation for the program if it is available? If not, why? Provide a brief timeline for seeking accreditation, if appropriate.*

The National Security Agency and U.S. Department of Homeland Security are currently revising standards for cybersecurity programs, with the possibility of review of new programs apparently planned starting in 2015. When appropriate, we will seek such accreditation for our program.

H. *For doctoral programs, list the accreditation agencies and learned societies that would be concerned with corresponding bachelor's or master's programs associated with the proposed program. Are the programs accredited? If not, why?*

Not applicable.

I. *Briefly describe the anticipated delivery system for the proposed program (e.g., traditional delivery on main campus; traditional delivery at branch campuses or centers; or nontraditional delivery such as distance or distributed learning, self-paced instruction, or external degree programs). If the proposed delivery system will require specialized services or greater than normal financial support, include projected costs in Table 2 in Appendix A. Provide a narrative describing the feasibility of delivering the proposed program through collaboration with other universities, both public and private. Cite specific queries made of other institutions with respect to shared courses, distance/distributed*

learning technologies, and joint-use facilities for research or internships.

The MS-Cybersecurity program will be delivered using traditional classroom teaching methods on the FIU main campus. The courses will be readily taught by faculty and accommodated by existing teaching facilities in the School of Computing and Information Sciences and the Department of Electrical and Computing Engineering. No special arrangement is needed.

IX. Faculty Participation

A. Use Table 4 in Appendix A to identify existing and anticipated ranked (not visiting or adjunct) faculty who will participate in the proposed program through Year 5. Include (a) faculty code associated with the source of funding for the position; (b) name; (c) highest degree held; (d) academic discipline or specialization; (e) contract status (tenure, tenure-earning, or multi-year annual [MYA]); (f) contract length in months; and (g) percent of annual effort that will be directed toward the proposed program (instruction, advising, supervising internships and practica, and supervising thesis or dissertation hours).

See Table 4 in Appendix A.

B. Use Table 2 in Appendix A to display the costs and associated funding resources for existing and anticipated ranked faculty (as identified in Table 2 in Appendix A). Costs for visiting and adjunct faculty should be included in the category of Other Personnel Services (OPS). Provide a narrative summarizing projected costs and funding sources.

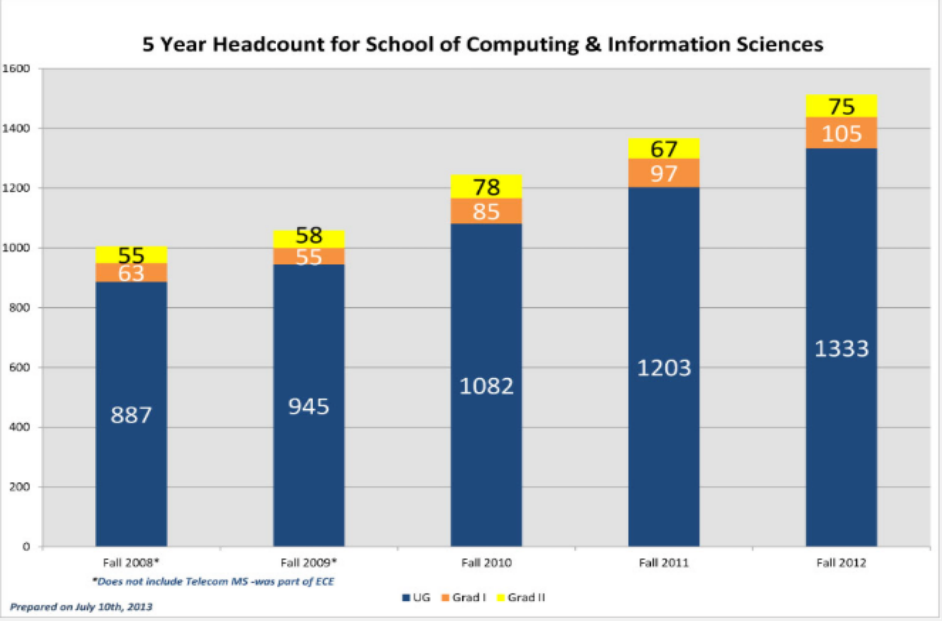
As detailed in Table 2 in Appendix A, the proposed budget includes funding for two new faculty members, two graduate assistants, and operational expenses in support of the new program.

