A Systems Approach to Cyber Assurance Education

Todd R. Andel
University of South Alabama
150 Jaguar Dr.
Mobile, AL 36688
1-251-460-6701
tandel@southalabama.edu

J. Todd McDonald
University of South Alabama
150 Jaguar Dr.
Mobile, AL 36688
1-251-460-7555
jtmcdonald@southalabama.edu

ABSTRACT

The demand for cybersecurity professions faces continual shortages. Real-world cyber threats continue to drive this demand as we face a daily barrage of attacks on our critical infrastructure, national, and private industry assets. To meet this demand, many cybersecurity and information assurance educational programs have emerged. These programs range from specialized tracks within traditional academic programs to specialized degree titles developed solely for the purpose of producing cyber capable graduates.

In this paper we document curriculum development that focuses on a systems level approach to cyber assurance education. This program incorporates both hardware and software aspects to ensure cyber security graduates are produced that can address adversaries that target complete system implementations.

Categories and Subject Descriptors

K.3.2 [**COMPUTERS AND EDUCATION**]: Computer and Information Science Education – *curriculum.*

General Terms

Documentation

Keywords

Cyber assurance, curriculum development, information security education

1. INTRODUCTION

Today within academic, government, and industry circles it is almost impossible to avoid running into the terms cybersecurity, information assurance (IA), and cybersecurity and IA education. This focus on cyber has its merit, new vulnerabilities and attacks are highlighted almost daily within the media and showcases cyber security problems we face in our national defense, critical infrastructure, financial institutions, and our reliance on computing for a way of life in the United States (although we are not alone in this problem).

The reliance on cyber and the threat of vulnerabilities is recognized at our highest levels of government, as seen in the February 12, 2013 Presidential Executive Order "Improving Critical Infrastructure Cybersecurity" [3]. To support this call, government programs, such as the NIST/DHS NICE framework [5] and the NSA/DHS CAE [4] programs aim to produce cyber education and training guidelines to increase the number of cyber capable workers needed to solve this problem.

This paper focuses on the education aspect, looking at formalized four year academic programs supporting cyber and information assurance requirements. More specifically, we take a look at current IA programs and document current curriculum development at the University of South Alabama's (USA) School of Computing (SoC). This development focuses on a new degree program that takes a systems level approach to cyber assurance education.

The remainder of this paper is organized as follows. Section 2 discusses IA programs that are tracks within traditional degree programs, Section 3 highlights the new trend of developing IA programs as specialized degrees, and Section 4 provides goals and justifications for the development of a new specialized degree program, along with a detailed program description to meet this need.

2. TRADITIONAL PROGRAMS PLUS IA

Cybersecurity and IA programs across the nation are widely varied in content and program intent. For the purposes of this discussion we focus on four year programs designated by the National Security Agency (NSA)/Department of Homeland Security (DHS) Center of Academic Excellence (CAE) program. As of February 2013 there are approximately 165 schools with the CAE designation[1], made up of Information Assurance Education (CAE-IAE), Research (CAE-R), and 2-year institutions (CAE-2Y). Also, the NSA has just recently added four institutions with a special emphasis on Cyber Operations.

Even within the standard 4-year CAE designation, the programs vary widely from STEM (Science, Technology, Engineering, and Math) focused sciences, such as computer science, computer engineering, electrical engineering, mathematics, to non-STEM focused degrees looking at policy and management, social sciences, political science focuses, and various other liberal arts degrees. This wide variety in programs produces graduates with a wide range of capabilities across the entire cyber spectrum. Numerous discussions with NSA, DHS, and National Science Foundation (NSF) personnel indicate this wide range approach is beneficial in filling federal jobs with varying needs for cyber security trained employees.

[1] This number is highly dynamic as new schools are added and current designations expire.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Information Security Curriculum Development Conference 2013
October 12, 2013, Kennesaw, GA, USA.
Copyright 2013 ACM 978-1-4503-2547-9-0/10/13…$10.00.

