Department of Electrical Engineering and Computer Science

United States Military Academy, West Point, New York

CLASS OF 1960 ENDOWMENT FOR THE WEST POINT CYBER RESEARCH CENTER

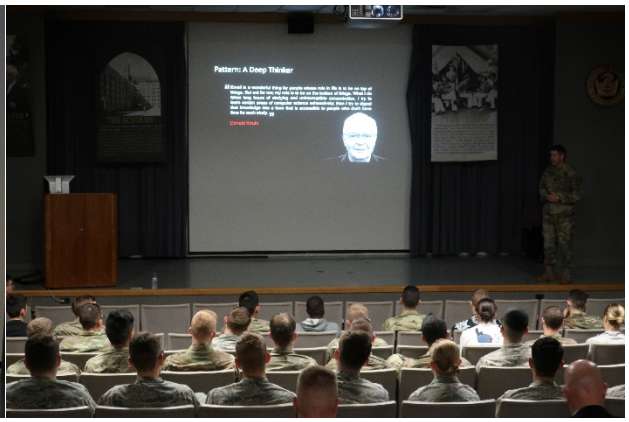
Academic Year 2018 – 2019

The Cyber Research Center (CRC) and the Department of Electrical Engineering and Computer Science (EECS) are extremely thankful for the Class of 1960's commitment to the CRC. The funding from the class endowment will provide significant margin-of-excellence opportunities for cadets to enhance their awareness and appreciation of cyber security and related cyber topics as they pursue their studies in computer science, electrical engineering, and information technology. These amazing opportunities would not be possible without your generosity.

The fall semester began with several new and exciting developments. One of these developments was splitting the Cadet Competitive Cyber Team (C3T) into three unique specialties. C3T now has a penetration testing (red) team, a defensive oriented (blue) team, and the traditional capture-the-flag (CTF) team. All three of C3T's elements competed in national level competitions as well as the NSA Cyber Defense Exercise (NCX) versus the other service academies. Also, LTC Ray Blaine took over as the Director of the CRC. Ray returned to the EECS team after 3 years leading Cyber Protection Teams out of Fort Gordon, Ga. He brings a fresh energy and operational context to our cyber efforts.

This report highlights a few of the events that the CRC sponsored for Cadets. The Cadets chosen and the faculty that support these opportunities typically come from the EECS major population, C3T, and the Cyber Leader Development Program. Your support helps the CRC continue as well as broaden these types of invaluable opportunities for the Cadets. This provides an immeasurable impact to the quality of education and experience that USMA provides.

DEFCON26. Just before the beginning of reorganization week at USMA a group of Cadets and faculty attended the world's largest hacker conference, DEFCON26. The conference was an imersive, expansive experience; even the badges were intricate puzzels. The USMA group and thousands of security professionals, were able to experience hundreds of speakers and cyber-related villages. Cadets split into small groups with related interestes, in order to experience as much of the conference as possible. The emphasis on hands on learning throughout the event provided cadets opportunities to gain interest and basic understanding of skills such as lock picking, subverting tamper evident techniques, drones, cryptography, hardware hacking, vehicle hacking, wearables, bio hacking, and much more. Group favorite speakers and talks included OSINT, offensive honeypots, fake science, tracker app security flaws, and DNA encryption. Cadets gained exposure to new topics and left with inspiration to pursue further understanding of these fields.



Army vs. Air Force Cyber Events. On Friday, 2 November 2019, the Cadet Competitive Cyber Team (C3T) competed in its first official head-to-head service academy star-match, the Army vs Air Force Capture-the-Flag (A2F CTF) competition. In addition to this six hour attack/defend style match, the CRC hosted a lunchtime Cyber Leader Development Keynote featuring LTC Petullo, Director of the Cyber Solutions Development Detachment (CSD) and a Junior Officer Panel with four USMA Graduates, and current members of the CSD. This collection of events served to inform, inspire, and challenge cadets to excel in their pursuit of entering the Cyber profession within the Army.

In his keynote LTC Petullo spoke to an audience of over 70 cadets as well as Staff and Faculty from across the Academy. He presented a framework of patterns that he has observed in high quality capability developers such as deep thinkers, constructors and re-constructors all in the context of an overarching philosophy. His talk went even further to provide cadets with actionable ways to prepare prior to commissioning and a insider's look at a potentially forthcoming developer specific career field, the 17D. These remarks provided invaluable insight for computing professionals and future Cyber Officers alike.

Following the keynote, LT Will Brattain ('15), LT Ed Woodruff ('16), LT Jessie Lass ('16), and CPT Christian Sharpsten ('14) provided candid commentary in a question and answer session with Cadets. As former members of C3T their perspective provided a bridge from CTF competitions into real world cyberspace operations. As technical experts and leaders themselves, the words of the panel were especially relevant and timely. These officers also volunteered and created the vulnerable services for the competition.

