Title Page

Program Title: Master of Science in Cybersecurity

Program Degree: Master of Science in Cybersecurity

Requested Program Implementation Term: 2016

School or College Governance

Department of Computer Science and Engineering
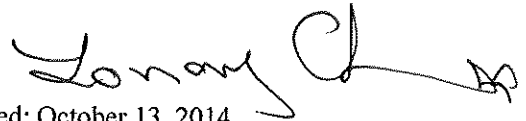
Date Submitted: December 16, 2013 Date Approved: January 17, 2014

Graduate Committee on Instruction

Date Submitted: January 20, 2014   Date Approved: January 21, 2014
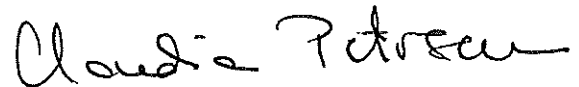
Dean School or College

Date Submitted: January 24, 2014   Date Approved: October 13, 2014

University Governance

Graduate Council

Date Submitted: October 13, 2014   Date Approved: November 04, 2015

Senate

Date Submitted Date Approved

Board of Trustees

Date Submitted Date Approved

Presidents Council

Date Submitted Date Approved

Oakland University

Graduate Council

One Page Abstract

Oakland University (OU) proposes a new program in cybersecurity at the master's level. This program would offer two paths, professional track and research track, aimed toward potential students with career aspirations in industry or academia. The Master of Science in Cybersecurity (MSC) degree will be offered in the Department of Computer Science and Engineering (CSE) within the School of Engineering and Computer Science (SECS), in collaboration with the Department of Decision and Information Sciences (DIS) within the School of Business Administration (SBA).

The MSC is designed to provide *a strong foundation and detailed technical knowledge in information security, computer security, network security, software security as well as an appreciation of the social, policy, ethical and legal aspects of security and privacy.* The program will require 16 semester hours of foundation and core courses, 16 semester hours of depth course work, which optionally includes a master's thesis, for a total of 32 semester hours.

Core courses in computer network security, host computer security, and information security provide the theoretical basis for understanding the source of vulnerabilities in computation and information systems while exposing students to state-of-the-art tools and techniques for identifying threats related to networking infrastructure, computer systems and the data and information flowing through the system. With this broad theoretical foundation, students can select courses from domain areas that provide both depth and breadth of coverage across a wide variety of topics in cybersecurity. The curriculum for the MSC program blends contemporary knowledge with advanced research concepts to deliver a cutting edge program.

The overall goal of the MSC program is to provide students with the background knowledge in theory and practice to understand current cybersecurity threats, but more importantly to be able to understand, adapt, and develop new techniques to confront emerging threats. The research component of the MSC embodied in the culminating thesis requires students to expand their beyond state-of-the-art technique by exploring new and creative approaches to address emerging threats.

According to the Bureau of Labor Statistics (BLS), employment of computer and information systems managers and administrators is projected to jump between 2008 and 2018. The number of computer and information systems managers is slated to increase 17%, while the amount of computer network, systems and database administrators is expected to skyrocket 30%. These workers help companies adopt new technologies, boosting corporate competitiveness and protection against cyber attacks. The Department of Homeland Security (DHS), meanwhile, is hiring 1,000 cyber experts in three years to protect the nation's cyber infrastructure. The Department of Defense is reportedly adding 50,000 security experts in coming years. Other government studies have indicated the need for at least 1,000 new cybersecurity graduates per year for the foreseeable future. Cybersecurity positions are growing rapidly in the banking sector as well.

Employment opportunities will continue to be available in both public and private sectors in areas of cyber risk and strategic analysis, vulnerability detection and assessment, cyber incident response, intelligence and investigation, networking and systems engineering. The proposed program would meet an under-served and growing need in industry, government and academia.

Oakland University

Graduate Council

Oakland University

Graduate Council

The Proposal

I. Rationale

Program need

Cybersecurity is a fast-growing field currently creating new jobs over the next decade as both government and industry plan significant investments to protect data and information systems. Norton's annual Cybercrime report says that an estimated 71 million people in the United States became cybercrime victims and the cybercrime has cost $110 billion in 2011. The problem is so severe that President Obama has declared that "the cyber threat is one of the most serious economic and national security challenges we face as a nation." The White House has stated that as many as 30,000 new cybersecurity professionals are needed in the coming years by the United States government alone. To address this growing need, many universities and industry organizations are considering establishing specialized graduate or training programs in the area of cybersecurity. For example, University of Maryland- Baltimore County has been offering a Master of Science in Cybersecurity since 2009. The growing number of cybersecurity related conferences, journals and trade shows that cybersecurity is a high-growth field experiencing a demand far greater than the supply of trained professionals available.

The consideration of a master's program in cybersecurity at Oakland University began in Fall 2012 during contacts with local industry leaders and faculty in other departments. Several companies and government agencies including, Merit Inc. and the State of Michigan (see also: Appendix H), have showed considerable interest in our offering a M.S. degree in cybersecurity. Upon learning about our plans for a master in cybersecurity, many of our students have been inquiring about the program and its start date. It, thus, appears that an M.S. in cybersecurity is certain to attract sufficient enrollment to justify its existence.

How the program relates to the institution's role and mission

The role and mission of the university identifies four essential ingredients: excellent and relevant instruction; high-quality basic and applied research and scholarship; responsive and effective public and community service; and a comprehensive schedule of student development activities.

The proposed M.S. program in cybersecurity is consistent with the role and mission of the university. It will provide excellent instruction in a focused discipline and help further develop applied research, scholarship, and practice. It is being proposed in response to the needs of local industry and as a community service to the state and nation.

Goals and objectives

The goal of this program is to prepare students who seek both a strong foundation and detailed technical knowledge in security, privacy, and cryptography applied to information systems, networks, and software as well as an appreciation of the social, policy, ethical and legal aspects of security and privacy. The program will strive to seek a balance between the theoretical and deep technical skills of cybersecurity. The program will be suitable for students who have received a

Oakland University

Graduate Council

baccalaureate degree in computer science or engineering and have a desire to join the cybersecurity research and workforce. The program will prepare our graduates to face the futuristic security related challenges emerging from our internet connected world, the rapid adoption of mobile devices, and the ever increasing role of software applications in our daily life.

The additional goals of the program are: (i) increase the enrollment; (ii) create more visibility for the department and the university by being a leader; (iii) improve the level of research and funding; and (iv) stimulate additional interaction with local industry.

Comparison with other programs

Cybersecurity is an emerging interdisciplinary area, which emphasizes the **techniques** *for providing the security and trustworthiness for the infrastructure and information of the cyberspace, and meanwhile it appreciates the ethical, legal, and social aspects of the cyber-enabled society. Information assurance is a more traditional area, which focuses on the* **management**, *policy-making, and administration aspects for protecting digital and non-digital information assets. The comparison made here between cybersecurity and information assurance is based on the following documents provided by Executive Office of the President and President's Council of Advisors on Science and Technology:*

- *"Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,"* May 2009.
- *"Trustworthy Cyberspace: Strategic Plan For The Federal Cybersecurity Research and Development Program,"* December 2011.
- *"Immediate Opportunities for Strengthening the Nation's Cybersecurity,"* November 2013.

Currently, there are more than three dozen programs in the country that offer a master's degree in cybersecurity or information assurance. Some of the prominent programs are at Carnegie Mellon University, George Mason University, Georgia Institute of Technology, Johns Hopkins University, University of Southern California, Boston University, University of Minnesota, George Washington University, University of Miami, Northeastern University, University at Buffalo, University of Washington and Polytechnic Institute of New York University.

However, programs in Michigan are offered at the University of Detroit Mercy, Eastern Michigan University and Davenport University. Davenport University offers the 37-semester credit hour Master of Science in Information Assurance (MSIA) focusing on Information Assurance and Computer Security, whereas the University of Detroit Mercy offers a program leading to the bachelor's and master's degrees over a five year (10 semester) period focusing on Information Assurance or Criminal Justice. The Information Assurance master's program in Eastern Michigan University offers three areas of concentration: Information Assurance Management, Network Security and Digital Investigations. All of them are in the area of information assurance.

Different from these programs offered in Michigan, our program will be in the area of cybersecurity. Our program will prepare students who seek not only a strong foundation and detailed technical knowledge in information security, computer security, network security, software security but also an appreciation of the social, policy, ethical and legal aspects of security and privacy. Further, our program can attract engineers and computer scientists working in local industry as well as graduating students, domestic and international, who will find our

Oakland University

Graduate Council

cybersecurity program attractive from future job prospects and career growth. Thus, our program is expected to serve the local and regional needs.

Oakland University
Graduate Council

II. Academic Unit – Current Status

How the goals of the unit are served by the program

The MS in Cybersecurity will:

- Produce competent graduates to meet the current and futuristic global and national cybersecurity challenges. These graduates will significantly improve the reputation of Oakland University by exemplifying their technical skills, leadership and professionalism.

- Develop an innovative program that is marketable to governmental and private industry agencies. Financial, health and defense related organizations are in dire need of skillful graduates.

- Attract qualified faculty with a cyber-security specialty.

- Increase enrollment to graduate students with career goals in cybersecurity.

- Meet industry staffing needs.

This program will require experienced faculty with expertise in information and network security. These faculty members require experience in teaching, evaluating student learning, helping them to research and grading. Current faculty with cybersecurity backgrounds will direct and facilitate development.

The faculty qualifications

The Department of Computer Science and Engineering currently employs several experienced academic professionals who could teach, evaluate student learning, and monitor student progression, as well as direct and facilitate courses and websites for courses. The qualified Department of Computer Science and Engineering faculty include Dr. Ishwar Sethi, Dr. Lunjin Lu, Dr. Dae-Kyoo Kim, Dr. Gautam Singh, Dr. Khalid Mahmood, Dr. Guangzhi Qu, Dr. Tao Shu, Dr. Nilesh Patel, Dr. Huirong Fu, Dr. Debatosh Debnath, Dr. Hua Ming, Dr.Yonghong Yan, and Dr. Wenjin Zhou.

The CSE department has a strong security faculty team whose research expertise spans a range of key subareas in cybersecurity, including network security, software security, wireless security, and data security and privacy, as elaborated below.

Dr. Huirong Fu: Dr. Fu has extensive research experience in information assurance, applied cryptography, trust management, and network security. She is an established cybersecurity researcher. She has been the PI or Co-PI for six NSF grants (total over $1.2 M), among them four are directly related to cybersecurity; She has published over 100 peer-reviewed journal and conference papers on network security, privacy, and trust management. She has developed four security-related courses at CSE department of OU, including CIT 448 (Information Security

Oakland University

Graduate Council

Practice), CSE 681 (Information Security), CIT 346 (System Administration and Security), and CSCI 790 (Advanced Topics on Network Security).

Dr. Lunjin Lu: Dr. Lu has a strong background on software verification, program analysis for software safety and reliability, and the diagnosis and detection of bugs in programs. He is a recipient of the prestigious NSF CAREER Award. He has been the PI for two NSF grants. He has published over 50 peer-reviewed papers on programming analytics and verification in top conference venues such as ICLP, ICECCS, ESOP, ICCL, and EDOC. He has supervised more than a dozen student projects on static program analysis and its application to verification of safety properties. He has also taught many times a graduate level course: CSE 535 – Programming languages and Compilers, which covers static program analysis extensively including inference of sufficient safety pre-conditions using backward analysis.

Dr. Dae-Kyoo Kim: Dr. Kim has a strong background on software access control systems. He has been the PI of one NSF grant on software security. He has published over 60 peer-reviewed journal/conference papers and book chapters on topics such as access control modeling, configuration, visualization, and privacy protection. He has supervised or is supervising 5 Ph.D. students, some of them are working on software security. Dr. Kim has extensive experience in teaching software security courses, including CSE 520 (Fundamentals of Software Modeling), CSE 530 (Software Prototyping and Validation), and CSE 538 (Software Verification and Testing).

Dr. Tao Shu: Dr. Shu has strong record in wireless security and privacy. He has published over 50 referred papers on wireless networking, security, and privacy in top journals and conferences. He is the PI of two current NSF grants and the Co-PI of one current NSF grant on secure and trustworthy cyber space. He is supervising two Ph.D. students, one of whom is working on security of participatory sensing. Dr. Shu has been teaching courses related to network security in the CSE department since Fall 2011, including CSE/CIT 247 (Introduction to Networks), CIT 448 (Information Security Practice), and CSE 549 (Wireless and Industrial Networks).

Dr. Wenjin Zhou: Dr. Zhou has a solid background on data science and multi-modality application-driven visualization. Her research develops efficient computational solutions for extraction of hidden information and physical properties in multi-modality data, explores powerful visualization tools for combining multi-dimensional information obtained from various modalities, and then designs efficient interactive user interfaces for understanding and exploring scientific data at multiple scales. She has successfully applied these techniques to biomedical and brain-related problems, and has published over 20 peer-reviewed papers in top conference and journal venues. Dr. Zhou is applying these multi-modality visualization techniques to network security and data security problems, by following a data-driven applied security visualization framework. This framework transforms log data into meaningful security information, so as to facilitate fast and efficient diagnosis, identification, and understanding of attacks, vulnerabilities, and risks, and then direct accurate removal of the threats.

Dr. Hua Ming: Dr. Ming's research and development experience mainly focuses on software engineering and programming languages. He has been involved in US Census Bureau/NSF funded projects to develop software applications to support Geo-spatial field data collection,

Graduate Council

through a tablet device where security and accuracy of data collection is of top priority. His efforts to apply data flow analysis techniques to functional programming language design and implementation led to enhanced assurance and protection over program data. More recently, he aims to resolve "vulnerable situation" problems arose from his research in developing context-oriented, situation aware systems. He has published more than 20 articles appeared as book chapters, journal papers as well as peer-reviewed conference papers.

Dr. Khalid Mahmood: Dr. Mahmood's research interests include integrated area of computer networks and semantic web. To cater futuristic security needs arising due to realization of IoT and smart cities, he is studying how Semantic Web Technology can be used to create ontologies that is capable of reasoning about security attributes and by using such ontologies based reasoning to design systems to prevent data breaches. Dr. Mahmood has the experience of teaching various network security courses at Oakland University, such as CSE/CIT 247 (Introduction to Networks) and CIT 448 (Information Security Practice).

Classroom, laboratory and/or studio space

Enrollment in the core and foundation classes will be combined into the current Computer Science graduate courses. The master in cybersecurity students will register in the classes that currently exist. The specialty classes will require some classroom, laboratory and/or studio space. See Section IV for details.

Equipment

The program may require additional equipment. The program will also utilize the online capabilities currently available for the Department of Computer Science and Engineering. See Section IV for details.

The CSE department has already established sufficient hardware and software capacity to support this program, therefore no budget is required for these items. In particular, the department has a newly-equipped, state-of-the-art, over 700 sqft Networking and Security Lab (EC554) located in the Oakland University's New Engineering Center, opened in September 2014. This spacious lab features a 16-bench setup, and can support up to 16 groups of students to do cybersecurity labs at the same time. The information technology infrastructure in this lab is fully equipped with a range of network components, including firewalls, Intrusion Detection System (IDS), routers, switches, DNS servers, ftp servers, workstations, and a portable education network (PEN, also known as Mobile Lab). Wireless and mobile networks are supported by this infrastructure through wireless routers and the PEN module. The entire infrastructure is designed to be isolatable from the Internet, and can be decomposed into three distinct policy domains: attack, target, and administrative, constituting an ideal stand-alone experimental cyberspace to allow students to experiment a full range of cyber attacks and defenses.