The majority of CAE schools incorporate IA tracks into their traditional programs of study, as opposed to generating a comprehensive new degree program. The IA track generally fills the elective portion, however, the overall degree and core background remains. For instance, most computer science (CS) CAE programs require traditional core CS courses and incorporate four to six IA elective courses focusing on data security, network security, secure operating systems, etc. In a program focused on business, the IA electives may include information security management, ethical hacking and response, information warfare, security policy, etc.

3. FOCUSED IA PROGRAMS

In a recent trend, programs solely focused on cyber and information assurance have begun to emerge. Such programs typically include words like *Cyber*, *Cyber Security*, *Information Security*, etc., in the title of their degree name. While there is nothing wrong with these degree titles, one must ensure (both from a student and hiring employer perspective) that the degree requirements and qualifications of graduates be fully understood. That is, with this new trend in naming, the core identity of what the degree is built around could be potentially masked. For example, two specialized degree titles from CAE institutions include:

- B.S. in Cybersecurity, University of Maryland University College
- B.S. in Cyber Engineering, Louisiana Tech University

By looking at the title only, a student or employer could assume both degrees to be equivalent in nature. However, digging deeper into program and course descriptions shows these programs are widely different and graduates of these programs will have different skill sets to offer employers. University of Maryland University College's B.S. in Cybersecurity is primarily focused on information technology and information systems with a strong emphasis on preparing students for commercial certificate exams. Louisiana Tech's B.S. in Cyber Engineering is a STEM-based, engineering centric program intended to prepare students for advanced cyber research and development positions.

To provide a full understanding of these two samples, we review each program in the following subsections. These two programs were selected solely to provide awareness that such differences exist. As we point out in Section 2, a wide variety of cyber degree programs produce various skill-sets to fill a wide variety of cyber related positions. However, a graduate of a cyber focused technology, policy, or management degree may not be ideal in a cyber focused engineering position, and vice versa.

3.1 B.S. in Cybersecurity, UMUC

The University of Maryland University College (UMUC) offers a 120 hour B.S. in Cybersecurity degree [13]. This program is broken into 33 major credits, 41 general education credits, and the remaining 46 credits used for a minor or other electives. This program provides cyber focused graduates for information technology and information systems type positions and provides a solid in-depth approach. Table 1 provides a brief summary of the 41 core cybersecurity major credits.

These core major courses primarily focus on cyber issues within the information systems and information technology fields. Three of the courses, CMIT 265, CMIT 320, and CMIT 425 assist the student in preparing for the CompTIA Network+, CompTIA Security+, and CISSP certification exams.

According to UMUC’s program bulletin, graduates from their Cybersecurity program will be suited for cyber related jobs in information technology and other information systems policy and management positions.

3.2 B.S. in Cyber Engineering, LA Tech

Louisiana Tech University (LA Tech) offers a 128 hour B.S. in Cyber Engineering degree which they began offering in fall 2012 [9]. This degree program is a cyber focused degree based on a multi-disciplinary mixture of courses in computer science (12 credits in data structures, operating systems, computer networks,

Table 1. UMUC Cybersecurity Major Courses [13]

Course	*Title*	*Description*
CSIA 301	Foundations of Cybersecurity	A comprehensive introduction to the protection of business information and the systems that support business processes.
IFSM 304	Ethics in Information Technology	A comprehensive study of ethics and of personal and organizational ethical decision making in the use of information systems in a global environment.
CMIT 265	Fundamentals of Networking	An introduction to networking technologies for local area networks, wide area networks, and wireless networks.
CCJS 321	Digital Forensics in the Criminal Justice System	An overview of the criminal justice system and the application of digital forensic evidence in criminal justice cases.
CSIA 303	Foundations of Information System Security	A survey of various means of establishing and maintaining a practical cyber and information security program to protect key organizational assets.
CSIA 412	Security Policy Analysis	A study of various aspects of information assurance and cybersecurity policy planning in an organizational context.
CSIA 413	Security Policy Implementation	A study of information security (IS) performance standards and policy implementation for IS system administrators.
CMIT 320	Network Security	A study of the fundamental concepts of computer security and its implementation.
CMIT 425	Advanced Information Systems Security	A comprehensive study of information systems security to enhance organizational security.
CSIA 459	Evaluating Emerging Technologies	A survey of emerging and leading technologies in the cybersecurity field.
CSIA 485	Practical Applications in Cybersecurity Management	Capstone project with goal to protect an organization's critical assets by ethically integrating cybersecurity best practices and risk management throughout an enterprise.

