New Program Proposal

MS : Cybersecurity

Overview

Department: Gianforte School of Computing (GSoC)
College: College of Engineering (COE)
Academic Level: Graduate
Program Type: Academic

Please review this program for financial aid eligibility. Yes
Suggested Program Code: Cybersecurity
Degree Code: Master of Science (MS)
Program Title: Cybersecurity
Abbreviated Program Title: Cybersecurity

Effective catalog when new program will be available to students: 2021-2022

One Paragraph Description of Program:

The Gianforte School of Computing (GSoC) at Montana State University (MSU)—Bozeman proposes to offer the state’s first MS in Cybersecurity. The MS in Cybersecurity requires 30 post-baccalaureate credits and is designed for those who have earned a baccalaureate degree in Computer Science (CS) or a related program. The proposed degree caters to students with a STEM background and also provides a path to doctoral studies. Bachelor’s degrees in cybersecurity are almost non-existent, and the ones offered tend to focus on enhancing vocational and operational skills, not foundational CS or engineering knowledge. Thus, we find that the best alternative to create positive impact in workforce development in the state of Montana is to offer a rigorous academic program with options for certifications and options for further academic pursuit. The MS in Cybersecurity would require students to take the same number of credits and fulfill the same requirements as a traditional MS in CS. This program would allow MSU BS students to take cybersecurity courses as part of their electives while reserving up to 12 credits during the BS as they transition into an MS program through our seamless BS/MS (4+1) option. Students in either a BS or MS could supplement their studies by taking additional (optional) courses from MSU’s Gallatin College that provide specific cybersecurity certifications. Although certifications are not necessary in academic settings, they are a necessity in industry.

Need

To what specific need is the institution responding in developing the proposed program?

The proposed MS in Cybersecurity degree meets critical employment and institutional needs.

1. Employment. The advancement of cyber adversaries has led to increased frequency and complexity of cyber-attacks on everything from U.S. military systems to the U.S. voting infrastructure. By 2021 it’s
expected that 3.5 million cyber security positions will be unfilled [1] and there is great need to automate
cyber security as completely as possible. According to the Bureau of Labor Statistics (BLS), the median annual
wage of cybersecurity analysts is $98,350 [6]. The creation of this new MS degree will help meet workforce
demand in the area of cybersecurity in the state of Montana.
The development of the Advanced Research Laboratory (ARL) at Montana State University has been
successful at procuring significant funding from private industry, DHS and DoD. More than $20M has been
booked since 2018. A significant portion of these funds were appropriated to pursue research in developing
cybersecurity solutions in both the School of Computing and the Department of Electrical & Computer
Engineering at Montana State University. Coupled with local industry such as Hoplite [5], the State of
Montana finds itself in a position where a pipeline of qualified workers is not readily available nor is there
sufficient graduate students with the necessary background to conduct research in the area of cyber. To
complement a lucrative field, the development of qualified workers is needed, and this program will not only
generate qualified scientists, but also engineers with the necessary skills to address Montana’s and the
nation’s future cybersecurity needs.

2. Undergraduate student retention. For several years, undergraduate students have been asking for an
opportunity to specialize in a high demand area like cybersecurity. The Gianforte School of Computing has
responded by recruiting a tenure track professor that specializes in cybersecurity, has included modules that
address cybersecurity aspects in their software engineering classes, has began relationships with the Idaho
National Laboratories (INL), is anticipating Department of Homeland Security (DHS) funding that will have
room to hire undergraduates, and was successful in obtaining a National Science Foundation (NSF) REU grant
themed in Cybersecurity algorithms that will support 10 undergraduate students every summer from 2020-
2022. These activities will have a clear impact in undergraduate student retention.

3. Carnegie I ranking. To maintain this prestigious national ranking and take Montana State University to the
next level it is imperative to keep pace with relevant and highly lucrative programs. It is impressive that the
state of Montana has a post-secondary institution that has achieved R-1 status. Such a recognition attracts
and retains some of Montana’s brightest students and the country's top faculty teachers and researchers.

How will students and any other affected constituencies be served by the proposed program?

1. Undergraduate retention. As indicated above, undergraduate students will have higher rates of being
retained and succeed academically in these courses because they address a growing and high demand area.
The Department will revise the undergraduate curriculum to reflect the addition of new courses that can be
used in an undergraduate and graduate program. Dual listed courses (4xx/5xx) allow undergraduate and
graduate students to benefit from the same curricula with slightly higher expectations from 5xx courses.

2. This program will provide a balance between vocational and academic skills that enable the development
of rigorous academic skills in cybersecurity while allowing students the opportunity to earn additional
certifications through either MSU’s Gallatin College or UM’s Missoula College.

3. The program will serve the Montana workforce well. This entails alignment with certain standards in the
field. These standards include:
   • Alignment with the NICE framework [2]
   • Meets certification criteria from the National Security Agency/Control Security Service (NSA/CSS)
     and Department of Homeland Security (DHS) –Center of Academic Excellence Cyber Defense
     (CAE-CD) [3]
   • Alignment with curricula recommendations from ACM and IEEE [4].
   • Allows students to sit for a subset of certification exams (CompTIA exams)
What is the anticipated demand for the program? How was this determined?