The Networking and Security Lab is also equipped with a full range of security software, as listed in the following table. These software are either freeware (doesn't need a license to run) or dependent on site licenses that are provided by the School of Engineering and Computer Science.

Oakland University

Graduate Council

These software have been extensively used in teaching various courses, such as CIT 448 and CSE/CIT 247.

List of Software	License
Microsoft Windows 10	License available
VMware Player 5.1	Free
Sam Spade version 1.14	Free
Advanced Port Scanner 1.3 For Windows	Free
NMap 6.00	Free
Microsoft Windows Defender	Free
Microsoft Baseline Security Analyzer	Free
Nessus 5.0.1 for Microsoft Windows	Free
Metasploit framework v4.3	License available
Windows XP installed	License available
Microsoft Security Compliance Manager	License available
NET Framework 4	License available
Microsoft Windows 2008 Server Standard Edition SP2	License available
Internet Explorer 9	License available
SyncToy version 2.1	Free
TrueCrypt version 7.1a	Free
MD5summer version 1.2.0.5	Free
FileVerifier++ version 0.6.3.5	Free
Internet Explorer	license available
Firefox version 17	Free
CCleaner version 3.24	free
Clean Disk Security version 8.1	Free
DBAN	Free
ZoneAlarm Free Firewall 2012	Free
Linksys firewall router hardware (WRT54G or similar)	Available
Linksys wireless access point (WAP) (WAP54G or similar)	Available
Microsoft Windows with IIS configured as a Web server	Available
libpcap-devel	Free
Snort version 2.9.4	Free
Snort ruleset	Free
Security Onion, a Linux distro customized	Free
WinPcap version 4.1.2	Free
Windows TCP Dump	Free

Oakland University

Graduate Council

Wireshark for Windows 1.8 or later	Free
Windows 2008 VPN Server	Available
Microsoft Windows 2008 Server R2 configured as a certificate authority (CA)	Available
PWDump7	Free
ClamWin Free version 0.97.5 or later	Free
AVG Free Antivirus 2013 or later	Free
Spybot – Search and Destroy	Free
Malwarebytes	Free
Adblock Plus	Free

Oakland University
Graduate Council

Current Resources and Impact of Increased Enrollment

Currently the Department of computer science has 1 full professor, 8 associate professors, 4 assistant professors, 3 special instructors, and 2 visiting professors to support the Master in Cyber Security program.

Enrollment in the School of Computer Science and Engineering undergraduate and graduate programs is expanding. Here is the summary of enrollment of master students (2011-2013).

Table I: Graduate Enrollment Data (CSE Department)

Semester	Discipline	Enrolled Students	Total Enrolled Graduate Students
Fall 2013	Computer Science	40	50
Fall 2013	Information Technology	10	
Summer 2013	Computer Science	15	21
Summer 2013	Information Technology	6	
Winter 2013	Computer Science	28	41
Winter 2013	Information Technology	13	
Fall 2012	Computer Science	25	39
Fall 2012	Information Technology	14	
Summer 2012	Computer Science	8	13
Summer 2012	Information Technology	5	
Winter 2012	Computer Science	12	24
Winter 2012	Information Technology	12	
Fall 2011	Computer Science	15	25
Fall 2011	Information Technology	10	
Summer 2011	Computer Science	3	7
Summer 2011	Information Technology	4	
Winter 2011	Computer Science	12	22
Winter 2011	Information Technology	10	

Oakland University
Graduate Council

III.   Program Plan

a. Admission Requirements

Prior to admission into the program, candidates must hold a bachelor's degree in computer science, computer engineering, electrical engineering, information systems, mathematics or a related technical area from an accredited academic institution, with an overall minimum grade point average of at least 3.0. Students may be admitted conditionally if they have an undergraduate grade point average of 2.7 or above and at least a 3.0 grade point average in technical courses related to cybersecurity.

Students are expected to have background knowledge of mathematics including calculus, linear or matrix algebra, discrete mathematics, probability and statistics. In addition, applicants are expected to have knowledge of programming, data structures, algorithms, computer networks, machine organization and operating systems. Student lacking background knowledge may be required to complete the missing course work prior to admission into the program, or they could be admitted conditionally contingent on the completion of prerequisite courses offered at OU. For example, an applicant from disciplines other than computer science can be admitted if he/she has completed the prerequisites of the three foundation courses and satisfactory grades were achieved for these prerequisites. Specifically, the prerequisites of CSE 551, CSE 647, and CSE 545 are CSE 252/CSE 445, CSE 247, and CSE 345, or equivalent, respectively. If the applicant is missing any of these prerequisites, he/she may be admitted under the condition that he/she must take the missing prerequisite(s) after being enrolled in the program.

Admissions offered on a rolling basis. Applicants should apply and complete application requirements as early as possible to guarantee consideration for the coming semester. Applicants should include a cover letter, a resume or CV, and transcripts of all academic work completed at the baccalaureate/undergraduate level and beyond, whether or not for credit or a degree. Applicants must also submit other materials, which may be required by Graduate Study.

The Admissions Committee requires two letters of recommendation, preferably from supervisors in a workplace setting or from professors in an academic setting. The Test of English as a Foreign Language (TOEFL), or International English Language Testing System (IELTS), is required for non-native English speakers.

b. Degree Requirements

The program will require 16 semester hours of foundation and core courses and 16 semester hours of depth/elective course work for a total of 32 semester hours. Professional track students are required to take at least 3 depth courses. Research track students are required to take Master's Thesis Research plus at least 2 depth courses.

Oakland University

Graduate Council

For course listing, see Appendix B.

Oakland University

Graduate Council

c. Curriculum Overview

See Appendix C and Appendix D.

d. Academic Progress, Probation and Dismissal

To stay in good academic standing, students must not allow their cumulative grade point averages (GPA) to drop below 3.0. The program follows the official Academic Policies and Procedures. (See university website for details.)

Inactive student status: At Oakland University, a matriculated graduate student is a student who has been previously admitted to and has enrolled in a graduate program. Graduate Study and Lifelong Learning classifies inactive, matriculated students into two categories: one category permits readmission to a graduate program, and the other category requires reapplication before an inactive student can re-enroll in a course. The periods of inactivity used to classify inactive students into the appropriate category are defined as follows:

Readmission: Students who have not enrolled for six or more consecutive semesters are permitted to submit a Request for Graduate Readmission form. Each request is evaluated in terms of the time limit established for completing degree requirements, performance in previous coursework, and progress made toward the degree. Students will not be readmitted to programs that have been suspended or discontinued. The catalog current at the time a student is readmitted will govern program requirements, policies and procedures.

Reapplication: Students who have not enrolled for seven consecutive years are considered inactive and their graduate student files are destroyed. These students are considered new applicants and must submit a new Application for Admission to Graduate Study and new supporting documents as specified in both the General Admission Requirements and the Program Admission Requirements.

e. Academic Direction and Oversight for the Program

The department chair will be responsible for the success of this program.

f. Interdisciplinary Programs

Academic home: The Master of Science in Cyber Security program will be administered in the Department of Computer Science and Engineering. A program committee will be designated to oversee the degree program. The role of the program committee is to administer program policies, curricula changes and petition approvals. The Chair of the Department of Computer Science and Engineering will determine the members of the program committee and select a program director.

Other participating academic units: Department of Decision and Information Sciences, School of

Oakland University

Graduate Council
Business Administration.

Statements of support: See Appendix H.

g. Accreditation

Not applicable.

h. Program Description

The Master of Science in Cybersecurity prepares practitioners with knowledge, skills, and leadership in combating today's cyber threats and protecting the cyber infrastructure of his/her institution. The program focuses on prevention, detection, countering, and recovery from cyber attacks from both technical and legal perspectives. Students learn about state-of-the-art technical tools and practices in safeguarding the security and privacy of information, data, software, and communication infrastructure, and obtain hands-on experience on these technologies through directed exercise and experiments in a security teaching lab. Students also study the legal weapons for protecting their intellectual property and cyber assets.

At the completion of the program, students acquire systematic knowledge on cybersecurity and privacy, establish necessary skill set in maintaining and managing the security of the cyber infrastructure of an organization, and create leadership in safeguarding today and tomorrow's cyber infrastructure from both technical and legal senses. A student is required to obtain at least 32 credits in order to successfully complete the program.

Graduates of the Master of Science in Cybersecurity program attain the following:

1. Explore leadership, theory, tools, skills, and practices as it applies to safeguarding the security and privacy of today and tomorrow's cyber infrastructure.
2. Understand fundamentals and state of the art of today's cyber technology.
3. Understand fundamentals and advanced issues of various threats faced by today's cyber infrastructure.
4. Understand cybersecurity and privacy needs of today's institution.
5. Acquire solid knowledge on applied cryptography, which serves as the basis for the development of mainstream cybersecurity models and methods
6. Acquire knowledge on information technology, software systems, and network systems, which serves as the basis for the development of many emerging non-cryptographic methods for protecting security and privacy.
7. Study commonly-used cybersecurity tools and acquire hands-on experience through directed exercise and experiments.
8. Understand intellectual property law and cyber law.
9. Describe the synthesis of data and information for risk (vulnerability) assessment for the cyber infrastructure.
10. Integrate evidence-based practice into system reviews to design, implement, and evaluate plans of security.

Oakland University

Graduate Council

11. Design, coordinate, evaluate, and deliver cybersecurity solutions in a timely and cost-effective manner.
12. Strategically plan on integrating cybersecurity within the overall improvement of the cyber infrastructure of the institution.
13. Provide cybersecurity-related recommendation to higher-level system administrator in key decision-making process
14. Understand the role, scope, and limitations of cybersecurity administrators, while incorporating professional standards into practice.
15. Explore the evolving role of cybersecurity administrator in an institution.
16. Analyze vertical and horizontal leadership strategies of cybersecurity administrator in an institution.
17. Apply appropriate teaching/learning strategies to facilitate learning and education of colleagues on cybersecurity.
18. Develop personal goals for professional development and continuing education.
19. Demonstrate skills of mentoring the next generation of cybersecurity professionals.
20. Integrate relevant research findings into cybersecurity practice.

The Master of Science in Cybersecurity will:

1. Prepare cybersecurity professionals who are competent to meet the cybersecurity and privacy needs of today's industry and institution.
2. Prepare cybersecurity professionals who can make significant contribution to the overall improvement of the cyber infrastructure of his organization.
3. Prepare cybersecurity professionals who will exemplify professionalism in their practice.
4. Prepare cybersecurity professionals who will demonstrate excellence in leadership.
5. Prepare cybersecurity professionals to mentor peers, students, and staff members, and to contribute to the general education of cybersecurity to the public population.

Relationship with major certifications:

Many employers demand quantifiable and verifiable proof of the expertise in form of certifications from employees. Keeping in view of this, the course contents of the proposed study plan are aligned with the various certificates in cyber security, including Secure Software Programmer (GIAC), Certified Secure Software Life Cycle Professional (CSSLP), Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), Securing Cisco Networks with Threat Detection and Analysis (SCYBER), Certified Information Systems Security Professional (CISSP), Comptia Security+, Certified Authorization Professional (CAP), Systems Security Certified Practitioner (SSCP).

To prepare the graduate students to take certification exams, we will ensure that course contents of offered courses will be aligned with certification topics. Table II shows the relationship between the proposed courses and various certificates.

Oakland University
Graduate Council

Table II: Relationship between Courses and Certificates

Course	Title	Credits	Certificates
CSE_	Software Security	4	GIAC, CSSLP
CSE 681	Information Security	4	SSCP, CISM
CSE_	Network Security	4	SSCP, CISSP, CEH, SCYBER
MIS 641	IS Privacy	3	
CIT 548	Information Security Practice	4	CISSP, Comptia Security+, SSCP
CSE_	Cyber law, Forensics and e-Discovery	4	CCFP
CSE_	Non Cryptographic Methods for Network Security and Privacy	4	CEH, Comptia Security+
MIS 680	ST: IT Governance, Business Continuity and Risk Management	3	CAP

i. Source of Students

- Graduates of the CS and IT undergraduate programs of the CSE department
- Graduates of other OU undergraduate programs (e.g., math and MIS) who have an interest in cybersecurity
- Graduates of other higher education institutions in Michigan and around the country
- Mid-career IT professionals in government agencies, businesses, hospitals, and non-profit organizations
- General public who are interested in cybersecurity and satisfy the admission requirement of the program

To get an idea of how many students would be interested in this program, we made two types of surveys, in-class survey and on-line survey, whose results are summarized in the following tables.

For in-class surveys, we sampled classes CIT448, CSE/CIT 247, and CSE/CIT337. We asked the students who are attending these classes to respond to the question of "Will you be interested in attending this program after your undergraduate program." Among the 56 responses received, 32 showed strong interest in the program. To sample the interested student body in a larger range, we have also conducted an online survey, in which a link to a SurveyMonkey page was sent to the students of the entire CSE department. 86 responses were received, among which 76 have expressed interests.
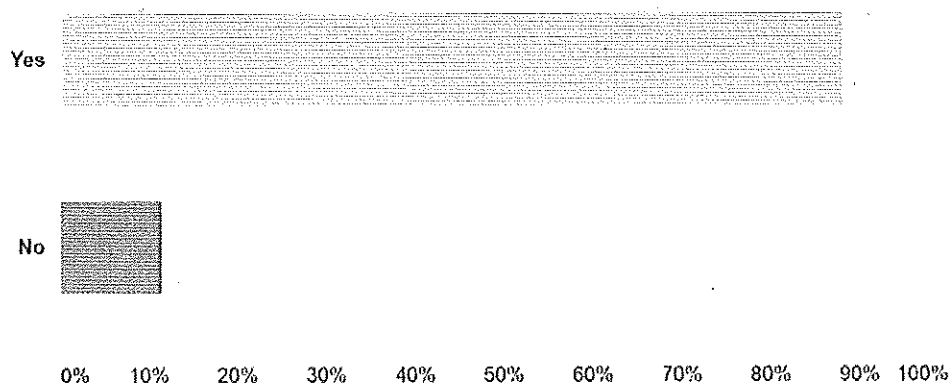
Oakland University

Graduate Council

Table III: Result of in-class survey

Course name	Total participants	Interested students	Percentage
CIT448	18	10	55.5%
CSE/CIT 247	27	17	62.9%
CSE/CIT 337	38	22	57.8%
Total	79	49	62%

Table IV: Result of on-line survey

Answered: 86   Skipped: 0

Answer Choices	Responses	
Yes	88.37%	76
No	11.63%	10
Total		86

j. Recruitment Plan

- Open House
- Radio
- Flyers
- Affiliating agencies
- Mailings

Graduate Council

- Newspapers and journal advertisement
- SECS and CSE web pages
- SBA and MIS web pages

The School of Engineering and Computer Science (SECS) has multiple recruitment sessions for SECS programs. SECS has great success with Recruitment Open Houses where faculty are available to talk to students about various programs. SECS also has information sessions where students can come and ask questions about specific programs. On a daily basis faculty advisors are also available to answer students' question regarding specific programs by setting up appointments.

k. Planned Program Enrollment

Year 1	Year 2	Year 3	Year 4	Year 5
20	35	35	35	35

l. Advising students

Students will be assigned to a faculty mentor upon admission into the program. SECS Graduate advisor will monitor Plan of Study and scheduling.

m. Retention Plan

Student retention is critical to ensure self-sustainability and high quality of the program. The program will strive to retain a high quality student enrollment by implementing the following retention plan:

- Set up mentoring for new students to ensure they have clearing understanding about the curriculum and milestones/requirements for the successful completion of the program.