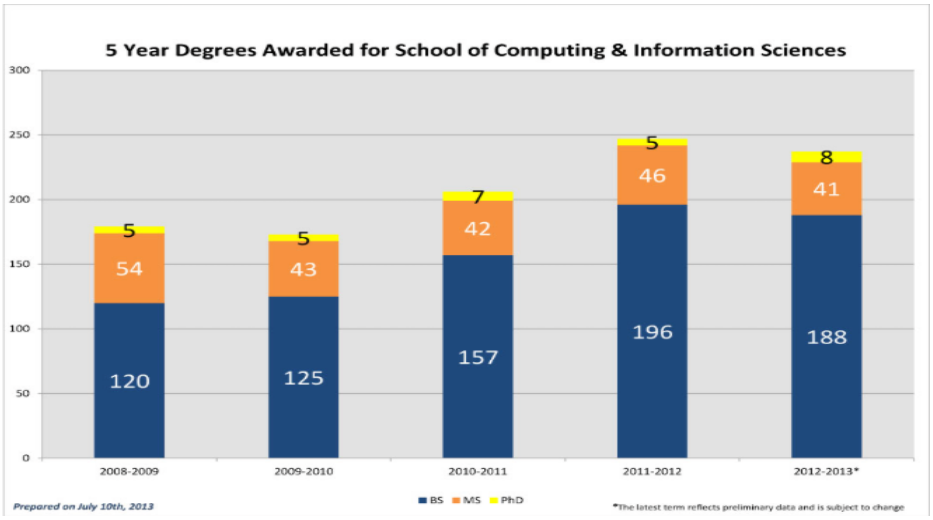
C. Provide in the appendices the curriculum vitae (CV) for each existing faculty member (do not include information for visiting or adjunct faculty).

See Appendix B for information on participating faculty members.

D. Provide evidence that the academic unit(s) associated with this new degree have been productive in teaching, research, and service. Such evidence may include trends over time for average course load, FTE productivity, student HC in major or service courses, degrees granted, external funding attracted, as well as qualitative indicators of excellence.

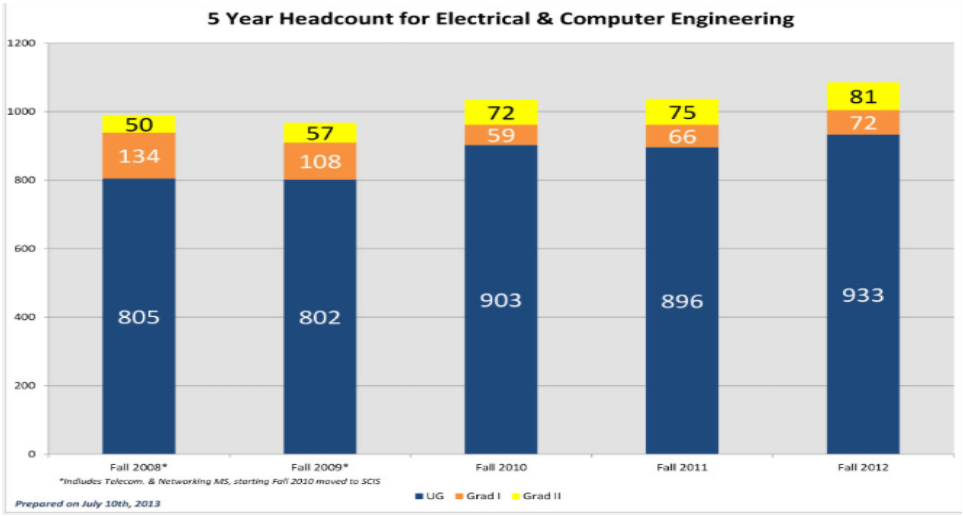
According to the 2012 edition of ASEE Profiles of Engineering & Engineering Technology Colleges, the School of Computing and Information Sciences awarded the sixth-most Computer Science degrees in the US, representing its highest ranking ever. SCIS is the only school in Florida offering BS and MS in both CS and IT. It also continues to lead the nation in training Hispanic PhD students. The program was ranked No. 1 among all state universities in Florida, resulting in a two-year $7.5M award from the State's Information Technology Performance Funding program. The School had a record high record of $6.2M external research funding this past year, including a sixth NSF Faculty CAREER Award, and made significant progress in increasing entrepreneurship and technology transfer activities.
The School has experienced a continued explosion in its undergraduate enrollments in both CS and IT programs, boasting over 1,350 majors in spring 2013. The School graduated its first MSIT students, and is now recruiting the first cohort of students for its weekend Professional MSIT program.

