UNIVERSITY OF MARYLAND

Honors College
Anne Arundel Hall
College Park, MD 20742
301-405-6771

To: Dean Donna Hamilton
Associate Provost for Academic Affairs and Dean for Undergraduate Studies

From: Professor William Dorland
Honors College Director

Date: September 10, 2012

RE: Advanced Cybersecurity Experiences for Students (ACES) Proposal
to the Provost's Living and Learning Oversight Committee

On behalf of the ad hoc committee tasked to work out the details of an Honors College ACES program, it is with great pleasure that I submit the first component of the ACES academic proposal to you for consideration by the Provost's Living and Learning Oversight Committee.

We would be most grateful if the Committee would consider ACES I, the freshman-sophomore Honors College living and learning program that is scheduled to begin in fall 2013.

This proposal also contains a description for ACES II, an upper-level program in cybersecurity, designed for third and fourth year students. We are not asking for a review of ACES II at this time. We present them in a single proposal as we anticipate that the majority of students who are admitted to ACES I as freshmen will continue through the entire four years of programming. Therefore, we wanted you to see the entire curriculum as it is currently envisioned.

Advanced Cybersecurity Experience for Students (ACES)
University of Maryland
Honors College
Maryland Cybersecurity Center (MC^2)
Northrop Grumman
A. James Clark School of Engineering
College of Computer, Mathematical, and Natural Sciences

Director:
Associate Professor Michel Cukier, mcukier@umd.edu, (301) 314-2804

The University of Maryland is poised to offer a full four-year undergraduate program in cybersecurity called Advanced Cybersecurity Experience for Students (ACES). The purpose of the new program is to educate future leaders in the field of cybersecurity by offering the first two-year living-learning undergraduate program in the nation exclusively for Honors students and a complementary two-year advanced program of study in cybersecurity. Students will have access to rigorous, intensive, hands-on learning experiences throughout their undergraduate careers. Through sustained engagement with business and industry, ACES students will be highly talented cybersecurity scholars with practical skill sets that are in high demand by corporate and government organizations.

Rationale

Cybersecurity is a field of growing importance that intersects with many disciplines, and requires a workforce with a range of talent, backgrounds, and expertise to meet current and future workforce demands. There is a shortage of adequately prepared students to fill existing cybersecurity employment opportunities in industry and government. As a result, employers are still investing resources to prepare recently hired graduates with new skill sets that they believe that university curricula should provide. The new ACES program seeks to: a) increase the persistence of students in STEM fields; b) develop deeper engagement with industry through the deployment of research-immersion experiences that provide high engagement in STEM degree fields and prepare students to immediately enter the cybersecurity workforce; and c) develop a new prototype for preparing leaders in an emerging, interdisciplinary field that requires practical application and real world experience.

Background

The UMD ACES program was initiated with a gift of $1.1 million from Northrop Grumman as part of the Business Higher Education Forum initiatives announced in June 2012. This program will enable academically talented undergraduates to study cybersecurity problems and issues. The students will have opportunities to interact with and learn from faculty members, graduate students, and industry and government professionals developing cybersecurity technologies, policies, and strategies. The program will draw on experts from computer science, engineering, and such wide-ranging fields as business, public policy, and social sciences to develop a new cadre of “cyber-enabled” graduates. For a company like Northrop Grumman, whose cybersecurity practice encompasses business units targeting a wide range of sectors (e.g., the financial and healthcare industries), this program will produce graduates with diverse academic and experiential backgrounds who could effectively “speak” to those sectors.

Overview

As the first Honors Undergraduate Program in Cybersecurity in the United States, ACES is designed to not just introduce academically talented students to the technical and non-technical aspects of this important emerging field, but is designed to set the foundation for them to be future leaders in the field of cybersecurity. The Cybersecurity curriculum consists of two linked academic programs over the course of four years, a freshman-sophomore living-learning program leading to Honors College Citation in Cybersecurity, (ACES I, 14 credits) and an upper-level course of study in cybersecurity (ACES II, 16-17credits). Each class cohort will be comprised of approximately 40-45 ACES students.