- Early identification of students who are performing poorly in the program and make sure appropriate support is presented to these students.

- Ensure sufficient academic advisory to students by coordinating efforts of both the faculty and the academic advisors

- Hosting regular cybersecurity seminars: bring experts to campus to update students the state of the art in the area

- Encourage students to attend professional societies such as IEEE and ACM, and participate in activities held by student-organized study groups such as CyberOU.

- Provide professional development opportunities and internships for students who are close to their graduation.

- Help potential employers who may be interested in the graduates of the program to know our program and graduates better by holding cybersecurity job fairs and workshops

- Help graduates to market themselves in their job placement by hosting their resume and homepage on the department's website

- Regularly invite program alumni to give presentation to current students, aiming at enhancing their connection with program alumni.

n. Provide list of businesses that would likely employ graduates of the program

The MS in Cybersecurity can take the responsibility in developing, improving, managing, and administering the security/privacy aspects of the IT infrastructure in his/her institute. Such a capability is needed, sometimes required, by almost every employer. We list the categories of potential employers below according to their nature. We also give a few representative examples under each category.

- Educational Institutions: All universities, high schools, middle schools, and elementary schools
- Government Agencies: State of Michigan, NSA, DoE, DoT, and all other agencies at the county, state, and federal levels
- Military: DoD, Army, Navy, Air Force, and military contractors
- Financial Institutions/Banks and Insurance: Chase, Citi, Bank of America, all local banks in Michigan
- Hospitals and healthcare: William Beaumont Hospital, Crittenton Hospital, St. Joseph Mercy Hospital, blue cross blue shield
- IT companies: Google, Apple, Microsoft, Amazon, Ebay, Facebook, Symantec
- All sectors of the Industry: GM, Chrysler, Ford, DTE, Comcast
- Chain Stores: Walmart, Sam's Club, Target, Sears, Costco

Oakland University

Graduate Council

IV. Needs and Costs of the Program

a. Summary of needs and costs

See also: Proforma Budget (Appendix E).

1) Faculty positions: Two new full time faculty
2) Staff positions: 25% advisor needed
3) Library Holdings: see library report
4) Graduate assistants: one projected
5) Space: none projected
6) Equipment: none projected
7) Supplies, services, travel and telephone: travel to security conference, offices supplies, and supplies for program marketing.

b. How the cost of the program will be met by graduate tuition revenue

The cost of the program initially will be covered by increase in tuition revenue. See Appendix E.

c. Other support that this program will give to the university

The university will benefit from this program in several ways, besides tuition revenue.

1) Grants: increased potential for grants from NSF
2) Tuition: increase tuition revenue from MSC students
3) Public service: This proposal will update CSE graduate programs to meet the demand for highly qualified security leaders. The MSC program will also support Homeland Security and other governmental agencies in the obtainment of qualified leaders to decrease cost and improve cybersecurity infrastructure.

V. Program Assessment Plan

The Department of Computer Science and Engineering already offers two master's degree programs. The new program would utilize the same assessment procedures. See Appendix G.

Oakland University
Graduate Council

VI. Appendices

A   Abbreviated Faculty Vitae
B   Degree Requirements
C   Typical Student Plan of Study – Full-Time Schedule
D   Detailed New Course Descriptions or Syllabi
E   Proforma Budget
F   Additional Personnel Support Descriptions
G   Graduate Assessment Plan
H   Support Letters
I   Timeline

Oakland University

Graduate Council

Abbreviated Faculty Vitae

Dr. Lunjin Lu
Dr. Ishwar Sethi
Dr. Huirong Fu
Dr. Dae-Kyoo Kim
Dr. Gautam Singh
Dr. Khalid Mahmood
Dr. Guangzhi Qu
Dr. Tao Shu
Dr. Nilesh Patel
Dr. Debatosh Debnath
Dr. Tom Lauer
Dr. Mohan Tanniru
Dr. Hua Ming
Dr. Yonghong Yan
Dr. Wenjin Zhou

Oakland University

Graduate Council

Faculty Name: Lunjin Lu Title: Associate Professor and Acting Chair School: Engineering and Computer Science	Office: EC 546	Office Phone: 2231 Office Email: L2LU
Degrees – School – Year Ph.D., University of Birmingham (UK), 1995 M.Eng., East China Normal University, 1985 B.Eng., Jiangsu University, 1982	Research Interest: Static program analysis, Software verification, Software testing, logic programming	

Grants Awarded:

Title: CAREER: An Integrated Framework for Semantic Based Analysis of Logic Programs *Source:* National Science Foundation CISE Career Program
Amount: $300,000

Title: Backward Analysis of Logic Programs
Source: National Science Foundation INT Program
Amount: $40,000

Title: Static Analysis for Verification Of Safety Properties of Critical Software
Source: Michigan Space Grant Consortium MSGC Research Seed Grant Program
Amount: $5,000

Most Recent Publications (limit to 6):

1. **Lunjin Lu** and Dae-Kyoo Kim, Required Behavior of Sequence Diagrams: Semantics and Conformance, ACM Transactions on Software Engineering and Methodology, Accepted. [29 pages]
2. **Lunjin Lu,** A Polymorphic Type Dependency Analysis for Logic Programs, New Generation Computing, 29 (4) 409—444. 2011. **[36 pages]**
3. Dae-Kyoo Kim, Sangsig Kim, **Lunjin Lu,** Suntae Kim, and Sooyong Park, A Feature-Based Approach for Modeling Role-Based Access Control Systems, Journal of Systems and Software 84(12): 2035-2052, 2011. **[18 pages]**
4. **Lunjin Lu,** Dae-Kyoo Kim, Yuanlin Zhu and Sangsig Kim, Verification of Structural Pattern Conformance Using Logic Programming, Journal of Universal Computer Science, 16(17): 2455--2474, 2010.
5. Suntae Kim, Dae-Kyoo Kim, **Lunjin Lu,** Sooyong Park: Quality-driven architecture development using architectural tactics. Journal of Systems and Software 82(8): 1211-1231, 2009.
6. **Lunjin Lu,** Improving Precision of Type Analysis Using Non-Discriminative Union, Theory and Practice of Logic Programming, 8(1): 33--79. Cambridge Press, 2008. [47 pages]

Graduate Courses Taught (relevant to new degree CSE 535: Programming Languages and Compilers CSE 561: Advanced Data Structures and Algorithms CSE 595: Multicore Programming	Prospective Graduate Courses (relevant to new degree) CSE 5xy: Software Security

Oakland University

Graduate Council

Faculty Name Ishwar K Sethi Title Professor School Engineering & Computer Science	Office EC 522	Office Phone 2820 Office Email isethi
Degrees – School – Year BS IIT, Kharagpur, India 1969 MS ---do--------------------- 1971 Ph.D. ---- do----------------- 1978	Research Interest Data Mining, Machine Learning, Pattern Recognition, Multimedia Information Processing	

Grants Awarded
None recently

Most Recent Publications (limit to 6)
Ching-she Wu, Wei-chun Chang and **Ishwar K Sethi**, "A Metric-Based Multi-Agent System for Software Project Management," 8th *IEEE/ACIS International Conference on Computer and Information Science (ICIS)*, pp. 3-8, Shanghai, China, June 2009 Jie Ouyang, Nilesh Patel and **Ishwar K Sethi**, "Chi-Square Test Based Decision Trees Induction in Distributed Environments," *Proceedings IEEE International Conference on Data Mining Workshops*, pp. 477-485, Pisa, Italy, December 2008 Jie Ouyang, Nilesh Patel and **Ishwar K Sethi**, "Multiclass Multifeature Split Decision Tree Construction in a Distributed Environment," *Proceedings MMIS*, Las Vegas, Nevada, August 2008 Ali Mustafa and **Ishwar K Sethi**, "Unsupervised Event Detection in Videos," *Proceedings 19th International Conf. on Tools for AI (ICTAI)*, pp. 179-182, Vol. 2, Patras, Greece, October 2007 Mingkun Li and **Ishwar K. Sethi**, "Confidence-based Active Learning," *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 28, pp. 1251 – 1261, August 2006.

Graduate Courses Taught (relevant to new degree	Prospective Graduate Courses (relevant to new degree)
None	None

Oakland University

Graduate Council

Faculty Name: Huirong Fu	Office: EC 528	**Office Phone** (248) 370-4456
Title: Associate Professor		**Office Email**
School: Engineering and Computer Science		fu@oakland.edu

Degrees – School – Year Ph.D Nanyang Technological University, Singapore 2000 M.Eng. Beijing University of Posts and Telecommunications, China 1997 B.Eng. Shanghai Jiao Tong University, China 1994	**Research Interest:** • Information Assurance and Security • Wireless and Mobile Networks • Sensor Networks • Internet Data Center • Multimedia Communication Systems • Resource Management and Quality of Service (QoS)

Grants Awarded:

2011-2014 PI NSF REU Program
REU Site: Undergraduate Computer Research (UnCoRe) $319,941
with Professors Jia Li (co-PI), Guangzhi Qu (Senior Personnel), Tao Shu (Senior Personnel), Nelish Patel(Senior Personnel), and Mohamed A. Zohdy (Senior Personnel)

2008-2011 PI NSF CCLI Program $115,096
CCLI - Phase 1: Information Assurance and Security Education with A Multidisciplinary Collaborative Approach in A Realistic Environment
with Professors Xiaodong Deng (co-PI) and Patrick Corbett (co-PI)

2007-2011 PI NSF Cyber Trust Program $255,999 (with supplement grant)
CT-ER: TrusT-US: Trustworthy Transportation Ubiquitous Systems
with Professors Fatma Mili (co-PI), Debatosh Debnath (co-PI), and Daniel Aloi (co-PI)

Most Recent Publications

1. Caixing Shao, Supeng Leng, Yan Zhang, and Huirong Fu, "A multi-priority supported medium access control in Vehicular Ad Hoc Networks," Computer Communications, Elsevier Science, Article in press. DOI:10.1016/j.comcom.2013.11.002

2. George P. Corser, Suzan Arslanturk, Jared Oluoch, Huirong Fu and George E. Corser, "Knowing the Enemy at the Gates: Measuring Attacker Motivation," International Journal of Interdisciplinary Telecommunications and Networking, Vol. 5, Issue 2, pp. 83-95, 2013.

3. Qing Wang, Supeng Leng, Huirong Fu, and Yan Zhang, "An IEEE 802.11p-based Multi-channel MAC Scheme with Channel Coordination for Vehicular Ad Hoc Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 13, no.2, pp. 449-458, 2012.

4. Hesiri D. Weerasinghe, Raymond Tackett, and Huirong Fu, "Verifying Position and Velocity for Vehicular Ad-Hoc Networks," Special Issue on Security and Privacy in Wireless Systems, Security and Communication Networks, vol. 4, no. 7, pp. 785-791, 2011.

5. Supeng Leng, Huirong Fu, Qing Wang, and Yan Zhang, "Medium Access Control in Vehicular Ad Hoc Networks," Wireless Communications and Mobile Computing, vol. 11, no. 5, pp.796-812, 2011.

Graduate Courses Taught (relevant to new degree) CSE 647: Advanced Topics on Networks CSE 681: Information Security	**Prospective Graduate Courses (relevant to new degree)** CSE__: Vehicular Ad-hoc Networking Security and Privacy

Oakland University
Graduate Council

Faculty Name: Dae-Kyoo Kim Title: Associate Professor School: Engineering and Computer Science	Office: EC 544	Office Phone: 2863 Office Email: kim2
Degrees – School – Year: Ph.D., Colorado State University, 2004	Research Interest: Design patterns, software architecture, access control modeling, smart grid, component-based development, software process.	

Grants Awarded

- Gift fund donated by Ministry of Security and Public Administration, Republic of Korea, $2,000, October, 2013.

- "Grid-Wise Information Base and Configuration Engine Development by Unifying IEC 61850 and IEC 61970", International Project: Oakland University (US), SISCO (US), Myongji University (Korea), Sejong University (Korea), Zenithtek (Korea), PI of foreign institutions, Korea Institute of Energy Technology Evaluation and Planning (KETEP), $1,380,000 (₩1,450,000,000) (OU: $308,000), 12/01/2011-11/31/2014.

- "Improving Design Quality of Software Systems via Pattern-Based Transformation", University Research Committee (URC) Fellowship, Oakland University, $8,500, 05/15/2010-8/15/2010.

- "An Aspect-Oriented Approach to Developing UML Models of Access Control Systems", The National Science Foundation (NSF), $218,229, 01/01/2006-12/31/2008. (CCF-0523101)

- "Checking Design Pattern Conformance of Software Models", University Research Committee (URC) Fellowship, Oakland University, $8,500, 05/15/2005-8/15/2005.

- "Legacy Transformation Using Pattern-Based UML Modeling", The Research Excellence Fund (REF), Oakland University, 01/2006-05/2006.

Most Recent Publications (limit to 6)

1. Lunjin Lu and **Dae-Kyoo Kim**, "Required Behavior of Sequence Diagrams Semantics and Refinement", ACM Transactions on Software Engineering and Methodology, 2013, to be published. (SCI)

2. **Dae-Kyoo Kim**, Byunghun Lee*, Sangsig Kim*, Hyosik Yang, Hyuksoo Jang, Deaseung Hong, and Herb Falk, "QVT-Based Model Transformation to Support Unification of IEC 61850 and IEC 61970", IEEE Transactions on Power Delivery, 2013, to be published. (SCI)

3. Sangsig Kim*, **Dae-Kyoo Kim**, Lunjin Lu, Suntae Kim*, Sooyong Park, "A Feature-Based Approach for Modeling Role-Based Access Control Systems", Journal of Systems and Software, Vol. 84, No. 12, pp. 2035-2052, 2011. (SCIE)

4. Lunjin Lu, **Dae-Kyoo Kim**, Yuanlin Zhu, Sangsig Kim*, "Verification of Structural Pattern Conformance Using Logic Programming", Journal of Universal Computer Science, Vol. 16, No. 17, pp. 2455-2474, 2010. (SCIE)

5. **Dae-Kyoo Kim**, Hyosik Yang, Hyuksoo Jang, Deaseung Hong, Herb Falk, Sangsig Kim*, and Byunghun Lee*, "A Metamodeling Approach to Unifying IEC 61850 and IEC 61970", the 4th IEEE PES Innovative Smart Grid Technologies Conference (ISGT), 2013, Washington DC. To be published (acceptance rate: 23%, 141/609).

