Cyber Secure: Industrial Control Systems Lab Takes Shape

Electrical and Computer Engineering faculty Kai Zeng and Jim Jones have been working with Peggy Brouse of the Department of Systems Engineering and Operations Research under a grant from the U.S. Army’s Private Public Partnership Initiative (P3I) program to develop hands-on labs for Industrial Control Systems (ICS) and drone security. Both of the labs are physical spaces with actual hardware: servers to host virtual machine workstations, 12 TB of connected storage, multiple tethered drones, and various programmable logic controllers (PLCs) and devices. Faculty and student administrators configure the labs for a specific scenario, then users access the equipment remotely to run the exercises.

In a recent exercise, the ICS lab was configured with Windows workstations, RSLogix PLC programming software, and Allen Bradley MicroLogix 1000 PLCs connected to various switches (inputs) and lights (outputs). Students accessed the Windows workstations remotely, monitored the local network traffic, monitored the communications to the PLC, manipulated the PLC operation in real time, and modified the program running on the PLC. These are some of the activities performed by cyber attackers when they take control of an ICS workstation, only their manipulations are turning pumps on or off (Maruchy Shire), closing or opening valves (Stuxnet), or turning off breakers (Ukraine), instead of just making lights go on or off.

This work will lead to a better understanding of how ICS systems may be attacked and defended, and it is being used to catalog the digital artifacts generated by such activity for forensic purposes. ECE and VSE students Abhijitt Dhavlle, Devang Motwani, Saurabh Deshpande, Brendan McGrath, Shyheim Gayles, and Shaquille White were instrumental in building and operating the ICS lab, which is now being used by students in classes, by external partners for testing and training, and for research purposes.

Continued on page 4
Spring 2017 Highlights

Dear Alumni and Friends,

The Department of Electrical and Computer Engineering, its programs, faculty, and students are moving upward in many different areas. For example, the bachelor of science in the Computer Engineering Program, established in 1998, reached a record enrollment this fall semester with 292 students declaring it as their major. This program has nearly doubled in size in the past five years. This growth mirrors the growth we are seeing at Mason Engineering and the university. Over the past five years, the Volgenau School of Engineering has increased its enrollment by 52.5 percent, and Mason has increased from 32,961 students to almost 36,297.

During the same period, the department has reached new levels in research funding for various programs. Between the years 2014 and 2017, the number of research awards to ECE faculty increased by 113 percent, and the number of research proposals increased by 278 percent with $27.8 million in proposals over the past 12 months. This trend in research awards should continue in the coming year.

With the increase in the size of the department comes the need for more lab space. The expansion of the Science and Technology Campus, located in Manassas, which is about 30 minutes to the east of the Fairfax Campus, will address this need. This campus will house a clean room, faculty offices, and new makerspaces for students to work on interdisciplinary projects. Adjacent to the campus will be a large facility that will be used, in part, to support new research projects in robotics.

Continuing our effort to keep our programs competitive, we are constantly developing courses and specialization areas in fields that are new to our department. Liling Huang, for example, is developing new courses in power systems, and Avesta Sasan is developing new courses along with a new degree specialization in the Internet of Things.

Another direction that the department is moving forward is upwards into space. The department is sponsoring two undergraduate students who are leading the Mason Rocket Club to compete in the Battle of the Rockets competition in April 2018. The team will be competing in the Sounding Rocket Event and the Target Altitude Events. More news on their success in the next newsletter.

I invite you to follow us on Facebook, and I look forward to sharing more news and stories of our department in the future.

Monson H. Hayes
Chair, Department of Electrical and Computer Engineering
Tahir Khan is a lifelong learner who is constantly trying to improve his knowledge of current technology and trends.

Khan, MS Computer Forensics ’11 (he was the top graduate in his class), has been teaching at Mason since 2012. He devotes his time, talent, and efforts to creating, designing, and teaching courses in penetration testing/ethical hacking, mobile device application security, anti-forensics, and cloud forensics. Khan also volunteers his time to teach high school students digital forensics at Mason/Infragard-sponsored cyber academies, and he is a member of the ECE Digital Forensics Advisory Board.

Khan currently works for Verizon as chief information security officer for Smart Cities and Venues. Verizon’s Smart Cities initiative is the ultimate in the internet of things (IoT). The initiative will network and manage telemetry for smart lights, video, traffic, and IoT security credentialing and includes the analytics to create value from that wealth of data.

Prior to Verizon, Khan worked for Electronic Transaction Systems (ETS) and Northrop Grumman. While at ETS, he was the chief information security officer for a company that processed more than $8.5 billion annually and offered financial services—such as payment processing, automate clearing, mobile payments, ecommerce, and financial software development—to clients in 23 countries across North America and Europe.

At Northrop, he led a design and architecture team for several command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) programs. Khan’s innovation includes developing an Android and Apple IOS multifactor authentication application, and he has developed a forensic tool suite to automatically capture cloud-based artifacts including memory and disk.