Students who are interested in pursuing a career in cybersecurity will usually complete both the Honors Citation (ACES I) and the upper-level course of study in Cybersecurity (ACES II) over the course of four years, in combination with an academic major. It is assumed that the majority of students who are admitted to ACES I as freshmen will continue in ACES II. However, it is possible for a student to complete just the ACES I or ACES II portion of the program separately. This will allow a small number of ACES I students to complete the Honors Citation and then move to other areas of academic interest without completing ACES II. It will also allow a small number of highly-qualified students (who may or may not be in the Honors College) and who are likely majoring in computer science or engineering, to join the highly selective program in cybersecurity beginning in the junior year through a competitive admissions process.

ACES I: Like other Honors College living-learning programs at the University of Maryland, the freshman-sophomore ACES I program will be a *living-learning experience,* where students live together in a cohort-based program in the first two years, working closely together inside and outside of the classroom. The curriculum emphasizes hands-on and experiential learning and focuses on the breadth of the emerging discipline of cybersecurity. It also takes full advantage of Washington DC area companies and government agencies involved in cybersecurity. A co-curricular and pre-professional program related to cybersecurity will complement the academic experience. It is expected that students who wish to join ACES II afterward will be majoring in or taking prerequisite coursework in CMSC or ENGR in addition to the ACES I coursework.

ACES II: The upper-level program in cybersecurity focuses on advanced technical coursework and advanced experiential learning opportunities for students who are capable of and interested in gaining advanced professional training in cybersecurity. It is most suited for but not restricted to students who are majoring in computer science or engineering. Students in ACES II will also have the opportunity to participate in ACES I as peer mentors, tutors, and advisors. ACES II will include regular interactions with corporate and governmental leaders in cybersecurity, who will serve as both mentors and professional contacts. It is anticipated that most students who participate in ACES I will progress to ACES II. Admission to ACES II is contingent upon completion of prerequisite coursework in CMSC and/or ENGR that is not part of the ACES I curriculum. Especially talented undergraduates who were not part of ACES I may apply to join ACES II beginning in the junior year.

Honors College Resources: Students in ACES I and ACES II will have access to Honors (HONR) seminars and departmental H-Version courses throughout their undergraduate careers and will enjoy all other rights and privileges of membership in the Honors College. Direct entry ACES II students will become Honors College students, just as Departmental Honors students become Honors College students, when they join the program, whether or not they were admitted to Honors College earlier in their academic careers.

Experiential program: The program strongly emphasizes experiential learning by providing ample opportunities for individual and group research projects as well as academic term and summer internships. This will enable first-hand exposure for students to the needs and demands of industry in the cybersecurity field. Moreover, this will provide the participating industrial partners hosting interns with a unique recruitment pipeline of top-notch, unparalleled talent. The unique nature of the program will provide opportunities for a range of flexible hands-on learning experiences that could be tied to and reinforce classroom learning. Furthermore, eligible ACES interns may have the opportunity to initiate the security clearance process. Acquiring a security clearance could augment the likelihood of ACES interns working in the industry after graduation.

Additional Opportunities: After the first semester, ACES students will be encouraged to apply for a spot on Maryland's competitive Cybersecurity Team coached by the Security and Policy Office of the Division of Information Technology and supported by the Maryland Cybersecurity Center (MC2). This team participates in a variety cybersecurity competitions. ACES students will also take a leadership role in educating the entire university Community about basic cyber hygiene recommendations. These and other opportunities may include academic credit in HACS278 and HACS478.

Timeline: ACES I will launch with the first cohort of students in fall 2013. ACES II will launch no earlier than fall 2014.

Facilities: The ACES headquarters will be located in Prince Frederick Hall (beginning in fall 2014). (The first cohort will be housed in LaPlata Hall in 2013-14). Prince Frederick Hall will include offices, meeting and entertaining spaces, specially designed laboratory space, and state of the art classrooms. ACES I students will reside in Prince Frederick Hall. Because Prince Frederick Hall is currently under construction, the ACES leadership team had an opportunity to provide input to some of the technical building specifications.