6. Lunjin Lu and **Dae-Kyoo Kim**, "Refinement Inference for Sequence Diagrams", the 39th International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM), pp. 432-444, 2013, Spindleruv Mlyn, Czech Republic. (acceptance rate: 31%, 37/117).

Graduate Courses Taught (relevant to new degree	Prospective Graduate Courses (relevant to new degree)
1. Software Engineering 2. Fundamentals of Software Engineering 3. Software Prototyping and Validation	1. Software Security 2. Design Access Control Models for Software

Oakland University

Graduate Council

Faculty Name Khalid Mahmood Title Assistant Professor School Engineering and Computer Science	Office EC 532	Office Phone (248) 370-3542 Office Email mahmood@oakland.edu
Degrees – School – Year Ph.D.- Tokyo Institute of Technology		**Research Interest:** • Semantic based Information Security & Data Loss Prevention • High assurance in Internet of Things

Grants Awarded:
1. K. Mahmood (P.I.)Bridging the Semantic Gap between Physicians and Electronic Medical Records using Semantic Web and Wearable Computing Technologies, Oakland University,2015
2. K. Mahmood (P.I.), Dae-Kyoo Kim (co P.I.)and Mike Wu (Co.PI) " Using Semantic Web Technologies to predict futuristic trends by analyzing social network reviews," Amerilodge group , Rochester Hills, MI, USA: $5,000, Fund# 39290, 2013.
3. Kinji Mori (P.I), Xiodong Lu (co P.I.), K. Mahmood (co P.I.), S. Murakami (co P.I.), "Pipe rupture detection in nuclear power plant using Wireless Sensor Network" Hitachi Central Research Lab, Tokyo, Japan, 5,000,000 (JPY), 2007.

Most Recent Publications (limit to 6)
1. Mahmood K., Hironao Takahashi, Asif Raza, Asma Qaiser and Aadil Farooqui, "Semantic based Highly Accurate Autonomous Decentralized URL Classification System for Web Filtering" IEEE Proc. Of ISADS 2015, Taiwan
2. Hironao Takahashi, Khalid Mahmood and Uzair Lakhani, "Autonomous Decentralized Semantic based URL Filtering System for Low Latency" IEEE Proc. Of ISADS 2015, Taiwan
3. Mahmood K., Hironao Takahashi, Yasukai Arakawa "Gateway Access Permission Technology for High Assurance" 32nd International Conference on Distributed Computing Systems (ICDCS), China, 2012.
4. Takahashi H., Mahmood K., K. Mori, "Autonomous L3 Cache Technology for High Responsiveness" IPSJ Transaction; Journal of Information Processing Japan, Vol.20 No.2, 2012.
5. Mahmood K., X.D. Lu, Y. Horikoshi and K. Mori, "Autonomous Pull-Push Community Construction Technology for High-Assurance", IEICE Trans. on INFO. & SYST., Vol.E92-D, No.10, pp.1836-1846, 2009.

Graduate Courses Taught (relevant to new degree CSE/CIT 447/547 Computer Networks	Prospective Graduate Courses (relevant to new degree) • Information Security • Information Security Practice • Advanced Topics on Computer Networks • Network Security (TBO, 4 credits) • Software Security (TBO, 4 credits)

Oakland University
Graduate Council

Faculty Name: Guangzhi Qu Title: Associate Professor School : Engineering and Computer Science	Office: EC 538	Office Phone : 2690 Office Email: gqu@oakland.edu
Degrees – School – Year Ph.D., University of Arizona, 2005 MS., Beijing University of Aeronautics and Astronautics, 1999 BS., Beijing University of Aeronautics and Astronautics, 1996	Research Interest : Data mining, Machine learning, Healthcare computing, security and networking	

Grants Awarded

1. SCIP Safety Checklist: Improving Perioperative Handover and Follow-up, Daniel Silvasi (PI), Craig Hartrick (Co-PI), Guangzhi Qu (Co-PI), Blue Cross and Blue Shield of Michigan Foundation and William Beaumont Hospitals, $65,000.00, 2012-2013.
2. HVAC Performance Improvement Based on Internet Data, Osamah Rawashdeh (PI), K. Cheok (Co-PI), Guangzhi Qu (Co-PI), Chrysler Group LLC, $47,652.00, 2012-2013.
3. APSiS: Acute Pain Service information System, Guangzhi Qu (PI), William Beaumont Hospital, $50,000.00, 2011-2012.
4. Local Analgesia Adverse Effects Prediction using Multi-Label Classification, Guangzhi Qu (PI), OU-Beaumont Multidisciplinary Award, $14,000.00, 2010-2011.
5. Subgroup Analysis of Pain Medicine, Guangzhi Qu (PI), OU-Beaumont Multidisciplinary Award, $14,000.00, 2009-2010.
6. Acute Pain Patient Bioinformatics, Craig Hartrick (PI), Guangzhi Qu (Co-PI), William Beaumont Hospitals Research Foundation, $40,000.00, 2009-2010.
7. Measurement and Prediction of Impulsivity Related Falls in Older Adults, Osamah Rawashdeh (PI), Guangzhi Qu (Co-PI), M. Ferrari (Co-PI), B.Harrison (Co-PI), Oakland University and William Beaumont Hospitals, $10,000.00, 2009-2010.
8. Self Protection against Opportunistic Attacks in Wireless Networks, Guangzhi Qu (PI), Michigan Space Consortium, $10,000.00, 2008-2009.
9. Multi-Level Information Fusion for Defense against Cyber Attacks, Guangzhi Qu (PI), Oakland University Research Fellowship, $8,500.00, 2007-2008.
10. Autonomic Network Defense (AND) System, Salim Hariri (PI), Guangzhi Qu (Co-PI), Army Research Laboratory, $250,000.00, 2007-2008.

Oakland University

Graduate Council

Most Recent Publications (limit to 6)

1. Yongli An, Yang Xiao, Guangzhi Qu, "Multi-Band Spectrum Auction Framework Based on Location Information in Cognitive Radio Networks", Journal of Systems Engineering and Electronics, vol. 23, no. 5, pp. 671-678, 2012.
2. Guangzhi Qu, Ishwar Sethi, Craig Hartrick, Hui Zhang, "Multi-Label Classification with a Constrained Minimum Cut Model", Annals of Information Systems, in press 2012.
3. Guangzhi Qu, Hui Wu, Craig Hartrick, Jianwei Niu, "Local Analgesia Adverse Effects Prediction using Multi-label Classification", Neurocomputing, vol. 92, pp. 18-27, 2012.
4. Tong Chao, Jianwei Niu, Guangzhi Qu, Xiang Long, Xiaopeng Gao, "Complex Networks Properties Analysis for Mobile Ad hoc Networks", IET Communications, vol. 6, Issue 4, pp.370-380, 2012.
5. Guangzhi Qu, Hui Wu, "Bucket Learning: Improving Model Quality through Enhancing Local Patterns", Knowledge-based System, vol. 27, pp. 51-59, 2011.
6. Guangzhi Qu, Hui Wu, "A Weighted-Graph-Based Approach for Diversifying Search Results", International Journal on Knowledge and Web Intelligence, vol. 2, no.1 pp. 15-35, 2011.

Graduate Courses Taught (relevant to new degree	Prospective Graduate Courses (relevant to new degree)
CSE 549: Wireless Networking CSE 552: Operating System I CSE 652: Operating System II	Database Security

Oakland University

Graduate Council

Faculty Name Tao Shu Title Assistant Professor School School of Engineering and Computer Science	Office EC 526	Office Phone (248) 370-2137 Office Email shu@oakland.edu
Degrees – School – Year Ph.D.- The University of Arizona – 2010 Ph.D.- Tsinghua University - 2003	Research Interest: Wireless Networking and Security, Applied Cryptography	

Grants Awarded:
1. Large-Scale Statistical Learning based Spectrum Sensing and Cognitive Networking, PI, funded by NSF, duration: 01/01/2014-12/31/2017 2. Securing Multi-hop Communications in Mobile Ad Hoc Networks, PI, funded by Oakland University Faculty Research Fellowship, duration: 01/01/2012-12/31/2012.

Most Recent Publications (limit to 6)
1. Tao Shu and Husheng Li, "QoS-compliant sequential channel sensing for cognitive radios," submitted to *IEEE Journal on Selected Areas in Communications (JSAC)*, under 2nd round review, Aug. 2013. 2. Tao Shu and Marwan Krunz, "Sequential opportunistic spectrum access with imperfect channel sensing," *Ad Hoc Networks Journal (Elsevier)*, vol. 11, no. 3, pp. 778-797, 2013. 3. Tao Shu and Marwan Krunz, "Finding the cheapest route in profit-driven opportunistic spectrum access networks: A truthful mechanism design approach," *IEEE/ACM Transactions on Networking (ToN)*, vol. 20, no. 2, pp. 530-543, Apr. 2012.

Graduate Courses Taught (relevant to new degree CSE 549 Wireless and Industrial Networks	Prospective Graduate Courses (relevant to new degree) Computer Networks Advanced Topics on Computer Networks Network Security Information Security Practice

Oakland University

Graduate Council

Faculty Name: Debatosh Debnath Title: Associate Professor School: Engineering and Computer Science	Office: EC 530	Office Phone: x2701 Office Email debnath@oakland.edu School: Engineering and Computer Science
Degrees – School – Year Dr.Eng., Kyushu Institute of Technology, Japan, 1998 MS, Bangladesh University of Engineering and Technology, Bangladesh, 1993 BS, Bangladesh University of Engineering and Technology, Bangladesh, 1991		**Research Interest** Design of Digital Systems, Computer Architecture, Novel Applications of FPGAs

Grants Awarded
D. Debnath (PI), "Developing and Assessing Impact of Problem-Based Learning Approaches in a Course on Microprocessor-Based System Design," $37,709, NSF, 2007-2010.
H. Fu (PI), D. N. Aloi (Co-PI), D. Debnath (Co-PI), and F. Mili (Co-PI), "TrusT-US: Trustworthy Transportation Ubiquitous Systems," $249,999, NSF, 2007-2010.

Most Recent Publications (limit to 6)
M. Radovnikovich and D. Debnath, Elliptic curve cryptography coprocessor for mobile ad-hoc networks, in Proc. International Conference on Security and Management, July 2013.
D. Debnath, "Synthesis of easily testable AND-EXOR networks," International Journal of Computers and Their Applications, Vol. 18, No. 2, June 2011.

M. Radovnikovich and D. Debnath, Embedded software implementation of a key agreement protocol using 160-bit Elliptic curve, in Proc. International Conference on Advanced Computing and Communications, Sept. 2010.

D. Debnath and T. Sasao, "A new equivalence relation of logic functions and its application in the design of AND-OR-EXOR networks," IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, Vol. E90-A, No. 5, pp. 932-940, May 2007.

D. Debnath and T. Sasao, "Efficient computation of canonical form under variable permutation and negation for Boolean matching in large libraries," IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No. 12, pp. 3443-3450, Dec. 2006.

Graduate Courses Taught (relevant to new degree	Prospective Graduate Courses (relevant to new degree)

Oakland University

Graduate Council

Faculty Name: Nilesh Patel	Office: EC 524	Office Phone: 7-2247
Title: Associate Professor		Office Email: npatel
School: Engineering and Computer Science		

Degrees – School – Year	Research Interest
PhD Wayne State University 1997 MS Wayne State University 1993 BE Gujarat University 1989	1. Bioinformatics 2. Data mining 3. Pattern Recognition 4. Computer Vision, Multimedia Information Systems, Medical Imaging

Grants Awarded (Sample grants)

Algorithms and a Web Based System for Correlating Patient Data and a Plurality of Translational - $130,000
Smart HMI for In-vehicle Displays - $79,000
Acquisition of Instruments for Mobile Computing Research in the Context of Automotive - $242,500

Most Recent Publications (limit to 6)

1. C. Gillies, M. Siadat, N. Patel, and G. Wilson, "A Simulation To Analyze Feature Selection Methods Utilizing Gene Ontology For Gene Expression Classification", - To appear in Journal of Bioinformatics.
2. C. Gillies, X. Gao, N. Patel, M. Siadat, and G. Wilson, "Improved Feature Selection by Incorporating Gene Similarity into the LASSO", - To appear in International Journal of Knowledge Discovery in Bioinformatics.
3. C. Gillies, N. Patel, J. Akervall, and G. Wilson, "Gene Expression Classification using Binary Rule Majority Voting Genetic Programming Classifier", *Journal of Advanced Intelligence Paradigms, Vol-4, pp: 241-255, No. ¾, 2012.*
4. Jie Ouyang, N. Patel, and Ishwar Sethi, "From Centralized to Distributed Decision Tree Induction using CHAID and Fisher's Linear Discriminant Function Algorithms", *International Journal of Intelligent Decision Technologies, Vol 5(2), March, 2011*
5. Aiyesha Ma, I Sethi, and N. Patel, "Multimedia Content Tagging using Multilabel Decision Tree",

Graduate Courses Taught (relevant to new degree	Prospective Graduate Courses (relevant to new degree)
1. Advanced Operating System 2. Software Engineering 3. Mobile and Smartphone Application Development 4. Information Retrieval and Knowledge Discovery	1. CSE 550 Operating Systems 2. CSE 681 Information Security

Oakland University
Graduate Council

Faculty Name: Tom Lauer	Office: EH 447	Office Phone: X3278 Office Email: lauer@oakland.edu
Title: Professor of Management Information Systems		
School: Business Administration		
	Research Interest:	
	• Information Systems Security • IS Privacy • Intellectual Property • Open Source Software	
Degrees – School – Year PhD, Indiana University, 1988		

Grants Awarded:

n/a

Most Recent Publications (limit to 6)

1. Majeske, K. D., Lauer, T. (2013). The Bank Loan Approval Decision from Multiple Perspectives. Expert Systems with Applications, 40(3), 1591-1598.
2. Majeske, K. D., Lauer, T. (2012). Optimizing Airline Passenger Prescreening Systems with Bayesian Decision Models. Computers & Operations Research, 39(8), 1827-1836.
3. Lauer, T., Deng, X. (2007). Building Online Trust through Privacy Practices. The International Journal of Information Security (IJIS), 6(5), 323-331.
4. Lauer, T. (2004). e-Voting, a Security Risk Analysis. Electronic Journal of e-Government, 15.
5. Cass, K., Lauer, T. (2004). Media Transitions: The cases of digital imagery and email. Information Technology and People, 11.

