Maryland Cybersecurity Center (MC2) Summer Newsletter

HONORS PROGRAM IN CYBERSECURITY ANNOUNCED

MC2 TO PLAY LEADING ROLE IN CURRICULUM & PROGRAM DEVELOPMENT

With support from MC2 and the Honors College, on June 11, UMD and Northrop Grumman announced a landmark honors program designed to educate the next generation of advanced cybersecurity professionals.

This unique program, the Advanced Cybersecurity Experience for Students (ACES), will immerse undergraduate students in all aspects of the field to deliver a superior education and help meet growing workforce needs in the state and nation. The program will start in the fall of 2013.

ACES will engage an elite, diverse group of students—

majors in computer science, engineering, business, and the social sciences— in an intensive living-learning environment. ACES will develop uniquely skilled cybersecurity leaders highly sought after by industry and government.

Each ACES student will have the option to intern with Northrop Grumman as part of this program. Students will participate in an advanced, interdisciplinary curriculum, and will interact directly with faculty, industry, and government mentors. Northrop Grumman is providing a grant of $1.1 million to launch the program, and UMD will match that amount.

MC2 will be playing a leading role in the development of the program's curriculum and its implementation. About 45 students will be selected for the ACES program each year.

"We are fully committed to developing solutions to help eliminate the nation's shortage of critical STEM-educated talent and by partnering with UMD and MC2, we will address workforce challenges in the increasingly important field of cybersecurity."

-Wes Bush, CEO, Northrop Grumman Corporation

NORTHROP GRUMMAN

DIRECTOR'S DIGEST: PROF. MICHAEL HICKS

DR. MICHAEL HICKS:

- Director, Maryland Cybersecurity Center
- Associate Professor in Computer Science
- Ph.D. University of Pennsylvania

Research Interests:

- Dynamic Software Updating
- Software Reliability

It was an eventful year for MC2, as you can see in this newsletter. We are proud of the corporate and academic connections we made, the programs we started, the research we have undertaken, and the wonderful faculty we recently hired. I am very thankful for the support of my colleagues at UMD, and of our corporate partners.

I'd like to use this space to inform you of one specific activity we are particularly proud of: in the spring 2012 semester, Rob Maxwell, of the Division of Information Technology, and I co-taught a course on penetration testing, called "Secure Maryland."

Our goals were for students to gain an understanding of

vulnerabilities in computer systems (primarily web applications), the tools and techniques for performing penetration testing, (cont.)

DIRECTOR'S DIGEST, CONTINUED

operating procedures of a penetration testing team in a professional setting, and, rules of ethical hacking. To augment class-room-style teaching, students were permitted to target real systems running on the UMD campus, which has several advantages:

1) Students train on real data, and are challenged to use creativity in the face of an unknown outcome—there is no assured "right answer."
2) The notion of ethical hacking was not abstract, but concrete: students had a real business contract between themselves (the pen tester) and the target owner (the campus), and must respect what actions are—and are not—permissible.
3) With each vulnerability found (and fixed), UMD's computer systems become more secure.

Students also learned more about why vulnerabilities were present and how pervasive they were, and thus had more data to help prevent future recurrence.

Safeguards were put in place to mitigate the risk of unhappy outcomes. For example, students were required to perform tests from a special network set up by the course administrators, where the network's traffic was monitored and it only reached public-facing machines. Students were only allowed to probe—not penetrate—systems at first. Critical systems were always out of bounds. Deeper tests were permitted after an operating agreement with system owners and/or permission from course instructors.

In the end, Secure Maryland was extremely successful. The seven students who took it learned a lot and helped make the campus more secure. I would encourage others to consider a course like this. In a sense, it adheres to the "teaching hospital" model: learning with real data, facilitating meaningful and impactful outcomes.

> **"Students were asked and expected to find real problems, and fix them. And they did, by the hundreds."**
>
> *-Professor Michael Hicks on the results of "Secure Maryland," a class he co-taught with Rob Maxwell this past spring semester.*

NEW MC2 FACULTY: ELAINE (RUNTING) SHI

> **"Nick and Elaine are fantastic researchers and educators.**
>
> **Their research is top-notch, and their energy will take MC2 to a new level."**
>
> **-Prof. Michael Hicks, Director, Maryland Cybersecurity Center**

Elaine (Runting) Shi is a new member of the faculty affiliated with the Maryland Cybersecurity Center. She joined the Computer Science Department in August 2012 as an Assistant Professor.

Elaine is interested in privacy, applied cryptography, system security, trusted computing, as well as security and privacy technologies for cloud computing and ubiquitous computing.

In 2008, Shi obtained a Ph.D. at Carnegie Mellon University. From 2008-2010, Elaine worked at PARC, a Xerox company, in Palo Alto, California.

Shi was a research scientist at UC-Berkeley from 2010-2012. For more information on Elaine and her research, please visit: **http://www.cs.umd.edu/~elaine/**

Dr. Elaine Shi will join MC2 in August 2012

CATCHING UP WITH MC2 FACULTY: NEWS AND NOTES

Dr. Jeff Foster: On July 1, Jeff was appointed as the Associate Chair for Graduate Education in the Computer Science Department. Jeff was also recently the recipient of a Google Research Award for a project entitled "*Using Distortion to Protect Privacy on Android.*"

Dr. Sennur Ulukus: Sennur was a featured lecturer at the 2012 European School of Information Theory. She lectured on Information Theoretic Security and addressed security of single-user and multi-user wireless communication systems.

EDUCATION UPDATE: REU CYBERSECURITY SCHOLARS ARRIVE AT UMD

By Michel Cukier, associate director for education, Maryland cybersecurity center

MC2 welcomed nine undergraduate Cybersecurity Scholars to UMD in June 2012. The scholars come from campuses across the United States. Cybersecurity scholars are funded by NSF under the Research Experience for Undergraduates (REU) program. Teams conduct research for nine weeks in the summer.