Khan is married and has one son. When he is not working or teaching, he enjoys hiking, fitness, and playing chess.

“Going through the Mason program made me realize the important role adjuncts play in shaping future generation of engineers. I wanted to be part of the solution that creates strong students and future entrepreneurs. I have found that there is nothing more rewarding than helping a student choose a career path or find a passion for an area they did not know existed.”
Remote Manipulation of an ICS Programmable Logic Controller

1. Original program
2. With toggle switches 1 and 2 on, lights 1 and 2 are on.
3. Altered program turns Toggle 2 off
4. Light 2 goes off, but Toggle switch 2 is still physically on

The drone security lab is equipped with Bebop drones and Crazyflie mini drones. A web-based remote access system was built to allow users to remotely log in, conduct experiments, collect experimental data, and analyze the results. This drone security lab can facilitate drone security risk analysis, drone forensics, drone detection, and various security attack and defense practice and analysis. Students who participated in building the drone security lab include Rongxin Zheng, a master’s student in data analytics engineering; Jonathan Wiley, an undergraduate student in the cybersecurity engineering; and Jixuan Zhi, a PhD student in computer science.

Drone Security lab with drones.
Mason Leads new DHS Center of Excellence for Criminal Investigations and Network Analysis

BY JIM JONES

In August 2017, the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) announced that George Mason University will lead a consortium of U.S. academic institutions and other partners for a new Center of Excellence (COE) in Criminal Investigations and Network Analysis (CINA). S&T will provide CINA with a $3.85 million grant for its first operating year in a 10-year grant period. The Criminal Investigations and Network Analysis Center develops strategies and solutions to enhance criminal network analysis, forensics, and investigative processes for on-the-ground use by agents and officers to predict, thwart, and prosecute crimes.

CINA projects will focus on four primary areas: criminal network analysis, dynamic patterns of criminal activity, forensics, and criminal investigative processes. Jim Jones of the Department of Electrical and Computer Engineering is leading the forensics area, which has the following research planned for the near term:

- Audio forensics to analyze voice recordings, specifically to profile hoax phone callers. Such calls are a known problem for first responders and entities such as the U.S. Coast Guard, and this work will help detect hoax calls and analyze evidence for prosecution.
- Video forensics to analyze content. Given the extraordinary volume of video data available to law enforcement and others, this work will automate analysis of video content so that it may be more effectively searched by investigators.
- Research to better prepare and package evidence for financial cases. This research will provide tools and training to more consistently prepare financial case evidence in a form most likely to be useful for the prosecution.
- Research to develop best practices for sharing and analyzing digital evidence. Digital evidence comes in many forms and formats, and different tools and techniques work with some of these forms and formats and not with others. This work will develop best practices to facilitate the sharing and effective analysis of digital evidence.

More information can be found at www.dhs.gov/science-and-technology/centers-excellence.

RESEARCH AWARDS FOR ECE DEPARTMENT, JANUARY TO DECEMBER 2017

Awards for Calendar Year by Area in Dollars

Over the past year, the department has been awarded approximately $5 million in grants. Faculty will lead new research initiatives in the areas of Computer Architecture, Internet of Things, Cyber Physical Systems Security, Wireless Communications and Signal Processing, Nanotechnology, and Controls and Robotics. The department is also involved in several research projects with faculty from other departments in the school and the rest of the university. The sponsoring agencies include U.S. Air Force Research Lab, National Science Foundation, Department of Homeland Security, NASA, and Office of Naval Research. For more details on individual grants please visit volgenau.gmu.edu/research/grants.
ECE Engages Citizen Scientists with Eclipse Mob Project

BY JILL NELSON

On August 21, a total solar eclipse passed across the continental United States, traveling from Oregon to South Carolina. Millions of people journeyed to the path of totality to view the amazing (but short—less than 2.5 minutes of totality) phenomenon of the sun fully blocked by the moon. Beyond the incredible visual spectacle, the total eclipse also offered scientists an opportunity to study the effects of the sun’s rays on the earth’s atmosphere. One project that leveraged this opportunity was EclipseMob, a crowdsourced effort to study the effect of the sun on the ionosphere, a region of the earth’s atmosphere in which particles are ionized by the sun’s rays. A solar eclipse provides a rare chance to observe how that ionization changes when the sun’s rays are briefly blocked by the moon.

How does one measure ionization levels in the atmosphere? In the case of EclipseMob, scientists used radio waves. Low-frequency (LF) radio wave propagation is directly affected by ionization of the atmosphere. When the lowest layer of the ionosphere is ionized by the sun’s rays, it absorbs LF radio waves; hence, the waves can travel only along Earth’s surface. In contrast, when the sun’s rays no longer reach the ionosphere, ionized particles recombine; LF waves pass through the lowest layer of the ionosphere and are reflected back to Earth by the ionosphere’s upper layers. In this environment, reflected waves can travel much farther by “bouncing” between the earth and the ionosphere. This phenomenon explains why faraway AM radio stations can be heard at night but not during the day.

