December 8, 2015
(Last update: 10/01/15)

Handouts of the Graduate Faculty Council

MichiganTech
The University Senate of Michigan Technological University

Proposal XX-15
(Voting Units: Full Senate)

Master of Science Degree Program in Cybersecurity

Department of Computer Science
Department of Electrical and Computer Engineering
School of Technology
Michigan Technological University
Houghton, MI 49931

Contacts:
Spiros Bakiras, Department of Computer Science
Guy Hembroff, School of Technology
James Frendewey, School of Technology
Daniel Fuhrmann, Department of Electrical and Computer Engineering
Jean Mayo, Department of Computer Science
Min Song, Department of Computer Science (Primary Contact)
Chee-Wooi Ten, Department of Electrical and Computer Engineering
Xinli Wang, School of Technology
Zhenlin Wang, Department of Computer Science

I. INTRODUCTION

This is a strategic proposal led by the Computer Science Department for a new Master of Science (M.S.) degree program in the emerging areas of Cybersecurity. The involved ACIA (Alliance of Computing, Information and Automation) faculty are gathered from the Computer Science Department, Electrical and Computer Engineering Department, and the School of Technology. The proposed new degree program will utilize the alliance expertise as well as most of the existing courses on cybersecurity in meeting the emerging job market. The proposed M.S. program is expected to attract domestic and international students to pursue cross-disciplinary graduate study of theories with the knowledge of science, engineering, and technology that would help advance the workforce. The curriculum design spans from individual computer units to networking as well as industrial control protection. The program is unique because of the combinations of training environment instilled by the three units in all aspects from theories, engineering, to current practice of security industries. The proposed M.S. program would also broaden the students' opportunities for their future career development with other professional certification such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in the Governance of Enterprise IT (CGEIT), and Certified in Risk and Information Systems Control (CRISC), which requires students to have years of work experience and fundamental cybersecurity training in order for the students to excel.
II. PROPOSAL

1. General description and characteristics of program

The study of information security has been generally focused on foundational areas of information confidentiality, integrity, and availability. Over the past decades, the emerging user population in cyberspace has tremendously increased and the protection against cyberattacks upon highly complex network of social interactions can be a challenging task both in terms of information tracing to those malicious units and voluminous information transferred to the clouds. As the massive cyberattacks can be executed in distributed fashion that can have enormous impact to the society as well as to the nation’s critical cyberinfrastructures, the stakeholders can establish a set of stringent security policies with in-depth understanding how to anticipate potential system impacts as well as strategic investment planning on security protection. This could save the systems from catastrophic effects of massive cyberattacks that can rapidly resume a system back in service avoiding millions of dollars in revenue loss. The proposed M.S. program in cybersecurity will also create a streamline of opportunities on cross-domain knowledge between industrial control systems of cyber-physical security. This is part of a critical infrastructure that would sharpen students’ knowledge to maximize their future potential that is available in engineering elective courses offered by department of electrical and computer engineering.

2. Rationale

The field of cybersecurity is a rapidly growing profession containing a great deal of scientific and computing research opportunities. The demand for cybersecurity professionals is expected to increase by 20 percent through the year 2020 in an effort to protect an increasingly volume of sensitive information stored and transmitted electronically around the globe. Although cybersecurity research topics are often highly focused, their impact is widespread, reaching many of the professional, technical, and scientific disciplines. Michigan Technological University has established a strong internationally-recognized research and education reputation in the areas of mathematics, computing, science, and engineering. With underlying courses in undergraduate cybersecurity education, coupled with existing strong computing and mathematics graduate programs consisting of innovative research relating to this specialized field, Michigan Tech is well-poised to establish a formal graduate program in cybersecurity.

Although the field of cybersecurity is not new, the establishment of graduate programs are rather recent, beginning in 2010. Regionally, there are no universities offering a graduate program in the area of cybersecurity. Nationally there are several good cybersecurity graduate programs, which we discuss them in the following section. However, none of them appear to offer a strong collaborative partnership and blended learning/research between departments as we do. Through a collaborative effort between the Department of Computer Science, Department of Electrical and Computer Engineering, and School of Technology, Michigan Tech will offer a unique and strategic delivery of a cybersecurity graduate program utilizing a wide-range of academic and industry experience in the field of cybersecurity across multiple disciplines, blended learning in both theoretical and applied research, along with shared resources and centers to provide students an excellent education and strong research opportunities.

The M.S. in Cybersecurity program is designed to:
- Deepen students’ understanding and knowledge of cybersecurity;
- Provide students with innovative research opportunities within the field of cybersecurity;
• Provide a cybersecurity curriculum containing both theory and applied research across multiple computing disciplines, preparing the graduates to succeed as a cybersecurity professional or researcher.