Academic Program

The academic curriculum for the ACES program is designed to meet the following learning outcomes for students:

1. Students will demonstrate the ability to apply advanced technical skills required to approach and resolve problems in cybersecurity through upper-level cybersecurity-related coursework in computer science, engineering, and related disciplines.

2. Students will demonstrate an understanding of and be able to apply the broad, interdisciplinary aspects of cybersecurity, such as the political, legal, and economic ramifications of local and global cybersecurity advances and decisions.

3. Students will demonstrate an understanding of the range of professional opportunities available in cybersecurity as a result of first-hand interactions with cybersecurity professionals in the private and public sectors though formal presentations, site visits, informal meals, topical and professional workshops.

4. Students will demonstrate hands-on experience and problem solving skills in cybersecurity through advanced coursework, experiential learning, and research.

Year	Courses	Description	Cr.	Gen. Ed. (Proposed)
	ACES I - FIRST AND SECOND YEAR CURRICULUM Honors College Citation in Cybersecurity (14 credits)			
1st yr	HACS 100 Foundations of Cybersecurity I (2 cr)	Fall	2	
	HACS 102 Foundation of Cybersecurity II (3 cr)	Spring	3	SIP
1st & 2nd yr	HACS 208 Seminar in Cybersecurity: Seminar topics listed below are initial offerings. Normally, there will be one section of HACS 208 offered each semester (22 seats/section.)	Choose 2	6	
	A. Cyberspace - Current Policy, Legal Issues, and Implications (3 cr)			HS, I-Series
	B. Cybersecurity Global Economic and Political Impacts (3 cr)			HS, I-Series, D-UPS
	C. Cybercrime - The Crime, The Hacker, and the Victim (3 cr)			HS, I-Series
2nd yr	HACS 278 Cybersecurity in Practice (3 cr) Individual or Small Group Technical Experiential Learning in Cybersecurity (by permission only; offered during regular term and during summer/winter)		3	SIP or Exper.Lear.
		TOTAL CREDITS	**14**	

	ACES II - THIRD AND FOURTH YEAR CURRICULUM (16-17 credits) **(Prerequisite coursework in CMSC and/or ENGR or equivalent is required for admission to ACES II.)**			
3^{rd} and 4th yr	HACS 408 Cybersecurity Professionals Colloquium Series (Offered about every two weeks, topics include cybersecurity threats, entrepreneurship and innovation in cybersecurity, cybersecurity policy)		1 (repeat-able to 2 cr)	
3rd or 4th yr	Upper-Level Technical Coursework in Cybersecurity (Courses from which students can choose may change from year to year.)	Choose 2	5-6	
	ENEE 359R Intermediate Topics in Computer Engineering: Reverse Engineering (2 cr) (Prerequisites: ENEE150 or CMSC132 and ENEE350)			
	CMSC 414 Computer and Network Security (3 cr) (Prerequisites: CMSC sequence including MATH141, CMSC131, CMSC132, CMSC216, CMSC250, CMSC330)			
	ENME 442 Information Security (3 cr) (Prerequisites: Senior standing or permission of instructor)			
	HACS 404 Tools for Information Security (3 cr) (Prerequisites: CMSC414 or ENME442 or permission of instructor)			
	CMSC 417 Computer Networking (3 cr) (Prerequisites: CMSC sequence including MATH141, CMSC131, CMSC132, CMSC216, CMSC250, CMSC330, CMSC351)			
	CMSC 498B Secure Maryland (3 cr) (Prerequisites: CMSC414, CMSC417 or permission of instructor)			
3rd or 4th yr	Capstone in Cybersecurity	Choose 3	9	
	HACS 478 Experiential Learning in Cybersecurity (3 cr)			SIP or Exper.Lear.
	HACS 479 Research in Cybersecurity (3 cr)			SIP or Exper.Lear.
	HACS 208 Seminar in Cybersecurity (3 cr) (Students who did not participate in ACES I must take at least 3 credits of HACS208. A maximum of 6 credits of HACS208 can be applied toward the minor.)			See above
	TOTAL CREDITS		**16-17**	

HACS 100 Foundations of Cybersecurity I (2 cr)

Prerequisite: Admission to ACES I.

