The University Senate of Michigan Technological University

Proposal 24-16

(Voting Units: Academic)

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 4471/5471 - 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 5231 - Energy Control Center Applications
- EE 5451 - Risk Management for Critical Infrastructure Protection
- EE 5455 - Cyber Security for Industrial Control Systems
- 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

University	Degrees Offered	Host	Notes
University of Southern California Viterbi	MS in Cyber Security Engineering	School of Engineering; Online/Distance	7 required courses plus electives
George Washington University	MS in Cyber Security	Department of Computer Science	Additional expose to cyber security
NYU Polytechnic	MS in Cyber Security	School of Engineering	Theory must translate into real-world solutions
New Jersey Institute of Technology	MS in Cybersecurity and Privacy	Department of Computer Science	6 core courses; 17 electives; 3 foundational courses
Johns Hopkins University	MS in Cybersecurity; Post-Master Certificate	JHU Whiting School of Engineering	3 core courses; 5 from the program; 2 electives
Northeastern University	MS and PhD in Information Assurance	College of Computer & Information Science	
Stevens Institute of Technology	MS in Cybersecurity	School of Engineering and Science	All courses are in CS department
UM Baltimore County	Master's in Professional Studies: Cybersecurity	Division of Professional Studies	6 required courses; 4 electives
UM University College	MS in Cybersecurity; MS in Digital Forensics and Cyber Investigation; MS in Cybersecurity Policy	Online	6 required courses; electives 3 different MS degrees
Maryland Cybersecurity Center	Master of Engineering in Cybersecurity	The center	6 required core courses; 2-4 electives
University of Alabama at Birmingham	MS in Computer Forensics and Security Management	Department of Computer and Information Science	Courses are offered from 6 departments; interdisciplinary

George Mason University	Information Security and Assurance, MS and Certificate; Applied Cyber Security Certificate; Telecommunications Forensics and Security Graduate Certificate	Department of Computer Science	Different for different degrees: MS, 6 required + electives
Purdue University	MS and PhD in Information Security	The Center for Education and Research in Information Assurance and Security	Interdisciplinary; different for different emphasis
Northern Michigan University	BS in Information Assurance and Defense	College of Business	
UW Parkside	Certificate on cybersecurity	CS Department	
University of Minnesota	MS in Security Technologies	Technological Leadership Institute	Most of the courses are in the security management/law areas
UW Madison	No		
Indiana Univ. Bloomington	No		
Virginia Tech	No		
UM Ann Arbor	No		
Michigan State Univ.	No		
Wayne State Univ.	No		

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 coursework option, a report 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). All students in this program need to choose one concentration.

For the coursework 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 coursework option.

All students in this program are required to take four core courses (12 credits) listed in Table 2a, and four concentration-required courses listed in Table 2b. Notice that Table 2b lists a total of 12 courses; four concentration-required courses (12 credits) in each concentration.

Students in the coursework option need to take two elective courses (6 credits) from the courses listed in the other two concentrations in Table 2b or those in Table 2c. Students in the report option can take up to six research credits but no less than two research credits. Students in the thesis option must take six research credits.

Table 2a. CORE – total 12 credits

CS	4471/5471	Computer Security	3	Existing
EE	4723	Network Security	3	Existing
CS	5000	National Cybersecurity Policy and Law	3	New

MA	3203	Cryptography	3	Existing

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

TSE	CS	5472	Advanced Topics in Computer Security	3	Existing
TSE	CS	4710	Model Driven Software Development	3	Existing
TSE	CS	5321	Advanced Algorithms	3	Existing
TSE	CS	5740	Development of Trusted Software	3	New
CIP	EE	5500	Probability and Stochastic Processes	3	Existing
CIP	EE	5231	Energy Control Center Applications	3	Existing
CIP	EE	5451	Risk Assessment for Critical Infrastructure Protection	3	New
CIP	EE	5455	Cybersecurity for Industrial Control Systems	3	Existing
NSM	SAT	5111	Security and Privacy	3	Existing
NSM	SAT	4812	Cyber Security II	3	Existing
NSM	SAT	5281	Healthcare Security Management	3	Existing
NSM	SAT	5816	Digital Forensics	3	New