3. Discussion of related programs within the institution and at other institutions

3.1 Security-related courses and research activities at Michigan Tech

A. Michigan Tech Cyber Security Course Summary

Department of Computer Science
- CS 3411 - Systems Programming
- CS 4411 - Operating Systems
- CS 4121 - Programming Languages
- CS 4471 - Computer Security
- CS 5471 - Advanced Topics in Computer Security
- CS 5321 – Advanced Algorithms
- CS 4710 - Model Driven Software Development
- CS 4711 - Software Processes and Management
- CS 5461 - Mobile Networks

Department of Electrical and Computer Engineering
- EE 4723 - Network Security
- EE 5500 - Probability and Stochastic Processes
- EE 5900 - Energy Control Center Applications
- EE 5900 - Penetration Testing for Critical Infrastructure
- EE 5900 - Cyber Security for Industrial Control
- EE 5511 – Information Theory

School of Technology
- SAT 3812 - Cybersecurity I
- SAT 4812 - Cybersecurity II
- SAT 5111 - Security and Privacy
- SAT 5211 - Medical Application Development and Security
- SAT 5231 - Statistical Methods for Intrusion Detection
- SAT 5241 - Designing Security Systems
- SAT 5251 - Advanced Topics in Network Security
- SAT 5281 - Healthcare Security Management

Mathematical Sciences
- MA 3203 – Cryptography

B. Security-related education and research activities at Michigan Tech

Drs. Jean Mayo and Ching-Kuang Shene have been conducting research on developing pedagogical methods and supporting tools in two areas: cryptography and access control. This work centers on the use of visualization to improve student learning. The effort in cryptography has produced tools to visualize operations and inner working of several commonly seen and taught ciphers, which include the Vigenère, DES, AES, RSA, SHA (Secure Hash Algorithm) and elliptic curve based ciphers. The effort in access control has produced three tools that allow students to develop and to explore and analyze
policies in the Domain Type Enforcement Language (DTEL), the multi-level (Bell-LaPadula) access control model, and the role-based access control (RBAC) model. The National Science Foundation funds both projects. Another NSF project focuses on secure programming using techniques from compiler design for the students to visualize insecure constructs in their programs. Moreover, Dr. Jean Mayo also conducts basic research achieving anonymity in peer-to-peer networks. An ongoing project is investigating use of a firewall model of file system access control. This model allows access requests to be moderated on a number of attributes, both of a process and of the environment, in addition to user credentials.

Drs. Spiros Bakiras, Min Song, and Xiaohua Xu have been conducting research on secure and privacy-preserving computations, applied cryptography, and malicious user detection. Furthermore, Dr. Spiros Bakiras has extensive teaching experience in cybersecurity-related courses, including network security, digital forensics, applied cryptography, network forensics, and secure operating systems. Drs. Min Song and Xiaohua Xu also developed network security algorithms using game theory.

Dr. Chee-Wooi Ten's primary area of interest is cyber security for power infrastructure systems. In particular, his research thrusts include risk-based assessment methodologies with respect to incidence response, validation of information integrity, cyber-threat contingency evaluation for SCADA framework, asset management of interoperability dependencies, and emerging data exchange paradigms within sub-transmission and distribution system networks.

Dr. Shiyan Hu is an associate professor in the ECE Department. His primary interests are in computer-aided design for very large scale integration (VLSI) circuits. He has done some work in the security aspects of this problem, related to the protection of intellectual property (IP) when the highly complex CAD work is done using network or cloud computing.

Dr. Xinli Wang and Guy Hembroff have been conducting research in the areas of cyber security, cloud computing, biometric application development and security, computer vision, and encryption. They have been funded by the NSF for the creation of cyber security labs for educators teaching in the area of cyber security and information technology. The two associate professors combine to teach courses in security and privacy, cyber security, and forensics.

Blue Marble Security (BMS) Enterprise. BMS is a large enterprise hosted in the ECE Department, with around 50 students and about 10 projects active at any given time. The theme of the enterprise is homeland security, very broadly interpreted. Recent projects have included airborne radar system simulation and video surveillance.

Institute of Computing and Cybersystems (ICC). ICC is the research arm of ACIA. It leads and promotes research and learning experiences in the areas of mobile computing, cybersecurity, and cyber systems. ICC is composed of four centers; one of them focuses on cybersecurity. ICC currently has 30 members including faculty members from the departments of Computer Science, Electrical and Computer Engineering, Mechanical Engineering, Civil Engineering, and the School of Technology.

3.2 Related programs at institutions in the State of Michigan

The University of Michigan offers several courses focused on cybersecurity concerns. The Electrical Engineering and Computer Science (EECS) department offers an undergraduate course on computer security teaches the principles and practices of computer security as they are applied to software,
host systems, and network. A graduate EECS course on computer and network security covers both foundational work and current topics in computer security. This graduate course prepares students for computer security research and provides hands-on experience designing and evaluating secure systems. The department has also offered a special topics course on medical device security. Relevant cybersecurity topics are covered in a number of EECS courses that do not center on security. These include undergraduate courses on operating systems and web database and information systems, and graduate courses on electronic commerce, correct operation for processors and embedded systems, operating systems, computer networks and mobile computing. Other departments within the University offer courses on cryptology (Math) and computer crime (Law). University faculty conduct research in several areas of cybersecurity.

At Michigan State University, there are a few cybersecurity-related courses offered by the department of Computer Science and Engineering (CSE) and the department of Electrical and Computer Engineering (ECE). At the undergraduate level, the CSE department offers the Introduction to Computer Security course, which is targeted towards Computer Science and Computer Engineering majors. The course addresses topics such as security engineering, security protocols, cryptography and cryptanalysis, and network security and intrusion detection. The department also offers a cybersecurity course for non-majors (Interdisciplinary Topics in Cybersecurity), which is a collaboration among faculty from six colleges (law, business, communication, criminal justice, medicine, and engineering). This course focuses on the technical, legal, criminal, medical business, and communication aspects of cybersecurity. At the graduate level, the CSE department offers a course on Computer and Network Security that discusses threat assessments, secure software, intrusions, and intrusion detection. Finally, the ECE department offers a graduate level course on Cryptography and Network Security that addresses issues such as cryptographic protocols, network and system security practices, e-mail security, IP security, web security, and firewalls.