The goal of the EclipseMob experiment is to obtain an understanding of how the eclipse affected LF radio wave propagation at locations across the United States. With funding from the National Science Foundation, a simple LF antenna and receiver were designed, and 150 “do it yourself” antenna and receiver kits were distributed to citizen scientists in 31 states and two countries. Citizen scientists built the antenna-receiver combo and used it to collect radio signals before, during, and after the eclipse.

A specialized EclipseMob smartphone app performed local oscillator signal generation, added GPS time and location stamps to the recordings, and allowed users to upload their recordings to EclipseMob’s cloud storage. The EclipseMob receiver was designed to observe the signal transmitted by WWVB, a NIST-operated transmitter in Fort Collins, Colorado, that transmits at 60 KHz and provides a precise time signal. Because WWVB’s nighttime coverage includes the full continental United States, all participants could observe the same signal, facilitating meaningful comparison of eclipse effects at geographically disparate receiver locations.

Now that the eclipse has passed, what remains is the exciting and challenging task of processing and analyzing the data. Particularly in daylight, the WWVB signal strength is quite low in many locations, and hence extracting the signal and tracking its amplitude variation during the eclipse requires processing that exploits the known structure of the WWVB transmission. As results become available, they will be shared with the citizen science community via the project website: eclipsemob.org.
Father-Son Team Spans Disciplines and Borders to Study Ocean Acidification

By Kenneth Hintz

It sounds easy. Create three coral culturing environments in the laboratory that replicate the effects of atmospheric CO2 concentrations in the oceans for three different time periods: 1) before the industrial revolution, 2) present day, and 3) predicted future elevated levels. The goal: to perform controlled studies of the effects of ocean acidification.

While the rate of change of the earth’s temperature captures the headlines, ocean acidification is an underreported cause of coral loss. Why are we worried about corals? Coral reefs are, second only to tropical rainforests, the most diverse ecosystems on the planet. While they are highly productive, these relatively small biomes are critical to maintaining our global fisheries, offer countless possibilities for biologically sourced medicines, and are great sources of economic prosperity through ecotourism.

A collaborative effort between Kenneth Hintz, an associate professor of electrical and computer engineering at Mason Engineering, Chris Hintz, a chemical oceanographer in the marine and environmental science department at Savannah State University, Savannah, Georgia, and Nicky Allison, a coral biologist at University of St. Andrews Scottish Ocean Institute, St. Andrews, Scotland, has resulted in a coral culturing facility at the University of St. Andrews. It not only controls the pH of culturing environments for a well-studied genotype of the fast-growing Porites lutea coral, but also properly doses and controls other trace minerals required for the maintenance of coral health.

Unique to this system is controlling the dissolved CO2 in the culturing environment as simple as measuring the pH with an electrode and either adding acid to lower pH or adding base to increase pH, but the complex chemistry in seawater and nonlinear relationships of atmospheric CO2, dissolved inorganic carbon, alkalinity, and pH preclude a simple approach. Further, the automated control system must overcome the constant biological consumption of CO2 (photosynthetic, symbiotic zooxanthellae in coral) and production of CO2 (respiration of corals themselves).

The three researchers integrated their knowledge of chemical oceanography, coral biology, and automatic control to create a fully functional system controlled by a custom Matlab program implemented on a standard PC. Two high-precision CO2 meters measure gas inputs and exhaust to supply to PID control algorithms that modify CO2 and air mixing control valves to maintain constant three levels of atmospheric CO2 (250, 400, and 700 ppm) dissolved in seawater. Further, the program also maintains constant alkalinity and calcium concentrations using automated microliter dosing pumps based on analytical measurements made by the St. Andrews research team.

Presently, only two culture systems in the world provide long-term control (months to years) with ± 2-5 ppm precision necessary to investigate ecologically relevant but slow-growing organisms. The St. Andrews culturing system has been in almost continuous operation for four years. The researchers have had one published paper and two other submissions to refereed journals. The net result of this controlled study of coral growth rate is a confirmation that increasing ocean acidification at a constant (25°C) temperature decreases hard coral growth rate. However, surprisingly at higher water temperature (28°C), the coral growth was not significantly altered. That’s marine science. That’s why we built this laboratory coral culturing facility—to enable the controlled study of an ocean environment that is constantly changing when studied in situ.
STAFF CONTACTS

Jammie Chang
Academic Program Manager,
PhD ECE Program
Office: Engineering 3104
Email: jchangn@gmu.edu
Phone: 703-993-1570

Patricia Sahs
Academic Programs Coordinator,
ECE MS-ELEN and MS-CPE Programs
Office: Engineering 3101-A
Email: psahs@gmu.edu
Phone: 703-993-1523

Toshiko Uchiyama
Academic Program Manager,
MS Telecommunications,
MS Computer Forensics Program
Office: Engineering 3300
Email: tuchiyam@gmu.edu
Phone: 703-993-3810