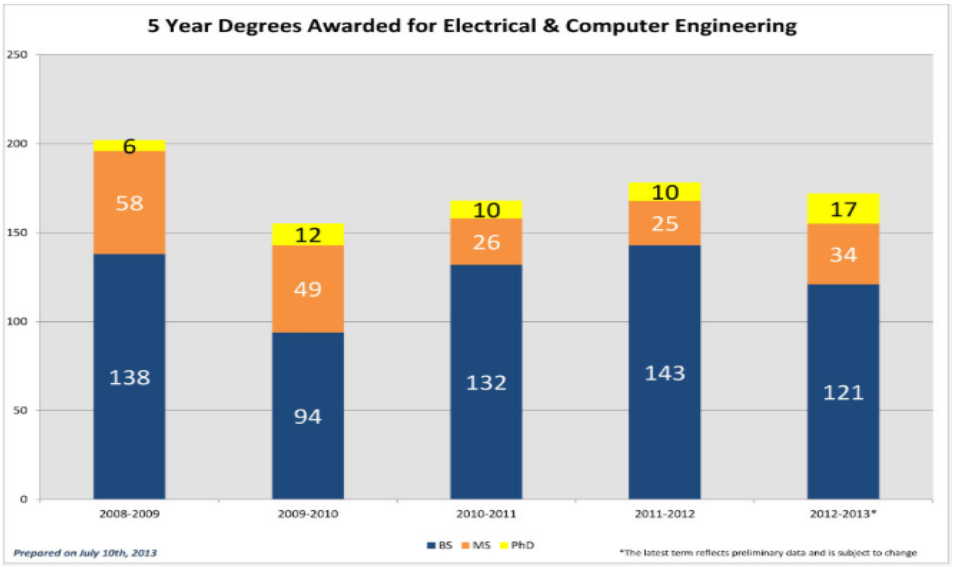


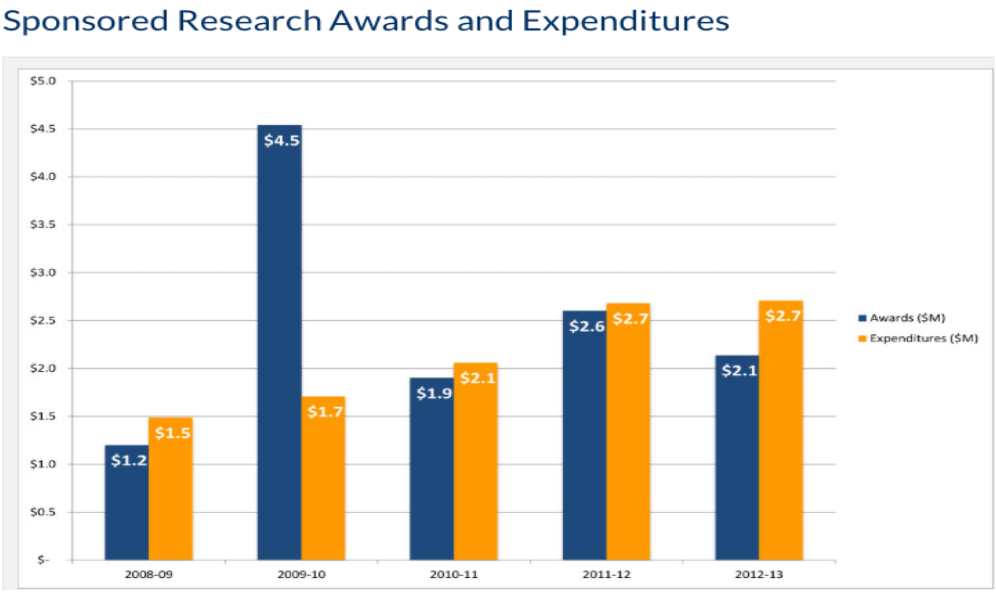


Sponsored Research Awards and Expenditures

The Department of Electrical and Computer Engineering (ECE) is continuing its growth and major accomplishments. The department's vision is to offer the best undergraduate program in the State of Florida and to be internationally recognized with its graduate programs, driven by excellent research that responds to the needs of the State of Florida, in particular, and the nation, in general. Furthermore, serving our community and maintaining our mission in providing excellence in undergraduate education allows our graduates to become critical thinkers, creative problem solvers and life-long learners.
The student body has continued to increase at all levels to now a record high of about 1,100 students. This past year, the faculty in the department graduated a record high of 17 doctoral students.







X. Non-Faculty Resources

A. Describe library resources currently available to implement and/or sustain the proposed program through Year 5. Provide the total number of volumes and serials available in this discipline and related fields. List major journals that are available to the university's students. Include a signed statement from the Library Director that this subsection and subsection B have been reviewed and approved.

The existing Library resources are abundant. Combined with Engineering, Computer Science related collections include 421 journals in print and 650 journals online. Also note that we have access to the complete ACM digital library as well as all societies periodical package of IEEE. ACM and IEEE are the premier organizations in our field.

B. Describe additional library resources that are needed to implement and/or sustain the program through Year 5. Include projected costs of additional library resources in Table 3 in Appendix A.

There are no additional library resources that would be necessary to sustain the MS-Cybersecurity program because the library already provides support for the Computer Science, Information Systems, and Computer Engineering.

Signature of Library Director **Date**

C. Describe classroom, teaching laboratory, research laboratory, office, and other types of space that are necessary and currently available to implement the proposed program through Year 5.

To support our existing BS, MS, and Ph.D. programs both in Computer Science and in Electrical and Computer Engineering, we have built excellent classroom, teaching laboratory, research laboratory, and office space. To implement this new MS-Cybersecurity program, we will require exactly the same facilities, and hence, will not create any additional burden on ourselves to support its curriculum.

D. Describe additional classroom, teaching laboratory, research laboratory, office, and other space needed to implement and/or maintain the proposed program through Year 5. Include any projected Instruction and Research (I&R) costs of additional space in Table 2 in Appendix A. Do not include costs for new construction because that information should be provided in response to X (J) below.

The MS-Cybersecurity program can be conducted with existing programs using the same facilities. No additional burden is needed to support its curriculum.

