

For additional information:

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

Karen Burke
Corman Communications
(650) 938-6852
kburke@cormancom.com

FOR IMMEDIATE RELEASE

**Cryptography Expert Paul Kocher Warns: Future DVDs Prime Target
for Piracy, Pay TV Foreshadows Challenges**

NAB 2004, LAS VEGAS, NV, April 20, 2004 – Movie piracy today is still immature in the United States, but as available storage space and bandwidth increase, so will the motivation and sophistication of movie pirates, warns security expert Paul Kocher, president and chief scientist of Cryptography Research, Inc. Kocher believes that future optical media formats – the successors to today’s DVD – will require dramatically advanced content protection technology and enforcement measures just to keep up with the better-funded and more-determined adversary of tomorrow.

Kocher believes the current pay television piracy problem can be seen as a harbinger of things to come for optical media. “Movies are still difficult enough to copy, so that for most people, it isn’t worth the hassle,” he said. In the United States today, the movie industry is primarily chasing mischievous college students, internal leakage and low-quality analog recordings as the sources of piracy, according to Kocher. “By contrast, in the pay television industry, we routinely face well-funded, technically sophisticated pirates, many of whom are closely connected with organized crime networks. It’s ultimately a question of whether people perceive piracy to be worthwhile,” he said.

Kocher believes the very thing that makes successors to DVD more attractive to consumers – high-definition content – will also make them more attractive to pirates. Although the larger file size of new high-quality optical media formats like Blu-ray or HD-DVD movies

will slow many pirate efforts by perhaps two years, high-definition content is a much more attractive target for attackers because, in many cases, it represents the best quality studios have to offer.

“While it’s unfortunate that security on the current DVD format is broken and can’t be reprogrammed, HD is what really matters. Once studios release high-definition content, there will be little or no distinction between studio-quality and consumer-quality,” said Kocher. “This means that HD is probably Hollywood’s one and only chance to get security right.”

According to Kocher, Hollywood is following a path common to other industries facing similar problems. “Typically, first-generation security systems fail irrecoverably, but later generations are designed to recover from failures,” Kocher said. As an example, he cites K-band (“big dish”) satellite TV systems, which suffered from devastating piracy because security flaws could not be corrected. Having learned this lesson, modern pay TV systems place critical security components in smart cards or security modules that can be replaced. While this approach is not optimal because hardware upgrades are expensive, it has enabled the industry to keep piracy at survivable levels.

For movie studios, optical media has so far followed a parallel path. The content protection system for DVDs was designed without renewable security, and has now been broken irrecoverably. “Just as the transition to digital broadcasts provided satellite providers with the opportunity to change to a better approach for security, new format initiatives such as Blu-ray and HD-DVD present an opportunity for the optical media industry to correct its dysfunctional security architecture,” Kocher said.

“The problem is urgent because it takes several years for security efforts to pay off. Everybody’s worst fear is that Hollywood will follow in the music industry’s steps and fail to make progress due to political maneuvering and a lack of technical leadership,” said Kocher. “On the other hand, if security decisions reflect a disciplined analysis of the long-term business requirements, I still think it is possible to keep piracy at a manageable level. Even in the best case, though, things are going to get much worse before they get better.”

About Paul Kocher

Paul Kocher has gained an international reputation for his work in the field of cryptography. Kocher has designed and co-authored many cryptographic applications and

protocols, including SSL v3.0. At Cryptography Research, he leads a team of scientists and engineers who specialize in developing technology to help solve real-world data security problems. Research efforts he directed include successfully building the record-breaking DES Key Search machine, discovering Differential Power Analysis, and developing technologies that are used widely to secure pay television systems and smart cards against attack.

About Cryptography Research, Inc.

Cryptography Research, Inc. provides technology and services 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 \$60 billion of commerce for wireless, telecommunications, financial, digital pay television, and Internet industries. For additional information or to arrange a consultation with a member of the technical staff, contact Jennifer Craft at 415-397-0329 or visit www.cryptography.com.

Cryptography Research is exhibiting at Booth SU7779 at the National Association of Broadcaster's annual conference, NAB 2004, April 17-22 in Las Vegas.

###