We have had another eventful year in MC2 and this newsletter reflects some key highlights.

We are particularly excited about the three new faculty who are joining MC2 as assistant professors in ECE: Dana Dachman-Soled, Tudor Dumitras, and Babis Papamanthou. You can read a little about their work above and learn more by visiting their web pages. They will add to the excellent group of faculty that are already part of MC2.

In addition, the Computer Science Department has just hired David Van Horn, currently a researcher at Northeastern, as an assistant professor. David’s research covers the cybersecurity-related areas of code analysis and monitoring, applied to mobile and web applications. We will continue to look to hire great people with another search this spring.

We are also excited to have completed our dedicated space for MC2 in 3400 A.V. Williams building. The open arrangement was designed to encourage collaboration (see page 7).
The MC2 space has offices for 10 faculty and 20 desks for graduate students and postdocs. It is equipped with several conference rooms, a kitchen, and a lounge area. While most of the students and faculty have moved in already, others will move in this fall. We will hold an open house soon to show off our new office space.

Our education and research activities continue to move ahead full throttle. The Advanced Cybersecurity Experience for Students (ACES) honors program officially begins this fall (see below). The cybersecurity specialization for computer science majors was approved last spring and is available to all students graduating this fall and beyond.

Over the past year we offered a slate of new courses, outreach events, and summer camps (see page 6). On the research side, MC2 faculty have landed several cybersecurity-related grants from the National Science Foundation, Army Research Lab, National Security Agency, and other organizations, and we all continue to publish papers in top venues (see page 3).

We showcased much of the work going on at our MC2 Symposium held this spring (see page 3). As with the inaugural event last year, we had a strong turnout with attendees from industry, government and academia.

I am excited about the strides we are making toward better understanding and responding to the cybersecurity threat, both on the research and education side. I heartily thank my colleagues at UMD, collaborators, and our corporate partners for their contributions to, and support of the work that goes on in MC2!

**DIRECTOR’S DIGEST (CONTINUED)**

Last year, UMD announced a landmark cybersecurity honors program, made possible by generous support from Northrop Grumman Corporation. Designed in partnership with MC2 and its affiliated faculty, the Advanced Cybersecurity Experience for Students (ACES) program is the nation’s first undergraduate honors program in cybersecurity, and aims to educate the next generation of advanced cybersecurity professionals. Michel Cukier, associate professor of reliability engineering and MC2’s associate director for education, leads the ACES program.

The first part of the program offers a two-year living and learning experience emphasizing breadth, and is followed by a complementary, two-year advanced technical program of study. Throughout the program, students will delve into technical and non-technical cybersecurity topics, and pursue experiential learning opportunities, such as research and internships. ACES Students will collaborate on group projects and engage with cybersecurity experts from industry, government, and academia. Students will also participate in a cyber-hygiene campaign to raise awareness of Internet safety best practices across campus and throughout the local community.

ACES welcomes its first cohort of 60 students this fall. Students’ diverse interests befit the ACES program’s goals, with areas of study including computer science, engineering, criminal justice, business, physics, and mathematics. This cohort will live together as one community in Ellicott Hall, and move into Prince Frederick Hall with the next cohort when the building is completed in 2014.

**ADVANCED CYBERSECURITY EXPERIENCE FOR STUDENTS**

**Michel Cukier**
Director
ACES Program

Prince Frederick Hall opens in Fall 2014

**RECENT MC2 FACULTY PROMOTIONS**

Two MC2 faculty members have been promoted to be full professors at UMD.

Michael Hicks (left) and Jonathan Katz (right) have been promoted to professor, Department of Computer Science.

We congratulate and celebrate with Dr. Hicks and Dr. Katz.
MC2 SYMPOSIUM RECAP
MAY 14-15, 2013

MC2 held its second annual public Symposium on May 14 and 15 in the Riggs Alumni Center on the UMD campus.

This year there were more than 140 registered participants. Many of these were students coming from UVA, Johns Hopkins, George Washington, and Georgetown. Most outside participants were from industry, both mainstream and research, with representatives from the government as well. Compared to last year, the audience was more technical with cybersecurity as a central topic of professional focus, rather than a side interest.

This year’s outstanding program featured talks from eight MC2 faculty. Participants particularly appreciated iSchool associate professor Jen Golbeck for her talk on privacy in social networks, and UMD Division of Information Technology senior staff member Rob Maxwell for his talk on the “Secure Maryland” penetration testing class.

There were four keynote addresses. The first address was given by Fred Schneider from Cornell University, who spoke on A Doctrine for Cybersecurity, making a compelling case that cybersecurity should be viewed as a public good similar to health care.