Graduate Courses Taught (relevant to new degree)

IST 641, Privacy and IT
MIS 524, Enterprise Information Systems
MIS 625, IT Planning and Strategy
MIS 640, IS Security
MIS 641, IS Privacy
MIS 643, Int'l Prop & Public Domain

Prospective Graduate Courses (relevant to new degree)

MIS 641, IS Privacy
MIS 643, Int'l Prop & Public Domain

Oakland University

Graduate Council

Faculty Name Mohan Tanniru	Office	Office Phone
Title Prof of MIS	200 I Elliott Hall	Office Email tanniru@oakland.edu
School School of Business Administration		

Degrees – School – Year	Research Interest
MS in Elec. Eng. – U of WI-Milwaukee, 1972 MBA - U of WI-Oshkosh, 1975 Ph.D. – Northwestern University, 1978	Knowledge Management Decision Support IT Strategy and Innovation

Grants Awarded:

Not Applicable

Most Recent Publications (limit to 6)

R. Lusch, Vargo S. and M. Tanniru, "Service, Value Networks and Learning: Converging Marketing and SCM on Service-Dominant Logic," Journal of Academy of Marketing Science, 29, January 2009.

K. Fadel, Brown, S. and M. Tanniru, "A Theoretical Framework for Knowledge Transfer in Process Redesign," Data Base, Vol.39, No.3, 2008.

L. Zhao, C. Hsu, H. Jain, J. Spohrer, M. Tanniru and H. Wang, "Panel Report: Bridging Service Computing and Service Management: How MIS Contributes to Service Science Orientation," Communication of the AIS, 2008, Vol. 22, Article, 22, pp: 413-428

M. Tanniru, "A Framework for Supporting Decisions in a Global Context – The Case of a Global DSS (gDSS) for financial planning," in DSS Handbook 2, eds. F. Burstein and C. Holsapple, 2008, Chapter 48, pp:239-260, Springer-Verlag.

Sugumaran, V., Storey, V and M. Tanniru, "A Knowledge-Based Framework for Extracting Components in Agile Systems Development," Information Technology and Management Special Issue on Architecture & Design for Application Agility, 2008, Vol.9, 37-53

Rajagopalan, B., M. Tanniru, D. Doane and K. York, "Enablers and Enterprise Systems Training Success- an Exploratory Investigation," International Journal of Information Systems, 2007, Vol. 2, No.3, 250-265.

Graduate Courses Taught (relevant to new degree)	Prospective Graduate Courses (relevant to new degree)
MIS Capstone Project Business Analytics IT strategy	MIS 680 – Special Topics: IT Governance, Continuity and Risk Management

Oakland University

Graduate Council

Faculty Name: Hua Ming	Office:	Office Phone (248)370-3769
Title: Assistant Professor	516 EC	Office Email:
School: School of Engineering and Computer Science		ming@oakland.edu

Degrees – School – Year	Research Interest:
PhD., Iowa State University 2012	• Software Engineering, Design and Semantics of Programming Languages • Situation Aware & Context Oriented Software Intensive Systems

Grants Awarded:

Most Recent Publications (limit to 6)

- Hua Ming, Carl K. Chang and Jingwei Yang. "Dimensional Situation Analytics: from Data to Wisdom". In *39th IEEE International Computer Software and Applications Conference (COMPSAC 2015), Vol 1, pp. 50-59*, 2015
- Tianyu Meng, Hua Ming, Yan Gao, Georgi Batinov, Michelle Rusch, Les Miller. "Understanding Situations in Map-based Applications" the 30th International Conference on Computers and their Applications, 2015

- Tsai, Hsine-Jen, Les Miller, Hua Ming, Sree Nilakanta, and Meher Vani Bojja. "Expanding the Disaster Management Knowledge Space through Spatial Mediation". In *System Sciences (HICSS)*, 2012 *45th Hawaii International Conference on* (pp. 3699-3708). IEEE, 2012

- Katsunori Oyama, Atsushi Takeuchi, Hua Ming, and Carl K. Chang. "A Concept Lattice in Real User Monitoring for Recognition of User Problems." *The Eighteenth Asia-Pacific Software Engineering Conference, December 5-8, 2011* (APSEC 2011)

- Hua Ming, Carl K. Chang, Katsunori Oyama and Hen-I Yang. "Reasoning about Human Intention Change for Individualized Runtime Software Service Evolution." *34th IEEE International Computer Software and Applications Conference (COMPSAC 2010), Seoul, Korea*. IEEE Computer Society Press. pp. 289-296, 2010.

- Carl K. Chang, Hsin-yi Jiang, Hua Ming, Katsunori Oyama. "Situ: A Situation-theoretic Approach to Human-Intention Driven Runtime Software Evolution to Context-Aware Service Evolution." *IEEE Transactions on Service Computing*, IEEE Computer Society. Vol. 2. No. 3. pp. 261-275, 2009.

Graduate Courses Taught (relevant to new degree)	Prospective Graduate Courses (relevant to new degree)
	CSE__: Vehicular Ad-hoc Networking Security and Privacy

Oakland University

Graduate Council

Faculty Name: Yonghong Yan Title: Assistant Professor School: Engineering and Computer Science	Office: EC 534	Office Phone (248)-370-4087 Office Email: yan@oakland.edu
Degrees – School – Year University of Houston, 05/2007, Ph.D. in Computer Science		Research Interest: Parallel and High Performance Computing, Programming Languages and Compilers, Distributed and Cloud Computing, and Computer Systems and Architectures

Grants Awarded:

Image Processing Cloud (IPC): A Domain-Specific Cloud Computing Infrastructure for Research and Education PI, NSF CISE CNS-1205708,

SHF:Medium:Collaborative: Compute on Data Path: Combating Data Movement in High-Performance Computing Co-PI, NSF CISE SHF-1409946

SHF:Small:Collaborative: Application-aware Energy Modeling and Power Management for Parallel and High Performance Computing, Lead PI, NSF CISE SHF-1422961

Most Recent Publications

1. Supporting Multiple Accelerators in High-Level Programming Models, Yonghong Yan, Pei-Hung Lin, Chunhua Liao, Bronis R. de Supinski, and Daniel J. Quinlan, 2015 International Workshop on Programming Models and Applications for Multicores and Manycores (PMAM 2014) in conjunction with PPoPP, 2015
2. Compiler Transformation of Nested Loops for GPGPUs, Xiaonan Tian, Rengan Xu, Yonghong Yan, Sunita Chandrasekaran, and Barbara Chapman accepted to the Journal of Concurrency and Computation: Practice and Experience, 2014
3. NAS Parallel Benchmarks for GPGPUs using a Directive-based Programming Model, Rengan Xu, Xiaonan Tian, Sunita Chandrasekaran, Yonghong Yan and Barbara Chapman, 27th International Workshop on Languages and Compilers for Parallel Computing (LCPC2014)
4. Predicting Cache Contention for Multithread Applications at Compile Time, Munara Tolubaeva, Yonghong Yan and Barbara Chapman, 16th Workshop on Advances in Parallel and Distributed Computational Models to be held in conjunction with IPDPS 2014, May 2014
5. Reduction Operations in Parallel Loops for GPGPUs, Rengan Xu, Xiaonan Tian, Yonghong Yan, Sunita Chandrasekaran, and Barbara Chapman, 2014 International Workshop on Programming Models and Applications for Multicores and Manycores (PMAM 2014) in conjunction with PPoPP, February, 2014

Graduate Courses Taught (relevant to new degree) CSE 536: Concurrent and Multicore Programming	Prospective Graduate Courses (relevant to new degree) N/A

Oakland University

Graduate Council

Faculty Name: Wenjin Zhou Title: Assistant Professor School: Department of Computer Science, School of Engineering and Computer Science	Office: Engineering Center 542	**Office Phone** (2208) **Office Email** wzhou@oakland.edu
Degrees – School – Year Ph.D., Brown University, 2012 Sc.M., Brown University, 2009 B.S., University of Nebraska, 2005	**Research Interest:** Interdisciplinary and collaborative research on data-intensive computing, information retrieval, image analysis and interactive visualization tools for medical imaging, brain and life science.	

Grants Awarded:

- **Research Excellence Fund, "A MRI-based Framework for Measuring Brain Micromorphology and Diagnosis of Neurological Disorders"**, Oakland University Center for Biomedical Research, PI, $25,000.
- **"The Full Electron Structure of CypA/CsA Complex: Why is CsA effective in organ transplant patients? Can we design better drugs?"**, University Research Committee , PI, $10,000.

Most Recent Publications

- **Wenjin Zhou and Allison M Rossettoa. Finding protein thermostability and spin-coupling constant using Bayesian statistics.** *Journal of Mathematical Chemistry*, 53:151–161, 2015. (Impact factor: 1.27).
- Allison M Rossettoa, **Wenjin Zhou**, Xiaodong Pang, and Linxiang Zhou. The full electron structure of the FKBP12/FK506 complex. *Journal of Biomolecular Structure and Dynamics*, 33:388–394, 2015. (Epub 2014 Jan 28, Impact factor: 4.986).
- David F. Tate, Jared Conley, Robert H. Paul, Kathryn Coop, Song Zhang, **Wenjin Zhou**, David H. Laidlaw, Lynn E. Taylor, Timothy Flanigan, Bradford Navia, Ronald Cohen, and Karen Tashima. **Quantitative diffusion tensor imaging tractography metrics are associated with cognitive performance among HIV-infected patients.** *Brain Imaging and Behavior*, 4:68–79, 2010. (Impact factor: 10.288).
- **Wenjin Zhou, EdwardWalsh, and David H. Laidlaw. DoubleAx:** *In-vivo* **Axon Measurement in the Human Corpus Callosum Using Angular Double-PFG MRI.** *Organization for Human Brain Mapping (OHBM) Annual Meeting*, 2013. (Chosen for podium talk, acceptance rate < 4%).
- Radu Jianu, **Wenjin Zhou**, Ryan Cabeen, Daniel Dickstein, and David H. Laidlaw. **Visualizing tractography metrics of cortical-connectivity integrity in diffusion imaging.** *International Society for Magnetic Resonance in Medicine–ISMRM*, 20:3614, 2012.
- **Wenjin Zhou and David H. Laidlaw. Measurement of axon radii distribution in orientationally unknown tissue using angular double-pulsed gradient spin echo (double-PGSE) NMR.** *International Society for Magnetic Resonance in Medicine–ISMRM*, 19:3938, 2011.
- **Wenjin Zhou, Matt G. Hall, and David H. Laidlaw. Inferring microstructural properties using angular double pulsed gradient spin echo NMR in orientationally unknown tissue.** *Computational Diffusion MRI (CDMRI) Workshop at International Conference on Medical Image Computing and Computer-Assisted Intervention– MICCAI*, 2010. (Chosen for podium talk).

Graduate Courses Taught (relevant to new degree) ~~CSE 791 Research Initiation~~ CSE 792 Research Seminar CSE 596 Professional Practice CSE 594 Independent Study	Prospective Graduate Courses (relevant to new degree) CSE 596

Oakland University

Graduate Council

Degree Requirements

PREPARATORY COURSES – undergraduate courses				
Course	Title	Credits	Prerequisites	

FOUNDATION COURSES – graduate courses required prior to core				
Course	Title	Credits	Prerequisites	New (x)
CSE 552(I)	Operating Systems	4		
CSE 647	Advanced Networking	4		
CSE 545	Database Design and Implementation	4		

CORE COURSES				
Course	Title	Credits	Prerequisites	New (x)
CSE 681	Information Security	4		

DEPTH COURSES				
Course	Title	Credits	Prerequisites	New (x)
CSE	Software Security	4		x
CSE	Network Security	4		x
MIS 641	IS Privacy	3		
CIT 548	Information Security Practice	4		
CSE	Cyberlaw, Forensics and e-Discovery	4		x
CSE ___	Non Cryptographic Methods for Network Security and Privacy	4		x
MIS 643	Intellectual Property and the Public Domain in the Age of Remix	3		
MIS 680	ST: IT Governance, Business Continuity and Risk Management	3		
CSE 549	Wireless and Industrial Networks	4		
CSE 524	Cloud Computing	4		
CSE 523	Mobile and Smartphone Application Development	4		

RECOMMENDED ELECTIVE COURSES				
Course	Title	Credits	Prerequisites	New (x)
CSE 791	Research Initiation	2		
CSE 792	Research Seminar	2		
CSE 691	Master's Thesis Research	2 to 8		
CSE 596	Professional Practice	4		
CSE 594	Independent Study	2 to 4		

Oakland University
Graduate Council

Typical Plan of Study – Full Time Schedule

Professional Track

STUDENT SCHEDULE		
Fall I CSE 647: Advanced Networking (4) CSE 545: Databases (4)	Winter I CSE ___: Network Security (4) CSE 681: Information Security (4)	Summer I
Fall II CSE 552(1): Operating Systems (4) MIS 680: Policy & Governance (3) CSE 792: Research Seminar (2)	Winter II CSE ___: Software Security (4) MIS 641: IS Privacy (3)	Summer II
Total Credits: 32		

Research Track

STUDENT SCHEDULE		
Fall I CSE 647: Advanced Networking (4) CSE 545: Databases (4)	Winter I CSE ___: Network Security (4) CSE 681: Information Security (4)	Summer I
Fall II CSE 552(I): Operating Systems (4) CSE 691: Master's Thesis Research (4)	Winter II CSE ___: Software Security (4) CSE 691: Master's Thesis Research (4)	Summer II
Total Credits: 32		

Note: We also offer courses in Summer I and Summer II to meet the needs of some students.

Oakland University
Graduate Council

<div align="center">

Typical Plan of Study – Winter Start

Professional Track

</div>

STUDENT SCHEDULE		
Winter I CSE ___: Network Security (4) CSE 681: Information Security (4)	**Fall I** CSE 647: Advanced Networking (4) CSE 545: Databases (4)	**Summer I**
Winter II CSE ___: Software Security (4) MIS 641: IS Privacy (3)	**Fall II** CSE 552(I): Operating Systems (4) MIS 680: Policy & Governance (3) CSE 792: Research Seminar (2)	**Summer II**
Total Credits: 32		

<div align="center">

Research Track

</div>

STUDENT SCHEDULE		
Winter I CSE ___: Network Security (4) CSE 681: Information Security (4)	**Fall I** CSE 647: Advanced Networking (4) CSE 545: Databases (4)	**Summer I**
Winter II CSE ___: Software Security (4) CSE 691: Master's Thesis Research (4)	**Fall II** CSE 552(I): Operating Systems (4) CSE 691: Master's Thesis Research (4)	**Summer II**

Note: We also offer courses in Summer I and Summer II to meet the needs of some students.

Oakland University

Graduate Council

<div align="center">

APPENDIX D
Detailed New Course Descriptions and Syllabi

</div>

CSE XXX Cyberlaw, Forensics and Electronic Discovery (4 credits): An overview of laws related to computers and the Internet, specifically the regulations related open access, digital copyrights, electronic contracts, privacy, social networking, protection of speech, online abuse and exploitation are reviewed. Topics related to internet crimes as well as forensics techniques for capturing digital evidence from file systems, email, and web-browsers are covered. With the increasing prevalence of Electronically Stored Information (ESI), the role of processing vast amounts of digital data potentially relevant to a civil lawsuit has become significant. Algorithms for managing, searching and classifying ESI are presented.

This course also provides a survey of intellectual property law for a technical (non-legal) audience. The various types of Intellectual Property Rights (IPR) including Patents (utility, plant, and design), Copyrights, Trade Marks, Trade Dress and Trade Secrets are differentiated and the strategies for protecting them are described. The course focuses on patent law and covers techniques for searching and analyzing related inventions in patent databases. Aspects of IPR valuations and models for business development are explored. Students develop a provisional patent applications complete with specifications and drawings.

