BEFORE THE COPYRIGHT OFFICE OF THE LIBRARY OF CONGRESS

IN THE MATTER OF
EXEMPTION TO PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS FOR ACCESS CONTROL TECHNOLOGIES

Docket No. RM 2008-8

Comment in Support of Proposed Exemptions 8A and 8B by[1]:

Ben Adida, PhD
Research Faculty
Harvard Medical School
Research Fellow
Harvard Center for Research on Computation and Society

Ross Anderson, PhD
Professor of Security Engineering
Computer Laboratory
University of Cambridge (UK)

Andrew W. Appel, PhD
Professor of Computer Science
Center for Information Technology Policy
Princeton University

Steven M. Bellovin, PhD
Professor of Computer Science
Columbia University

Matt Bishop, PhD
Professor of Computer Science
Co-Director, Computer Security Laboratory
University of California, Davis

John R. Black, PhD
Associate Professor of Computer Science
University of Colorado at Boulder

Matt Blaze, PhD
Associate Professor of Computer and Information Science
University of Pennsylvania

Nikita Borisov, PhD
Assistant Professor of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

Jesse Burns
Principal Partner
iSEC Partners

William Cheswick
Lead Member of Technical Staff
AT&T Research

Roger Dingledine
Project Leader and Director
The Tor Project

David Evans, PhD
Associate Professor of Computer Science
University of Virginia

Edward W. Felten, PhD
Professor of Computer Science and Public Affairs
Director, Center for Information Technology Policy
Princeton University

Michael J. Freedman, PhD
Assistant Professor of Computer Science
Princeton University

[1] All affiliations are listed for identification purposes only and do not necessarily reflect the opinion or endorsement of the affiliated institutions of the commentators.

Ian Goldberg, PhD
Assistant Professor
David R. Cheriton School of Computer Science
University of Waterloo (CA)

Dirk C. Grunwald, PhD
Associate Professor of Computer Science
University of Colorado at Boulder

Peter Honeyman, PhD
Research Professor of Information
Adjunct Professor of Electrical Engineering and Computer Science
Scientific Director, Center for Information Technology Integration
University of Michigan

Markus Jakobsson, PhD
Principal Scientist
Palo Alto Research Center

Ari Juels, PhD
Chief Scientist and Director
RSA Laboratories

Aggelos Kiayias, PhD
Assistant Professor of Computer Science and Engineering
Head, Crypto-DRM Laboratory
University of Connecticut

Tadayoshi Kohno, PhD
Assistant Professor of Computer Science and Engineering
University of Washington

Markus Kuhn, PhD
Lecturer in Computer Science
University of Cambridge (UK)

Patrick D. McDaniel, PhD
Associate Professor of Computer Science and Engineering
Co-Director, Systems and Internet Infrastructure Security Laboratory
Pennsylvania State University

Fabian Monrose, PhD
Associate Professor of Computer Science
University of North Carolina at Chapel Hill

Steven Myers, PhD
Assistant Professor of the School of Informatics
Member of the Center for Applied Cybersecurity Research
Indiana University

Peter G. Neumann, PhD
Principal Scientist
SRI International Computer Science Lab

Niels Provos, PhD
Senior Staff Engineer
Google Inc.

Eric Rescorla
Founder
RTFM

Ronald L. Rivest, PhD
Andrew and Edna Viterbi Professor of Electrical Engineering and Computer Scince
Founder, Cryptography and Information Security Group
Massachusetts Institute of Technology
Founder
RSA Security

Aviel D. Rubin, PhD
Professor, Computer Science
Technical Director, Information Security Institute
Johns Hopkins University

Stefan Savage, PhD
Associate Professor of Computer Science and Engineering
University of California, San Diego

Bruce Schneier
Chief Security Technology Officer
BT Group

Hovav Shacham, PhD
Assistant Professor of Computer Science and Engineering
University of California, San Diego

Douglas C. Sicker, PhD
Assistant Professor of Computer Science
Director, Interdisciplinary Telecommunications Program
University of Colorado at Boulder

Eugene H. Spafford, PhD
Professor of Computer Science
Executive Director, Center for Education and Research in Information and Security (CERIAS)
Purdue University

Alex Stamos
Principal Partner
iSEC Partners

Adam Stubblefield, PhD
Co-Founder
Independent Security Evaluators (ISE)
Assistant Research Professor of Computer Science
Johns Hopkins University

David Wagner, PhD
Associate Professor of Computer Science
University of California, Berkeley