The goal of this course is to provide an introduction to cybersecurity without assuming a prerequesite knowledge. The course's topics include: how to manage cybersecurity, the main security models and how to evaluate cybersecurity, and how security is implemented in operating systems (Unix and Windows), databases, software, networks, web, and mobile devices. Security approaches will be classified into prevention, detection and tolerance. Both the defense and the attacker perspectives will be addressed. HACS 100 is offered for two credits to ensure that ENGR majors can fit it into their schedules in the first term.

HACS 102 Foundations of Cybersecurity II (3 cr)

Prerequisite: HACS 100.

The goal of this course is to provide a hands-on project-based introduction to several aspects of cybersecurity based on the concepts introduced in HACS 100 and presented during the first lectures of HACS 102. The course learning objectives will include understanding the basic premises of the cybersecurity experience through the planning, investigation, design, development, implementation and evaluation of a security solution, within the context of a team setting.

HACS 208 Seminar in Cybersecurity (3 cr)

It is anticipated that successful sections of HACS208 will be relatively stable and repeated year after year. However, in the first few semesters/years there is the possibility of new topics as the ACES faculty and curriculum develop.

A. Cyberspace - Current Policy and Legal Issues and Implications (HS, I-Series)
This course explores the current pressing questions in cybersecurity policy and law. Topics to be addressed will include implications of technology on privacy, cybersecurity legislation, international agreements, codes of conduct and treaties, data breach notification, ethical and moral behavior online, as well as an overview of the implications of economic and state-sponsored espionage.

B. Cybersecurity - Global Economic and Political Impacts (HS, D-UPS, I-Series)
This course explores the main concepts in economics and political science and will ask how they apply to cybersecurity. This course will allow students to better understand cyberthreats and how to mitigate them once having identified the main forces/models driving economical and political decisions.

C. Cybercrime - The Crime, The Hacker, and The Victim (HS, I-Series)
This course explores technical and social aspects of cybercrime and asks questions about the relevant theories and tools that best enable scientific exploration of this phenomenon. How are definitions of cybercrime and typologies determined? The course includes a discussion of the hacker, the victim and the IT manager, a review of various theories of crime causation, and an consideration of the relevance of these theories in the context of cyberspace.

HACS 278 Cybersecurity in Practice

Prerequisite: HACS 100, HACS 102 and permission of program; 1-3 credits. Not Repeatable. Semester-long experiential learning with an agency or company with a signed contract between the student, site supervisor, and Cybersecurity program director.

Initially experiential learning will include options such as an internship with a corporate partner such as Northrop Grumman or with a government partner to the Maryland Cybersecurity Center. It might also include an internship with OIT on campus, a study abroad/research opportunity related to cybersecurity*, or a leadership role on the Maryland Cybersecurity Competition Team. Each experience will be reviewed and approved by the ACES Director.

*Opportunities for students to study cybersecurity abroad may initially include experiences through existing partnerships with ENSIB, a French engineering school that awards a degree in cybersecurity engineering, or in Morocco, which currently has the highest percentage of Internet users in Africa and some interesting and unique opportunities at two universities to study cybersecurity.

HACS 408 Cybersecurity Professionals Colloquium Series

This seminar series will be offered about every two weeks by cybersecurity professionals. Topics include how to combat cybersecurity threats, entrepreneurship and innovation in cybersecurity, cybersecurity policy, how to become a leader in cybersecurity.

ENEE 359R Software Reverse Engineering

Prerequisite: ENEE 150 or CMSC 132 and ENEE 350.

This course provides in-depth, hands-on training for reverse engineering tools, including the IDA Pro disassembler, the Wireshark network protocol analyzer, debuggers, and binary tools. Students will become familiar with the x86 instruction set through both assembly programming and disassembly. Class exercises include revealing back doors and exploiting buffer overflows. Each student will develop a network-based application and in turn reverse engineer and exploit one of their peer's completed applications.

CMSC 414 Computer and Network Security

Prerequisite: CMSC sequence including MATH 141, CMSC 131, CMSC 132, CMSC 216, CMSC 250, CMSC 330.