Kathleen Fisher, a program manager at the Defense Advanced Research Projects Agency (DARPA), discussed research to address the need to develop better high-assurance systems in critical areas like hospitals and military applications, where hackers’ intrusions can have devastating consequences.

Randy Sabet, J.D., counsel at ZwillGen PLLC, explored the currently controversial idea of “active cyber defense,” which advocates preemptive strikes against hackers.

Steve Bellovin, Chief Technologist at the Federal Trade Commission and a Professor at Columbia, discussed flaws in the critical infrastructure used to protect web users—trusted certificate authorities—and how their being compromised can have a cascading negative effect on on-line security.

In a post-event feedback survey, one respondent wrote: “Overall, very well done. Sessions that didn’t look that interesting, turned out to be very informative. Glad there weren’t too many ‘security is a problem, we have to do something about it’ talks. If there is a security problem presented, some framework for a solution should be provided. I liked the inclusion of the hard core technical talks, even if they were over most people's (including my) head—thanks!”

The symposium’s tutorials were also well received by the technical audience. One participant wrote: “I enjoyed the symposium; my only possible complaint is that the tutorials were too short and I regret not being able to attend all of them. The practical knowledge gained was of a lot higher value to me than the technical talks.”

Several MC2 corporate partners, including Tenable Network Security, SuprTEK, Sourcefire and ManTech participated in the event.

RECENT FUNDING
FOR MC2 FACULTY

Rajeev Barua (Entrepreneurial lead), Kapil Anand (Mentor), Satish Tamboli (University of Michigan Cohort), "Source Recovery from Binaries Using SecondWrite," NSF, Innovation Corps Team (I-Corps), $50,000 (2012 - 2013).

Jeffrey S. Foster (PI), Michael Hicks (co-PI), "Protecting against Malware on Android," UMD Partnership with the Laboratory of Telecommunications Sciences, $185,309 (2013 - 2014).


Elaine Shi (PI), "Truly Practical Dynamic Proofs of Retrievability," Google Faculty Research Award, $50,000 (2013).

MC2 hosts and organizes the Google and University of Maryland Cybersecurity Seminar series. The series features a diverse group of speakers from industry, academia, and government addressing a broad range of topics related to cybersecurity, including technology, policy, and economics. Invited speakers examine the impact that cybersecurity threats and protective measures are having on privacy, social networks, businesses and national security.

Last year we opened the fall 2012 semester with Kevin Mandia, Chief Executive Officer at MANDIANT. Mandia spoke about “The State of the Hack” by describing the many and varied data branches MANDIANT has investigated.

In October, we welcomed Wenke Lee, professor in the School of Computer Science at Georgia Tech whose talk “Internet Monitoring via DNS Traffic Analysis” discussed how cyber criminal activity is visible in various DNS traffic patterns.

In December, Úlfar Erlingsson, who leads efforts in security research at Google, joined the series. Erlingsson’s talk, titled “Cloud Computing and Security,” was hosted at Google’s Washington, DC office and explored how cloud computing offers new challenges beyond traditional distributed systems.

We opened the spring semester in February with Michael Franz, a professor of computer science at the University of California, Irvine. Franz spoke about “Software Defenses Using Compiler Techniques,” in which a compiler can add artificial diversity to a program, greatly complicating exploitation.

In March, we welcomed Ari Juels, Chief Scientist of RSA, the Security Division of EMC, and Director of RSA Laboratories. His talk titled “Aggregation and Distribution in Cloud Security,” covered both novel attacks and defenses against the cloud.

Nicolas Christin closed out the spring Google Seminar Series with his talk, “Network Security Economics: Identifying Choke Points and Understanding Incentives to Improve Online Security.” His talk moved beyond technology to understand the cat-and-mouse game of attack and defense. Dr. Christin is the Associate Director of the Information Networking Institute at Carnegie Mellon University.

The fall 2013 series is already taking shape with talks by researchers at Adobe, NSA, and the University of Pennsylvania.

For more information about the series please visit the website at: http://www.cyber.umd.edu/events/google-seminars. Or, to join our seminar mailing list, please e-mail cflowers@umiacs.umd.edu.

MC2 EXTERNAL ADVISORY BOARD

In October 2012, the MC2 External Advisory Board (EAB) held its inaugural meeting, at which MC2’s purpose, mission and charter were discussed. Professors Hicks and Cukier delivered overview briefings on the state of MC2, its research, and its educational and outreach efforts. Larry Gordon (Business School) and Elaine Shi (Computer Science) delivered presentations on their research in cybersecurity economics and cloud computing, respectively. The EAB also met informally following the conclusion of the first day of the second annual MC2 cybersecurity symposium. The MC2 EAB members are:

Jim Barrineau, VP for Strategic Cyber Initiatives, URS-Apptis, Inc.