E. *Describe specialized equipment that is currently available to implement the proposed program through Year 5. Focus primarily on instructional and research requirements.*

The complete inventory of our equipment necessary to satisfy the instructional and research requirements is included in Appendix-C.

F. *Describe additional specialized equipment that will be needed to implement and/or sustain the proposed program through Year 5. Include projected costs of additional equipment in Table 2 in Appendix A.*

No additional specialized equipment is needed.

G. *Describe any additional special categories of resources needed to implement the program through Year 5 (access to proprietary research facilities, specialized services, extended travel, etc.). Include projected costs of special resources in Table 2 in Appendix A.*

No additional special categories of resources are needed.

H. *Describe fellowships, scholarships, and graduate assistantships to be allocated to the proposed program through Year 5. Include the projected costs in Table 2 in Appendix A.*

Funding for two graduate assistantships is included in each year. Such assistantships will be used to attract outstanding students to the program and to provide some teaching assistant support for its courses.

I. *Describe currently available sites for internship and practicum experiences, if appropriate to the program. Describe plans to seek additional sites in Years 1 through 5.*

Through existing agreements with our industry partners such as IBM, Siemens, and Motorola, we can offer student internship opportunities relevant to support the MS-Cybersecurity program as needed. The academic requirements for these internships remain to be determined.

J. *If a new capital expenditure for instructional or research space is required, indicate where this item appears on the university's fixed capital outlay priority list. Table 2 in Appendix A includes only Instruction and Research (I&R) costs. If non-I&R costs, such as indirect costs affecting libraries and student services, are expected to increase as a result of the program, describe and estimate those expenses in narrative form below. It is expected that high enrollment programs in particular would necessitate increased costs in non-I&R activities.*

No such costs are anticipated.

APPENDICES

APPENDIX A
BOG Tables, including
Table 1-B (Grad Enrollment)
Table 2 (Budget)
Table 3 (Reallocation)
Table 4 (Faculty)

APPENDIX B
Faculty Biographic Sketches

APPENDIX C
Laboratory Facilities

APPENDIX A Tables

[Attached at end of document.]

APPENDIX B Faculty Biographic Sketches

Dr. Bogdan Carbunar

PhD Purdue
Homepage: http://users.cis.fiu.edu/~carbunar/

Research Description

Dr. Bogdan Carbunar's interests lie at the intersection of security, privacy and distributed systems, with a focus on attacks and defenses against wireless and online social networks. His most recent projects include safe cities through mobile and social networking technologies, and detecting and handling fake information in geosocial networks.

Selected Publications

1. Bogdan Carbunar, Rahul Potharaju. You Unlocked the Mt. Everest Badge In Foursquare! Countering Location Fraud in GeoSocial Networks. To appear in the *9th IEEE International Conference on Mobile Ad hoc and Sensor Systems (MASS)*, Las Vegas, October 2012.
2. Jaime Ballesteros, Mahmudur Rahman, Bogdan Carbunar, Naphtali Rishe. Safe Cities. A Participatory Sensing Approach. To appear in the *37th IEEE Conference on Local Computer Networks (LCN)*, Orlando, October 2012.
3. Bogdan Carbunar, Radu Sion, Rahul Potharaju, Moussa Ehsan. The Shy Mayor: Private Badges in GeoSocial Networks. In Proceedings of the *10th Applied Cryptography and Network Security (ACNS)*, 2012.
4. Bogdan Carbunar,Michael Pearce, Shivajit Mohapatra, Loren J. Rittle, Venu Vasudevan, Octavian Carbunar. Secure Synchronization of Periodic Updates in Ad Hoc Networks. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, Volume 21, Issue 8, 2010. Extends IEEE ICNP 2008 paper.
5. Bogdan Carbunar, Radu Sion. Write-Once Read-Many Oblivious RAM. *IEEE Transactions on Information Forensics and Security (TIFS)*, Volume 6, Issue 4, 2011. Extends ACNS 2010 paper.

Dr. Jason Liu

PhD Dartmouth
Homepage: http://www.cis.fiu.edu/~liux/

Research Description

Dr. Liu's research focuses on parallel and distributed simulation, high-performance modeling and simulation of computer systems and computer networks. A central theme of his research is to investigate enabling technologies for building high-fidelity high-performance simulation and emulation testbeds to facilitate discoveries and innovations of large-scale complex computer networks and computer systems. Specific areas of Dr. Liu's research include: enabling scalable and high-performance parallel and distributed simulation on high-end computing platforms; designing network testbeds based on hybrid simulation, emulation, and high-performance modeling techniques; and applying high-performance modeling, parallel simulation, and interactive simulation and emulation techniques in various specific areas of research.

Selected Publications

1. Liu, Jason, and Rong Rong. Hierarchical Composite Synchronization. *Principles of Advanced and Distributed Simulation (PADS), 2012 ACM/IEEE/SCS 26th Workshop on*. IEEE, 2012.