Introduction to the topic of security in the context of computer systems and networks. Identify, analyze, and solve network-related security problems in computer systems. Fundamentals of number theory, authentication, and encryption technologies, as well as the practical problems that have to be solved in order to make those technologies workable in a networked environment, particularly in the wide-area Internet environment.
(Spring 2012: http://www.cs.umd.edu/~jkatz/security/s12/)

ENME 442 Information Security

Prerequisite: Senior standing or permission of instructor.

One third of the lectures will focus on the fundamentals of computer security like identification, authentication, access control, and security models. The second third will focus on the practice of computer security using Unix and Windows NT as case studies. Some virus attacks will also be studied. An overview of security evaluation will be provided. The last third will be dedicated to security in distributed systems including network security and World Wide Web security.

HACS 404 Tools for Information Security

Prerequisite: CMSC 414 or ENME 442.

Students will perform host- and network-based security tasks relating to security, investigation, compliance verification and auditing using a wide selection of commonly used tools on both Windows and Linux platforms, with emphasis on open source tools.

CMSC 417 Computer Networking

Prerequisite: CMSC sequence including MATH 141, CMSC 131, CMSC 132, CMSC 216, CMSC 250, CMSC 330, CMSC 351.

Computer networks and architectures. The OSI model including discussion and examples of various network layers. A general introduction to existing network protocols. Communication protocol specification, analysis, and testing.
(Spring 2012: http://www.cs.umd.edu/class/spring2012/cmsc417/)

CMSC 498B Secure Maryland - pen testing

Prerequisite: CMSC 414, CMSC 417 or permission of instructor.

This course is about assessing the security of computer systems. It has three main goals:
1.To teach students the art of penetration testing, with a focus (though not exclusive) on exploiting vulnerabilities in web applications.
2.To teach students about ethical hacking, i.e., the non-technical aspects of penetration testing, including rules of engagement, how to protect confidential data, etc.
3.To harden the computer systems of the University of Maryland, College Park, by using them as a target of penetration tests. Students may probe Maryland systems, assess their vulnerabilities, and ultimately attempt to exploit them. Students report successful exploits to system owners and work with those owners to fix the problems.
(Spring 2012:
http://www.cs.umd.edu/~mwh/securemd/CMSC498B__Secure_Maryland/Home.html)

HACS 478 Experiential Learning in Cybersecurity

Prerequisite: Admission to ACES II Minor and permission of program; 1-6 credits. Repeatable to 9 credits. Individual or group experiential learning opportunity with an agency or company with a signed contract between the student, site supervisor, and Cybersecurity program director.

Initially experiential learning will include options such as an internship with a corporate partner such as Northrop Grumman or with a government partner to the Maryland Cybersecurity Center. It might also include an internship with OIT on campus, a study abroad opportunity related to cybersecurity, or a leadership role on the Maryland Cybersecurity Competition Team. Each experience will be reviewed and approved by the ACES Director.

HACS 479 Research in Cybersecurity

Prerequisite: Admission to ACES Ii Minor and permission of program; 1-6 credits. Repeatable to 9 credits. Research and data collection under individual faculty supervision, leading to a publication-quality written research report or presentation.

Due to the interdisciplinary nature of the ACES program, individual and group research projects will normally include an interdisciplinary component and will normally be supervised by at least one faculty member affiliated with MC2. Prior approval of all research proposals by the faculty mentor(s) and the ACES Director will be required for all research projects.

Experiential Program

Industry will play a vital role in the success and broader impact of the ACES program. For example, the close partnership between ACES and Northrop Grumman will include a deep and sustained level of engagement between the students, faculty, and industry representatives. With an emphasis on deepening learning, increasing student persistence in STEM, and aligning undergraduate learning with workforce needs, industry-based activities in the program will include:

- co-developing new courses to help ensure that the competencies needed by industry are addressed;
- serving as guest lecturers in specific classes and courses throughout the ACES curriculum;
- serving on a highly engaged industry advisory board specific to the program;
- providing real-world problems that student teams are tasked to address;
- developing multi-year internship programs directly tied to students' course work; and,
- contributing advisors and mentors for the capstone projects.