Table 2c. Elective

CS	4711	Software Processes and Management	3	Existing
CS	5461	Mobile Networks	3	Existing
CS	5811	Advanced Artificial Intelligence	3	Existing
CS	5431	Advanced Computer Architecture	3	Existing
CS	5441	Distributed Systems	3	Existing
EE	5511	Information Theory	3	Existing
EE	5497	Multimedia Security	3	New
SAT	5211	Medical Application Development and Security	3	Existing
SAT	5231	Statistical Methods for Intrusion Detection	3	Existing
SAT	5241	Designing Security Systems	3	Existing
SAT	5251	Advanced Topics in Network Security	3	Existing

6. New course descriptions

CS 5000 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 5740 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 5497 Multimedia Security
Digital media security, data protection, and the analysis of digital media for purposes of authentication and protection against tampering and forgery. Electronic tamper detection. Secure exchange of digital content over the Internet or electronic media. Cryptographic processors. Topics include both software and hardware aspects of security.

EE5451 - Risk Assessment for Critical Infrastructure Protection
Fundamentals of risk assessment and vulnerabilities for industrial control environments including electrical power grids. Cyber-physical attack tools and techniques. Interaction of cybersecurity issues with physical systems and physical security. Limitations of current cybersecurity technologies. Design and cost considerations for a range of defensive postures and capabilities.

SAT 5816 Digital Forensics
This course introduces students to the basic principles and technology of digital forensics, including acquisition, preservation, and recovery and investigation of the evidence stored in digital devices. 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
- IEEE Transactions on Dependable and Secure Computing
- IEEE/ACM Transactions on Networking
- IEEE Security & Privacy Magazine
- IEEE Transactions on Information Theory

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/ME-EM
- Daniel Fuhrmann, Department of Electrical and Computer Engineering
- Guy Hembroff, School of Technology
- Shiyan Hu, Department of Electrical and Computer Engineering
- Robert Maatta, School of Technology
- 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
- Sumit Paudyal, Department of Electrical and Computer Engineering
- Michael Roggemann, Department of Electrical and Computer Engineering
- Timothy J. Schulz, Department of Electrical and Computer Engineering
- Ching-Kuang Shene, Department of Computer Science
- Min Song, Department of Computer Science
- Jinshan Tang, School of Technology
- 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

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/

All of the faculty listed above will support the program through the teaching of regular lecture courses. Some, but probably not all, will be available to support the program via research if they are research-active and are supervising Plan A (thesis option) or Plan B (report option) students.

Given below is a table of all the courses listed in the proposal and the most likely instructors.

Course	**Instructor**
CS 4471/5471 Computer Security	Jean Mayo
CS 4710 Model Driven Software Development	Nilufer Onder
CS 4711 Software Processes and Management	Charles Wallace
CS 5472 Advanced Topics in Computer Security	Spiros Bakiras
CS 5321 Advanced Algorithms	Ali Ebnenasir
CS 5431 Advanced Computer Architecture	Soner Onder
CS 5441 Distributed Systems	Zhenlin Wang
CS 5461 Mobile Networks	Min Song
CS 5740 Development of Trusted Software	Jean Mayo

CS 5000 National Cybersecurity Policy and Law	New hire or Adjunct
MA 3203 Cryptography	Vladimir D. Tonchev
EE 5500 Probability and Stochastic Processes	Michael Roggemann
EE 5511 Information Theory	Timothy J. Schulz
EE 5231 Energy Control Center Applications	Sumit Paudyal
EE 5451 Risk Assessment for Critical Infrastructure Protection	Chee-Wooi Ten
EE 5455 Cybersecurity for Industrial Control Systems	Steven Goldsmith
EE 5497 Multimedia Security	Saeid Nooshabadi
SAT 4812 Cybersecurity II	Xinli Wang
SAT 5111 Security and Policy	Yu Cai
SAT 5211 Medical Application Development and Security	Robert Maatta
SAT 5231 Statistical Methods for Intrusion Detection	Xinli Wang
SAT 5241 Designing Security Systems	Yu Cai
SAT 5251 Advanced Topics in Network Security	Jinshan Tang
SAT 5281 Healthcare Security Management	Chunming Gao
SAT 5816 Digital Forensics	Xinli Wang

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

The external advisory committee will provide feedback on program quality and relevance to current needs in industry. Members of the external advisory committee will serve as external reviewers for our eventual program review, now being put in place for all Michigan Tech graduate programs following the latest mid-cycle accreditation review by the Higher Learning Commission.

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.

Flowcharts for Proposal 24-16