and computer architecture), electrical engineering (8 credits in digital design, microprocessors, and embedded systems), engineering (15 credits in engineering problem solving, statics, dynamics and electrical networks), mathematics (21 credits in engineering math, four calculus classes, discrete math, differential equations, and linear algebra), and physics (6 credits), as well as traditional general education requirements and electives (36 credits). In additional to these foundational advanced mathematics and theory based courses, the program includes 30 credit hours of cyber specific courses that we review in Table 2.

As indicated in LA Tech's program documentation, graduates from the LA Tech Cyber Engineering program should be well versed for cyber research and development positions within government laboratories and research centers as well as commercial development in the cybersecurity field.

4. SYSTEMS APPROACH

While providing standardization to this new naming trend may clarify program differences, agreement on such an issue is highly unlikely. As new programs race to the academic seen to attract students, the naming problem will more than likely increase confusion. We ourselves are guilty of adding to the naming pool with this current program, but do intend to seek subsequent ABET certification which will at a minimum externally validate its technical rigor. To ensure no confusion we provide clear documented goals and objectives, a program description, and identify what skills this program's graduates are expected to possess.

In developing our B.S. in Cyber Assurance program we take a systems level approach to focus on both hardware and software elements. The following sections provide our justifications for this program and document the curriculum development.

4.1 Justification and Guidelines

As security of a system relies mutually on hardware and software aspects, both government and industry require cyber professionals to be fluent in each aspect.

Traditionally, computing students either specialize in hardware or software. Most computer science programs are software centric, computer engineering students can focus in either hardware or software, and electrical engineering students focus primarily on hardware aspects. However, the traditional boundaries between hardware and software are now blurred, as indicated in Figure 1. Hardware can be specified as software via a Hardware Description Language (HDL) and software programs can also be specified in an HDL or be represented as a sequence of logic gates. Part of this trend is resultant on the commodity status of reconfigurable logic, such as Field Programmable Gate Arrays (FPGAs), and porting software to this hardware results in faster execution time.

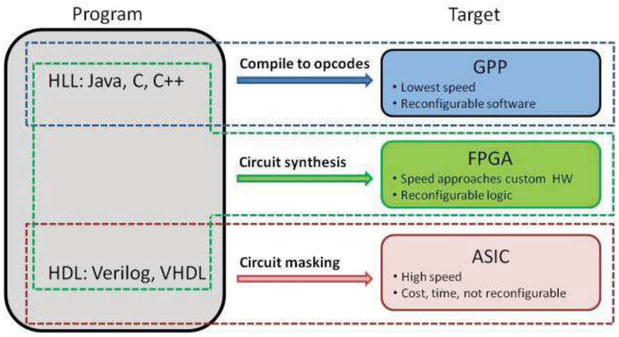

Figure 1. New Model of Software and Hardware

As an example of industry interest for combining hardware and software as a comprehensive education program, we look at Auburn’s program for wireless engineering [6]. This program emerged in the early 2000’s with direct industry input to fill the need for graduates in the ever expanding wireless industry. The Auburn curriculum was based on an interdisciplinary mesh between electrical and computer engineer, computer science, and software engineering. While the Auburn wireless engineering program is not focused on cybersecurity, its industry demand and successful implementation provide a sound approach for other industry and specialized areas to follow.