Wayne State University offers a couple network security courses that directly or indirectly touch on the subject of cybersecurity. Currently, there are three faculty members in the Computer Science Engineering department working on the security-related research that can provide some pilot courses at the graduate level. However, these courses are not listed on the official department website. There are some training courses related to the university IT security but none of them is related to the part that can be used for a coursework degree program. Individual faculty members may promote directed studies on security-related topics to the graduate students who are interested in their research for the training on wireless, embedded, or database security subjects.

Northern Michigan University has a B.S. in Information Assurance and Cyber Defense program, which is housed within in the College of Business. Students will take courses dealing specifically with cyber security as well as business and computer information systems, and learn hacking skills from hands-on activities and learn how to think like hackers so the students can better protect against them. Security related courses include IS 436 Network Security Tools and Techniques and CIS 226 Introduction to Networks and Security.

### 3.3 Related programs at other institutions

The graduate program in cybersecurity at other universities nationally exist. We searched 22 universities, including four from the State of Michigan and 18 outside Michigan. Results are given in Table 1. Most of the searched universities outside Michigan offer M.S. degree in cybersecurity or
information security and assurance. Some of them offer graduate certificate. Only Northeastern University offers Ph.D. degree in Information Assurance. University of Michigan, Michigan State University, Wayne State University, and Northern Michigan University do not have a specific graduate program in cybersecurity.

Most of the graduate programs in cybersecurity and information assurance are an interdisciplinary program. The number of core courses ranges from 3 to 7, along with a number of electives from different departments. Topics of the courses cover computer science, computer engineering, information technology, justice, psychology, management, accounting, social science and so on. Courses are taught by faculty from multiple departments. Some programs are more theory-oriented, studying additional theoretical materials. Most of the programs highlight technical components. Students from different fields can have different concentrations to earn the degree.

### Table 1 Studied Universities

<table>
<thead>
<tr>
<th>University</th>
<th>Degrees Offered</th>
<th>Host</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>University of Southern California Viterbi</td>
<td>MS in Cyber Security Engineering</td>
<td>School of Engineering; Online/Distance</td>
<td>7 required courses plus electives</td>
</tr>
<tr>
<td>George Washington University</td>
<td>MS in Cyber Security</td>
<td>Department of Computer Science</td>
<td>Additional exposure to cyber security</td>
</tr>
<tr>
<td>NYU Polytechnic</td>
<td>MS in Cyber Security</td>
<td>School of Engineering</td>
<td>Theory must translate into real-world solutions</td>
</tr>
<tr>
<td>New Jersey Institute of Technology</td>
<td>MS in Cybersecurity and Privacy</td>
<td>Department of Computer Science</td>
<td>6 core courses; 17 electives; 3 foundational courses</td>
</tr>
<tr>
<td>Johns Hopkins University</td>
<td>MS in Cybersecurity; Post-Master Certificate</td>
<td>JHU Whiting School of Engineering</td>
<td>3 core courses; 5 from the program; 2 electives</td>
</tr>
<tr>
<td>Northeastern University</td>
<td>MS and PhD in Information Assurance</td>
<td>College of Computer &amp; Information Science</td>
<td></td>
</tr>
<tr>
<td>Stevens Institute of Technology</td>
<td>MS in Cybersecurity</td>
<td>School of Engineering and Science</td>
<td>All courses are in CS department</td>
</tr>
<tr>
<td>UM Baltimore County</td>
<td>Master’s in Professional Studies: Cybersecurity</td>
<td>Division of Professional Studies</td>
<td>6 required courses; 4 electives</td>
</tr>
<tr>
<td>UM University College</td>
<td>MS in Cybersecurity; MS in Digital Forensics and Cyber Investigation; MS in Cybersecurity Policy</td>
<td>Online</td>
<td>6 required courses; electives</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 different MS degrees</td>
</tr>
<tr>
<td>Maryland Cybersecurity Center</td>
<td>Master of Engineering in Cybersecurity</td>
<td>The center</td>
<td>6 required core courses; 2-4 electives</td>
</tr>
<tr>
<td>University of Alabama at Birmingham</td>
<td>MS in Computer Forensics and Security Management</td>
<td>Department of Computer and Information Science</td>
<td>Courses are offered from 6 departments; interdisciplinary</td>
</tr>
<tr>
<td>George Mason</td>
<td>Information Security and</td>
<td>Division of</td>
<td>Different for different</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>University</td>
<td>Program</td>
<td>College/Department</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>University Assurance, MS and Certificate; Applied Cyber Security Certificate; Telecommunications Forensics and Security Graduate Certificate</td>
<td>Computer Science degrees: MS, 6 required + electives</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purdue University</td>
<td>MS and PhD in Information Security</td>
<td>The Center for Education and Research in Information Assurance and Security</td>
<td>Interdisciplinary; different for different emphasis</td>
</tr>
<tr>
<td>Northern Michigan University</td>
<td>BS in Information Assurance and Defense</td>
<td>College of Business</td>
<td></td>
</tr>
<tr>
<td>UW Parkside</td>
<td>Certificate on cybersecurity</td>
<td>CS Department</td>
<td></td>
</tr>
<tr>
<td>University of Minnesota</td>
<td>MS in Security Technologies</td>
<td>Technological Leadership Institute</td>
<td>Most of the courses are in the security management/law areas</td>
</tr>
<tr>
<td>UW Madison</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indiana Univ. Bloomington</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virginia Tech</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>UM Ann Arbor</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Michigan State Univ.</td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wayne State Univ.</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.4 Projected enrollment and economic impact

The projected enrollment in the proposed M.S. in cybersecurity program would be about 20 students. We anticipate eventually reaching 40 students enrolled per year as the program gains some visibility and prominence.

