



February 24, 2012

Cryptography Research Executives to Participate in Four Sessions at RSA Conference 2012

SAN FRANCISCO--(BUSINESS WIRE)-- Cryptography Research, Inc.:

Who: Cryptography Research, Inc., a division of Rambus Inc.

Where: RSA Conference 2012
Moscone Convention Center
San Francisco, CA

When: February 27 — March 2, 2012

At the 2012 RSA Conference, executives at Cryptography Research, Inc. (CRI), a division of Rambus, will lead and participate in four sessions and panels that address topics ranging from general security matters to mobile device threats to bringing promising security technologies to scale.

Additionally, Paul Kocher, president and chief scientist at CRI, will be participating as a judge in RSA's Innovation Sandbox, a half-day program dedicated to exploring and evaluating new and promising information security technologies.

CRI will also demonstrate (Booth # 1039) and discuss its differential power analysis (DPA) countermeasures as well as its hardware-based security core solution, CryptoFirewall™. For additional details, visit www.cryptography.com

Cryptography Research, Inc. Presentations:

Monday, February 27, 2012

Title: Security Basics Seminar

8:30 a.m. — 5:00 p.m. — Room 307

Benjamin Jun, vice president & chief technology officer at CRI and executives at CERT, Cigital, Delphiis, iSEC Partners, Juniper Networks, Omgeo and RSA

In this day-long course, Benjamin Jun will join other security thought-leaders to discuss some of the most important security principles and technologies. The course is designed to lay a foundation of essential concepts that will enhance participants' understanding of the advanced security issues to be discussed throughout the RSA Conference.

Title: New Technology Innovation Sandbox

1:00 p.m. — 6:00 p.m.

Paul Kocher, president and chief scientist at CRI, and executives at Greylock Partners, In-Q-Tel, Red Cross, Sophos and The McGraw-Hill Companies

In this half-day program, Paul Kocher and other leading security leaders will explore and evaluate new technologies that promise to transform the information security industry, now and in the future, including the "Most Innovative Company at RSA Conference 2012" contest.

Wednesday, February 29, 2012

Title: Innovation and Technology Transfer in Security: From the Lab to General Use

8:00 a.m. — 9:10 a.m. — Room 310

Paul Kocher, president and chief scientist at CRI, and executives at Cigital, Fortify Software, the National Science Foundation, and the Naval Postgraduate School

In this session, Paul Kocher will join other distinguished innovation experts and entrepreneurs to discuss their experiences in making technology transfer work; exploring key gaps in a system where security technologies move from start-ups, to early adopters, to global technologies.

Title: Minding the App Store - Protecting Software and Device Features

9:30 a.m. — 10:10 a.m. — Room 302

Benjamin Jun, vice president & chief technology officer at CRI

This talk focuses on "app store" business models—the shiny new platform capabilities that can be unleashed with simple enablement messages, and the potential vulnerabilities that occur when locked features are valuable. Learn developer techniques for protecting platform features, building infrastructure for cryptographic authorization management, and defending software clients from unauthorized upgrades.

Friday, March 2, 2012

Title: Is Your Mobile Device Radiating Keys?

8:00 a.m. — 8:50 a.m. — Room 305

Benjamin Jun, vice president & chief technology officer at CRI and Gary Kenworthy, senior principal engineer at CRI

In this session, CRI will explain why EM emission from mobile devices may be leaking cryptographic keys. A mobile app can inadvertently radiate secret data as cryptographic processing is done by the CPU. The session will include a live demonstration where a simple antenna and radio are used to perform key extractions from several modern handheld devices. Participants will learn several techniques developers can use to mitigate risk whenever applications use high-valued cryptographic keys.

About Cryptography Research, Inc.

Cryptography Research, Inc. (CRI), a division of Rambus Inc., is a leader in semiconductor security research and development. Established by internationally renowned cryptographer Paul Kocher, CRI develops and licenses innovative technologies in areas including tamper resistance, content protection, anti-counterfeiting, network security, and financial services. Over six billion security products are made each year under license from CRI. Security systems designed by CRI scientists and engineers protect hundreds of billions of dollars in commerce annually. Additional information is available at www.cryptography.com.

[Rambus Inc.](#)

Carolyn Robinson, 408-462-8717

crobinson@rambus.com

or

Schwartz MSL for CRI

Dan O'Mahony, 415-512-0770

cri@schwartzmsl.com

Source: Cryptography Research, Inc.

News Provided by Acquire Media