Another interesting theme appearing in literature is the idea of the

Table 2. LA Tech Cyber Engineering Courses [9]

Course	*Title*	*Description*
CYEN 120	Introduction to Computer Programming	Introductory programming, problem analysis and solution, modeling and abstraction.
CYEN 122	Intermediate Computer Programming	Analysis, design and implementation of programs
CYEN 301	Computer Network Security	Overview of computer network security, broad coverage of cyber security concepts, computer network defense, computer network attack, and wireless security
CYEN 400	Cyber Futures	An overview that seeks to understand what is likely to continue, what is likely to change, and what is novel in the context of cyber.
CYEN 401	Digital Forensics and Steganography	An overview of forensics and steganography including methods to uncover and exploit digital evidence; cyber crime, steganalysis, forensics analysis techniques, data hiding.
CYEN 402	Access Control Logic and Covert Channels	An overview of access control logic and covert channels. Topics include access control concepts and logic, covert channel detection, future security predictions.
CYEN 403	Wireless and Mobile Security	An overview of wireless and mobile security providing students with practical and theoretical experiences. Topics include threat analysis, security infrastructure, security services, wireless network security components.
CYEN 480	Theory of Cyber Science	An overview of formal languages, the abstract models of computing capable of recognizing those languages, and grammars.
CYEN 481	Software Design and Engineering	Design, construction and maintenance of large software systems. Project planning, requirements analysis, software design methodologies, software implementation and testing, maintenance.
CYEN 482	Senior Capstone	Social and ethical aspects of computing and cyber engineering.

"science of cyber security". In [11] Schneider describes the idea of viewing cyber security as a science. He indicates that there should be solid scientific laws pertaining to security in systems. The focus should not be on identifying vulnerabilities, since this is a continual game of cat and mouse, but to *"...organize a set of abstractions, principles, and trade-offs for building secure systems, given the realities of the threats and of our cybersecurity needs"* [11]. Similar concepts are developed in the MITRE "*Science of Cyber-Security"* report from the JASON project [8].

Following these observations, we set to develop a curriculum that incorporates both hardware and software aspects focused on a scientific approach to cyber assurance properties. During our curriculum development we ran across two pieces of work that guided our direction; an article in IEEE Security and Privacy [10] and an article in Air Force Space Command's High Frontier—The Journal for Space and Cyberspace Professionals [7]. We discuss these influences in the following two subsections.

4.1.1 Security Jewels

A recent 2012 article [10] in IEEE Security and Privacy provides historical "*security jewels*" that can be used as a core for IA education. The authors discuss foundational and timeless security principles that remain constant, even as new cyber threats appear on a continual basis. Table 3 is an excerpt of a larger, overall table in [10] that summarizes their objectives and maps to disciplines and applications.

In the designing of our Cyber Assurance curriculum, we incorporate these core foundational concepts as we focus on a complete system. This approach is justifiable in the fact, as the authors in [10] indicated, that even secure algorithms (e.g., certain cryptographic primitives) may be implemented or realized in an insecure manner. They also assume that at some point any system will be physically available for examination by an attacker.

4.1.2 The Jabbour Model

A 2010 article by Dr. Kamal Jabbour [7], the Air Force Senior Scientist for Information Assurance, outlines the call to develop a Bachelor of Science in Cyber Engineering. He highlights how computer engineering evolved out of electrical engineering and now it is time for cyber engineering as the logical next step of educational evolution. The impetus in his reasoning is that computer engineering focuses on reliability without the full understanding of operating in a contested cyber environment riddled with inherent vulnerabilities and external threats.

This program, we refer to as the Jabbour model, is an aggressive approach that was formulated from a traditional computer engineering degree and adapted it into a cyber engineering curriculum. The program focuses on a comprehensive approach based on the following three thrusts [7]:

1. Increased mathematical content: additional courses in discrete math, cryptography, and formal methods.
2. Incorporation of defensive design to all design based courses: hardware design, software design, and systems design.
3. New courses in tactical cyber offense, operational cyber defense and strategic vigilance (i.e., situational awareness).