As mentioned previously, none of the four major universities in Michigan offer an M.S. degree in cybersecurity. However, according to Michigan Cyber Initiative 2015 (http://www.michigan.gov/cybersecurity), the state of Michigan blocks more than 650,000 cyberattacks daily. Annually, the state blocks 2.5 million web browser attacks, 179.5 million HTTP-based attacks, 79.5 million network scams, and 5.2 million intrusions. As such, our program will fill the need for cybersecurity education in the state of Michigan, and establish Michigan Tech as the premier institution for cybersecurity professionals in the state. To understand the significance of cybersecurity today, it is worth noting that the annual U.S. cybercrime costs are estimated at around $100 billion (http://www.wsj.com/articles/SB10001424127887324328904578621880966242990). As a result, private enterprises as well as government organizations are constantly increasing their IT security budgets for protecting their data against cyberattacks. For example, according to a recent report by a top security firm (McAfee), the annual spending on cybersecurity software worldwide is
$60 billion, growing at about 8% per year (http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf). Furthermore, in 2012, U.S. federal agencies spent over $15 billion on cybersecurity projects, which was about 20% of the total federal spending on IT. Our program will produce a stream of highly qualified cybersecurity experts that will take advantage of this emerging technology field.

4. Scheduling plans
The classes will be taught on the Michigan Tech campus.

5. Curriculum design
The program has a non-thesis option and a thesis option. A minimum of 30 credits are required for the program. Three concentrations are available: Trusted Software Engineering (TSE), Critical Infrastructure Protection (CIP), and Network Security Management (NSM).

For the non-thesis option, the course structure of proposed curriculum is threefold: core, concentration required, and elective. The core courses are required for all students in the program. The concentration required courses are required for students in a particular concentration. The elective courses are provided for all students in the program. Such curriculum design is similar to most of the Master’s programs. However, the option of providing large selection of elective courses offers students with great flexibility in choosing classes within the three units and helps them to maximize their domain-specific knowledge of interests. For example, the students in electrical engineering who are very interested to improve their knowledge both in theory and implementation, they could take more courses from Computer Science Department and School of Technology as meeting their elective requirement. Similarly, the computer science students would be able to do the same to take more electrical engineering courses. A blend of practicality, theory, and implementation would enrich students’ learning experience in the Master’s program to better prepare them for their future security career. Tables 2a, 2b, and 2c enumerate all course requirements for the non-thesis option.

Table 2a. CORE – total 12 credits

<table>
<thead>
<tr>
<th>CS</th>
<th>4471/5471</th>
<th>Computer Security</th>
<th>3</th>
<th>Existing</th>
</tr>
</thead>
<tbody>
<tr>
<td>EE</td>
<td>4723</td>
<td>Network Security</td>
<td>3</td>
<td>Existing</td>
</tr>
<tr>
<td>CS</td>
<td>5090</td>
<td>National Cybersecurity Policy and Law</td>
<td>3</td>
<td>New</td>
</tr>
<tr>
<td>MA</td>
<td>3203</td>
<td>Cryptography</td>
<td>3</td>
<td>Existing</td>
</tr>
</tbody>
</table>

Table 2b. Concentration Required – total 12 credits for each concentration (TSE/CIP/NSM)

<table>
<thead>
<tr>
<th>TSE</th>
<th>CS</th>
<th>5090</th>
<th>Advanced Topics in Computer Security</th>
<th>3</th>
<th>Existing</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSE</td>
<td>CS</td>
<td>4710</td>
<td>Model Driven Software Development</td>
<td>3</td>
<td>Existing</td>
</tr>
<tr>
<td>TSE</td>
<td>CS</td>
<td>5321</td>
<td>Advanced Algorithms</td>
<td>3</td>
<td>Existing</td>
</tr>
<tr>
<td>TSE</td>
<td>CS</td>
<td>5090</td>
<td>Development of Trusted Software</td>
<td>3</td>
<td>New</td>
</tr>
<tr>
<td>CIP</td>
<td>EE</td>
<td>5500</td>
<td>Probability and Stochastic Processes</td>
<td>3</td>
<td>Existing</td>
</tr>
<tr>
<td>CIP</td>
<td>EE</td>
<td>5900</td>
<td>Energy Control Center Applications</td>
<td>3</td>
<td>Existing</td>
</tr>
<tr>
<td>CIP</td>
<td>EE</td>
<td>5900</td>
<td>Penetration Testing for Critical Infrastructure</td>
<td>3</td>
<td>New</td>
</tr>
</tbody>
</table>
A student can take any two courses from other concentrations listed in Table 2b and the courses listed in Table 2c. That is, the number of elective courses is up to 19 courses.