2. Van Vorst, N., M. Erazo, and J. Liu. PrimoGENI for hybrid network simulation and emulation experiments in GENI. *Journal of Simulation* 6.3 (2012): 179-192.
3. Van Vorst, Nathanael, Ting Li, and Jason Liu. How low can you go? Spherical routing for scalable network simulations. *Modeling, Analysis & Simulation of Computer and Telecommunication Systems (MASCOTS), 2011 IEEE 19th International Symposium on*. IEEE, 2011.
4. Liu, Jason, and Yue Li. Parallel hybrid network traffic models. *Simulation* 85.4 (2009): 271-286.
5. Erazo, M. A., Li, T., Liu, J., & Eidenbenz, S. (2012, June). Toward comprehensive and accurate simulation performance prediction of parallel file systems. In *Dependable Systems and Networks (DSN), 2012 42nd Annual IEEE/IFIP International Conference on* (pp. 1-12). IEEE.
6. Li, Yue, Michael Liljenstam, and Jason Liu. Real-time security exercises on a realistic interdomain routing experiment platform. In *Proceedings of the 2009 ACM/IEEE/SCS 23rd Workshop on Principles of Advanced and Distributed Simulation*. IEEE Computer Society, 2009.

Dr. Deng Pan

PhD Stony Brook
Homepage: http://users.cis.fiu.edu/~pand/

Research Description

Dr. Deng Pan's research interests are generally in high speed computer networks, and his recent research focuses on resource and energy efficiency in data center networks. The ongoing projects are: management of multiple deterministic and stochastic resources in data centers, load-balanced multipath routing for data center networks, and joint host-network energy optimization for data centers.

Selected Publications

1. Y. Li and Deng Pan, OpenFlow based load balancing for fat-tree networks with multipath support, *IEEE International Conference on Communications (ICC)*, Budapest, Hungary, Jun. 2013.
2. H. Jin, T. Cheocherngngarn, D. Levy, A. Smith, D. Pan, and Niki Pissinou, Joint host-network optimization for energy-efficient data center networking, *IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, Boston, MA, May 2013.
3. H. Jin, D. Pan, J. Xu, and N. Pissinou, Efficient VM placement with multiple deterministic and stochastic resources in data centers, *IEEE Global Communications Conference (GLOBECOM)*, Anaheim, CA, Dec. 2012.
4. H. Jin, D. Pan, J. Liu, and N. Pissinou, OpenFlow based flow level bandwidth provisioning for CICQ switches, *IEEE Transactions on Computers*, accepted for publication.
5. D. Pan and Y. Yang, Flow based performance guarantee scheduling in buffered crossbar switches, *IEEE Transactions on Communications*, accepted for publication.

Dr. Niki Pissinou

PhD University of Southern California
Web page: http://www.cis.fiu.edu/facultystaff/view/?faculty=13

Research Description

Professor Pissinou's interests include network security, sensor network security, and web security, and social networks.

Selected Publications

1. H. Jin, T. Cheocherngngarn, D. Levy, A. Smith, D. Pan, and Niki Pissinou, Joint host-network optimization for energy-efficient data center networking, *IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, Boston, MA, May 2013.

2. H. Jin, D. Pan, J. Xu, and N. Pissinou, Efficient VM placement with multiple deterministic and stochastic resources in data centers, *IEEE Global Communications Conference (GLOBECOM)*, Anaheim, CA, Dec. 2012.
3. H. Jin, D. Pan, J. Liu, and N. Pissinou, OpenFlow based flow level bandwidth provisioning for CICQ switches, *IEEE Transactions on Computers*, accepted for publication.

Dr. Geoffrey Smith

PhD Cornell
Homepage: http://users.cis.fiu.edu/~smithg/

Research Description

Dr. Geoffrey Smith's research is focused on the foundations of computer security. For many years, he has studied the *secure information flow* problem, which aims to prevent confidential information from being leaked, and trusted information from being tainted. More recently, he has focused on *Quantitative Information Flow*, which aims to justify the intuition that certain improper flows can be tolerated on the grounds that they are "small". His current interests are centered on the mathematical theory of quantitative leakage measures and on static analyses for analyzing leakage in software.

Selected Publications

1. Barbara Espinoza and Geoffrey Smith, Min-Entropy as a Resource, *Information and Computation (Special Issue on Information Security as a Resource)*, vol. 226, pp. 57-75, April 2013.
2. Mário S. Alvim, Kostos Chatzikokolakis, Catuscia Palamidessi, and Geoffrey Smith, Measuring Information Leakage using Generalized Gain Functions, *Proc. CSF 2012: 25th IEEE Computer Security Foundations Symposium*, pp. 265–279, Harvard University, Cambridge, MA, June 2012.
3. Boris Köpf and Geoffrey Smith, Vulnerability Bounds and Leakage Resilience of Blinded Cryptography under Timing Attacks, *Proc. CSF 2010: 23rd IEEE Computer Security Foundations Symposium*, pp. 44–56, Edinburgh, UK, July 2010.
4. Geoffrey Smith, On the Foundations of Quantitative Information Flow, *Proc. FoSSaCS 2009: Twelfth International Conference on Foundations of Software Science and Computation Structures*, Luca de Alfaro (Ed.), LNCS 5504, pp. 288–302, York, UK, March 2009.
5. Geoffrey Smith and Dennis Volpano, Secure Information Flow in a Multi-threaded Imperative Language, *Proc. POPL 1998: 25th ACM Symposium on Principles of Programming Languages*, pp. 355-364, San Diego, California, January 1998.
6. Dennis Volpano, Geoffrey Smith, and Cynthia Irvine, A Sound Type System for Secure Flow Analysis, *Journal of Computer Security*, vol. 4, nos. 2,3, December 1996, pp. 167–187.

