Cybercraft is a multi-year research initiative sponsored by the AFRL Information Directorate designed to tackle problems that cyber warriors face every day. In particular, how can we defend our Air Force network assets in a timely manner and with a high degree of predictability so that we keep our vital missions supported? The Cybercraft initiative brings together researchers in academia and industry to answer the question of whether automated defense response is achievable and trustable by commanders of the future. CCR team members have played a vital role in the project since its inception, with active participation in research groups, working groups, and bi-annual workshops. The effort has supported 1 PhD dissertation and 4 Master’s thesis efforts and spawned a variety of related research interest among faculty and students.

Recently, CCR team members have applied their expertise in systems and software engineering to provide the strategic and architectural vision to the project, working with the AFRL team to adopt an end-to-end acquisition mindset related to the research vision. Because the strategic long-term challenge focus areas considered by Cybercraft research are significant, CCR faculty members have conducted several working group meetings to lay the foundations for a holistic, architectural view of the system.

Using the Department of Defense Architecture Framework (DoDAF) and its products (such as the OV-1 seen below) as a basis for refining the project vision and requirements, CCR has helped mold and shape the future success of the effort by creating architectural views that capture the Cybercraft goals. In the end, our faculty have shared their skills, expertise, and background so that the initiative will provide a truly novel technology to meet the needs of the cyber warriors of tomorrow.
The mission of the 57th IAS and 177 IAS is to train USAF, Joint and Allied personnel by replicating current and emerging threats as a professional Information Operations (IO) Organization (OPFOR). This total force team is part of the 57th Adversary Tactics Group (57 ATG) whose mission is to know, teach and replicate threats in air, space and cyberspace. The 177 IAS was attached to the 57 ATG in August 2006 and the 57 IAS was created and activated under the 57 ATG in January 2007. The 57 IAS and 177 IAS have five products and services: 1) Threat academics, 2) Information Operations Roadshow (an installation attack), 3) Tactical-level exercise support (e.g., RED FLAG), 4) Operational-level exercise support (e.g., VIRTUAL FLAG, BLUE FLAG, etc) and 5) Training Syllabus Support with the 67th Network Warfare Wing. As the USAF’s IO Red Team, these squadrons are the “bad guys” for cyberspace warriors to practice and train against, honing and improving capabilities, tactics and operator skills. During 2008, these squadrons trained over 31,500 personnel on IO threats advanced cyberspace topics and integration of cyber into exercises.

The 57 ATG and CCR are building a professional working relationship to share information, leverage each others’ skills, stimulate research and development, and ultimately evolve USAF capabilities to ensure our air, space and cyberspace forces can meet the challenges of today and tomorrow.

“This total force team has been able to make a difference. Despite our short lifetime, we have made an impact by improving friendly forces through threat education and new or expanded training opportunities. Our squadrons focus primarily on training friendly forces which is different from other service/agency Red Teams. Why the emphasis on training? All Airmen play a key part in our network defenses. Everyone who operates on NIPRNet or any classified network is a potential entry point to allow adversaries access to our critical or personal information on those networks. If we do not train people about the threats and how to counter, then our networks will leak vital information to our adversaries.”

Reb Butler, Lt Col, USAF, Commander, 57 IAS

Operational Community Highlight: 57th and 177th Information Aggressor Squadrons

On October 30, 2008, former CCR student Master Sergeant Terry Levoy was selected for promotion to E-9 (Master Gunnery Sergeant) in the United States Marine Corps. Since his graduation from AFIT in June 2006, he served as the Network Defense Plans Chief in the Marine Corps Network Operations and Security Command (MCNOSC) located at Quantico, Virginia. The MCNOSC provides global network operations and computer network defense for the Marine Corps Enterprise Network (MCE), MSgt Levoy is responsible for identifying future security requirements and to plan for the implementation and sustainment of technical security solutions that ensure effective MCEN Computer Network Defense in support of USMC operational requirements.

The USMC Information Assurance field currently only has four E-9 billets. Of these, 75% are currently filled by AFIT Information Assurance Scholarship Program (IASP) senior enlisted graduates, MGySgt Artie Crawford, MGySgt Irene Johnson, and MGySgt (Selec) Terry Levoy.

CCR Graduate promoted to the highest enlisted tier in the US Marine Corps Information Assurance Field

Michael Russell Grimaila (CISIM, CISSP, NSA IAM/JEM) is an Associate Professor of Information Resource Management in the Systems and Engineering Management department. He received a BS and MS degree in Electrical Engineering, and a Ph.D. in Computer Engineering at Texas A&M University. He has authored more than 60 articles in the areas of information assurance, information operations, information warfare, critical technology protection, and computer design and testing.

“The cyberspace domain has evolved into the domain of uncertainty with so many intricate pieces. Whether it be looking at computer networks, voice and satellite communications, or even electronic warfare, completing a cybersecurity thesis has presented me with several possible topics of interest. Dr. Grimaila has been instrumental in hammering out my small piece of the cyberspace domain to be successful. He presented me with his vast knowledge of topics and allowed me to choose one and run with it. Dr. Grimaila’s guidance, insight, patience and support throughout the course of my research has been invaluable to ensuring my academic success.”

Thomas Moore, 1st Lt, USAF, AFIT Masters in Cyber Operations

Faculty Focus: Dr. Michael R. Grimaila

Dr. Grimaila is the primary investigator on the Cyber Incident Mission Impact Assessment (CIMIA) project, sponsored by Air Force Research Laboratory Human Effectiveness Directorate (AFRL/RH), which is developing an operational process that provides timely mission impact notification and impact assessment, information operations, information warfare, critical technology protection, and computer design and testing. Dr. Grimaila joined the Center for Cyber-space Research in August 2004 and has supported more than 20 research grants providing benefits to the Air Force, the DoD, and other national agency sponsors. He has successfully chaired research committees for 28 MS students and served on numerous other PhD and MS committees.

A&M University, AFRL Human Effectiveness Directorate, and AFRL Information Directorate.

Student Highlight: Karl Schrader, Major, USAF

Major Karl Schrader joined AFIT in Fall 2007 in the Computer Engineering Master’s Program. His thesis, “A Novel Methodology for Detecting and Tracking Capture-Preempt Peer-to-Peer Protocols,” built a hardware-based forensic tool to analyze peer-to-peer (P2P) traffic on a network to identify specific files. Several methods have already been developed to accomplish this task and are in use today. However, all of these methods depend on the use of honeypots to lure targets into downloading contraban material. In contrast, Karl’s research created a suite of hardware and software tools to detect peer-to-peer transmissions on a target network, classify them by specific peer-to-peer protocol, compare the digital file being transmitted against a contraban list, and identify the sender and recipient by internet protocol (IP) address. The most valuable feature of the suite is the targets have no way of knowing they are being monitored. The suite can analyze all peer-to-peer traffic on a high-utilization (90 Mbps of traffic) network with near 100% efficiency. To demonstrate the robustness of the tools, Maj Schrader added the ability to simultaneously track Voice over IP (VoIP) calls and provide both sender and receiver phone numbers. In fact, the tool suite provides a flexible platform that allows additional P2P protocols to be added easily with minimal performance reduction. Given the suite’s versatility, it provides numerous benefits to the US Government and law enforcement agencies by helping to identify senders and receivers of child pornography transferred over networks, detecting exfiltration of sensitive files from networks, and tracking VoIP call patterns in criminal organizations. Major Schrader is sponsored by AFIOC and advised by Dr. Barry Mullins. Karl is scheduled to graduate in March 2009 with a follow-on assignment tentatively with United States Joint Forces Command.