**Table 2c. Elective – total 6 credits**

<table>
<thead>
<tr>
<th>CS</th>
<th>4711</th>
<th>Software Processes and Management</th>
<th>3</th>
<th>Existing</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS</td>
<td>5461</td>
<td>Mobile Networks</td>
<td>3</td>
<td>Existing</td>
</tr>
<tr>
<td>CS</td>
<td>5811</td>
<td>Advanced Artificial Intelligence</td>
<td>3</td>
<td>Existing</td>
</tr>
<tr>
<td>CS</td>
<td>5431</td>
<td>Advanced Computer Architecture</td>
<td>3</td>
<td>Existing</td>
</tr>
<tr>
<td>CS</td>
<td>5441</td>
<td>Distributed Systems</td>
<td>3</td>
<td>Existing</td>
</tr>
<tr>
<td>EE</td>
<td>5511</td>
<td>Information Theory</td>
<td>3</td>
<td>Existing</td>
</tr>
<tr>
<td>EE</td>
<td>5900</td>
<td>Multimedia Security</td>
<td>3</td>
<td>New</td>
</tr>
<tr>
<td>SAT</td>
<td>5211</td>
<td>Medical Application Development and Security</td>
<td>3</td>
<td>Existing</td>
</tr>
<tr>
<td>SAT</td>
<td>5231</td>
<td>Statistical Methods for Intrusion Detection</td>
<td>3</td>
<td>Existing</td>
</tr>
<tr>
<td>SAT</td>
<td>5241</td>
<td>Designing Security Systems</td>
<td>3</td>
<td>Existing</td>
</tr>
<tr>
<td>SAT</td>
<td>5251</td>
<td>Advanced Topics in Network Security</td>
<td>3</td>
<td>Existing</td>
</tr>
</tbody>
</table>

For the thesis option, students take all the courses listed in Table 2a and four courses listed in Table 2b based on their concentrations in addition to the thesis research, which is equivalent to 6 credits.

6. **New course descriptions**

**CS 5090 National Cybersecurity Policy and Law**
This course introduces the role of government in securing cyberspace. Students will learn the basic national cybersecurity policy and law. Topics include federal, state, and local entities involved in cybersecurity; relevant laws and regulations; concepts of civil liberties, intellectual property, and privacy; development and diffusion of standards; and national security.

**CS 5090 Development of Trusted Software**
This course exposes students to the concept of secure software development. Students will learn how to develop high-quality software that is resistant against cyber-attacks, by minimizing the number of vulnerabilities that can be exploited by an attacker. Topics include access control, race conditions, buffer overflows, code injection, fuzzing techniques, cryptographic software, web application security and Java security.

**EE 5900 Multimedia Security**
This course covers topics in digital media security. This includes examination and analysis of digital media for the purpose of detection against tampering and forgery, authentication, water marking,
and visual and audio detection. Topics include digital media watermarking, digital watermarking protocol, digital rights management & multimedia security, steganography & steganalysis, biometrics recognition and authentication, fingerprinting & non intrusive digital forensics.

EE5900 - Penetration Testing for Critical Infrastructure
This course covers the fundamental of penetration testing in the industrial control environment. The course will introduce the typical industrial and substation automation Intranet and its connections to other networks with a boundary protection. Topics of discussion include the available tools as an ethical hackers and what would be required for them to get started while at the same time what defenders would do the best to prevent successful electronic intrusion to the Intranet.

SAT 5900 Digital Forensics
This course introduces students to the investigative process involved in computer crimes. Students will learn how to collect, preserve, and analyze computer and network data that may be used in a courtroom. Topics include computer data acquisition and preservation, file system analysis, file carving techniques, memory forensics, network data collection and analysis, and mobile device forensics.

7. Library and other learning resources
The following required security journals and proceedings are available in the library:

- ACM SIGPLAN Print : Programming Languages
- ACM SIGCOMM: Computer Communication Review
- ACM SIGOPS : Operating System Review
- ACM SIGCOMM: Computer Communication Review
- ACM SIGACT : Algorithms and computational
- IEEE Transactions on Information Forensics and Security
- Journal of Computer security
- Journal of Network & Computer Application
- Journal of Systems and Software

No additional library or learning resources are required.

8. Computing access fee
This program does not require additional computing access fee other than the existing lab fee applied to some of the courses.

9. Faculty resumes
Graduate faculty serving this new program are:

- Spiros Bakiras, Department of Computer Science
- Jeremy Bos, Department of Electrical and Computer Engineering
- Laura Brown, Department of Computer Science
- Yu Cai, School of Technology
- Ali Ebnenasir, Department of Computer Science
- Chunming Gao, School of Technology
- Steven Goldsmith, Department of Electrical and Computer Engineering
- Daniel Fuhrmann, Department of Electrical and Computer Engineering
• Guy Hembroff, School of Technology
• Shiyan Hu, Department of Electrical and Computer Engineering
• Jean Mayo, Department of Computer Science
• Saeid Nooshabadi, Department of Computer Science and Department of Electrical and Computer Engineering
• Nilufer Onder, Department of Computer Science
• Soner Onder, Department of Computer Science
• Michael Roggemann, Department of Electrical and Computer Engineering
• Ching-Kuang Shene, Department of Computer Science
• Min Song, Department of Computer Science
• Chee-Wooi Ten, Department of Electrical and Computer Engineering
• Charles Wallace, Department of Computer Science
• Xinli Wang, School of Technology
• Zhenlin Wang, Department of Computer Science
• Xiaohua Xu, Department of Computer Science

The curriculum vitae of the faculty members are given at
http://www.mtu.edu/cs/department/faculty-staff/faculty/
http://www.mtu.edu/ece/department/faculty/
http://www.mtu.edu/technology/about/faculty/

10. Description of available/needed equipment
The Computer Science Department, Electrical and Computer Engineering Department, and the School of Technology are well equipped with modern research laboratories:
http://www.mtu.edu/cs/facilities/labs/
http://www.mtu.edu/ece/research/focus/
http://www.mtu.edu/technology/about/labs/

No additional equipment is required for this new graduate degree program.

