



OFFICIAL BUSINESS

DEPARTMENT OF THE AIR FORCE
 AIR FORCE INSTITUTE OF TECHNOLOGY
 CENTER FOR CYBERSPACE RESEARCH
 AFIT/ENG
 2950 HOBSON WAY
 WRIGHT-PATTERSON AFB OH 45433-7765



Vol. 3, No. 2
 July 2010

The Center for Cyberspace Research (CCR), established in March 2002, conducts defense-focused research at the Master's and PhD levels. The CCR is forward-looking and responsive to the changing educational and research needs of the Air Force, the Department of Defense, and the federal government. The CCR faculty teaches and performs research to understand and develop advanced cyber-related theories and technologies. These theory and technology advancements include efforts in network intrusion detection and avoidance, insider threat mitigation, cyberspace situational awareness, network visualization, software protection, and anti-tamper technologies development. On June 19, 2008 AFIT was designated by the SECAF and CSAF as the Air Force Cyberspace Technical Center of Excellence.

CENTER FOR CYBERSPACE RESEARCH

Director: Dr. Richard Raines; Deputy Director: Colonel Harold Arata
 Associate Director: Dr. Rusty Baldwin
 Marketing Specialist: Carrie Solberg
 Questions, concerns, feedback, email carrie.solberg.ctr@afit.edu
 Visit our web site: www.afit.edu/en/ccr/

CCR News is published by the Center for Cyberspace Research. All material contained herein reflects the opinions of the authors and editors and does not necessarily reflect U.S. Air Force or AFIT policy.



Vol. 3, No. 2

July 2010

AFIT CCR Distinguished Review Board Visit Spring 2010

On April 20, 2010 the Air Force Institute of Technology (AFIT) Center for Cyberspace Research (CCR) held its semi-annual Distinguished Review Board (DRB) and Board of Advisors (BoA) meeting at AFIT with Maj. Gen. Michael J. Basla Vice Commander, Air Force Space Command, Peterson Air Force Base, CO presiding.

CCR presented the latest in cyber research and education as well as its role as the Air Force's Cyberspace Technical Center of Excellence. Tremendous advocacy of CCR and its support of the Air Force cyberspace mission was evident. Maj. Gen. Basla commented that "This group brings together great minds. We look to this group to advise and guide us on what we are doing in this world of cyberspace and critique our ideas to ensure we walk away with a stronger way forward".

The DRB guides the CCR Director in developing, implementing, and evaluating the research and academic programs that promote the growth of cyber professionals for the Department of Defense (DoD). The DRB provides extra-agency reviews that ensure research and academic



programs at CCR are scientifically sound, relevant, and meet the needs of the DoD. The BoA ensure key Air Force representatives provide oversight and direction to the Air Force Cyberspace Technical Center of Excellence (AF CyTCoE). The organizational makeup of the BoA make sure that current operational issues guides the center's operations and that these activities receive broad advocacy across the Air Force. The BoA also reviews applicable training programs which provides a cohesive and integrated approach to cyberspace education and training.

Other distinguished board members in attendance included representatives from the Air Force Space Command, Air Staff, National Security Agency, Department of Homeland Security, 688th Information Operations Wing, and many more from both industry and academia. The joint meeting of the DRB and BoA provides CCR a vision and direction for ever-changing cyber domain.

For additional information please visit the Center for Cyberspace Research's website at <http://www.afit.edu/ccr/>.

Visit the CCR web site: www.afit.edu/en/ccr/



AFIT CCR Hosts the 5th International Conference on Information Warfare (ICIW)



The Air Force Institute of Technology's Center for Cyberspace Research (CCR) was delighted to host the International Conference on Information Warfare (ICIW) on April 8-9, 2010 at the Hope Hotel and Conference Center at Wright-Patterson Air Force Base.

Over 100 researchers from the United States, Estonia, Finland, France, India, Portugal, South Africa, Turkey, and the United Kingdom attended this year. According to the conference chair, Dr. Michael Grimaila from CCR, "ICIW provides a unique venue where researchers can discuss advancements of scientific and technical knowledge as it pertains to information warfare and cyberspace." This year we were fortunate to have two excellent keynote speakers: Dr. Michael VanPutte from the Defense Advanced Research Projects

Agency (DARPA), who discussed mission assurance and Dr. Steve Rogers from the Air Force Research Laboratory (AFRL) Sensors Directorate, who spoke about integrating humans and computers to address "wicked problems." The keynote speeches resonated well and generated many discussions about the complexity of operating in cyberspace.

Dr. Rogers summarized the discussions this way, "This conference served as a forum to the information warfare community as we transform our focus and research programs to successfully tackle some of the most complex and important technology problems facing the nation. Attendees got refreshed and motivated by the common purpose of providing the nation with needed technological breakthroughs. It's time to get to work!"