Dr. Jinpeng Wei

PhD Georgia Tech
Homepage: http://www.cis.fiu.edu/~weijp/

Research Description
Dr. Jinpeng Wei's research interests are in the area where systems software (e.g., Operating Systems and middleware) and computer security overlap. In particular, he explores novel systems mechanisms and implementations to make widely deployed systems software (e.g., the Linux OS, the Windows OS, and MapReduce) robust against malicious attacks, while still keeping it efficient and easy to use. Recently, he has worked on defense against kernel queue injection rootkits, automated derivation of data invariants for system runtime integrity monitoring, and integrity assurance of MapReduce in cloud computing.

Selected Publications
1. Jinpeng Wei, Feng Zhu, and Calton Pu. KQguard: Binary-Centric Defense against Kernel Queue Injection Attacks. The *18th European Symposium on Research in Computer Security (ESORICS 2013)*, September 9 - 13, 2013, Egham, UK.

2. Jinpeng Wei, Calton Pu. Towards a General Defense against Kernel Queue Hooking Attacks. *Computers & Security*, Elsevier Ltd., March 2012, Volume 31, Issue 2, pages 176-191. doi: 10.1016/j.cose.2011.12.007.
3. Jinpeng Wei, Feng Zhu, and Yasushi Shinjo. Static Analysis Based Invariant Detection for Commodity Operating Systems. *7th International Conference on Collaborative Computing (CollaborateCom 2011)*, Orlando, FL, October 15-18, 2011.
4. Jinpeng Wei, Bryan D. Payne, Jonathon Giffin, Calton Pu. Soft-Timer Driven Transient Kernel Control Flow Attacks and Defense. Proceedings of the *24th Annual Computer Security Applications Conference (ACSAC'2008)*, Anaheim, CA, December 8-12, 2008.
5. Yongzhi Wang, Jinpeng Wei. VIAF: Verification-based Integrity Assurance Framework for MapReduce. Proceedings of the *Fourth IEEE International Conference on Cloud Computing (CLOUD 2011)*, IEEE Computer Society, Washington, DC, July 4-9, 2011, pages 300 – 307.
6. Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, Vasanth Bala, and Peng Ning. Managing Security of Virtual Machine Images in a Cloud Environment. Proceedings of the *2009 ACM Cloud Computing Security Workshop (CCSW)*, co-located with the *16th ACM Conference on Computer and Communications Security (CCS)*, Chicago, IL, Nov. 9-13, 2009.

APPENDIX C Laboratory Facilities

SCIS Resources

The School of Computing and Information Sciences (SCIS) maintains a data center, research and instructional labs, and computer classroom facilities housed in the Engineering and Computer Science Building (ECS). The facility is maintained by a dedicated professional IT support staff.

The School provides computing services such as file, compute, web, email, XMPP, backup, print, and other computing services. Our networking services include a 10 Gigabit Ethernet core network that interconnects rack mounted switches and servers. All school desktop systems are connected by 1 Gigabit switched ports. Our network is highly redundant with multiple fiber and copper paths and is designed with routing fail-over capacity. We provide automated monitoring of our network and servers 24x7. Our network interconnects at 10GBs to the campus backbone, which provides a 10GBs connection to the NAP of the Americas to provide for connections to Internet, Internet2, Florida and National Lambda Rail, and CLARA (South American Research) networks.

Our systems feature a variety of open source and commercial development and scientific software products from numerous vendors including IBM, Microsoft, ESRI, MathWorks, etc. We provide middleware technologies to support web services. Our environment takes advantage of hundreds of open source software solutions including Apache with full mods, PHP, Perl, and many others.

Student Laboratories: SCIS operates four instructional laboratories for use by undergraduates and graduate students in support of our computer science and information technology degree programs. Our instructional labs offers students access to Windows 7/XP, CentOS Linux, and Mac OS X which run a variety of software development tools, libraries, databases, and have the capacity to host virtual machines. The School has dedicated servers for student files and/or computing services and a printer in each lab. Each student receives at least 1,000MB of backed up file storage space. Students can login remotely into several Linux and Solaris file and compute servers. The labs provide a "laptop bar" for students to connect their laptops to the SCIS network and a "design bar" outfitted with 42" LCD displays where students are able to collaborate on programming assignments or other joint projects. The classrooms ECS 141 and ECS 235 offer sophisticated teaching facilities.

