

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

Cryptography Research Study Concludes Risk Management Key to Controlling Piracy of Digital Media

Forensic Marking, Programmable Code Offer Most Practical, Effective Solution

SAN FRANCISCO, Calif. April 15, 2003 – As part of an a multi-year effort to study technical solutions for controlling piracy, Cryptography Research, Inc. today publicly released a paper entitled "Self-Protecting Digital Content".

The paper's contributions include the first practical methods for securely embedding forensic data in decrypted output from consumer devices as a way to enable publishers to determine the specific methods and devices used to produce pirate copies. The new forensic marking techniques can discourage would-be pirates by addressing the anonymity of piracy, but would not affect the privacy of legitimate users.

The research shows how programmable security logic can be integrated with content, allowing publishers to design new security features for each title instead of relying on static player-based protection mechanisms. According to the authors, the combination of forensic marking and programmable security can enable publishers to control piracy using risk management techniques analogous to those used to protect credit/debit card payment networks. Forensic marking can provide the risk management requirement to identify and trace attacks, while programmable security mechanisms provide the ability to respond to piracy.

From a policy perspective, the research is significant because it offers a middle ground in the debate over whether to mandate anti-copying technologies in all new products. The research also shows that future distribution formats can reduce the burden on device makers to provide

security by allowing content owners to define their own security mechanisms and control their own risk.

The study also highlights the need for rights holders to provide stronger leadership in the effort to improve security, as other participants lack the motivation, expertise or resources to ensure the deployment of effective anti-piracy technologies. "Investments in security have been inadequate relative to the major economic threat posed by piracy," said Benjamin Jun, vice president of Cryptography Research. "After successfully lobbying for the Digital Millennium Copyright Act, publishers have failed to present a coherent long-term technical strategy."

The architecture described by Cryptography Research incorporates a simple virtual machine with decoding devices. During playback, content-specific code running on the virtual machine would obtain information about the playback environment from player APIs and would analyze the results to decide and control whether and how decoding should proceed. The content's code can also authenticate output devices, support player-specific security features, validate user actions (e.g., copy vs. play), check for malicious software on PCs, determine whether media is consumer-recordable, and implement locale-specific requirements. By allowing publishers to define the security system for each title, new countermeasures and security improvements can be deployed even after a standard has been widely adopted.

"Unfortunately, piracy is not going to go away," said Paul Kocher, president of Cryptography Research. "Our work assumes that pirate attacks are inevitable and focuses on the question of how future distribution systems can allow publishers to limit the damage when compromises do occur."

By all accounts, piracy is a serious problem for owners of intellectual property. For example, the Motion Picture Association of America estimates that the U.S. motion picture industry loses in excess of \$3 billion annually to piracy. In 2000, over 20 million pirate optical discs were seized, and 4.5 million videos were seized worldwide. The International Intellectual Property Alliance estimates that book publishers, recording and movie studios and software developers already lose more than \$20 billion a year from piracy.

To download the executive summary or request a copy of the complete report, visit Cryptography Research's website at <http://www.cryptography.com/research/spdc.html>.

About The Content Security Research Initiative

The Content Security Research Initiative is an ongoing effort funded by Cryptography Research, Inc. to solve security problems for the content distribution industry. This effort has yielded significant advances in securing pay television broadcasts, Internet downloads and optical media. Results from the study, including the approaches presented in this report, are protected by U.S. patents #6,298,442, #6,327,661, #6,304,658, #6,188,766, #6,289,455, #6,381,699, and #6,278,783; other U.S. and international patents are pending. Please contact Cryptography Research for more information about the initiative and research results.

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.

###