CSE XXX Software Security (4 credits): Introduction to research in foundations of software security. This course surveys common software vulnerabilities, including buffer overflows, format string attacks, cross-site scripting, and botnets. The course also discusses common defense mechanisms, including static code analysis, reference monitors, language-based security, secure information flow, and others.

CSE XXX Non-cryptographic Methods for Network Security and Privacy (4 credits): This course introduces the latest development of non-cryptographic designs that give networks built-in security and privacy features by exploiting physical layer, link layer, and network layer characteristics of the system, including wireless link/channel signatures, wireless device signatures, traffic footprint, randomized and multipath routing and forwarding, traffic-assisted security replenishment, spread spectrum, frequency hopping, truthful network mechanism design, and network measurement and inference. Important security and privacy applications enabled by these features include secret key establishment and distribution, group key management, attack detection and mitigation, anti-jamming, secure data collection, identity authentication, spoofing detection and mitigation, security replenishment, strategy-proof protocol design, intrusion detection, etc. A key advantage provided by this type of methods is that their security strength is usually protected by the physical difficulties and constraints in breaking the system, rather than relying on the computational hardness assumption in solving certain hard problems (e.g., the discrete logarithm problem), whose validity has been seriously challenged by the tremendous computation capacity of today's high performance computing technology. Such methods are usually orthogonal to conventional cryptographic approach, and can be combined

Oakland University

Graduate Council

with cryptographic approach to significantly enhance the overall security and privacy of the system.

CSE XXX Network Security (4 credits): Network Security will provide students a good understanding of different security aspects related to computer networks. Methods of network attacks and ways to defend against them will be discussed. Topics include attacks in different layers, security technologies, link layer security, network layer security, transport layer security, and application layer security.

Oakland University
Graduate Council

CSE XXX Cyberlaw, Forensics and Electronic Discovery (4 credits):

This course provides a general overview of the fundamentals of computer forensics, the role of a cyber forensics specialist, computer forensic evidence, and introduction of real world problems in collecting and processing digital evidence. The course covers the laws and procedures for acquisition, recovery, analysis and preservation of digital evidence for purposes of criminal law enforcement and civil litigation. The course provides a background into Investigation of computer crime scenes, intellectual property thefts, and cyber-torts where computers are used as instrumentalities. The course aims at preparing students in formulating and implementing policies for organizational readiness for computer discovery and forensic investigations.

Prerequisite: *Major Standing*

Major Topics:
- Digital Forensic Science and Laws related to Computer Forensics
- Computer Crimes and Cyber Forensics
- Seizure of Digital Evidence and Crime Scene Analysis
- Forensics Tools for Recovery of Data from Computers and Disks
- E-Mail and Network Forensics

Course Audience:

This is an elective course for CS & IT majors and eligible for graduate plans of study.

Course Instructor: Gautam
B. Singh, PhD, JD
x2129, singh@oakland.edu

Book

John Vacca and K. Rudolph, "System Forensics, Investigation, and Response," Jones and Bartlett, ISBN-13: 9780763791346, 2011.

Labs

There will be 2 case assignments. Each of the teams will be working as "forensic experts" to try and ascertain as much evidence as needed for developing either a civil or criminal case against an individual or group of individuals. For each lab assignment, there will a group designated as the person seeking to **admit** the evidence, and a group that will seek to deem it inadmissible by critically questioning the other teams' evidence gathering expertise.

Oakland University
Graduate Council

Schedule

WEEK	Topics	Chapter
Week 1	Introduction to Systems Forensics	1
Week 2	Cyber-crimes	2
Week 3	Laws related to Privacy and Computer Crimes	14
Week 4	Search and Seizure - Fourth Amendment	
Week 5	Rules of Evidence, Digital Evidence	7
Week 6	**Case 1 - Arguments**	
Week 7	Forensics Methods	4, 5
Week 8	Winter Recess - No Class	
Week 9	*Review and Mid Term Test*	
Week 10	Collecting, Securing, Protecting Evidence. Daubert	6, 7
Week 11	Hidden Data, Live Monitoring, Data Recovery	8, 9
Week 12	**Project Presentations**	
Week 13	E-Mail Forensics	10
Week 14	Network Forensics	11
Week 15	**Case 2 - Arguments**	
Week 16	*Review*	
Week 17	**Final Examination**	

Grade Distribution	
Homework, In-class Assignments and Participation	25%
Project Report (10%) Presentation (5%)	15%
Case I - Fourth Amendment Issues	15%
Case II - Forensics Analysis - Report and Presentations	20%
Mid Term Test	15%
Final Exam - 25 Multiple Choice Questions	10%

Oakland University

Graduate Council

CSE XXX Software Security (4 credits):

Course Description

Introduction to research in foundations of software security. This course surveys common software vulnerabilities, including buffer overflows, format string attacks, cross-site scripting, and botnets. The course also discusses common defense mechanisms, including static code analysis, reference monitors, language-based security, secure information flow, and others.

Course Objectives

Students are exposed to principles and techniques of secure software development. The student shall be able to

- Acquire knowledge of common software security threats and mitigation techniques;
- Assess security risk of a software system under development using threat models and security metrics and write security requirements by developing misuse use cases
- Apply secure coding techniques;
- Perform security testing including white box, grey box, black box and penetration testing techniques; and
- Verify security requirements using static analysis and code inspection techniques.

Required and Recommended Textbooks

- Gary McGraw. Software Security: Building Security In. Addison-Wesley, ISBN 978-321-35670-3 (Required).
- Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw and Nancy Mead. Software Security Engineering: A Guide for Project Managers. Addison-Wesley, ISBN 978-0-32-150917-8.
- Neil Daswani, Christoph Kern, Anita Kesavan, *Foundations of Security: What Every Programmer Needs to Know*, APress, 2007. ISBN-10: 1590597842, ISBN-13: 978-1590597842.
- Charles P. Pfleeger and Shari Lawrence Pfleeger. *Analyzing Computer Security*. Prentice Hall, Upper Saddle River, NJ, 2011. ISBN 978-0-13-278946-2.
- Matt Bishop. *Introduction to Computer Security*. Addison-Wesley, Boston, 2005. ISBN 0-321-24744-2.
- Michael Howard and David D. LeBlanc. Writing Secure Code. Microsoft Press. 2nd Edition, 2003. Chapter 4 Threat Modeling.
- Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F. Sutherland, David Svoboda, Java Coding Guidelines: 75 Recommendations for Reliable and Secure Programs, Addison-

Oakland University

Graduate Council

Wesley Professional; 1 edition. September 2013, ISBN-10: 032193315X, ISBN-13: 978-0321933157.

- Robert C. Seacord, Secure Coding in C and C++. Publisher: Addison-Wesley Professional; 2 edition, April 2013, ISBN-10: 0321822137, ISBN-13: 978-0321822130.

Tentative Schedule

Week	Topics
1	Course Introduction and Security Goals
2	Security threats and mitigation techniques
3	Threat Modeling
4	Security Requirements Analysis
5	Secure programming techniques
6	Secure programming techniques
7	Mid-term Security testing
8	Security testing
9	Static code analysis
10	Static code analysis
11	Information flow analysis
12	Code inspection
13	Project Presentation
14	Project Presentation

Assessment and Grading Scheme:

The final grade will be based upon the following components and their related weights:

- Assignments   15%
- Quizzes   10%
- Project   20%
- Mid-term   25%
- Final   30%
- Grading Scale:

90+	4.0	
80 – 89	3.x	linearly in-between
70 – 79	2.x	linearly in-between
60 – 69	1.x	linearly in-between
0 – 59	0.0	

Academic Honesty

Students are encouraged to discuss the projects and course material with each other, for their mutual benefit. However, no form of plagiarism (e.g., copying other groups work,) of any material submitted for grading, is permitted. All students must be aware of the contents of Academic

Oakland University

Graduate Council

Conduct Regulations listed through the following url:
http://www2.oakland.edu/deanofstudents/handbook/acr.cfm

Oakland University

Graduate Council

CSE XXX Non-cryptographic Methods for Network Security and Privacy (4 Credits)

General Information

Instructor: Tao Shu, Ph.D.
Office: EC 526
email: shu@oakland.edu
Office Hours: by appointment

Course Description

This course introduces the latest development of non-cryptographic designs that give networks built-in security and privacy features by exploiting physical layer, link layer, and network layer characteristics of the system, including wireless link/channel signatures, wireless device signatures, traffic footprint, randomized and multipath routing and forwarding, traffic-assisted security replenishment, spread spectrum, frequency hopping, truthful network mechanism design, and network measurement and inference. Important security and privacy applications enabled by these features include secret key establishment and distribution, group key management, attack detection and mitigation, anti-jamming, secure data collection, identity authentication, spoofing detection and mitigation, security replenishment, strategy-proof protocol design, intrusion detection, etc. A key advantage provided by this type of methods is that their security strength is usually protected by the physical difficulties and constraints in breaking the system, rather than relying on the computational hardness assumption in solving certain hard problems (e.g., the discrete logarithm problem), whose validity has been seriously challenged by the tremendous computation capacity of today's high performance computing technology. Such methods are usually orthogonal to conventional cryptographic approach, and can be combined with cryptographic approach to significantly enhance the overall security and privacy of the system.

Textbooks

There is no required textbook. Most of the course materials will be based on recent research papers. Required reading list will be posted before each class. However, the following reference books will be beneficial for you to understand the basic concepts heavily used throughout the lecture.

1. D. Tse and P. Viswanath, "Fundamentals of Wireless Communication," Cambridge University Press, May 2005. An online version is available
http://www.eecs.berkeley.edu/~dtse/book.html

Oakland University

Graduate Council

2. K. Pahlavan and P. Krishnamurthy, "Principles of Wireless Networks: A Unified Approach", Prentice Hall.

3. James F. Kurose and Keith W. Ross , "Computer Networking: A Top-Down Approach," 6th Edition, Pearson, 2012.

Course Objectives

- To provide a comprehensive survey of the state of the art for the non-cryptographic methods for network security and privacy.
- To understand the theory and technology that is foundational for non-cryptographic methods for network security and privacy.
- To explore the best practices in the field.

Topics and Schedule (tentative)

1. Wireless networking fundamentals (2 week)
   - Course overview (challenges, applications, mobility, security, layered network architecture)
   - OSI model
   - PHY layer: Signals, channel models, multi-antenna, frequency hopping
   - Link layer: ALOHA, CSMA, Hidden terminal and exposed terminal
   - Network layer: link-state routing, distance vector routing, routing in MANETs (AODV and DSR), geographic routing, multi-path routing
   - Application layer: location-based service (LBS), localization, social computing

2. PHY based non-cryptographic methods (3 weeks)
   - Physical layer encryption
   - Wireless channel signatures (SISO, MIMO, SIMO, MISO)
   - Wireless device signatures
   - AP anti-spoofing and attack detection
   - Anti-jamming (constant jammer, random jammer, reactive jammer)

3. Link layer based non-cryptographic methods (3 weeks)
   - Information-theoretic secrecy vs. computational secrecy
   - Channel-based key establishment and exchange
   - MIMO-assisted key establishment and exchange
   - OFDM-assisted key establishment and exchange
   - Multi-channel key establishment and exchange
   - Mobility-assisted/distance-assisted secret key exchange
   - Traffic footprint

Oakland University

Graduate Council ·

- Traffic-assisted security replenishment

4. Network layer non-cryptographic methods (3 weeks)
- Randomized multipath routing methods
- Secure/privacy-preserving data collection (phantom routing, ghost source/destination, dummy source/destination, spatial cloaking, mixing-zone)
- Computational geometry based anonymity communication
- Game theoretic models for strategy-proof networking mechanism design

5. Application-layer non-cryptographic methods (3 weeks)
- Location privacy for LBS (k-anonymity, m-observability, mixing-zone, pseudonym-based methods)
- Localization privacy algorithms (ranging-based and range-free models)
- Privacy-preserving social computing (crowdsourcing, range search, matching, pairing, geometric methods and applications)

Evaluation and Grading

There will be no midterm and final exams. Your final grade will be evaluated based on the following components and weights:

Homework: 20%
Survey presentation: 30%
Quizzes: 10%
Project: 30%
Attendance: 10%
Total: 100%

Your final GPA is converted from your weighted average points according to the following: 4.0 (A): 90 points and above; 3.0 to 3.9 (B): 80 – 89 points; 2.0 to 2.9 (C): 65 – 79 points; 1.0 to 1.9 (D): 50 – 64 points; 0.0 (F): 49 and below. A small margin (e.g., 1 to 2 points below the boundary) may be considered in the conversion.

Homework

Homework will be assigned on topics covered in class. There will be approximately 4-5 homework assignments of equal weights. Assignments will be posted on Moodle at least one week before the due date. Unless specified explicitly, students are expected to finish each assignment **independently**. For a question that allows collaboration, the level of collaboration will be specified in the question description. The submission of your homework will be due to Moodle, and the required form of submission (e.g., code or report) will be given along with the homework itself. **Late submission will not be graded.**

The homework grades will be based upon the following components:

Oakland University

Graduate Council

- Correctness of the solution to the problem assigned.
- Clarity and justification of the solution.
- Clear and concise explanation when answering conceptual questions.

Survey Presentation

Each student is expected to give one 30-minute survey presentation on one advanced topic selected by the instructor. For each topic, usually the instructor will first present the basic background information and then the student presents in-depth survey of the state of the art in the area. The student's talk will be around 25 minutes, leaving about 5 minutes for Q&A. To facilitate the student to better prepare his/her talk, the instructor will assign a minimum set of papers that should be covered in the survey. Student's presentation will be evaluated based on the quality of the survey and the talk, along with the quality in answering questions.

Quizzes

At the end of each topic an in-class quiz will be given to the class to test whether the material has been well received by the students. In total 5 quizzes will be given in the semester and each quiz carries equal weight.

Project

A team-based project will be conducted in the second half of the semester. A team will consist of 2 to 3 students, and will work on a reasonable set of tasks proposed by the team and approved by the instructor. The topic of the project must fall into the areas covered by the course. The project can be either an implementation of a new idea, or an improvement over an existing idea. Each team must submit a one-page project proposal describing the tasks to be performed, justifying why it is a good idea to perform those tasks, and outlining the task assignment for each team member. The last week of the class (the first week of December) is reserved for project presentation. Each team should also submit a project report by end of the last class meeting.

Attendance

In order to achieve the best studying effect, every student is **required** in principle to attend every lecture of the class. Attendance will be taken in randomly selected classes. To account for unexpected situations that are out of the control of the student, each student is allowed with at most 4 unexcused missing lectures. Beyond that 4-lecture limit, a student who cannot attend a lecture must send the instructor an email notification at least 4 hours before the class to explain the reason why he/she cannot attend the class. Beyond the 4-lecture limit, each unexcused

Oakland University

Graduate Council

missing lecture will receive a 1% penalty in the student's final GPA, up to the 10% maximum allocated to the attendance component. Late arrival and side talking during the meeting are strongly discouraged.

