

*For additional information on Cryptography Research:*

Patrick Corman  
Corman Communications  
(650) 326-9648  
Patrick@cormancom.com

David Finkelstein  
Corman Communications  
(917) 523-1161  
david@cormancom.com

**FOR IMMEDIATE RELEASE**

## Radical New Development Methods Needed To Avert Potential Security Disasters

Expert Offers New Solutions for Improving Flawed Security Development Processes at RSA Conference & Expo

**SAN FRANCISCO, Calif., April 11, 2003** -- The best computer security teams focus on preventing unwanted surprises, yet according to security expert Benjamin Jun, many managers continue to apply technology management methods that are inadequate for high-risk environments. Jun, vice president of Cryptography Research, Inc., believes it is time to rethink how managers approach the development of mission-critical security projects. He will present his views, along with techniques for managing secure projects in his seminar on Monday, April 14 at the RSA Conference 2003 in San Francisco.

According to Jun, mission-critical security systems require fundamentally different engineering processes than conventional engineering efforts. While traditional engineering design is focused towards meeting functional requirements, designers of mission-critical systems also must minimize the probability that a security failure will be present. Good project managers avoid security problems by using disciplined engineering to prevent bugs and applying well-coordinated development and validation to screen for problems.

"Designers working on mission-critical security must focus on minimizing the odds of security flaws, yet most engineers have had little, if any, training to teach them the skills necessary to do this effectively," said Jun. "While students at every medical school meet weekly to discuss surgical errors and methods for preventing them, I don't know of a single computer

science program that meets even once a semester to discuss software bugs or practical ways to avoid them."

Jun describes the security technology industry as a field still in relative infancy and relates security development processes with more mature high-risk fields, such as nuclear power plant operations, surgical medicine, and aircraft carrier deck operations. He discusses radical methods that can be adopted by managers of mission-critical systems for developing staff, generating specifications, validating designs, and responding to disasters.

"Although it's impossible to prove that a system will be secure, many managers fail to take even simple steps towards reducing the possibility that they'll ship a disaster," said Jun. "By failing to consider how engineering choices affect the system's life cycle, managers can create systems that are impossible to validate and impractical to repair."

Benjamin Jun's talk, "It Takes A Village: Managing a Mission-Critical Security Project," is part of the Security Solutions Track at the RSA Conference 2003, and will be presented on Monday, April 14, at 10:15 a.m. in Theater 9 at the Sony Metreon theater complex adjacent to the Moscone Convention Center in San Francisco.

Benjamin Jun is vice president at Cryptography Research, where he specializes in the design, evaluation and repair of high-assurance security modules for software, ASIC and embedded systems. He heads the consulting practice and participates in the company's research efforts. Jun holds B.S. and M.S. degrees from Stanford University, where he is a Mayfield Entrepreneurship Fellow.

### **About Cryptography Research, Inc.**

Cryptography Research, Inc. provides consulting services and technology to solve complex security problems. In addition to security evaluation and applied engineering work, CRI is actively involved in long-term research in areas including tamper resistance, content protection, network security, and financial services. This year, security systems designed by Cryptography Research engineers will protect more than \$50 billion of commerce for wireless, telecommunications, financial, digital television, and Internet industries. For additional information or to arrange a consultation with a member of the company's technical staff, please contact Jennifer Craft at 415-397-0329 or visit [www.cryptography.com](http://www.cryptography.com).

###