"Spotlight on Research" Engineering Mission Assurance in Critical Infrastructure Control Systems

By: Juan Lopez Jr., and Lt. Col. Jeffrey Humphries



Mission assurance enables government agencies to integrate security continuity and risk management practices to develop a day-to-day operational model that safeguards employees and the business. This same philosophy can be applied to DoD Supervisory Control And Data Acquisition (SCADA) networks through the careful integration of risk management and information assurance controls to achieve mission assurance objectives. However, current

DoD Information Assurance (IA) controls have not been updated since 2003 and do not adequately address the security of DoD SCADA systems. This research interviewed U.S. Air Force Civil Engineering subject matter experts representing eight Major Commands that manage and operate SCADA systems across the Air Force enterprise. They ranked 30 IA controls in three categories, and evaluated eight SCADA specific IA controls for inclusion into the DoD IA control framework managed by the Assistant Secretary of Defense for Networks and Information Integration. There was a high preference for system and information integrity, and encryption as key IA controls to mitigate cyber risk. Equally interesting was the strong agreement among

raters on ranking certification and accreditation dead last as an effective IA control. These results are valuable to the Air Force Civil Engineer Support Agency (AFCESA) as they continue to look for innovative ways to reduce the attack surface of USAF control systems. This research was part of a multiyear Critical Infrastructure Protection project sponsored by HQ USAF A4/7. The work was presented at the 9th annual Conference on Security and Management in Las Vegas, NV July 12-15, 2010.



NSA's Cyber Defense Exercise Students Earn Top Score Again!

Students from the Center for Cyberspace Research (CCR) "AFIT" team again earned the best score in the NSA's prestigious Cyber Defense Exercise (CDX)! The annual CDX, held this year April 20-23, pits the cyber security experts from the National Security Agency (NSA) against students from the U.S. military service academies and DoD post-graduate schools. The exercise is sponsored and run by the NSA's Information Assurance Directorate.

The Air Force Institute of Technology's teams participated under the leadership of Mr. Tim Lacey. The team performed very well and had some of the most brilliant cyber students CCR faculty and staff have had the pleasure of working with. In addition to achieving the best score, AFIT virtually aced the cyber forensics inject with 995 out of a possible 1000 points. While AFIT won bragging rights, the coveted CDX trophy is reserved for the undergraduate service academy with the best score. That honor this year went to the United States Naval Academy (USNA) who performed superbly. In addition to AFIT's team and the

USNA, teams from the other U.S. military academies participated including the U.S. Military Academy, U.S. Air Force Academy, U.S. Merchant Marine Academy, and the U.S. Coast Guard Academy. Also participating were the Naval Postgraduate School and the Royal Military College of Canada.



The CDX gives AFIT students real-life experience protecting critical computing resources while their computers are attacked by the NSA "red team" for five days. The computers must operate through the attack and students must ensure computing services remain available to users. The entire exercise is conducted on Virtual Private Networks which provide an isolated environment for the exercise and prevents interference with real-world networks.

Mr. Lacey provided some insight into the 2010 CDX, "This year's exercise incorporated additional realism by adding users who perform typical tasks that end up compromising their computer. For instance, a user opened an e-mail attachment from someone they did not know which immediately installed a virus on their computer that connected back to an attacker at the NSA. Through this, students learned firsthand how difficult it is to secure a network where unsuspecting users inadvertently infect their own computers with viruses.

Student Highlight: Center for Cyberspace Research Excellence Award

The Cyberspace Research Excellence Award was presented to Second Lt. Michael L. Stamat at the Air Force Institute of Technology Graduation Awards Ceremony on March 26, 2010. Lt. Stamat was nominated by Dr. Barry Mullins, "He is academically brilliant, a forward-thinking researcher, and by far demonstrated the most initiative. He is very articulate and writes exceedingly well."

His research built a first-of-its-kind Public Key Infrastructure testbed emulating the entire DoD enterprise. Given the testbed's versatility, it provides an invaluable platform to evaluate authentication techniques for DoD and other federal agencies. The Virtual Infrastructure for Public-key Evaluation & Research (VIPER) provides a framework to assess the leading security services in a Public Key Infrastructure (PKI): smart card logon, encrypted/signed email, and web authentication. VIPER integrates PKI's defensive mechanisms with an elaborate sensor network capable of investigating the strength of its security posture. This unique platform delivers a scalable and adaptable architecture that supports the continued modernization of military systems. Lt. Stamat is currently Crew Commander for the 624th Operations Command.



Dr. Richard Raines presents Lt. Stamat with The Cyberspace Research Excellence Award on March 26, 2010.