Academic Integrity

Students are expected to comply with the Academic Conduct Policy of the Oakland University. Suspected breaches of academic honesty will be taken before the Academic Conduct Committee. Academic misconduct includes—but not limited to—cheating in quizzes and exams, unauthorized collaborations in assignments, and plagiarizing the work of others. Students found guilty of academic misconduct in this course will receive a grade 0.0 for the course in addition to any penalties imposed by the conduct committee. Please refer to the undergraduate catalog and on-line Academic Conduct Regulations at http://www.oakland.edu/handbook/ for details.

Oakland University

Graduate Council

CSE xxx: Network Security (4 credits)

Prerequisites: CSE 681, C/C++ and/or Java.

Course Description: Network Security will provide students a good understanding of different security aspects related to computer networks. Methods of network attacks and ways to defend against them will be discussed. Topics include attacks in different layers, security technologies, link layer security, network layer security, transport layer security, and application layer security.

Course Contents:

- Attacks in Different Layers

- Security Technologies

- Link-Layer Security

- Network Layer Security

- Transport Layer Security

- Application Layer Security

Course Objectives:

- Learn the recent trends in network security attacks and cyber-attacks in general.

- Analyze a variety of attacks in different layers and countermeasures.

- Understand the design and analysis of network security architectures, protocols, and services. Most of these protocols are based on cryptographic primitives and can be used as building blocks for more sophisticated networked systems.

- Obtain an in-depth coverage of today's network security standards, their functionality and limitations, e.g., SSL/TLS, IPsec, and WPA.

Instructor: Dr. Huirong Fu

Office hours: By appointment and walk-ins welcomed.

Oakland University

Graduate Council

Office phone:	(248) 370-4456
Office:	EC 528
Email address:	fu *at* oakland *dot* edu

Class location: EC 554

Day and time: Saturdays, 9:00 am - 12:20 pm

Required texts: **Charlie Kaufman, Radia Perlman, and Mike Speciner, *Network Security - Private Communication in a Public World*, Prentice Hall (2nd Edition), 2002. ISBN-13: 978-0130460196, ISBN-10: 0130460192.**

Reference texts: William Stallings, *Network Security Essentials: Applications and Standards*, Prentice-Hall. ISBN 0-13-035128-8.

Charles P. Peleeger, *Security in Computing*, Prentice-Hall. ISBN 0-13-337486-6.

Ross Anderson, *Security Engineering: A Guidance to Building Dependable Distributed Systems*, John Wiley & Sons Inc. ISBN 0-471-38922-6.

Dorothy E. Denning, *Information Warfare and Security*, Addison Wesley. ISBN 0201433036.

Edward Amoroso, *Fundamentals of Computer Security Technology*, Prentice-Hall, 1994. ISBN 0-13-108929-3.

Bruce Schneier, *Applied Cryptography* (2nd ed.), John Wiley, 1996. ISBN 0-471-11709-9.

William R. Cheswick and Steven M. Bellovin, *Firewalls and Internet Security*, Addison-Wesley, 1994. ISBN 0-201-63357-4.

W. Richard Stevens, *TCP/IP Illustrated, Volume 1*, Addison-Wesley, 1994.

Oakland University

Graduate Council

ISBN 0-201-63346-9 (v.1).

J. Kurose and K. Ross, *Computer Networking, a Top Down Approach Featuring the Internet*, Addison-Wesley, 2005. ISBN 0-321-22735-2.

A. Gupta and S. Laliberte, *Defend I.T.: Security by Example*, Addison-Wesley, 2004. ISBN 0-321-19767-4.

Assignments and Labs: Homework assignments, in-class discussions and assignments, each including paper-and-pencil questions and/or programming problems. The course has a substantial hands-on component. In addition to the conceptual problem sets, each team of students is required to perform several laboratory assignments.

Project(s): There will be a term project. You will do independent research in small groups (e.g., teams of 2–3). Projects may cover any topic of interest in network security, interpreted broadly (it need not be a topic discussed in class); ties with current research are encouraged. A conference-style or NSF proposal-style report and a project presentation on your results will be due at the end of the semester.

You are encouraged to start thinking of topics of interest early. Be ambitious! I expect that the best papers will probably lead to publication (with some extra work).

More details can be found at Moodle.

Moodle: Moodle is the tool to be used for our class web page. This website will include notes and schedules (including exam dates) for our course. Assignments will be available for download from this site. Please check this site often for updates. Use your OU email account name and password to login to the system.

The address is https://moodle.oakland.edu/

Grading: Assignments, In-class Quizzes, Discussions and Assignments, and Labs 80%, Project 20%. No final exam.

You may discuss homework assignments with classmates but all solutions must be original and individually prepared. **Homework assignments should be**

Oakland University

Graduate Council

submitted by their due date. No late assignments will be accepted.

Logistics: Outside of class and office hours, questions regarding assignments, course material, etc. send me emails. Please feel free to make suggestions, complaints, etc., at any time including making comments anonymously.

Special needs: Any students with disabilities or other special needs, who need special accommodations in this course are invited to share these concerns or requests with the instructor as soon as possible.

Rules: The "Academic Conduct Policy" is explained on page 100 of the Oakland University 2008-2009 Undergraduate catalog. It may also be found on the OU website at http://www2.oakland.edu/oakland/ouportal/index.asp?item=3423&site=75. Students suspected of cheating will be referred to the Academic Conduct Committee according to the "Academic Conduct Policy". Any student found guilty of cheating by that committee will receive a 0.0 grade in the course. In particular, no student may represent or imply that the work of another person is her or his own.

As a computer user, you are expected to behave in responsible ways. You should always follow computer usage policies (of your company, your department, or Internet Service Provider, etc). The discussion in this class does not give your permission to violate computer usage policies.

Oakland University

Graduate Council

Proforma Budget

Proforma Income Statement

Program Title	Master of Science in Cybersecurity (MSC)
Program Type: (New, INC,CRCE, MUC)	New
Fiscal Year	2016
Incremental Analysis	
Fund Number	

Revenue Variables:		2016	2017	2018	2019	2020
Headcount		20	35	35	35	35
Number of Sections @ 2 cr.		0	0	0	0	0
Number of Sections @ 3 cr.		0	0	0	0	0
Number of Sections @ 4 cr.		0	0	0	0	0
Number of Sections @ other		0	0	0	0	0
Total Credit Hours		320	560	560	560	560
Undergraduate		0	0	0	0	0
Graduate		320	560	560	560	560
Doctoral		0	0	0	0	0
UG FYES		0	0	0	0	0
Graduate FYES		20	35	35	35	35
Doctoral FYES		0	0	0	0	0
Total FYES						
Tuition Rate Per Credit Hour		656.3675	676.0585	696.3403	717.2305	738.7474
Undergraduate						
Graduate			$	$	$	$
Enrollment Fees per Semester						
Other Fees						
Revenue		$ 210,037.6	$ 378,592.8	$ 389,950.6	$ 401,649.1	$ 413,698.5
Tuition		$ 210,037.6	$ 378,592.8	$ 389,950.6	$ 401,649.1	$ 413,698.5
Enrollment Fees						
Course Fees						
Other Fees						
Total Revenue		$ 210,037.6	$ 378,592.8	$ 389,950.6	$ 401,649.1	$ 413,698.5
Expenses	ACCT					
Salaries/Wages						
Faculty Startup		$ 30,000	$ 30,000			
Faculty Salaries	6101	$ 90,000.00	$ 185,400.00	$ 190,962.00	$ 196,690.90	$ 202,591.60

Oakland University

Graduate Council

Visiting Faculty	6101					
Administrative	6201	$ 22,866.48	$ 23,552.47	$ 24,259.05	$ 24,986.82	$ 25,736.42
Clerical	6211					
Administrative - IC	6221					
Faculty Inload (Replacement Costs)	6301	$ 24,000.00				
Faculty Overload	6301					
Part-time Faculty	6301					
Graduate Assistant	6311	$ 14,000.00	$ 14,000.00	$ 14,000.00	$ 14,000.00	$ 14,000.00
Wages	6401					
Out of Classification	6401					
Overtime	6401				..	
Student	6501					
Total Salary Expenses		*$ 180,866.50*	*$ 252,952.50*	*$ 229,221.00*	*$ 235,677.70*	*$242,328.00*
Fringe Benefits	6701	$ 61,589.92	$ 94,028.61	$ 96,849.47	$ 99,754.96	$ 102,747.60
Total Salary and Fringe Benefits		*242,456.40*	*$ 346,981.10*	*$ 326,070.50*	*$ 335,432.60*	*$ 345,075.60*
Operating Expenses						
Supplies and Services	7101	5,000.00	5,000.00	5,000.00	5,000.00	5,000.00
Graduate Assistant Tuition	7101	$ 10,196.00	$ 10,501.88	$ 10,8160.94	$11,141.44	$11,475.69
Facility Charges	7101					
Travel	7201					
Telephone	7301					
Equipment	7501					
Library	7401	$ 4,805.00	$ 2,986.00	$ 3,234.00	$ 3,505.00	$3,800.00
Total Operating Expenses		*$ 20,001.00*	*$ 18,487.88*	*$ 19,050.94*	*$ 19,646.44*	*$ 20,275.69*
Total Expenses		*$ 262,457.40*	*$ 365,469.00*	*$ 345,121.50*	*$ 355,079.10*	*$ 365,351.30*
Net Income/Loss		*$ (52,419.8)*	*$ 13,123.81*	*$ 44,829.10*	*$ 46,569.99*	*$ 48,347.24*
Percentage of Expenses to Tuition		124.95%	96.53%	88.50%	88.41%	88.31%

Oakland University
Graduate Council

Additional personnel support required

A 25% program coordinator will assist the CSE Chair. This job description will include:

- Assist CSE chair in development and oversight of course scheduling, enrollment administration analysis and decision making, creation of program communications and outreach efforts, assessment activities and event conceptualization and planning.☐
- Collaborate with faculty to shape the strategic planning of future external funding grants.☐
- To mentor the junior faculty in writing research proposals that meet the necessary requirements of funding agencies. Also assist them to develop and manage interim reports for industry sponsors, funding agencies and institutional review board to ensure that program projects are moving toward timely completion. The coordinator will also act as liaison, if required, between the research team and funding agencies or significant parties.☐
- Supervise teaching assistant and visiting faculty member(s) by hiring, training, assigning course, providing constructive feedback, and monitoring performance for accuracy and completeness.
- Preparation of the Oakland University assessment reports for the MS in Cyber Security program. Oversee assessment initiatives, including student feedback questionnaires and focus groups. Develop and implement procedures to ensure integrity and confidentiality of collected data. Prepare and distribute questionnaires and compile and distribute results to appropriate instructional team members, administrators and staff. Plan and conduct periodic focus groups and/or needs assessments.☐
- Manage changes to the academic catalogs.☐
- Conduct various national and international outreach activities by collaborating with department and school. Also to ensure that department website contain updated content and publications.☐
- Provide recommendations to CSE chair on transfer course equivalencies, petitions, graduation audits, and admission applications.☐
- Be available to students to address issues relating to admission and the curriculum (i.e., via email, phone and in-person meetings).☐
- Be the liaison to the SECS Tutoring Center.☐
- Assist students to find the internships in the industry.☐
- Assist CSE chair in frequent interaction with administrators of various Oakland University units (such as Registrar office, Dean office, CTO office, Library, Research office), faculty and staff in a variety of academic schools as well as creating and maintaining relationships with a variety of campus and community partners.☐
- Manage instructional and lab space usage by coordinating with other
- Serve as Master in Cyber-security program representative in advising meetings and stay apprised of academic advising issues and practices in order to make informed recommendations to the CSE chair regarding academic offerings. Conceptualize and

Oakland University

Graduate Council

execute all aspects of academic affairs programmatic activities and events from ideas to implementation.

- Develop new events for Master in Cyber security including webinars, panels, workshops, trainings, and retreats with collaboration with academic and student bodies. □
- Manage interdepartmental workload of teaching and servicing tasks and strategically combining efforts and/or reassigning tasks depending on program need.

Funding is also included for a Ph.D. graduate assistant stipend to support a Ph.D. graduate student as a TA.

Role and Responsibilities of TA:

- To provide assistance to instructor in designing the course, preparation of tests, to prepare materials, and grading assignments.
- To work with students one-on-one; learn about problems they are having with the course material.
- To Grade tests, exams, essays, and quizzes.
- Depending upon nature of courses, sometime TA might need to meet scheduled lab classes and lead discussions, answer questions, clarify materials.
- To review labs in advance, ask and answer student queries, and evaluate students.

Two new faculty members are planned to meet the following needs:

- 4 new courses will be developed and offered for the proposed program.
- Some courses, e.g., CSE 681, need to be offered more than once per year for the increased number of students.
- More faculty members are needed to supervise the students in research track.

Oakland University

Graduate Council
MS in Cybersecurity Assessment Plan

APPENDIX G

Goal Cited In OU Mission	Relevant Goal Of Unit	Student Learning Outcomes	Methods of Assessment	Individual(s) Responsible for Assessment Activities	Procedures for Using Assessment Results to Improve Program
Programs and activities within the Computer Science and Engineering (CSE) department are in line with the following goals of the Oakland University:	A. To provide high-quality graduate programs of instruction in Computer Science and Engineering to prepare graduates for careers in the coming decades,	1. Explore leadership, theory, tools, skills, and practices as it applies to safeguarding the security and privacy of today and tomorrow's cyber infrastructure.	External evaluation;	Course instructors and CSE Dept.	The CSE Dept. faculty meet each semester to review external and end-of-course evaluations and develop plans for improvement.
A. It offers instructional programs of high quality that lead to degrees at the baccalaureate, master's and doctoral levels as well as programs in continuing education;	B. To advance knowledge through basic and applied research in Computer Science and Engineering, and,	2. Understand fundamentals and state of the art of today's cyber technology. 3. Understand fundamentals and advanced issues of various threats faced by today's cyber infrastructure. 4. Understand cybersecurity and privacy needs of today's institution. 5. Acquire solid knowledge on applied cryptography, which serves as the basis for the development of mainstream cybersecurity models and methods	Student end-of-course evaluations	faculty	
B. It advances knowledge and promotes the arts through research, scholarship, and	C. To provide service to the Computer	6. Acquire knowledge on information technology, software systems, and network systems, which serves as the basis for the development of many emerging non-cryptographic methods for protecting security and privacy. 7. Study commonly-used cybersecurity tools and acquire hands-on experience through directed exercise and experiments. 8. Understand intellectual property law and cyber law. 9. Describe the synthesis of data and information for risk (vulnerability)			

Oakland University

Graduate Council

| creative activity; and C. It renders significant public service. | Science and Engineering profession. | assessment for the cyber infrastructure.
10. Integrate evidence-based practice into system reviews to design, implement, and evaluate plans of security.
11. Design, coordinate, evaluate, and deliver cybersecurity solutions in a timely and cost-effective manner.
12. Strategically plan on integrating cybersecurity within the overall improvement of the cyber infrastructure of the institution
13. Provide cybersecurity-related recommendation to higher-level system administrator in key decision-making process
14. Understand the role, scope, and limitations of cybersecurity administrators, while incorporating professional standards into practice.
15. Explore the evolving role of cybersecurity administrator in an institution.
16. Analyze vertical and horizontal leadership strategies of cybersecurity administrator in an institution.
17. Apply appropriate teaching/learning strategies to facilitate learning and education of colleagues on cybersecurity.
18. Develop personal goals for professional development and continuing education.
19. Demonstrate skills of mentoring the next generation of cybersecurity professionals.
20. Integrate relevant research findings into cybersecurity practice. | | | |

Oakland University

Graduate Council

APPENDIX H

Support Letters

State of Michigan
Merit Network
Oakland University Business School

Oakland University
Graduate Council

STATE OF MICHIGAN

RICK SNYDER
GOVERNOR

DEPARTMENT OF TECHNOLOGY, MANAGEMENT & BUDGET
LANSING

JOHN E. NIXON, CPA
DIRECTOR

November 1, 2013

Dr. Lunjin Lu, Associate Professor and Interim Chair
Department of Computer Science and Engineering (CSE)
Oakland University
2200 N. Squirrel Rd.
Rochester, MI 48309

Dear Dr. Lu,

As the CIO and the CSO of the State of Michigan, we hereby support the efforts of Oakland University's Computer Science and Engineering (CSE) department to develop a new academic program to confer a master's degree in cybersecurity.