The ACES program offers Northrop Grumman, the founding sponsor, a unique opportunities to not only invest in students' success, but to develop long-term relationships with them, potentially leading to employment. Key federal agencies involved in cybersecurity, such as the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST), which leads the National Initiative for Cybersecurity Education, will be invited to serve in an advisory capacity as well.

Admission to ACES I and ACES II

Admission to ACES I: The ACES I curriculum is designed to introduce a small group (40-45 per cohort) of academically talented Honors College freshmen who have an interest in cybersecurity to the hands-on technical and non-technical aspects of the field beginning in the freshman and sophomore years. This program takes full advantage of the cybersecurity expertise at the University of Maryland as well as our partnerships with Northrop Grumman and our geographic proximity to experts in the National Security Administration, Department of Defense, and other private companies and government agencies in the Washington DC area with cybersecurity expertise.

High school seniors who are interested in cybersecurity should apply to the University of Maryland by the November 1 deadline for best consideration for the Honors College admission. All students who are admitted to the Honors College in January are then invited to express a preference for Honors College Living-Learning Programs, including the ACES Living-Learning Program. To be considered for the ACES Living-Learning Program students should have an outstanding academic record in mathematics and science courses in high school and should be taking or have taken the **AP Calculus BC** course. Since not all high schools offer AP Computer Science, it is not required. However, students with a strong interest and some first-hand experience with computer languages will be the best-suited for the ACES I Program.

Admission to ACES II: ACES II is designed for students who already have a good working knowledge of computer science (e.g., computer programming, computer systems, programming languages, and algorithms) and who are interested in studying the more advanced hands-on technical aspects of cybersecurity. ACES II combines advanced technical coursework in computer science/engineering with extensive opportunities for hands-on experiential learning and research opportunities in cybersecurity. If a student wishes to join ACES II he/she should begin taking the introductory computer science sequence (CMSC 131, CMSC 132, CMSC 216) or the parallel sequence in electrical engineering (ENEE 140, ENEE 150 or equivalents) in the first and second years of college.

Admission to ACES II requires:

- Completion of the Honors College Citation in Cybersecurity (ACES I), a 3.2 overall GPA, completion of the introductory CMSC or ENGR course sequence, and the recommendation of the ACES Program Director

or

- Completion of CMSC 216 and CMSC 330 (or equivalent) with a grade of B or higher (or equivalent experiences) and a 3.5 overall GPA or higher and the recommendation of the ACES Program Director

Estimate of demand: Based on the proposed majors of incoming Honors College freshmen in fall 2012, 64% have chosen STEM majors (28% will choose majors in CMNS (including 5% in computer science), 36% will choose majors in ENGR). This is a large potential audience for ACES. The ACES academic program is designed to take full advantage of the technical strengths these students will have and to focus on interdisciplinary and experiential components that build on these strengths. The CMSC courses related to cybersecurity (CMSC 414, CMSC 417) are already very popular offerings.

Faculty Participation and Teaching

HACS 100 and **HACS 102** will be taught by the Cybersecurity Director, Associate Director, or a campus faculty member affiliated with the MC2.

HACS 208 sections will be taught by BSOS/START/PUAF campus faculty (as an overload or buyout) or by highly qualified and credentialed adjunct faculty who are professional cybersecurity experts in the Washington DC area and hired by the ACES Director on the ACES budget.

HACS 278, 478, and 479 experiential and research learning opportunities will be overseen by the Director of the ACES Program and implemented by the Associate Director and Coordinator of ACES who will assemble personal contacts and a database of experiential opportunities and who will advise individual ACES student, approve individual proposals on a semester-by-semester basis, communicate with site/research supervisors, and submit experiential learning grades for students.

Upper Level Technical Coursework in Cybersecurity will be offered by the academic departments, especially CMSC and ENEE. It is anticipated that the vast majority of ACES II students who enroll in these courses will already be majoring in these academic programs, so it should not impact departmental enrollments in these courses. In the event that a non-departmental ACES II students who is qualified to take a given ACES II course requests permission from the department, these requests will be handled on a case-by-case basis by the Undergraduate Director for the Department and the ACES Director.