Staffing: The school maintains all its computing facilities (total research and instruction: 25 labs, 350+ desktops, 100+ servers, layer 2 and 3 networking) via a dedicated Technology Group. The SCIS Technology Group consists of 4 FTE of permanent professional staff assigned to all of the school's research and instructional laboratories management. In addition, there are at least 2 FTE of temporary students specifically assigned to laboratory assistance. The SCIS Technology Group staff is organized into two groups: Engineering Services, including Networking, Systems, Desktop, and Help Desk Support, and Business Services including Technology Procurement, Asset Management, and Budget/Contract Management.

ECE Resources

The Department of Electrical and Computer Engineering (ECE) hosts a large suite of cybersecurity-related resources, maintained by Dr. Alexander Perez-Pons and Dr. Fasial Kaleem, including the following:

- 50 smartphones and mobile devices of various brands (Samsung, Apple, etc.) provided by Verizon.
- Data plan available to each smartphone and mobile device, courtesy of Verizon.
- Mobile Phone and Portable GPS Jammer -10 Meter Range.
- Sensitive Handheld Signal Jammer of CDMA / GSM / DCS / PHS / WiFi / 3G.
- Device Seizure, a comprehensive kit (including necessary hardware and software) from Paraben Corporation to perform advanced Logical/Physical extraction and analysis of data from mobile

devices.

- XRY, a power and advanced forensic solution from Micro Systemation.
- SANS Investigative Forensic Toolkit (SIFT), a multi-purpose forensic operating system.
- Popular forensic tools like Oxygen Forensic Suite, MobilEdit Forensic, viaExtract, Elcomsoft iOS Forensic Toolkit (EIFT), EnCase, and FTK.
- Virtual Machine (VM) images have been developed that are loaded with specialized version of linux distributions that are designed to perform digital forensics and malware analysis. Some of these open source distribution include Santoku-Linux, Kali-Linux, REMnux, and LosBuntu, which contains very powerful forensic and malware analysis tools (7zip, Abiword, Autopsy, Bleachbit, Bkhive, Chntpw, Clamtk, Dcfldd, DFF, ewf-tools, Filezila, Flashplugin-installer, Foremost, Furiusisomount, dconf, GDdrescue, Parted, Gparted, Hexedit, Hfsprogs, Hfsutils, jacksum, John, Mountmanager, Nautilus-open-terminal, Pasco, Photorec, Python-TK, Rar, Rifiuti2, Samdump2, Scalpel, SSH, Testdisk, Vinetto, Vlc, W3m, Wine, Wireshark, Xmount, Zenmap, Avg, AlalyzeMFT, BigDict.txt, Bulkextractor, Crunch, Exfatsupport, Fileinfo, FRED, Ftk Imager, Google-chrome, Guymager, Liblnk, Libmsiecf, Lnk-parse-1.0, Log2timeline, Web-browserPasswordRecovery, Process monitor indicator, Regripper plus plugins, Sleuthkit, Stegdetect, Truecrack, Truecrypt, Unetbootin, Volatility, Vshadowmount, Yaru).

APPENDIX A

TABLE 1-B
PROJECTED HEADCOUNT FROM POTENTIAL SOURCES
(Graduate Degree Program)

Source of Students (Non-duplicated headcount in any given year)*	Year 1		Year 2		Year 3		Year 4		Year 5	
	HC	FTE	HC	FTE	HC	FTE	HC	FTE	HC	FTE
Individuals drawn from agencies/industries in your service area (e.g., older returning students)	20	11.25	21	11.81	22	12.38	23	12.94	24	13.50
Students who transfer from other graduate programs within the university**	3	1.69	3	1.69	4	2.25	3	1.69	2	1.13
Individuals who have recently graduated from preceding degree programs at this university	15	8.44	18	10.13	23	12.94	27	15.19	33	18.56
Individuals who graduated from preceding degree programs at other Florida public universities	2	1.13	2	1.13	2	1.13	2	1.13	2	1.13
Individuals who graduated from preceding degree programs at non-public Florida institutions	2	1.13	2	1.13	2	1.13	2	1.13	2	1.13
Additional in-state residents***	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
Additional out-of-state residents***	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
Additional foreign residents***	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
Other (Explain)***	0	0.00	0	0.00	0	0.00	0	0.00	0	0.00
Totals	**42**	**23.63**	**46**	**25.88**	**53**	**29.81**	**57**	**32.06**	**63**	**35.44**

* List projected annual headcount of students enrolled in the degree program. List projected yearly cumulative ENROLLMENTS instead of admissions.
** If numbers appear in this category, they should go DOWN in later years.
*** Do not include individuals counted in any PRIOR category in a given COLUMN.