Dr. Jabbour indicates that Louisiana Tech's B.S. in Cyber Engineering degree, as discussed in Section 3.2, is the first (and to our knowledge the only), degree program to incorporate his model. In fact, due to Dr. Jabbour's major influence over this program, he spoke to the inaugural cohort that stared Louisiana Tech's program in fall of 2012 [1].

Syracuse University has also followed the Jabbour Model by developing a single "*Cyber Engineering Semester*" that started in 2011 [12]. This program offers a specialized 18 credit semester for traditional computer science, computer engineering or electrical engineering students. Due to Syracuse's geographical proximity, the program is taught in conjunction with the Air Force Research Laboratory's Information Directorate, located at Rome, NY where Dr. Jabbour is currently assigned.

4.2 Curriculum Development

Our goal in developing a B.S. in Cyber Assurance (CA) is to provide a rigorous STEM based curriculum following the Jabbour model and the IA educational objectives as described in Table 3. The program is based on a complete systems level view including both software and hardware aspects. We feel the specialization and focus for such a program does not fall within one of the current ACM Computing Curricula [2], which includes computer engineering, computer science, information systems, information technology, and software engineering. In fact, USA's School of Computing hosts programs in computer science, information systems, and information technology. While each academic program includes security related courses, our new CA program is intended to provide a highly specialized focus that cannot be achieved within one of our existing programs.

Table 3. IA Security Objectives

	Security Objectives	***Disciplines***	***Applications***
1.	Cryptographic systems' security shouldn't rely on obscurity for their secrecy.	Mathematical foundations, cryptographic algorithm design, and cryptographic primitives	Factoring, elliptic curves, quantum states, public key, private key, encryption, decryption, and signatures
2.	Mathematical primitives can help achieve privacy and authentication.		
3.	Algorithms that are provably secure in theory might still have unexpected vulnerabilities when implemented in real systems.	Implementation and realization	Side-channel analysis and reverse engineering
4.	Mathematical primitives can help achieve authentication and secure message passing	Communication protocols	Key exchange, message exchange, and identity verification
5.	Expect the limits of cryptographic security to be tested by polynomially-bounded adversaries.		
6.	Using cryptographic primitives doesn't guarantee privacy or authentication.		

4.2.1 Program Outline

Our program follows the Jabbour model in a different approach than the LA Tech program. Our program uses computer science as a starting point since this curriculum will be taught primarily in a computing school and not within a college of engineering. Our development also followed general ABET Computing Accreditation Commission guidelines, as we intend to seek such accreditation on par with our three existing accredited computing programs.

The B.S. in Cyber Assurance will consist of 132 hours, using computer science as a foundational core. The curriculum includes traditional computer science courses (26 credits in programming, data structures, computer networking, computer architecture, operating systems, software engineering, and programming languages), computer engineering courses (7 credits in circuit analysis and digital logic), mathematics (20 credits in calculus, discrete math, applied statistics, number theory, and cryptography), physics (12 credits) and 6 additional elective credits in either computer science or computer engineering. Additionally, the program consists of 36 general education requirements as well as 25 credits in cyber focused courses. Table 4 provides an overview of these specialized cyber courses.

4.2.2 Program Assessment

We anticipate graduates from our program will be well versed for cybersecurity research, development, and analytical positions within various government agencies or supporting commercial development in the cybersecurity field.