Most scholars work in teams with at least one graduate fellow and a faculty mentor. Scholars are trained in team skills, project organization, and research competencies vital to

successful collaboration in science and engineering. The REU program also addresses issues of concern to women and minorities in science and engineering and provides guidance to the scholars about preparing for graduate school and careers in academia. Scholars conclude their time at UMD with a Scholar's Research Symposium where each team presents the results of their research efforts.

Students conducted research on one of four projects: modeling vulnerabilities and exploitability of software systems;

enhancing security and privacy on Android; experimental criminology in cyberspace: how surveillance impacts attacker behavior; and, analysis of random key pre-distribution in wireless sensor networks.

2012 REU Cybersecurity Scholars:

Aisha Browne (UCSB), **Sarah Cobb** (University of Massachusetts Amherst), **Allison Doren** (Washington University in Saint Louis), **Anat Gilboa** (Virginia Commonwealth University), **Rebecca Norton** (University of Vermont), **Sarah Spall** (University

of Utah), **Abigail Ward** (Princeton), **Andres Cordero** (University of Puerto Rico-Mayagüez), and **Jack Lestina** (University of Tulsa).

BELOW: REU SCHOLARS discuss their project with PROF. MICHEL CUKIER

NEW MC2 FACULTY: NICK FEAMSTER

Nick Feamster will join MC2 as the Darnell-Kanal Associate Professor of Computer Science in the fall of 2012. Nick comes to MC2 from Georgia Tech, where he directed the Network Operations and Internet Security Lab. Nick is a recipient of the Presidential Early Career Recipient and is a Sloan Fellow.

Nick's research focuses on networked computer systems, with a strong emphasis on network operations, network

architecture and protocol design, high performance (i.e., high availability, high throughput) wired and wireless networks, and anti-censorship techniques and systems.

Nick's research aims to help network operators run their networks better, and to enable users of these networks to experience high availability and strong end-to-end performance.

His research is supported by a number of agencies, including

DARPA, the Office of Naval Research, IBM, Yahoo!, the Department of Homeland Security, and the National Science Foundation, among others.

Feamster received his Ph.D. from MIT, and will bring eight doctoral students and two postdoctoral researchers with him, to UMD. For more information about Nick and his research, see: **http://www.cs.umd.edu/~feamster/**

Dr. Nick Feamster comes to MC2 from Georgia Tech.

MC2 SYMPOSIUM RECAP: MAY 15-16 2012

The first annual MC2 Symposium occurred May 15-16, 2012, in the Samuel Riggs Alumni Center on the campus of the University of Maryland. Approximately 160 people attended the two-day event.

The symposium featured keynote addresses by Dr. Gary McGraw, CTO of Cigital, and Dr. Andrew Myers of Cornell.

Welcome addresses were delivered by Congressman Dutch Ruppersberger (UMD alumnus) and William "Brit" Kirwan, Chancellor of the University System of Maryland. The symposium showcased eight technical talks by MC2 faculty from the Departments of Computer Science and Electrical and Computer Engineering.

Four in-depth tutorials were featured at the symposium:
-Secure Web Programming in Ruby on Rails;
-Dyninst: A Binary Analysis and Modification Framework;
-Effective Use of FindBugs in Large Software Development Projects; and,
-An Overview of Cybersecurity Laws, Regulations and Policies.

Panel discussions on the state of cyber education and prospects for enactment of cybersecurity legislation in the 112th Congress were also held. Thanks to everyone who participated, and we look forward to seeing everyone next year! For a complete list of symposium speakers see:
http://umiacs.umd.edu/mc2symposium/

Contact the Maryland Cybersecurity Center :
Eric Chapman: 301 405 7136
echapman@umd.edu

3400 AV Williams Building
University of Maryland College Park
College Park, MD 20742

www.cyber.umd.edu

Maryland Cybersecurity Center

Meaningful, Lasting Partnerships: By Eric Chapman, Associate Director of MC2

MC2 is uniquely situated among the federal agencies who play a key role in protecting our nation from cyber attacks, electronic espionage, and cyber criminals. However, the significant—and growing—cluster of cybersecurity companies in the greater Washington, DC., area provides a unique forum for industry to engage with MC2 and UMD. Corporate interest in student engagement, participation in unique seminars and symposia, as well as faculty collaboration are among a few of the reasons why corporations seek to partner with MC2. Corporate engagement extends beyond philanthropy: it provides a meaningful vehicle through which MC2 can develop lasting and mutually beneficial relationships. For example, Future Skies, Inc., became an MC2 partner in November 2011. When asked about the rewards of partnering with MC2, here is what Matthew Wilson, Director of Business Development at Future Skies, said:

> "Our partnership with MC2 has been highly beneficial to our corporate goals. The symposium and technical talks help us effectively direct our research efforts toward relevant emerging technologies within the cyber arena and also among wider engineering disciplines. As a small business with a growing presence in Maryland, MC2 provides opportunities to connect with students to developing our hiring pipeline. **MC2's leadership is dedicated to creating a meaningful organization for students, faculty and industry and Future Skies looks forward to continuing to benefit from this relationship.**"

MC2 THANKS ITS GENEROUS CORPORATE PARTNERS:

FUTURE SKIES™

NORTHROP GRUMMAN

TENABLE Network Security®

MAR INCORPORATED

cyberpoint

LOCKHEED MARTIN

lunarline Solutions Built on Security™

SUPRTEK

SAIC From Science to Solutions

Google™

SOURCEfire®

LINCOLN LABORATORY MASSACHUSETTS INSTITUTE OF TECHNOLOGY

ADVANTECH Technology for Competitive Performance