The development of the Advanced Research Laboratory (ARL) at Montana State University has been successful at procuring significant funding from private industry, DHS and DoD. More than $20M has been booked since 2018. A significant portion of these funds were appropriated to pursue research in developing cybersecurity solutions in both the School of Computing and the Department of Electrical & Computer Engineering at Montana State University. Coupled with local industry such as Hoplite [5], the State of Montana finds itself in a position where a pipeline of qualified workers is not readily available nor is there sufficient graduate students with the necessary background to conduct research in the area of cyber. To complement a lucrative field, the development of qualified workers is needed, and this program will not only generate qualified scientists, but also engineers with the necessary skills to address Montana’s and the nation’s future cybersecurity needs.

We have also explored sites like Cyberseek [7] that clearly describe a need and demand for cyber positions in the state of Montana, with the latest statistics showing greater than 800 openings. At capacity, we anticipate 10 students in the MS program, graduating 4 to 6 per year.

Institutional and System Fit

What is the connection between the proposed program and existing programs at the institution?

The MS in Cybersecurity is synergistic with an array of current institutional programming across the MUS system. Further, the MS program described herein does not overlap nor duplicate any other program in the MUS system and addresses an academic need that goes beyond all other programs offered.

1. Gallatin College offers a certificate in cybersecurity in the Bozeman campus. Students in the MS program will be allowed to (optionally) participate in courses that can offer complementary training for potential certifications.

2. Great Falls College at Montana State University offers an Associate of Applied Science (ASS) program in cybersecurity. This is a two-year program focusing on IT related cyber topics.

3. Missoula College currently offers a certificate of technical skills in cybersecurity (CTS)

4. The University of Montana, in collaboration with Missoula College, and Excelsior College offer a BS in Cybersecurity for students with an AAS degree

How does the proposed program serve to advance the strategic goals of the institution?

This proposal is in alignment with Montana State University’s “Choosing Promise” strategic plan [https://www.montana.edu/strategic plan]. Specifically:

i. Goal 1.2. Expanding high quality graduate education. The MS in Cybersecurity program will increase the number of graduate students while serving the state of Montana in an area of crucial need. An MS in Cybersecurity supports Goal 1.2’s aim to increase the number of research doctoral degrees from 66 to 90 and the number of Master’s degrees from 566 to 650.

ii. Goal 2.1. Enhance the significance and impact of scholarship. The MS is Cybersecurity contributes directly to one of the four grand research challenges articulated in the strategic plan, namely “Securing
the future of Montana.” The MS in Cybersecurity will also help with the aims of increasing expenditures by 25% by 2022, and increasing the creation/authorship of the number of scholarly products by 10% each year.

iii. Goal 3.2. Grow mutually beneficial partnerships across Montana. The MS in Cybersecurity will help develop a capable workforce that is able to meet local, state, regional and national needs. Students, industry, and academics from all across Montana will benefit.

Program Details

MS in Cybersecurity Curriculum

Two tracks will be provided:

1. **Proposed Professional MS (courses-only) in Cybersecurity (Track: Infrastructure)**
   
   Requirement from prior degree (provisional courses if not in student’s background):
   
   - CSCI 112 (Programming in C)
   - CSCI 466 (Networks)
   - CSCI 460 (Operating Systems)

   Core:
   
   - CSCI 532, Algorithms, 3 credits
   - CSCI 538, Computability, 3 credits
   - CSCI 476, Computer Security, 3 credits
   - CSCI 576, Advanced Computer Security, 3 credits
     - New course developed by Dr. Travis Peters
   - CSCI 566, Advanced Networking, 3 credits
     - These courses would need revamping to include cyber modules. Dr. Mike Wittie
   - CSCI 4xx/5xx, Systems Security, 3 credits
     - Needs development (cryptography -applied or math based)
   - CSCI 4xx/5xx, Defensive Security (Cyber Defense, IA fundamentals, monitoring, event analysis, risk assessment), 3 credits
     - Needs development
   - CSCI 4xx/5xx, Software Engineering Cyber Systems (Reverse engineering, static analysis, vulnerabilities, weaknesses, SecDevOps), 3 credits
     - Needs development
   - CSCI 4xx/5xx, Penetration Testing, 3 credits
     - Needs Development
   - CSCI 4xx/5xx, Malicious Code Analysis, 3 credits
     - Needs development, but students must have OS, assembly experience, portable executable files.
     - Requires a lab that is isolated from the internet

2. **Proposed Professional MS (courses-only) in Cybersecurity (Track: Industrial Control Systems)**

   This track would typically allow students with a background in CE/EE to focus on ICS specializations. Some prerequisites in EEE (i.e. control systems) is necessary. Prerequisite courses could be taken as provisional.