Since our program is targeted to start in fall 2014, direct program assessment data is not currently available. However, we have developed a preliminary assessment approach as part of our curriculum development process. The approach will follow ABET guidelines for the review and assessment of computing programs, and is consistent with the processes required by Southern Association of Colleges and Schools (SACS), the regional accrediting body for the institution. We currently have ABET accredited computer science, information systems, and information technology programs that use questions embedded into tests and assignments that are used to support formative assessment. We will use a similar approach in identified key courses within our new program. We also plan to track graduate employment or advanced education opportunities. Of special interest in this analysis of employment will be an assessment of how many of the program graduates are employed in government or military related positions, thus contributing to meet national needs. We will additionally compare these results against our

Table 4. Specialized Cyber Focused Courses

Course	*Title*	*Description*
MA 481	Cryptography	Introduction to classical and modern methods of message encryption and decryption (cryptography) as well as possible attacks to cryptosystems (cryptanalysis). Topics include information theory, classical (symmetric) cryptosystems (DES, AES), public-key (asymmetric) cryptosystems (Diffic-Hellman, RSA, ElGamal), one-way and trapdoor functions, and hash functions.
CSC 340	Secure Software Engineering	Course focused on risk management framework for software engineering efforts and best practices for software security including code reviews, architectural risk analysis, penetration testing, risk-based security tests, abuse cases, security requirements, and security operations. Reviews common flaws that lead to exploitation to identify and mitigate such errors.
CSC 399	Concurrency and Distributed Computing	Course focused on security in concurrent and distributed systems. Includes cloud computing security, secure multi-threading, agent-based security, security policy composition, and secure compartmentalization.
CSC 400	Network and OS Vulnerabilities	Course takes a systems approach to detection and analysis of cyber vulnerabilities in the networks and operating systems. Includes common vulnerabilities and exploitation tactics, detection of intrusions and malware, vulnerability analysis and common tools, and best practices to reduce vulnerability footprint.
CSC 401	Cyber System Verification I	Introduction to system verification applicable to both software and hardware domains. Provides an introduction to formal methods, system modeling and reasoning via system logic proofs based on propositional and predicate logic. Includes Hoare Logic, weakest preconditions, and Communicating Sequential Processes.
CSC 402	Cyber System Verification II	Second course in the systems verification for both the software and hardware domains. Focuses on simulatability and the use of model checkers to verify and test system security properties for cyber systems.
CSC 403	Implementing Secure Systems I	Course serves as the introduction for secure systems, focused on building and evaluating secure hardware. Students learn the fundamentals of HDLs (VHDL or Verilog) with synthesis of simple cryptographic circuits onto FPGAs.
CSC 404	Implementing Secure Systems II	Lab focused course aimed to provide team development of a secure hardware design using a HDL and synthesized on a FGPA platform. Implementation topics include, but not limited to: anti-tamper technologies, side-channel countermeasures, and the design and implementation of Intellectual Property Protection features.
CSC 405	Cyber Warfare	Course provides an in-depth study of the nature of cyber warfare and its impact on information system security and information assurance. It provides a foundational understanding of both strategic and tactical effects of cyber warfare, legal aspects, problems related to positive retribution, and issues relating to cause and effect. A key focus is on the national information infrastructure, its potential vulnerabilities, and the impact of vulnerability exploitation.

Table 5. Cyber Specific Course Mappings

USA Courses	SO1	SO2	SO3	SO4	SO5	SO6	JM1	JM2	JM3
MA 481	X	X		X	X		X		
CSC 340								X	
CSC 399								X	
CSC 400								X	
CSC 401	X	X			X	X	X		
CSC 402	X	X			X	X	X		
CSC 403			X			X		X	
CSC 404			X			X		X	
CSC 405									X

current computing programs to determine if our focused cyber assurance program produces opportunities beyond what our current graduates of our other programs are afforded.

4.2.3 Program Mapping

We do not provide a direct comparison of our program against either the UMUC or LA Tech programs, to ensure we do not inadvertently misrepresent existing curricula. UMUC's program is intended more towards information technology and information systems professionals, while our program is a STEM based approach to produce graduates aimed towards research and development positions. Our program is similar to LA Tech's program since they are both based on the Jabbour model. However, our program additionally maps to the IA security objectives outlined in [10], which was published after LA Tech initiated their program. Additionally, USA's program is hosted within a computing school which is non-engineering focused and LA Tech's program is being hosted within an engineering school.