APPENDIX A

TABLE 2
PROJECTED COSTS AND FUNDING SOURCES

Instruction & Research Costs (non-cumulative)	Year 1							Year 5					
	Funding Source							Funding Source					
	Reallocated Base* (E&G)	Enrollment Growth (E&G)	Other New Recurring (E&G)	New Non-Recurring (E&G)	Contracts & Grants (C&G)	Auxiliary Funds	**Subtotal E&G, Auxiliary, and C&G**	Continuing Base** (E&G)	New Enrollment Growth (E&G)	Other*** (E&G)	Contracts & Grants (C&G)	Auxiliary Funds	**Subtotal E&G, Auxiliary, and C&G**
Faculty Salaries and Benefits	0	0	258,000	0	0	0	**$258,000**	258,000	0	0	0	0	**$258,000**
A & P Salaries and Benefits	0	0	63,000	0	0	0	**$63,000**	63,000	0	0	0	0	**$63,000**
USPS Salaries and Benefits	0	0	0	0	0	0	**$0**	0	0	0	0	0	**$0**
Other Personal Services	0	0	0	0	0	0	**$0**	0	0	0	0	0	**$0**
Assistantships & Fellowships	0	0	48,000	0	0	0	**$48,000**	48,000	0	0	0	0	**$48,000**
Library	0	0	0	0	0	0	**$0**	0	0	0	0	0	**$0**
Expenses	0	0	20,000	0	0	0	**$20,000**	20,000	0	0	0	0	**$20,000**
Operating Capital Outlay	0	0	10,000	0	0	0	**$10,000**	10,000	0	0	0	0	**$10,000**
Special Categories	0	0	0	0	0	0	**$0**	0	0	0	0	0	**$0**
Total Costs	**$0**	**$0**	**$399,000**	**$0**	**$0**	**$0**	**$399,000**	**$399,000**	**$0**	**$0**	**$0**	**$0**	**$399,000**

*Identify reallocation sources in Table 3.

**Includes recurring E&G funded costs ("reallocated base," "enrollment growth," and "other new recurring") from Years 1-4 that continue into Year 5.

***Identify if non-recurring.

Faculty and Staff Summary

Total Positions	Year 1	Year 5
Faculty (person-years)	2	2
A & P (FTE)	0.75	0.75
USPS (FTE)	0	0

Calculated Cost per Student FTE

	Year 1	Year 5
Total E&G Funding	$399,000	$399,000
Annual Student FTE	23.63	35.44
E&G Cost per FTE	$16,885	$11,258

APPENDIX A

TABLE 3 (DRAFT)
ANTICIPATED REALLOCATION OF EDUCATION & GENERAL FUNDS*

Program and/or E&G account from which current funds will be reallocated during Year 1	Base before reallocation	Amount to be reallocated	Base after reallocation
	0	0	**$0**
	0	0	
	0	0	
	0	0	
	0	0	
	0	0	
Totals	$0	$0	**$0**

*** If not reallocating funds, please submit a zeroed Table 3**

APPENDIX A

TABLE 4 (DRAFT)
ANTICIPATED FACULTY PARTICIPATION

Faculty Code	Faculty Name or "New Hire" Highest Degree Held Academic Discipline or Speciality	Rank	Contract Status	Initial Date for Participation in Program	Mos. Contract Year 1	FTE Year 1	% Effort for Prg. Year 1	PY Year 1	Mos. Contract Year 5	FTE Year 5	% Effort for Prg. Year 5	PY Year 5
A	Bogdan Carbunar, Ph.D. Computer Science	Asst. Prof.	Ten. Track	Fall 2014	9	0.75	22.00	16.50	9	0.75	22.00	16.50
A	Geoffrey Smith, Ph.D. Computer Science	Assoc. Prof.	Tenure	Fall 2014	9	0.75	22.00	16.50	9	0.75	22.00	16.50
A	Jinpeng Wei, Ph.D. Computer Science	Asst. Prof.	Ten. Track	Fall 2014	9	0.75	22.00	16.50	9	0.75	22.00	16.50
C	Alexander Perez-Pons, Ph.D. Computer Engineering	Visiting Prof.	MYA	Fall 2014	9	0.75	33.00	24.75	9	0.75	44.00	33.00
C	New Hire, PhD Computer Science/Engineering	Asst. Prof.	Ten. Track	Fall 2014	9	0.75	22.00	16.50	9	0.75	44.00	33.00
	New Hire, Degree Academic Discipline				0	0.00	0.00	0.00	0	0.00	0.00	0.00
	New Hire, Degree Academic Discipline				0	0.00	0.00	0.00	0	0.00	0.00	0.00
	New Hire, Degree Academic Discipline				0	0.00	0.00	0.00	0	0.00	0.00	0.00
	Total Person-Years (PY)							**90.75**				**115.50**

Faculty Code		Source of Funding	PY Workload by Budget Classsification Year 1	Year 5
A	Existing faculty on a regular line	Current Education & General Revenue	0.00	0.00
B	New faculty to be hired on a vacant line	Current Education & General Revenue	0.00	0.00
C	New faculty to be hired on a new line	New Education & General Revenue	0.00	0.00
D	Existing faculty hired on contracts/grants	Contracts/Grants	0.00	0.00
E	New faculty to be hired on contracts/grants	Contracts/Grants	0.00	0.00
		Overall Totals for	**Year 1** **0.00**	**Year 5** **0.00**