Sameer Bhalotra, COO, Imperium

Robert F. Brammer, President and CEO, Brammer Technology, LLC

Larry D. Cox, President and CEO, Data Design Corporation

Matthew Wilson, Director, Future Skies

Gary McGraw, CTO, Cigital, Inc.

Ron Gula, CEO & CTO, Tenable Network Security

Mark Raugas, Director of CyberPoint Labs, CyberPoint

Hart Rossman, Principal Solutions Architect, Amazon

Francis Sullivan, Director, IDA Center for Computing Sciences

Lt. Gen. (Ret) Charlie Croom, Vice President, Lockheed Martin Corporation

Chris Goodrich, Sr. Vice President, ManTech
RESEARCH EXPERIENCE FOR UNDERGRADUATES

MC2 welcomed six undergraduate Cybersecurity Scholars to a nine-week research experience this summer. The scholars were part of research teams consisting of faculty mentors and graduate fellows and had the opportunity to learn team skills, project organization, and research competencies.

This year the students were from the University of Maryland, the University of Maryland Baltimore County (UMBC), Johns Hopkins University, Washington and Lee University, West Chester University, and Bryn Mawr College. The National Science Foundation (NSF) funds this effort under the Research Experience for Undergraduates (REU) program. The MC2 REU is led by Michel Cukier, associate director for education at MC2.

Students worked on four topics this summer: Securing PHP Web Applications via Settings; Analyzing Intruders’ Actions: A Command-Driven State Machine Approach; Building a Platform for Analyzing Intruders’ Actions; and Forensic Analysis Using Electric Network Frequency. Each project included mentorship by experienced computer science faculty members, technical seminars and workshops, team building activities, student presentations, and other professional development opportunities.

Students attended talks by UMD faculty members. In addition, the students read two books: “Ask For It: How Women Can Use the Power of Negotiation to Get What They Really Want” and “America the Vulnerable.” They also took a field trip to NSA’s National Cryptologic Museum and learned about the history of women in computing.

Scholars concluded their time at UMD with a Scholar's Research Symposium where each team presented the results of their research efforts to an audience of their research teams, faculty, staff, family and friends.

“SECURE MARYLAND” UNDERGRADUATE COURSE

Our second run of Secure Maryland was a great success.

In spring 2013, students could enroll in CMSC 498B: Secure Maryland, a three-credit course on penetration testing. The unique feature of the course is that students put theory into practice by “attacking” the University's networks. In so doing, they learn the practice of ethical hacking while helping to pinpoint, and precipitate fixes to, real vulnerabilities.

Students discovered hundreds of insecure devices, including a few connected to high-visibility services, and worked with their owners to secure them.

Additionally, groups of students worked closely with four different departments to carry out in-depth security testing of their IT infrastructure. The result was very specific recommendations for security improvements across their entire network. The students left with an understanding of the professional world of penetration testing.

TUDOR DUMITRAS AWARDED HONORABLE MENTION BY NSA

One of MC2’s recent hires, Tudor Dumitras, along with co-author Leyla Bilge, was awarded an honorable mention in the National Security Agency’s "Science of Security" best paper competition.

The paper, "Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World," answered a long-standing open question in security: for how long do zero-day attacks typically occur before they are discovered? (Answer: approximately 10 months). The research involved analyzing data collected on 10 million hosts to understand the lifecycle of vulnerabilities.

This careful measurement of attack behavior could be used in the U.S. government's efforts to protect systems from such attacks.

You can read more about this award at: http://www.nsa.gov/public_info/press_room/2013/2013_sos_competition.shtml.
CYBERSECURITY SUMMER CAMPS

This summer, MC2 collaborated with the CyberWatch K-12 Division of the National CyberWatch Center to offer two new cybersecurity summer programs at UMD. The goal of these programs was to stimulate early interest in cybersecurity in a way that is different from what they would typically learn in school. Both programs were led by experienced instructors who were assisted by UMD undergraduate student teaching assistants and counselors. The instructors, teaching assistants, and counselors also served as mentors to the participants, as they encouraged the participants' pursuits of STEM (science, technology, engineering and math) fields.

The first camp, Cyber Defense Training Camp, was a program for incoming high school juniors and seniors. Students get a taste of college life by living on campus for the week. Participants explored pertinent cyber realms of knowledge and skillsets including cracking passwords, data theft, and spear phishing attacks. This year, the program had students from Maryland, Virginia, Washington, D.C., North Carolina, Tennessee, New Jersey, New York and California.

The second camp, CyberSTEM, was a one-week commuter summer program at UMD for middle school (incoming 7th and 8th grade) girls interested in cybersecurity. This five-day experience provided hands-on activities focused on STEM and cybersecurity topics. Attendees learned and applied basic concepts of programming, forensics, cryptography, and program management from a series of gaming, modeling, and simulation activities, which explored the interconnections of science, math, technology, and computers. The girls also visited the NSA National Cryptologic Museum and heard from female professionals in the field.

