

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

Paul Kocher to Present Keynote Talk at RSA Conference 2003

Security Expert Warns Most Security Products Ineffective for Protecting High-Threat Systems

RSA CONFERENCE 2003, SAN FRANCISCO, Calif. April 14, 2003 -- While off-the-shelf security products may be adequate for protecting most computer systems, they have a poor track record against the rational, determined and intelligent attackers that target critical installations, according to Paul Kocher, president and chief scientist of Cryptography Research. In his keynote address at the RSA Conference 2003, to be presented Tuesday, April 15 at 3:45 p.m. at Moscone Center in San Francisco, Kocher explains why those wanting to secure such high-threat systems need to pursue radically different approaches than those used for lower-threat environments.

According to Kocher, 95 percent of computer users have relatively meager security needs, having only to worry about being caught in the crossfire of Internet security attacks. Most computer users today are primarily exposed to relatively random security incidents which, while disruptive, can largely be addressed with conventional products. The remaining 5 percent – high-threat systems such as those used to prevent financial fraud, espionage, piracy, and other crimes – have to be secure against targeted attacks from intelligent adversaries.

"In many cases, an organization simply seeks to avoid operating the easiest system to attack," said Kocher. "These organizations are well served by off-the-shelf products, which are great at blocking most Internet threats. Unfortunately, high-risk systems under attack by motivated individuals are not so easily protected. In high-risk environments, you need confidence that your security can resist attacks from intelligent adversaries. The problem largely

comes down to one of software quality: although lots of vendors claim to be secure, the dirty secret is that most of these products have bugs or design flaws that make them insecure."

Kocher suggests a variety of techniques that companies can use to increase assurance and to handle difficult security risks. For example, Kocher suggests that instead of allowing Internet access from networks that contain critical information, companies can reduce their risks by providing two computers to each of their users, and operating separate high-security and low-security networks. According to Kocher, the security benefits of separation justify the additional costs in many high-threat environments.

Kocher recommends treating security as a business problem by assigning a dollar-value to major risks and using this estimate as a basis to determine whether security spending is worthwhile. Kocher's other suggestions for protecting high-threat environments include minimizing complexity, making realistic assumptions, looking out for overconfidence, making proper use of evaluations and testing, maintaining a healthy dose of skepticism, planning for the unexpected, and employing both internal and external expertise.

Paul Kocher has gained an international reputation for his consulting work and academic research in cryptography. His research projects have included designing and co-authoring SSL v3.0, discovering timing attack cryptanalysis, and architecting the record-breaking DES Key Search machine, Deep Crack. At Cryptography Research, he also led the team that discovered Differential Power Analysis, as well as the countermeasures for securing smart cards and other devices against these attacks. His work has been reported in forums ranging from technical journals and *Scientific American* to CNN, National Public Radio, and the *New York Times*. Paul holds a B.S. degree in biology from Stanford University.

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.