   Requirement from prior degree (provisional courses if not in student’s background):
• CSCI 112 (Programming in C)
• CSCI 466 (Networks)
• CSCI 460 (Operating Systems)

Core:
• CSCI 532, Algorithms, 3 credits
• CSCI 538, Computability, 3 credits
• CSCI 476, Computer Security, 3 credits
• CSCI 576, Advanced Computer Security, 3 credits
  o New course developed by Dr. Travis Peters
• CSCI 566, Advanced Networking, 3 credits
  o These courses would need revamping to include cyber modules. Dr. Mike Wittie
• CSCI 4xx/5xx, Systems Security, 3 credits

Additionally,
• EELE 467, 468 (SoC FPGA I, and SoC FPGA II), 6 credits
  o These courses would need revamping to include cyber modules related to ICS
• EELE 528 (Advanced Controls and Signals), 3 credits
• EELE 4xx/5xx (Embedded Cybersecurity), 3 credits
  o Needs development

Describe the planned implementation of the proposed program, including estimates of numbers of students at each stage.

Implementation activities include:
• Complete curriculum development and approval
• Hiring 1 new TT faculty in the first two years,
• Hiring 1 new NTT faculty in the first two years focused on teaching,
• Hiring GRAs commensurate with levels of funding available to faculty.

If approved by May 2020, the MS in Cybersecurity would follow the following implementation milestones:

Facilities Milestone (Must be reached before Launch Milestone)
• Space is identified
• Funds are identified to furnish the room
• Funds are identified for recurring costs

Faculty Milestone (Must be reached before Course Milestone)
• Faculty with the proper expertise to develop and teach the minimal set of new courses are on staff

Course Milestone (Must be reached before Launch Milestone)
• A minimal set of new courses necessary to offer the degree are approved and in the course catalog

Launch Milestone
• The degree is available to students

Program Learning Outcomes
1. Expertise in Cybersecurity Foundations
• Develop substantive mastery of major concepts, theoretical perspectives
• Develop a deeper understanding of cybersecurity solutions in one of two areas of choice: IT or Industrial Control Systems (ICS)
• Develop substantive mastery of operational skills in lab setting environments
• Show an ability to understand and evaluate various tools used in the field

2. Expertise in analytic approaches and methods
• Show a foundational understanding and ability to evaluate different solutions in traditional IT and industrial control systems scenarios
• Analyze and interpret complex problems in practice using tools of the trade.
• Effectively communicate complex information and research results orally and in writing.

3. High ethical standards in the application of cybersecurity practices
• Participate in professional development seminars
• Practice white hacking skills

Resources

Will additional faculty resources be required to implement this program? Yes

Please Explain:

The GSoC will require the addition of at least two faculty in cybersecurity. This is necessary to meet the certification standards of CAE and the need to staff additional courses. The GSoC faculty expertise in Cybersecurity consists of 2 tenure/tenure track professors, we also seek to hire 2 additional faculty (1 TT, 1 NTT) to help with the demands of the new curriculum. At capacity, we expect 2 students/year to be supported through GTAs, 2/year to be supported through grant funded GRAs, and 4-6/year (most half-time, some full-time) to be self-funding or funded through private industry partnerships. Stipends for the GTAs are anticipated to be commensurate with current levels in the GSoC for 10 months ($1,200 - $1400/month) with 6 credits of tuition.

Are other, additional resources required to ensure the success of the proposed program? Yes

Please Explain:

Cybersecurity programs require isolated laboratory facilities that can handle experimentation with malware for analysis purposes. There exist some options, but the best solutions are typically commercial and offer a fully functional cyber range. The adoption of a cyber range requires the need of staff to oversee the daily administration of the isolated network and the provisioning of its servers to serve all classes.

Assessment

How will the success of the program be measured?

The success of the MS in Cybersecurity will be assessed by the following:

1. Successful achievement of Program and individual course learning outcomes
2. Students begin graduating from the program within 3 years of program offering

Process Leading to Submission

Describe the process of developing and approving the proposed program. Indicate, where appropriate, involvement by faculty, students, community members, potential employers, accrediting agencies, etc.
The process leading to this Level II submission has been through two years of planning. We have worked with Idaho National Laboratories (INL) who shared their cybersecurity curriculum for the Naval 10th fleet and provided their feedback, we have worked with industry advisors, notably Will Peteroy, an entrepreneur, founder of Gigamon IT security company, and current advisor at ARL. Further, Dr. Izurieta has participated in many cybersecurity education conferences to assess programs and resources necessary to bootstrap a successful program.

During 2019, ARL business development helped MSU obtain $14M for FY20 approved appropriations that are tied to the Applied Research Lab (ARL). Of these funds, $3M are slated for cybersecurity research. These opportunities prompted the GSoC to begin preparing a program to meet the needs of an MS in cybersecurity. After meeting with advisors and creating an initial strawman proposal, Dr. Izurieta and Dr. Brock LaMeres from the Electrical Engineering department worked with the GSoC director (Dr. Paxton), and the Dean of the COE (Dr. Gunnink) to review the details.

Our Intent to Plan went to OCHE, where it was well received. After meeting with the MSU Provost (Dr. Mokwa), VP of Research (Dr. Carter) and the new dean of the graduate school (Dr. Ogilvie), we are now moving forward with this Level II proposal to first be vetted through MSU's institutional review process; and based on these results, this Level II will be amended if necessary and move forward to the BOR consideration.

References