11. Additional resources required
A new faculty line at the rank of assistant professor level is requested to help cover the new courses. The College of Science and Arts and the Provost’s office will provide resources for the new faculty line.

12. Space
No additional space is required to accommodate this new graduate degree program.

13. Policies, regulations and rules
None besides curricular requirements outlined above.

14. Accreditation requirements
Not applicable.

15. Internal status of the proposal
• September 4, 2015: the M.S. in Cybersecurity Task Force Committee (Jean Mayo at Computer Science Department, Spiros Bakiras at Computer Science Department, Chee-Wooi Ten at Electrical and Computer Engineering Department, and Xinli Wang at School of Technology) approved the proposal and submitted to the CS Department Graduate Committee.

• September 8, 2015: the CS Department Graduate Committee approved the proposal and submitted to the ACIA Executive Committee (Chair of Computer Science Department, Chair of Electrical and Computer Engineering Department, and Dean of School of Technology).

• September 14, 2015: the ACIA Executive Committee approved the proposal. Supportive suggestions were received.

• September 15, 2015: the revised proposal was approved by CS Department faculty. Supportive suggestions were received.

• September 22, 2015: the revised proposal was discussed in the council meeting of the College of Science and Arts. The College Council approved the proposal. Supportive suggestions were received.

• September 29, 2015: the revised proposal was approved by the Dean of the College of Science and Arts.

16. External Advisory Committee

• Kent Blossom, Vice President, IBM Security Solutions, kblossom@us.ibm.com
• Nasir Memon, Professor of Computer Science and Engineering, NYU Poly, memon@nyu.edu
• Eoghan Casey, Lead Cyber Security Engineer at the MITRE Corporation, ecasey@mitre.org
• Bruce Schneier, CTO at Resilient Systems, schneier@schneier.com
• Jamie Levy, Senior Researcher at Volatility Foundation, jamie@memoryanalysis.net
• Steve Bellovin, Professor, Bell Labs and Columbia, smb@cs.columbia.edu
• Jeff Voas, Computer Scientist, Computer Security Division, NIST, jeff.voas@nist.gov

17. Planned implementation date

Fall semester 2016.

18. Program Governance

The program will be administrated by the Computer Science department. Computer Science department is the Home Department of this program, and is responsible for the admission, advising and other administrative duties.
Flow Chart for TSE Track with Course Option

**Fall 1 (9)**
- CS 4710/5471 (3) Computer Security
- EE 4723 (3) Network Security
- CS 4710 (3) Model Driven Software Development

**Spring 1 (9)**
- CS 5090 (3) National Cybersecurity Policy and Law
- MA 3203 (3) Cryptography

**Fall 2 (12)**
- CS 5090 (3) Advanced Topics in Computer Security
- CS 5321 (3) Advanced Algorithms
- Elective (3)

**Required Total: 30**

**Elective (3)**
Flow Chart for TSK Track with Thesis Option

**Fall 1 (9):**
- CS 4471/5471 (3) Computer Security
- EE 4723 (3) Network Security
- CS 4710 (3) Model Driven Software Development

**Spring 1 (9):**
- CS 5090 (3) National Cyber Security Policy and Law
- MA 3203 (3) Cryptography

**Summer 1 (3):**
- Thesis Research (3)

**Fall 2 (9):**
- CS 5090 (3) Advanced Topics in Computer Security
- CS 5321 (3) Advanced Algorithms
- CS 5090 (3) Development of Trusted Software

**Thesis Research (3)**

**Total: 30**

*Color Reference Chart:*
- Yellow = Core
- Teal = Concentration
- Orange = Thesis Research
Flow Chart for CIP Track with Course Option

**Fall 1 (9)**
- CS 4471/5471 (3) Computer Security
- EE 4723 (3) Network Security
- EE 5500 (3) Probability and Stochastic Processes

**Spring 1 (9)**
- CS 5090 (3) National Cyber Security Policy and Law
- MA 3203 (3) Cryptography

**Fall 2 (12)**
- EE 5900 (3) Cyber Security for Industrial Control
- EE 5900 (3) Penetration Testing for Critical Infrastructure
- Energy Control Center Applications

**Elective or (3)**
- Elective (3)

**Required Total: 30**

**Color Reference Chart:**
- Yellow = Core
- Blue = Concentration
- Orange = Elective
Flow Chart for CIP Track with Thesis Option

**Fall 1 (9)**
- CS 4471/5471 (3) Computer Security
- EE 4723 (3) Network Security
- EE 5500 (3) Probability and Stochastic Processes

**Spring 1 (9)**
- CS 5090 (3) National Cyber Security Policy and Law
- MA 3203 (3) Cryptography

**Summer 1 (3)**
- Thesis Research (3)

**Fall 2 (9)**
- EE 5900 (3) Cyber Security for Industrial Control
- EE 5900 (3) Penetration Testing for Critical Infrastructure
- EE 5900 (3) Energy Control Center Applications
- Thesis Research (3)

