2017-02-07

NPS Faculty, Students Develop Innovative Cyber Defense for Front Line Operators

DON Innovation; CHIPS Magazine

U.S. Department of the Navy

CHIPS THE DEPARTMENT OF THE NAVY'S INFORMATION TECHNOLOGY MAGAZINE

NPS Faculty, Students Develop Innovative Cyber Defense for Front Line Operators

By MC2 Patrick Dionne, Naval Postgraduate School - June 23, 2017

In the realm of cyber defense, timing is critical ... An immediate, structured response to a cyber-incident can make a critical difference in mitigating an attack. In order to meet this challenge, faculty and students at the Naval Postgraduate School (NPS) have spent that last two years working on the tools front line operators need to do just that.

Over that time, several students in the university's Master of Cyber Systems and Operations, and Master of Applied Cyber Operations (MACO) programs have left their mark on the Cyber Defense Operational Sequencing System (CDOSS) project. CDOSS is an effort to develop a set of properly sequenced standard procedures that give Sailors immediate and follow on actions in the case of an incident, mirroring what a cyber expert would do.

NPS Director of Information Warfare and Innovation, U.S. Navy Cmdr. Pablo Breuer plays a lead role in the project, guiding his team of students in the development of this intricate set of cyber defense counter measures in hopes of improving the fleet's shipboard cyber capabilities.

"Everyone these days deals with computers, and when most of us think about a computer, we think about a desktop or a laptop. But most of us don't realize, even things such as our cars have about 40-50 computers and 100 million lines of code," said Breuer. "The same thing happens on a Navy ship. The engineering systems, the combat systems, the fire control systems, all of these things have computers in them and our Sailors' lives and missions rely on these things."

CDOSS operates as a list of cards containing tools, tactics and techniques, providing Sailors a way to identify and correct casualties in computing systems without having a background in computer science.

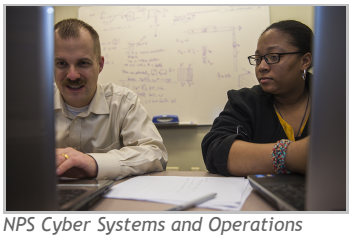
"When I was first commissioned, I worked as a Boiler's Officer when the Navy still had Boiler Technicians, and even though none of them had experience in thermodynamics or mechanical engineering, they kept the plant running," said Breuer. "They were able to do this because of an Engineering Operational Sequencing System, or EOSS, that told them how to mediate casualties. This inspired me to create a more universal system because, as time went on, ships, like the rest of the world, begun to rely more heavily on computers."

CDOSS gives unit commanders organic capabilities to continue on mission and rely less on the Navy Cyber Defense Operations Center (NCDOC) and similar cyber support groups. The effort is in direct accordance with Commander, Fleet Cyber Command and Commander, U.S. Tenth Fleet, Vice Adm. Michael Gilday's call for a decentralization of the Navy's cyber operations.

"We can't move terabytes of data back to a central location in order to do aggregation and collection," Gilday said during the AFCEA West conference in February 2017. "Those analytics have to be distributed as well, and the force must be decentralized, much like how the fleet fights in a distributed manner."

During its development, Breuer and his team looked to the Navy's Consolidated Afloat Networks and Enterprise Services (CANES) program, which is the Navy's next generation tactical afloat network. CANES represents the consolidation and enhancement of shipboard network programs to provide a common computing environment for more than 40 command, control, intelligence and logistics applications.

"The first thing we had to figure out was what tools do we have on Navy units to support this, and



NPS Cyber Systems and Operations students Lts. Tye Wylkynsone, left, and Simone Mims, right, conduct research in support of the Cyber Defense Operational Sequencing System (CDOSS) project. CDOSS is an effort to develop a set of properly sequenced standard procedures that give Sailors immediate and follow on actions in the case of an incident, mirroring what a cyber expert would do.

Related CHIPS Articles

CWIX 2017: NATO Tests Cyber, Innovation and Adaptation

DoD Lab Day: 3-D Printed Quadcopter with Electronic Warfare and Cyber Warfare Payloads

SPAWAR's Cybersecurity Summer Camp Expands Student Enthusiasm in STEM Careers

"Cybersecuring" the internet of things

CIWT Announces Civilians of the Quarter

Related DON CIO News

DON IT Conference Presentations Available

DON IT East Small Business Networking Opportunity

Join Us At DON IT East 2017

Strengthening the DON's Cybersecurity Posture

DON Cyberspace (Cyber) IT and Cybersecurity Workforce - Who Are We?

Related DON CIO Policy

DON Cyberspace IT and Cybersecurity Workforce Management and Qualification Manual

Coding of DON Positions Performing Cybersecurity Functions

we did this by taking a standard CANES installed computer system on a destroyer and found that there was an unused computer network intrusion detection system on all CANES installed networks," said Breuer. "Once we did some network discovery, the next step was to take this new tool and figure out how we should configure it. Now that we know what we have and what we are looking for, we can summarize ways to mediate any issue we may come across."

Breuer, who graduated from NPS' Department of Computer Science in 2008, said he and his team of students were able to use experience and opportunities gained on campus, which he calls a "nexus of advanced research for the Navy," to better get the CDOSS project off the ground.

"It was personally very satisfying knowing that what I was working on as an NPS degree requirement would have a direct and immediate impact in the fleet," said Chief Warrant Officer Robert Labrenz, an NPS alumnus who contributed to the project during his studies in the MACO program.

"While working on CDOSS, I was able to employ a unique perspective from my enlisted experience to forge an important piece of the overall project, in order produce a product that a junior enlisted Sailor could read, understand, and put to use in defending the network," he added.

After two years of development and research, nine student theses on CDOSS have been released, with the product being reviewed both by NCDOC and surface forces, paving the way for its upcoming follow on fleet testing in order to get proper feedback from Sailors on its effectiveness and usability.

"I think it is going to have tremendous impact," said Breuer. "A lot of people would tell you that the Internet and cyber space is really big, but in reality, you can get from any point in cyber space to another in under 600 milliseconds, so if our cyber defense relies on us packing up a hard drive and putting it on a helicopter, then we are not operating at the speed of cyberspace. This will allow ships to gain that advantage and give ships a better understanding of their systems."

TAGS: Cybersecurity, NEN, Telecommunications, Workforce

DON Implementation Of The Risk Management Framework For DoD IT

DON Adoption of the DoD Mobile Classified Capability

Cyberspace/IT Workforce Continuous Learning

CHIPS is an official U.S. Navy website sponsored by the Department of the Navy (DON) Chief Information Officer, the Department of Defense Enterprise Software Initiative (ESI) and the DON's ESI Software Product Manager Team at Space and Naval Warfare Systems Center Pacific.

Online ISSN 2154-1779; Print ISSN 1047-9988