Information Assurance Workshop

October 24-25, 2005

UAF UNIVERSITY OF ALASKA FAIRBANKS

Agenda

8:30-9:45 a.m.	UAF and CAE Programs, *Dr. Kara L. Nance*
9:45-10:00 a.m.	Break
10:00-11:00 a.m.	Reasons Why Businesses Should Care about Information Warfare, *Dr. Julie Ryan*
11:00-12:00 p.m.	Institutional and Professional Liability in Information Assurance, *Dr. Dan Ryan*
12:00-1:00 p.m.	Lunch
1:00-2:00 p.m.	Information Assurance Outreach, *Dr. Melissa Dark*
2:00-3:00 p.m.	Virtualization (VMware) and Laboratory Construction, *LtC Ronald C. Dodge, Jr.*
3:00-3:15 p.m.	Break
3:15-4:00 p.m.	ASSERT Lab tour

Biographies

Dr. Kara Nance is a Professor of Computer Science and Software Engineering at the University of Alaska Fairbanks. After receiving her Ph.D. from the University of Oklahoma, Kara taught at Medaille College before returning to Alaska to teach at UAF. She is currently the director of the Advanced System Security Education, Research and Training (ASSERT) Center, and has also served as the Director of the Syncon Environmental Data Center at the University of Alaska Fairbanks since 1999. Her current research interests include computer security, artificial intelligence, and data systems.

Dr. Melissa Dark is Associate Professor in Computer Technology and Asst. Dean in the School of Technology at Purdue University. She has extensive experience in post-secondary science, technology, engineering, and mathematics (STEM) education. Melissa is the Asst. Director for Educational Programs for CERIAS at Purdue, and leads several outreach projects for the program. She is a member of the CERIAS internal advisory board that oversees the interdisciplinary M.S. in IA and Security, and teaches a service learning class in information security risk assessment wherein students perform information security risk assessments for K12 school districts in Indiana. She is working with CS faculty from across the nation on a project to produce a book in information security ethics, and has been active in helping define the IA discipline by leading a group that worked on a common body of knowledge in information security education.

Dr. Julie Ryan began her career as an intelligence officer after graduating from the Air Force Academy in 1982. She transitioned from active duty Air Force to civilian service with the Defense Intelligence Agency, where she supported early attempts to understand how to develop multi-level secure computer systems, including directing and monitoring the design, development, and delivery of secure databases. Her responsibilities spanned budget and program management techniques, system design and engineering practices, data base design, intelligence data requirements, information security concepts, user capabilities and knowledge base, and human engineering. Since leaving government service, Dr. Ryan has continued working in security engineering, and has prepared various white papers, including an Information Order of Battle concept briefing, a concept exploration of intelligence support to information warfare. Dr. Ryan currently teaches and directs graduate research in information security related topics at George Washington University in Washington, D.C. Dr. Ryan is co-author of *Defending Your Digital Assets*, as well as numerous papers and monographs.

Dr. Daniel J. Ryan is a Professor of Systems Management at the National Defense University, teaching information security, information assurance, cryptography, network security and computer forensics. Prior to joining NDU, he was a lawyer in private practice, a businessman and an educator teaching law and information security for George Washington University. He has served as Corporate V.P. of Science Applications International Corporation with responsibility for information security for government and commercial clients who operate worldwide and must create, store, process and communicate sensitive information and engage in electronic commerce. Dr. Ryan has also served as Exec. Assistant to the Director of Central Intelligence, and has served as Director of Information Systems Security for the Office of the Secretary of Defense. His specific areas of responsibility spanned information systems security (INFOSEC), classification management, communications security (COMSEC) and cryptology, computer security (COMPUSEC) and transmission security (TRANSEC), as well as TEMPEST, technical security countermeasures (TSCM), operational security (OPSEC), port security, overflight security and counter-imagery. Dr. Ryan began his extensive career at the National Security Agency.

Lieutenant Colonel Ronald C Dodge, Jr., Ph.D. has served for over 17 years as an Aviation officer and is a member of the Army Acquisition Corps in the U.S. Army. His military assignments range from duties in an attack helicopter battalion during *Operation Just Cause* in the Republic of Panama to the United States Military Academy. Currently he is an Asst. Professor permanently stationed at the U.S. Military Academy and the Director of the Information Technology and Operations Center (ITOC). Ron received his Ph.D. from George Mason University, Fairfax, Virginia in Computer Science. His current research focuses are information warfare, network deception, security protocols, internet technologies, and performance planning and capacity management. He is a frequent speaker at national and international IA conferences and he has published many papers and articles on IA topics.

Presentation Abstracts

Institutional and Professional Liability in Information Assurance

We cannot teach students to defend information infrastructures without teaching them how to attack such infrastructures either in theory or in practice. Sooner or later, even if due diligence is exercised in choosing whom to teach and what to teach them, some student will abuse the information and techniques we have taught them. Those harmed when such an abuse occurs may seek redress by seeking to impose liability on the institutions and professors who taught the student the skills and perhaps provided the tools used to commit the harm. Clearly we have a responsibility to teach our students ethical and legal constraints that apply to their uses of the knowledge we impart. Regarding hazardous activities, we also have a duty to ensure they understand the societal expectations regarding even such activities that we do not teach them.

Reasons Why Businesses Should Care about Information Warfare

When geopolitical entities, such as nation-states, go to war, infrastructures that also support civilian enterprises are always involved and generally are targeted or used by the military forces. Today, that includes the information infrastructure -- that engine that powers the global supply chain, just in time logistics, telecommuting, and other vital aspects of modern life. Who owns and operates that infrastructure? Another way of posing that question is: Who stands to lose? The answer includes not only the direct service providers and physical plant owners, but also the enterprises that rely on that infrastructure as a critical enabler of business processes.

Information Assurance Outreach

This presentation will focus on IA outreach activities at CERIAS, some of the key components of successful outreach, and approaches to starting a successful outreach program.