

*For additional information on Cryptography Research:*  
Patrick Corman  
Corman Communications  
(650) 326-9648  
Patrick@cormancom.com

**FOR IMMEDIATE RELEASE**

## Moore's Law Threatens Computer Security

Security Expert Paul Kocher to Address Issues and Offer Solutions at Upcoming  
USENIX Conference

**SAN FRANCISCO, Calif., August 7, 2002** – Moore's Law, the prediction that computational power would continue to double roughly every 18 months, may have a dark side, according to security expert Paul Kocher, creating a crisis situation where computing systems are much more vulnerable to attacks. Kocher believes it's time to rethink how secure systems are designed, and will present his views, along with techniques to make systems more secure, in his seminar tomorrow, Thursday, August 8 at the 11<sup>th</sup> USENIX Security Symposium in San Francisco.

According to Kocher, the rapid increase in computing horsepower – first expressed by Intel co-founder Gordon E. Moore and known as Moore's Law – has been the driving force behind the creation of increasingly complex systems. But as complexity increases, so do the number of avenues and opportunities for attack. Kocher's talk will show techniques used by evaluators and attackers to break overly complex, poorly tested designs, and will review basic engineering approaches that can improve security assurance.

"Moore's Law, coupled with the business imperative to be more competitive, is driving vendors to build systems of exponentially increasing complexity without making security experts exponentially smarter to compensate," said Kocher, president of Cryptography Research, Inc. "Doubling the number of components or lines of code in a product quadruples the number of possible interactions, making security flaws increasingly difficult to avoid or detect."

According to Kocher, security specifications themselves are becoming so complex that often no single person even understands the entire system. "There is a general belief that cryptography gets stronger as systems get faster. While this is true for simple brute force attacks, design and implementation flaws are how attackers actually break into systems," he said. Kocher

will offer attendees techniques and tools they can use to manage this complexity and make systems more secure.

Paul Kocher has gained an international reputation for his consulting work and academic research in cryptography. An active contributor to major conferences and standards bodies, Kocher has designed and co-authored many cryptographic applications and protocols, including SSL v3.0. He also directed research efforts that designed a record-breaking DES Key Search machine, discovered Differential Power Analysis, and have helped secure smart cards and other devices against attack.

### **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 \$30 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, contact Jennifer Craft at 415-397-0329 or visit [www.cryptography.com](http://www.cryptography.com).

###