Collegiate Penetration Testing Competition (CPTC). The Red Team component of the Cadet Competitive Cyber Team (C3T-Red) competed at the National Collegiate Penetration Testing Competition (CPTC) over Columbus Day weekend. The cadets made an excellent first showing at the event, placing 6th of 11 regionally. C3T-Red finished ahead of the other first time participating schools, with a very narrow point gap between 4th and 6th. USMA is the first military academy to attend in any region, ahead of the Navy, Air Force, and the Coast Guard Academies.

The Cadets had 9 hours to assess a realistic network environment for vulnerabilities and 6 hours to write a report on their findings. Using TTPs they learned in the Ethical Hacking course, SANS training, and club practice, the cadets discovered and enumerated systems, determined and documented vulnerabilities, and finally exploited them. Throughout the 9 hours the team dealt with injects based on real-world events including the recent denial-of-service (DOS) attack on GitHub.

The Cadets honed their technical and communication skills, gained the experience of assessing a complex network environment, and competed with some of the best teams across the nation.

Only six of eight Red Team Cadets were alowed on the network, but the host (Penn State University) created a CTF for remaining team members and coaches. At the close of the competition, C3T-Red was leading the CTF!

SHMOOCON 2019. Friday through Sunday, 18-20 January 2019, 29 Cadets and four faculty members from USMA attended ShmooCon, an annual computer security and hacking convention in Washington, DC. A group from the United States Naval Academy also participated. The group attended more than 50 presentations from individual security researchers, industry representatives, and cybersecurity luminaries; the conference also included various security training events, social networking opportunities, and hacking challenges.

Cadets on the trip experienced several talks directly applicable to their future careers. Matt Blaze, the McDevitt Chair of Computer Science and Law at Georgetown University, presented research into the various failures of U.S. government agencies to apply basic security standards to their work, along with suggestions for improving these issues within those agencies. Another talk, given by career special operations officer Paul Brister and Naval War College scientist Nina Kollars, focused on the human side of educational and training programs to develop skills "intended to skirt laws and bypass security systems." Yet another, titled "The Beginner's Guide to the Musical Scales of Cyberwar," and given by Jessica Malekos Smith, the Reuben Everett Cyber Scholar at Duke University Law School, covered conceptualizing the Law of Armed Conflict in cyberspace and the mitigation or escalation of cyber conflict.

Aside from these and many other talks, ShmooCon is known for challenges and competitions. Many of the Cadets participated in lockpicking and cryptography challenges throughout the conference. A small group of Cadets and instructors also participated in a competition known as HackFortress, which merges the popular video game Team Fortress 2 with a series of capture-the-flag style hacking puzzles for team members to solve. Paired against the defending champion team, the USMA contingent was able to keep up on the hacking challenges, but their video game skills were simply not up to par.

Many currently-serving Signal Corps and Cyber Branch personnel, as well as USMA graduates in the private sector, were also in attendance at the conference and Cadets had several networking opportunities. One of these included a mixer hosted by Bryson Bort, who is a USMA graduate (class of 2000) and the founder of the GRIMM and SCYTHE cybersecurity companies.

NSA Cyber Exercise (NCX). 37 USMA Cadets participated in the annual National Security Agency (NSA) Cyber Exercise (NCX) held at the United States Air Force Academy (USAFA) from April 15-17, 2019. Participants included members of West Point's Cadet Competitive Cyber Team (C3T), Cyber Policy Team, as well as additional cadets across multiple departments.

The NCX is a three-day competition that challenges Cadets and Midshipmen from the U.S. Military, Naval, Air Force, Coast Guard, and Merchant Marine Academies in full-spectrum cyber operations to test their cybersecurity skills, teamwork, planning, communication, and decision-making. The exercise consists of four modules including digital forensics, cyber policy, data analysis, and secure coding. The NCX culminates with an eight-hour cyber combat exercise that allows the participants to exercise the full spectrum of offensive and defensive capabilities against each other in the Cyber Domain.

The exercise coincided with the Joint Service Academy Cyber Summit (JSA) allowing the Cadets to attend. JSA brings in leaders from industry and DoD to speak and collaborate on important cyber issues. This year the Cadets were able to hear progress about the Cyber Moonshot. The Cadets also heard from the Commander of CYBERCOM and the Commanders of each of the service component commands. A truly unique opportunity to be exposed to so many key leaders in one event.

The members of the Cyber Research Center and the Department of Electrical Engineering and Computer Science, both Cadet and Faculty alike, are deeply appreciative of the Class of 1960 Endowment. This tremendously impactful gift will pay significant dividends in the education of future leaders about the newest domain of warfare. We look forward to many more wonderful opportunities for our Cadets provided by your class. Thank you again for your support. Beat Navy!

BLAINE.RAYMOND.WESLEY.1106506228

Digitally signed by BLAINE.RAYMOND.WESLEY.1106506228
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI, ou=USA, cn=BLAINE.RAYMOND.WESLEY.1106506228
Date: 2019.06.12 09:20:16 -04'00'

Raymond W. Blaine, Ph.D., P.E.
LTC, CY
Director, Cyber Research Center