Department of Computer Science Colloquia Series
Distinguished Speaker

Dr. Michael T. Kurdziel

Senior Manager/Chief Cryptographer
Communications Security Products Group
Harris Corporation, RF Communications Division

Tuesday, February 17th, 2009, 1 p.m.
GCCIS room 70-3435

Military Threat Model and Cryptographic Response MK-128

Abstract: With the continued international proliferation and advancement of military communication technology, equipment vendors are challenged to provide communications security (COMSEC) solutions that are appropriate to these applications. Here, the impact of a security compromise is significantly more severe than in either industrial or consumer applications. In military applications, the threat is targeted and extreme. This presentation begins with an introduction to the military tactical radio threat model. This provides the background for discussion on the unique requirements for COMSEC products in Military and Government applications. The presentation is concluded with an overview of the Harris MK-128 cryptographic algorithm. This algorithm was designed specifically to meet the security requirements of international government and military communication applications and to counter the associated threat model.

Bio: Michael Kurdziel is Sr. Managing Engineer, Secure Communications Products Group, for Harris Corporation. His area of technical expertise is secure communications systems design. This includes the design of encryption, key management and authentication systems and algorithms. Dr. Kurdziel is a member of the International Interoperable Communications Working Group (I-ICWG). The charter of this group is the development and propagation of the Secure Communications Interoperability Protocol (SCIP). He is the principal algorithm architect for the MK-128 and MK-256 algorithms used in the Citadel and Citadel II Encryption Devices. The devices are Harris Corporation's primary encryption solution for non-Type 1 applications. The algorithm designs have been critically reviewed by industry experts and have been found to have superior cryptographic strength. Papers on the Citadel and Citadel II architectures were presented to critical acclaim at the IEEE's 1998 and 2004 MILCOM conferences, respectively.