The State of Michigan is especially committed to defending against cyber threats, one of the most significant homeland security challenges now facing the nation. For example, this year, as part of the National Governors Association's (NGA) ongoing effort to address cybersecurity, Michigan Gov. Rick Snyder briefed the Congress on governors' efforts to protect citizens and our economy against cyber-attacks. He released *Act and Adjust: A Call to Action for Governors for Cybersecurity*, a paper that provides strategic recommendations governors can immediately adopt to improve their state's cybersecurity posture.

A graduate degree would provide a valuable educational foundation and career credential for future managers and administrators, and would align with the Governor's vision to grow and develop a strong cybersecurity industry in the State of Michigan.

To help educate future leaders, and to help make the Internet a safer place, we wholeheartedly endorse the efforts of Oakland University to develop a graduate program in cybersecurity. We wish you continuing success in protecting the Internet in our state, our country and the world at large.

Sincerely,

David Behen, CIO
State of Michigan

Daniel Lohrmann, CSO
State of Michigan

Document version: October 30, 2015

Oakland University

Graduate Council

merit
NETWORK INC

1000 Oakbrook Drive
Suite 200
Ann Arbor, Michigan 48104-6794

Phone: 734-527-5700
Fax: 734-527-5790
www.merit.edu

November 1, 2013

Dr. Lunjin Lu, Associate Professor and Interim Chair
Department of Computer Science and Engineering (CSE)
Oakland University
2200 N. Squirrel Rd.
Rochester, MI 48309
(248) 370-2200
l2lu@oakland.edu

RE: Letter of Support, Master of Cybersecurity (MSC) Degree, Oakland University

Dear Dr. Lu,

Please support the proposal by Oakland University's Computer Science and Engineering (CSE) department to develop a new academic program to confer a master's degree in cybersecurity.
I am the President and CEO of Merit Network, Inc. Merit Network Inc., a non-profit corporation governed by Michigan's public universities, which owns and operates America's longest-running regional research and education network. Since its formation, Merit Network has remained on the forefront of research and education networking expertise and services. Merit provides high-performance networking solutions to Michigan's public universities, colleges, K-12 organizations, libraries, state government, healthcare, and other non-profit organizations. (For more details see www.merit.edu) Oakland University has been a member of Merit's Board of Directors for over 20 years.

Merit Network, Inc. is a recognized national leader in cybersecurity education. Just this past week we hosted the Michigan Cyber Range Exercise at the Michigan Cyber Summit 2013, hosted by Michigan Governor Rick Snyder. The Michigan Cyber Range, a collaboration between education, government and private Industry is unique in the world and is a great resource to Michigan's universities.

I myself have contributed to national security generally, and cybersecurity specifically. While a professor at the United States Military Academy, I helped start our Cyber Security academic program and was an active researcher in the field.

Please join us and others in Michigan to educate future cybersecurity leaders. Michigan can lead the nation in addressing this serious threat to our lives and livelihoods. Oakland University is a great institution and it can make an important contribution educating professionals at all levels, including the master's level. Again, please support the efforts of Oakland University to develop a master's program in cybersecurity.

Sincerely,

Donald J. Welch, Ph.D.
President and CEO

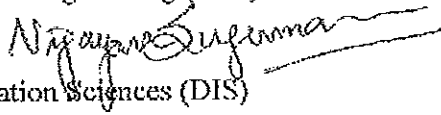Connecting Organizations, Building Community

Oakland University
Graduate Council

MEMORANDUM

January 14, 2015

TO: Lunjin Lu, Acting Chair
     Department of Computer Science and Engineering (CSE)

FROM: Vijayan Sugumaran, Chair
      Department of Decision and Information Sciences (DIS)

SUBJECT: Proposed Master of Science in Cyber Security – Support Letter

On behalf of the DIS department, I am writing this memo to express our support for the Master of Science degree in Cyber Security being proposed by the Department of Computer Science and Engineering. We greatly appreciate CSE's engagement of DIS department in the design of the Master's program in Cyber Security to obtain feedback, suggestions, and collaboration to avoid course duplication and to use the managerial/organizational body of knowledge coverage needed for the students in the program. The DIS department is supportive of the inclusion of the following 3 MIS courses in the basket of 10 courses students can choose from to complete the 20 credit hours needed beyond the core courses:

- MIS 641 – Information Systems Privacy (3 credits, Fall offering)

- MIS 643 – Intellectual Property and Public Domain in the Age of Remix (3 credits, Winter offering)

- MIS 680 - Special Topics Course: IT Governance, Business Continuity, and Risk Management (3 credits, To be numbered as a standing course offered each Fall)

As I mentioned in our last meeting, the DIS department is in the process of creating a concentration in Information Security Management (ISM) within our MSITM program. As part of this concentration, we would like to include some of the courses offered by your department. This

Oakland University
Graduate Council

will facilitate our students to pursue some technical aspects of Cyber Security, if they so choose. The primary focus of our ISM concentration will be on the policy, managerial and organizational aspects of Information Security and Assurance from a business perspective. It is our view that your Master of Science in Cyber Security program and our MSITM ISM Concentration complement each other and would serve a broad set of students. We welcome the opportunity to have closer collaboration between our two departments in the future and contribute to the success of the Master's Degree in Cyber Security as well as the MSITM Concentration in Information Security Management. Both programs are well positioned to provide the much needed education in Cyber Security and Information Security Management, which will lead to good career opportunities for our students.

Once again, the DIS department reiterates its full support for the Master of Science degree in Cyber Security being proposed by the Computer Science and Engineering Department at Oakland University.

Oakland University

Graduate Council

**OAKLAND
UNIVERSITY.**
——— ⟫ ———

Libraries

Knowledge Unbound

November 13, 2014

TO: Huirong Fu, Associate Professor, Dept. of Computer Science and Engineering

FROM: Shawn V. Lombardo, Associate Dean, University Libraries

RE: Library collection evaluation for Proposed MS in Cybersecurity

In developing this collection evaluation, I reviewed the draft proposal for the master's program in cybersecurity, as well as title lists of core journals and resources in the field. In addition, faculty from the Computer Science and Engineering department provided a list of their most important resources. Overall, the library is well-positioned to support the proposed program; only a few resources should be added to strengthen the collection. Below is a very brief description of the resources currently available, those that should be acquired, and a five-year cost estimate for additional library resources.

Journals and Conference Proceedings

Currently, the library subscribes to the IEEE Library, which includes all journals, proceedings and standards produced by the IEEE, as well as journals from IEE. The library also maintains online access to all Association of Computing Machinery (ACM) journals, magazines, transactions and conference proceedings through the ACM Digital Library. The library's current subscriptions to the Springer publisher package and to Elsevier's Science Direct and the ScienceDirect Freedom Collection, provide most of the journal and proceedings literature. Appendix A provides a list of the major journals and proceedings on cybersecurity; it is clear that the library's serials holdings in this area are strong. The library does recommend starting subscriptions to two important journals, highlighted in grey in Appendix A.

Indexes

To access the journal and conference literature in computer science, Kresge Library maintains subscriptions to a number of online indexes. The most important of these are *Scopus* (from Elsevier), *Compendex* (via Engineering Village), a bibliographic index to journals and conference proceedings in engineering and computing from 1969 to the present, and *Science Citation Index* (available online through the Web of Science platform), which indexes journals from 1980 to present in the sciences. The library also provides access to *Applied Science and Technology Abstracts*, which covers both academic and trade journal literature in science and technology, and Computer Database, an index to computer-related news and reviews. Other important resources include *Criminal Justice Abstracts*, which covers legal and ethical aspects of cybercrime and cybersecurity, and *ABI/Inform*, which

Oakland University
Graduate Council

provides full-text access to a number of MIS-related journals. No additional indexes are needed to support the program adequately.

Monographs and Reference Sources

The library purchases the complete collection of Springer eBooks each year, which includes the essential book series *Lecture Notes in Computer Science* and other book and book series, totaling more than 26,000 volumes related to computer science. Beyond the Springer eBook collection, the library only purchases a minimal number of books related to computer security. The monograph collection, then, should be supplemented with materials from other publishers.

Library Budget Request

Appendix B provides cost estimates for new resources needed to support the proposed master's-level program: two new journals and funding to purchase approximately ten new books on topics related to cybersecurity each year (average cost for a monograph is $108), with additional funds in year one to purchase important reference works and to support a small amount of retrospective collection development of previously-published but essential materials. Because this program will rely heavily on existing library resources, we have also included funding to cover anticipated annual inflationary cost increases for the library's current journals and research databases (historically averaging eight percent or more per year) in computer science. Without additional funding, the library cannot guarantee that we will be able to continue to subscribe to our current resources. Therefore, we ask that the library be given funds each year to assist us in continuing to subscribe to these necessary resources for computer science faculty and students.

C: Nancy Bulgarelli, Interim Dean, OU Libraries
        Kristine Condic, Library representative, Graduate Council

Oakland University

Graduate Council

300 Kresge Library | 2200 North Squirrel Road, Rochester, Michigan 48309-4484 (248) 370-2486 | Fax: (248) 370-2474 | library.oakland.edu

Appendix A

Top Cybersecurity Journals and Conference Proceedings		
Titles	**Publisher**	**OU Access**
Journals		
ACM Transactions on Information and System Security	ACM	yes
ACM Transactions on The Web	ACM	yes
Ad Hoc Networks	Elsevier	yes
Applied Soft Computing	Elsevier	yes
Computer Communications	Elsevier	yes
Computer Fraud & Security	Elsevier	yes
Computer Law & Security Review	Elsevier	yes
Computer Networks	Elsevier	yes
Computers & Security	Elsevier	yes
Designs, Codes and Cryptography	Springer	yes
IEEE ACM Transactions on Networking	IEEE/ACM	yes
IEEE Security & Privacy	IEEE IeL	yes
IEEE Transactions on Dependable and Secure Computing	IEEE IeL	yes
IEEE Transactions on Information Forensics and Security	IEEE IeL	yes
IEICE Transactions on Information and Systems	IEICE	no
IET Information Security	IEEE IeL	yes
Information Management & Computer Security	MCB University Press	1 year embargo ABI/Inform
Information Sciences	Elsevier	yes
Information Security Journal: A Global Perspective	Taylor & Francis	18 month embargo Business Source Premier
International Journal of Computer Science and Network Security	IJCSNS	yes - open access
International Journal of Information and Network Security	IAES	yes - open access
International Journal of Information Security	Springer	yes
International journal of information security and privacy	IDEA	yes
International Journal of Network Security	Inderscience	no
International Journal of Communication Networks and Information Security	Kohat UP	yes
International Journal of Cyber-Security and Digital Forensics	SDIWC	yes
IT Professional	IEEE IeL	yes
Journal in Computer Virology and Hacking Techniques	Springer	yes
Journal of Computer Security	IOS Press	9 month embargo ($1,375)
Journal of Cryptographic Engineering	Springer	no ($430)
Journal of Cryptology	Springer	yes
Journal of Grid Computing	Springer	yes
Journal of Information Security and Applications	Elsevier	yes
Journal of Network and Computer Applications	Elsevier	yes
Journal of Networks	Academy Publisher	yes
Journal of Strategic Information Systems	Elsevier	yes
Knowledge and Information Systems	Springer	yes
Lecture Notes in Computer Science	Springer	yes
Networks	Wiley	yes
Network Security	Elsevier	yes
Security and Communication Networks	IEEE IeL	yes
Wireless Networks	Springer	yes
Conference Proceedings		
ASIACRYPT - Theory and Application of Cryptology and Information Security	Springer	yes
CCS - ACM Conference on Computer and Communications Security	ACM	yes
CHES - Cryptographic Hardware and Embedded Systems	Springer	yes
CRYPTO - International Crytology Conference	Springer	yes
CSFW - Computer Security Foundations Workshop	IEEE	yes
ESORICS - European Symposium on Research in Computer Security	Springer	yes
EUROCRYPT - Theory and Application of Cryptographic Techniques	Springer	yes
NDSS - Network and Distributed System Security Symposium	open access	yes
S&P - IEEE Symposium on Security and Privacy	IEEE	yes

Document version: October 30, 2015

Appendix B
Proposed Five-Year Library Budget
to Support Proposed MS in Cybersecurity

	Year 1	Year 2	Year 3	Year 4	Year 5
Reference books/Monographs [1]	$ 2,000	$ 1,000	$ 1,050	$ 1,103	$ 1,158
Journals [2]	$ 1,805	$ 1,986	$ 2,184	$ 2,402	$ 2,643
Support for current library resources [1]	$ 1,000	$ 1,100	$ 1,210	$ 1,331	$ 1,464
Total	$ 4,805	$ 2,986	$ 3,234	$ 3,505	$ 3,800

[1] Reflects a 5 percent annual inflationary increase in years 3-5.

[2] Reflects a 10 percent annual inflationary increase in years 2-5.

Document version: October 30, 2015

Oakland University

Graduate Council

Typical Timeline for Approving Program Proposal

The following table contains critical points in the internal and external review process for program which is to begin in September. These dates assume that the process is not delayed by significant revisions.

Date	Event	Materials Needed
Sept. 2014	Review and approval of complete proposal by School of College	Completed proposal.
Oct. 2014	Informal review by Graduate Study	Completed proposal.
June 2015	Completion of Library Report.	Completed proposal.
Sept. 2015	Initial review of complete proposal by the Graduate Council. (2 readings)	Completed proposal.
Nov. 2015	Final reviews of revised proposal by the Senate Planning Review Committee and by the Senate Budget Review Committee.	Completed proposal.
Jan. 2016	Review by the University Senate (2 readings)	Final proposal and final cost estimate.
March 2016	Review by Board of Trustees.	Final proposal.
May 2016	Release by Provost to advertise	Final proposal
June 2016	Presentation to Academic Affairs Officers Committee of the President's Council of State Colleges and Universities	Final proposal.
Sept. 2016	Approval for program start	Release curriculum code