Table 5 provides a mapping our developed cyber assurance program against the six IA security objectives identified in Table 3 (indicated as SO1, SO2, etc.,) and to the three thrusts by the Jabbour model (indicated as JM1, JM2, and JM3). It can be seen that our cyber specific courses provide a complete covering over both the indicated objectives and thrusts.

5. CONCLUSION

The demand for IA and cybersecurity professionals with a wide range of qualifications will continue for the foreseeable future. To generate this supply of cyber professionals many information assurance programs, both traditional programs with specialized tracks and entire newly focused programs, have been developed.

As we move toward more focused information assurance and cybersecurity programs, we must ensure the programs are fully documented as now the underlying foundational core may not be readily evident. Looking at these programs, it is vital that both students and employers fully understand the qualifications and skill sets a given degree can provide. This skill set can range from non-STEM focused degrees looking at policy and management, social sciences, political science focuses, and various other liberal arts degrees all the way to STEM focused sciences, such as computer science, computer engineering, electrical engineering, and mathematics. This wide variety in programs prepares varying skill sets in order to have full spectrum cyber capabilities.

In this paper we document the development of a B.S. in Cyber Assurance at the University of South Alabama. This program takes a systems level approach by incorporating both hardware and software aspects within the cybersecurity domain. To the best of our knowledge and from informal conversations with Dr. Kamal Jabbour, USA's B.S. in Cyber Assurance program is only the second degree program to follow the Jabbour model and the first non-engineering program to do such. While adding yet another program title to the naming confusion for cyber education, we present our program as a potential baseline for a standardized STEM degree program for a B.S. in Cyber Assurance for programs hosted outside of a college of engineering.

6. REFERENCES

[1] Cyber Boosters Taking Program to the Nation. Cyber Innovation Center Press Release: http://www.cyberinnovationcenter.org/ cyber-boosters-taking-program-to-the-nation/, September 2012.

[2] ACM Curricula Recommendations. [Online] http://www.acm.org/education/curricula-recommendations, 2013.

[3] Executive Order – Improving Critical Infrastructure Cybersecurity. [Online] http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, February 2013.

[4] National Centers of Academic Excellence. [Online] http://www.nsa.gov/ia/academic_outreach/nat_cae/, August 2013.

[5] National Initiative for Cybersecurity Education. Technical report, NIST, 2013.

[6] Cheryl Cobb. AU on Forefront of Wireless Technology Boom. Auburn University Press Release, http://www.ocm.auburn.edu/news_releases/wireless.html, January 2005.

[7] Kamal Jabbour. The Time Has Come for the Bachelor of Science in Cyber Engineering. *High Frontier: The Journal for Space and Cyberspace Professionals*, 6(4):20–23, 2010.

[8] JASON Project Office. Science of cyber-security. Technical report, MITRE, 2010.

[9] Louisiana Tech University. University Catalog 2013-2014. [Online] http://www.latech.edu/registrar/bulletin/louisiana_tech_university_catalog_2013-2014_r3.pdf.

[10] J.T. McDonald and T.R. Andel. Integrating Historical Security Jewels in Information Assurance Education. *Security Privacy, IEEE*, 10(6):45–50, 2012.

[11] Fred B. Schneider. Blueprint for a Science of Cybersecurity. *The Next Wave*, 19(2):47–57, 2012.

[12] Syracuse University. First Cyber Engineering Semester completed by Inaugural Cohort. Press Release: http://giving.syr.edu/2011/12/13/first-cyber-engineering-semester-completed-by-inaugural-cohort/, December 2011.

[13] University of Maryland University College. 2013-2014 Undergraduate Catalog. [Online] http://www.umuc.edu/students/catalogs/upload/2013-2014-Undergraduate-Catalog.pdf.