

# RFID Security Consortium Receives \$1.1 Million NSF Grant

Comprised mostly of academics, the group hopes to develop ways to improve security measures for RFID systems, and to incorporate the study of RFID into engineering curricula.

By Mary Catherine O'Connor

Sept. 8, 2006—The National Science Foundation (NSF) has awarded a \$1.1 million grant to a consortium studying the privacy and security implications of RFID technology. This group, the RFID Consortium for Security and Privacy (RFID CUSP), is comprised of academics and industry representatives tasked with researching ways in which RFID applications may impact consumer security and privacy. The group will also suggest methods for ensuring that RFID is deployed in a manner that makes it safe both for consumers and for companies incorporating the technology into their businesses. CUSP hopes to develop cryptographic protocols and work with standards bodies to incorporate stronger data protection tools into standard tag and reader protocols, as well.

The \$1.1 million grant will be used by professors and graduate students at two academic institutions: the University of Massachusetts Amherst (UMass) and The Johns Hopkins University. Kevin Fu, assistant professor in the computer science department at UMass, is leading the consortium, with assistance from Wayne Burleson, UMass professor of electrical engineering, and from Adam Stubblefield, assistant research professor of computer science at Johns Hopkins. Fu and his colleagues in the consortium applied for the NSF grant last year.

Computer security firm RSA Laboratories, represented by its manager and principal research scientist, Ari Juels, is taking a central role in the consortium, as both a sponsor and by participating in the development of security tools and protocols. Fu hopes the grant will also be used to develop undergraduate engineering courses focused on RFID technology and security tools.

"Our plan is to look at ongoing [RFID] deployments and how to make them strong in respect to privacy and authentication," Fu says, adding that the RFID security tools and software the group generates will be freely available as open-source software.

For the past few years, RSA has been examining security vulnerabilities of RFID-based systems for payment and automatic-identification applications (see RSA Security Designs RFID Blocker, Attack on a Cryptographic RFID Device and Tag Implants May Be Dangerous for Security Apps, Says Group). As a developer of security tools for the Internet, RSA provides ways for RFID systems to protect data collected from or encoded to tags.

In addition to enabling payment and automatic-ID applications, Juels explains, RFID systems can also be used as security tools, such as key fobs for cars or contactless smart cards in access control. However, as currently deployed, these types of tags do not have sufficient protections from hackers. Adding cryptography to tags, especially to passive ones with small amounts of onboard processing power, represents a major challenge to

cryptographers. Still, overcoming this hurdle is of increased importance as RFID technology proliferates.

When securing data in an RFID system, Juels says, there are two main goals: to scale security down to the constraints (limited memory) of the tag; and to scale security up in the back-end systems that also store sensitive data.

The consortium will include an advisory committee, currently composed of RSA and California's Bay Area Rapid Transit (BART). According to Juels, the consortium hopes to grow the committee. Its role will be to present an industry perspective on the security tools and policies proposed by the consortium. "[The advisory group] has committed to giving [CUSP] a dose of reality as to whether what we devise makes sense in real-world applications," explains Juels.

William Wong, principal engineer of the Automatic Fare Collection Capital Program for Transit System Development department at BART, will sit on this advisory committee. "BART is interested in the technology used to improve the security of smart cards," he says, "and the research that Professor Fu is conducting may benefit mass transit in the future." BART has piloted an RFID-based transit-card system and has begun to roll it out.

"Our plan is to look at ongoing deployments and how to make them strong in respect to privacy and authentication," explains Juels. The consortium's first planning meeting is scheduled for later this month. CUSP does not yet have any other fixed timeline at present. However, in the next year or so, it hopes to develop authentication techniques compatible with Electronic Product Code (EPC) tags and readers (interrogators).

Copyright ©2005 RFID Journal, Inc. All Rights Reserved