**Required Total: 30**

**Color Reference Chart:**
- Yellow = Core
- Blue = Concentration
- Orange = Thesis Research
Flow Chart for NSM Track with Course Option

- **Fall 1 (9)**
  - CS 4471/5471 (3) Computer Security
  - EE 4723 (3) Network Security
  - SAT 5111 (3) Security and Privacy

- **Spring 1 (9)**
  - CS 5090 (3) National Cyber Security Policy and Law
  - MA 3203 (3) Cryptography
  - SAT 4812 (3) Cyber Security II

- **Fall 2 (12)**
  - SAT 5990 (3) Digital Forensics
  - SAT 5281 (3) Healthcare Security Management
  - Elective (3)

- **Required Total: 30**

**Color Reference Chart:**
- Yellow = Core
- Blue = Concentration
- Orange = Elective
Flow Chart for NSM Track with Thesis Option

- **Fall 1 (9)**
  - CS 4471/5471 (3) Computer Security
  - EE 4723 (3) Network Security
  - SAT 5111 (3) Security and Privacy

- **Spring 1 (9)**
  - CS 5090 (3) National Cyber Security Policy and Law
  - MA 3203 (3) Cryptography
  - SAT 4812 (3) Cyber Security II

- **Summer 1 (3)**
  - Thesis Research (3)

- **Fall 2 (9)**
  - SAT 5990 (3) Digital Forensics
  - SAT 5281 (3) Healthcare Security Management
  - Thesis Research (3)

**Required Total: 30**

**Color Reference Chart:**
- Yellow = Core
- Blue = Concentration
- Orange = Thesis Research
Appendix: Financial documentation for Master of Science in Cybersecurity

I. Relation to university strategic plan
   a. Relation of program to the university’s educational and research goals: This new Master program supports Goal 2.1 of the university strategic plan (Integration of instruction, research, and innovation to achieve the University Student Learning Goals.). Specifically, “promote mutual appreciation and collaborative opportunities across academic disciplines,” and “continually review and update existing programs and develop new offerings in emerging disciplinary and interdisciplinary areas.”
   b. Consistency with the university’s resource allocation criteria: The proposed program intended to attract new graduate students to the university based on existing instruction and research resources.

II. Impact on university enrollment
   a. Projected number of students in the program: The projected enrollment in the proposed M.S. in cybersecurity program would be about 20 students. We anticipate eventually reaching 40 students enrolled per year as the program gains some visibility and prominence.
   b. Source of new students; in particular, will the students be drawn from existing programs, or will they be students who would otherwise not have come to MTU? It is expected that majority of the students in the program will be new graduate students who would otherwise not have come to MTU. Some of the students in the program will be our own B.S. graduates who would otherwise go to other cybersecurity programs in other institutions.
   c. What is the likely correlation between demand for the new program and existing enrollment patterns at MTU? The field of cybersecurity is a rapidly growing profession containing a great deal of scientific and computing research opportunities. The demand for cybersecurity professionals is expected to increase by 20 percent through the year 2020 in an effort to protect an increasingly volume of sensitive information stored and transmitted electronically around the globe. This program is expected to attract students to pursue cross-disciplinary graduate study of theories with the knowledge of science, engineering, and technology that would help advance the cybersecurity workforce. Three concentrations are available: Trusted Software Engineering (TSE), Critical Infrastructure Protection (CIP), and Network Security Management (NSM). This will likely attract students from non-CS background into the department of computer science and thus diversify the existing enrollment patterns at the departmental level.
   d. What is the current enrollment in the unit? Fall 2015: 45 graduate students.

III. Impact on resources required by department in which the program is housed
   a. Faculty lines: The projected enrollment would be about 20 students in the first couple of years, and 40 students as the program gains some visibility and prominence. These students are expected to be self-supported. So the total tuition revenue generated in year 1 from this program is expected to be
($861.50 per credit X 18 credits + $950 surcharge per semester X 2) X 20

= $348,140

Tuition revenue is expected to be more in the subsequent years.

To help cover the new courses, a new faculty line at the rank of assistant professor level is requested. The College of Science and Arts and the Provost’s office will provide resources for the new faculty line.

b. Faculty and student labs, including ongoing maintenance: Existing research labs are adequate to support this program.

c. Advising: Students in this program will be advised by the graduate faculty listed in the proposal.

d. Assessment: The Computer Science graduate committee will monitor and evaluate the enrollment and student performance of the new program in an annual basis.

IV. Impact on resources required by other units within the university

a. Other academic (e.g., Gen Ed) units with regard to faculty, labs and assessment. We do not expect any significant impact to other units although some of the existing classes may occasionally see an increase of enrollment.

b. Information Technology, the Library, central administration and career planning with respect to the impact on the need for computing services, library resources, advising, record keeping, development of employer relations etc. There should be no significant impact on other units.

V. Assessment of the ability to obtain the necessary resources assuming requested funds are obtained. For high demand fields (e.g., business fields, etc.), will it be possible to fill allocated lines? Not applicable as we do not need addition resources.

VI. Past proposals

The Computer Science Department has not initiated any new Master degree programs for about 34 years. Our Master program in Computer Science was approved in 1981, and our Computer Science Ph.D. program was approved in 2002.