Dan Wallach, PhD
Associate Professor of Computer Science
Rice University

Brent Waters, PhD
Assistant Professor of Computer Science
University of Texas

Moti Yung, PhD
Security Team
Google Inc.
Adjunct Professor of Computer Science
Columbia University

--

February 1, 2009

Pursuant to the Notice of Proposed Rulemaking in the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, we respectfully express our support for the exemptions proposed by J. Alex Halderman numbered 8A and 8B:

> *8A: "Literary works, sound recordings, and audiovisual works accessible on personal computers and protected by technological protection measures that control access to lawfully obtained*

> *works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities."*
>
> *8B: "Video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities."*

I. Summary of Argument

As academic and professional experts in the field of computer security research, we agree that the proposed exemptions will mitigate the chilling effect of the Digital Millennium Copyright Act ("DMCA") on independent security researchers. Adoption of these exemptions will promote increased security for personal computers by facilitating computer security research. Accordingly, we support an exemption from the DMCA anti-circumvention measures for the class enumerated by proposed exemption 8A with no further tailoring. In the alternative, we support an exemption for the class enumerated by proposed exemption 8B with no further tailoring.

II. PC-Based DRM Technologies Have Presented Serious Security Risks

As Professor Halderman asserted in his briefs to the Copyright Office during the present rulemaking and its previous iteration in 2006, digital rights management ("DRM") tools included in PC-accessible audio compact discs and video games have created serious security risks for consumers. Examples of such DRM tools include XCP, MediaMax, and SafeDisc. DRM software can disable system functionality and expose personal computer users to the risk of acquiring viruses, worms, Trojan horses, spyware and other types of malware. DRM software is also capable of compromising personal and corporate data, slowing down networks, and enabling e-mail spam. These risks are a serious problem and, left unchecked, degrade the security ecosystem required for efficient and safe computing.

III. PC-Based DRM Technologies Are Likely to Present Security Risks in the Future

DRM tools are likely to continue to pose serious security risks to consumers. Despite the widespread public outcry over Sony-BMG's introduction of serious computer security vulnerabilities through use of DRM in consumer products, the content industry has continued to deploy DRM. This trend of DRM deployment continues, despite the security risks posed. The recent inclusion of SafeDisc DRM tools in consumer software provides a contemporary example. Controversy currently exists around potential security risks posed by SecuROM, a commonly used PC-based video game DRM tool. DRM use is currently being planned for other types of PC-accessible content, including streaming video. Accordingly, it seems likely that PC-based DRM technology will continue to pose security risks in the future.

IV. PC-Based DRM Technologies Are Likely to Carry Inherent Security Risks

Problems inherent in the design of PC-based DRM tools are likely to lead to more security risks for PC users. DRM systems on general-purpose PCs are typically complex and are often implemented using underdeveloped and unsupported techniques. This makes it likely that security vulnerabilities will be unintentionally introduced in DRM software. In fact, the stated goal of most DRM systems (preventing PC owners from accomplishing certain tasks on their PCs) is inherently in conflict with primary security principles, which require that PC owners be informed about and able to control the operation of their PCs. It follows, then, that many PC-based DRM tools are likely to carry inherent security risks.

V. The Digital Millennium Copyright Act Chills Security Researchers From Discovering and Fixing Security Flaws in PC-Based DRM Technologies

The inability or unwillingness of many in the content industry to investigate security risks in DRM-equipped products prior to their release leaves independent security researchers as the primary security watchdogs for consumers. However, the threat of potential liability under the anti-circumvention measures of the Digital Millennium Copyright Act ("DMCA") chills security researchers acting in good faith from discovering, providing information about, and fixing security flaws in DRM systems included with PC-based content.

For the foregoing reasons, we express our strong support for the proposed exemptions.

Sincerely,

/s/

Ben Adida
Ross Anderson
Andrew W. Appel
Steven M. Bellovin
Matt Bishop
John R. Black
Matt Blaze
Nikita Borisov
Jesse Burns
William Cheswick
Roger Dingledine

David Evans
Edward W. Felten
Michael J. Freedman
Ian Goldberg
Dirk C. Grunwald
Peter Honeyman
Markus Jakobsson
Ari Juels
Aggelos Kiayias
Tadayoshi Kohno
Markus Kuhn

Patrick D. McDaniel
Fabian Monrose
Steven Myers
Peter G. Neumann
Niels Provos
Eric Rescorla
Ronald L. Rivest
Aviel D. Rubin
Stefan Savage
Bruce Schneier
Hovav Shacham

Douglas C. Sicker
Eugene H. Spafford
Alex Stamos
Adam Stubblefield
David Wagner
Dan Wallach
Brent Waters
Moti Yung