SATURDAY CYBER EDUCATION WORKSHOP

This past March, MC2 held its first Cybersecurity Awareness Workshop, in an effort to stimulate interest in cybersecurity and technology to female youth. The program, titled “Cybersecurity and Cybersafety for Girls” attracted over sixty middle school girls from Maryland and Washington, D.C.

Throughout the day, the girls worked together on hands-on, interactive activities led by enthusiastic UMD undergraduate and graduate student volunteers, who served as mentors. Workshop participants were excited to use logic, creativity, and persistence to complete a lock-picking exercise using aluminum cans and a combination lock.

At the workshop, the girls rotated through four stations: Internet Privacy, Computer Safety, Password Protection, and Lock-Picking. All activities were interactive and allowed for discussion between the girls and the undergraduate facilitators. With the recent attention on cybersecurity and internet safety issues, there has been significant interest from local families who want to have their children attend these types of programs.

Following this success, MC2 plans to offer this type of program in the fall and spring of each year.
A GREAT YEAR FOR THE CYBERSECURITY CLUB

The University of Maryland Cybersecurity Club is a student-run organization whose mission is to develop and encourage cybersecurity awareness and application by providing students with the tools and education they need to advance their cybersecurity careers. To accomplish this goal, the club organizes community outreach programs about security related topics, hosts tech talks and guest speakers, and participates in security related competitions and conventions.

This year, the club’s competition team won first place in the college division of the Maryland Cyber Challenge and Conference (MDC3) at the CyberMaryland Conference held at the Baltimore Convention Center on October 17, 2012.

Teams were challenged to a six-hour "Capture The Flag/King of the Hill" contest which consisted of hacking into machines and protecting their own from other competitors' attacks. The UMD team won the top prize among the top 8 finalists within the college teams. Each team member received a $5,000 prize.

The Cybersecurity Club student competition team also qualified for the 2013 National CyberWatch Center Mid-Atlantic Collegiate Cyber Defense Competition (CCDC) Regional Finals, which were held April 10-13 at Johns Hopkins University Applied Physics Laboratory.

A total of 28 schools, representing undergraduate and graduate students from two- and four-year schools in the region, competed in virtual qualifying rounds March 19-20, 2013 for a chance to qualify for the Mid-Atlantic CCDC Regional Finals. The Mid-Atlantic CCDC is one of 10 regional competitions across the U.S., all part of the Deloitte National CCDC.

The Cybersecurity Club is moving forward into the 2013-14 year preparing for new challenges and looking for new members. Please visit csec.umd.edu for more information.

MC2 UNVEILS NEW COLLABORATIVE WORKSPACE

THE NEW HOME FOR MC2 FACULTY AND STUDENTS IS LOCATED IN 3400 A.V. WILLIAMS BUILDING
In February 2013, MC2 and ManTech International Corporation announced a two-year partnership to pursue advanced research in cybersecurity, including systems engineering and full-spectrum computer network operations.

UMD and ManTech will engage students and faculty in a comprehensive research effort that explores ways to apply advanced cybersecurity techniques to evolving technologies associated with cloud computing and other developing trends, as well as emerging threats. “We are very excited about working with UMD to explore new ideas, techniques and practices in the field of cybersecurity,” said H. Christopher Goodrich, Senior Vice President of ManTech’s Mission, Cyber & Intelligence Solutions, SIGINT Solutions and Cyber Operations Business Unit. “UMD has the talent and resources to bring new perspectives that will undoubtedly result in new ways to advance cybersecurity as emerging technologies continue to develop.”

Through the partnership, ManTech will start a new cybersecurity scholarship program that will provide four $5,000 scholarships to meritorious undergraduates with demonstrated interest and activities in the cybersecurity field. “ManTech is a leader in cutting-edge cybersecurity technology and solutions. This partnership will enable us to develop a much greater collaboration with ManTech, and the prestigious scholarships in their name will be of significant benefit to our impressive undergraduate students in this space,” added Eric Chapman, associate Director of MC2. “ManTech has made a real commitment to helping advance cybersecurity education here at UMD, and I think this is just the beginning of a mutually beneficial and enduring relationship,” Chapman said.

For those companies that seek the closest working relationships, MC2 offers exclusive opportunities for partnerships in cybersecurity aimed at fostering collaborations in research, education, and technology development. For more information on how to become a corporate partner, contact Eric Chapman at 301.405.7136 or echapman@umd.edu.

Maryland Cybersecurity Center
University of Maryland Institute for Advanced Computer Studies
3400 AV Williams Building
University of Maryland, College Park, 20742

www.cyber.umd.edu