VII. Departmental budget contribution

All figures are for 2014-15.

a. What is the department’s total general fund budget? The general fund base budget was $2.55 million.

b. How much tuition does the department generate? This information should be provided for both the credit hours taught by the department and the number of credit hours taken by the department’s majors. The total tuition the department generated credit hours taught by the department are $520 X 9093 SCH = $4,728,360. And the number of credit hours taken by the department’s majors are approximately 400 students x 30 (average credits for fall / spring combined) credits = 12,000 SCH.

VIII. How do the benefits from this program compare to other alternatives that are currently under consideration or development? The proposed M.S. in cybersecurity degree program will attract students from diverse undergraduate backgrounds, including but not limited to computer science. The course structure is threefold: core, concentration required, and elective. The core courses are required for all students in the program. The concentration required courses
are required for students in a particular concentration: Trusted Software Engineering (TSE), Critical Infrastructure Protection (CIP), and Network Security Management (NSM). The elective courses are provided for all students in the program. The option of providing large selection of elective courses offers students with great flexibility in choosing classes within the three units and helps them to maximize their domain-specific knowledge of interests. For example, the students in electrical engineering who are very interested to improve their knowledge both in theory and implementation, they could take more courses from Computer Science Department and School of Technology as meeting their elective requirement. Similarly, the computer science students would be able to do the same to take more electrical engineering courses. A blend of practicality, theory, and implementation would enrich students’ learning experience in the Master’s program to better prepare them for their future security career.
Request:
Place a Registration Hold on graduate students who have not named their Graduate Advisor on the Advisor and Committee Recommendation Form by the end of the second term of enrollment in their program.

Reason:
Information regarding Graduate Faculty Advisor is loaded into Digital Measures Activities Insight, from Graduate School information in Banner, for purposes of merit increase and promotion and tenure of faculty. Accurate, timely data is needed to satisfy faculty in this regard. Currently, students are not required to submit this information and are instead reminded, sometimes repeatedly, by the Graduate School. There are students with five years enrollment and no Advisor and Committee Recommendation Form with graduate advisor on file. Overall, there currently are 15% of students who have completed two terms that have no record of an advisor (per Deb Charlesworth). Placing a hold on registration would increase compliance by students to submit this form and information.

Result:
A registration hold resulting in student compliance for completing Advisor and Committee Recommendation Form identifying Graduate Faculty Advisor would create accurate, timely data for Digital Measures. This would save person hours for faculty, Information Technology staff, and Graduate School staff, which is currently required for attempts with resolving a missing Graduate Faculty Advisor problem. Currently, there are times when the problem does not get resolved because even after reminders, students do not file the form in a timely manner.

A side benefit would be that the Graduate School would have Graduate Faculty Advisor information earlier for purposes of notification for student issues, such as medical absence or timely completion of degree.

..
Curricular Practical Training for F-1 Students

What is CPT? CPT can provide valuable work experience by sharpening and adding to the skills you are learning in school.

CPT Facts

- Must have been enrolled full-time at Michigan Tech for at least one full academic year.
- CPT is available only prior to the completion of your degree program and you must have a job offer at the time of application.
- Employment must be directly related to your major.
- Remain in F-1 status while on CPT.
- You can work on CPT either full-time or part-time.
- Your advisor, the Graduate School, if graduate level, and the Career Services Office must approve and you must be registered full-time in co-op credits to be on CPT during Fall and Spring semesters (undergrads, 2 co-op credits; grad students, 1-6 co-op credits). The Career Center manages both graduate and undergraduate co-op registration: http://www.mtu.edu/career/students/coops-internships/resources/forms/.
- Students must meet with IPS to receive approval and new I-20 before starting CPT.
- Students are not eligible for OPT if they have completed 365 fulltime days of Curricular Practical Training (CPT).
November 10, 2015

Greetings Graduate Faculty Council:

It was a pleasure to meet with you all briefly yesterday afternoon. As requested, this is a summary of my desired plan regarding CPT.

- As F-1 visa holders (degree-seeking students, both undergraduate and graduate) the primary purpose for them being here is to study. With that, the government requires that they are making satisfactory academic progress toward their degree program. My concern right now is that there isn’t an institutional policy limiting students part-time vs. full time nor the amount of consecutive CPT opportunities that an international student can register for. This can result in students taking 3-4 back-to-back full-time CPT opportunities. I am alarmed that students in these cases aren’t making satisfactory academic progress toward their degrees if they are not enrolled for a full academic year.

I did conduct research regarding institutional policies of other institutions and found that there isn’t a consistent policy across the board. For example, most universities such as University of California Santa Cruz, Penn State and University of Michigan requires their students to register for a full-time course load during the academic year. Thus, students can register for part-time CPT ONLY during the academic year to ensure that students are making satisfactory academic progress during the academic year. While University of Detroit Mercy – does not allow students to participate in two full-time experiences in a row, again to ensure that students are making satisfactory academic progress. There are a few institutions such as Northeastern University that doesn’t appear to have any limitations related to full time enrollment or consecutive CPT opportunities.

- I am considering incorporating an institutional policy limiting the amount of consecutive full-time CPT opportunities to two semesters. With this policy in place, IPS and the institution would be postured to have a system in place to ensure that students are making demonstrated satisfactory academic progress toward their degree.

I wanted to discuss this change with stakeholders on campus, including GFC, the Provost Office and Career Services before making it an institutional policy. Any feedback you have is appreciated.

Regards,

Darnishia L. Slade
dslade@mtu.edu