

For additional information contact:

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

Karen Burke
Corman Communications, LLC
(650) 938-6852
karen@cormancom.com

FOR IMMEDIATE RELEASE

Cryptography Research to Present at RSA Conference 2004

Security Experts Paul Kocher, Benjamin Jun and Nate Lawson Selected to
Contribute to Conference Program

RSA CONFERENCE 2004, SAN FRANCISCO, Calif., February 23, 2004 – Cryptography Research, Inc. announced that its staff was selected to lead a number of program lectures and panel discussions at RSA® Conference 2004, San Francisco, February 23-27, 2004. Talks will be presented by Paul Kocher, president and chief scientist; Benjamin Jun, vice president; and Nate Lawson, senior security engineer. The talks will present lessons from the staff's experience with working on some of the world's most challenging and high-threat security systems.

“Cryptography Research continually works with market leaders in a variety of industries to secure financial transactions, Hollywood movies, pay television, PC hardware, and critical infrastructure,” said Kit Rodgers, director of licensing at Cryptography Research, “We are pleased that our technology staff lead in their fields and continue to be selected as contributors to the world's largest security conference.”

Paul Kocher will dispel the myth that security experts are mysterious scientists with vast stores of incomprehensible knowledge in his talk, “How to Think Like a Cryptographer.” His talk shows how tackling “impossible” security problems involves a process of recognizing tiny security cracks and finding creative ways to combine seemingly inconsequential defects into a complete attack.

In another session, “Self-Protecting Digital Content,” Kocher will describe a new security architecture based on risk management approaches to control piracy. This architecture,

developed by Cryptography Research, is a leading contender with Hollywood studios and consumer electronics companies for securing high-definition movies on next-generation high-definition optical media formats.

Kocher will also participate in two panel discussions. In the Cryptographer's Panel, Kocher will join Bruce Schneier, Whitfield Diffie, Adi Shamir and Ron Rivest to discuss recent security events and new cryptographic developments. In "Proactive and Reactive Security: What's the Best Mix?," Kocher and other panel members will explore and debate the advantages of two opposing approaches to security.

Benjamin Jun will address the challenges of authoring security specifications on the Secure System Development panel. Jun will show actual security system designs that either addressed or spectacularly failed to meet a system's security needs. By understanding the root causes of security flaws, the panel seeks to help developers reduce the probability of future surprises.

Nate Lawson takes a look at the future of platform security in "Designing and Attacking Virtual Machines." Lawson will describe how attackers use virtual machines to break content protection systems and how engineers use them to sandbox hostile code. He will address many of the emerging security issues, such as emulation detection, API security, and performance issues.

Cryptography Research Conference Talk Schedule

Tuesday, February 24, 2004

11:00 AM – Cryptographers' Panel, Paul Kocher

3:00 PM – Secure System Development, Developers Track, Benjamin Jun

5:15 PM – How to Think Like a Cryptographer, Developers Track, Paul Kocher

Wednesday, February 25, 2004

9:00 AM – Proactive and Reactive Security: What's the Best Mix?, Applied Security Track, Paul Kocher

Thursday, February 26, 2004

11:15 AM – Designing and Attacking Virtual Machines, Hackers & Threats II Track, Nate Lawson

Friday, February 27, 2004

9:00 AM – Self-Protecting Digital Content, Wireless and Embedded Systems
Track, Paul Kocher

About the Presenters

Paul Kocher, president and chief scientist, has gained an international reputation for his consulting work and academic research in cryptography. An active contributor to major conferences and standards bodies, Paul has designed many cryptographic applications and protocols including SSL v3.0. His development of timing attacks to break RSA and other algorithms received front-page coverage in several major publications. More recently he has led research to develop Differential Power Analysis and designs for securing smart cards and other devices against these attacks, as well as to design a record-breaking DES Key Search machine. Paul holds a B.S. degree from Stanford University.

Benjamin Jun, vice president, heads the consulting practice and the company's Content Security Research Initiative. He leads engineering groups in the design, evaluation and repair of high-assurance security modules for software, ASIC and embedded systems. Ben holds B.S. and M.S. degrees from Stanford University, where he is a Mayfield Entrepreneurship Fellow.

Nate Lawson, senior security engineer, is focused on the design and analysis of network security devices. He is the original developer of ISS's RealSecure and several storage appliances. At InfoGard Laboratories, Nate assisted Netscape, IBM and Motorola with their FIPS 140 cryptographic certifications. He also consulted with various companies to develop various tools including a fast network mapper (win32), NAT TCP splicer, and layer 2 IPSEC appliance. Nate co-founded and built Elite.Net, a central California ISP.

About the RSA Conference

Now in its 13th year, the RSA Conference brings together decision-makers and influencers from all major markets, including consumer, education, financial, government, computer networking, telecommunications, Wall Street and the media for one of the industry's premier e-security and cryptography events. For more information, visit www.rsaconference.com.

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 our technical staff, please contact Jennifer Craft at 415-397-0329 or visit www.cryptography.com.

###