UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In re SONY BMG CD TECHNOLOGIES LITIGATION	:	Civil Action No. 1:05-cv-09575-NRB
	:	CLASS ACTION
This Document Relates To:	:	DECLARATION OF STEVEN M. BELLOVIN IN SUPPORT OF THE RICCIUTI CLASS REPRESENTATIVES' MOTION FOR AN AWARD OF ATTORNEYS' FEES AND REIMBURSEMENT OF EXPENSES
ALL ACTIONS.	:	

EXHIBIT A

Steven M. Bellovin

smb at cs.columbia.edu
http://www.cs.columbia.edu/~ smb

Education

1982 Ph.D., University of North Carolina at Chapel Hill. Dissertation: *Verifiably Correct Code Generation Using Predicate Transformers*; advisor: David L. Parnas.

1977 M.S., University of North Carolina at Chapel Hill.

1972 B.A., Columbia University.

Employment

2005-now Professor of Computer Science, Columbia University.

2002-2004 Adjunct Professor of Computer Science, University of Pennsylvania.

1998-2004 AT&T Fellow, AT&T Labs—Research.

1987-1998 Distinguished Member of the Technical Staff, AT&T Bell Laboratories and AT&T Labs—Research.

1982-1987 Member of the Technical Staff, AT&T Bell Laboratories.

1977-1978 Instructor, Dept. of Computer Science, University of North Carolina at Chapel Hill.

Honors

2001 Elected to the National Academy of Engineering.

1998 Named an AT&T Fellow.

1995 Received the Usenix Lifetime Achievement Award ("The Flame"), along with Tom Truscott and Jim Ellis, for our role in creating Usenet.

Books and Chapters

- Stephen T. Kent and Lynette I. Millett, editors. *Who Goes There? Authentication Through the Lens of Privacy*. National Academies Press, 2003.
- John L. Hennessy, David A. Patterson, and Herbert S. Lin, editors. *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*. National Academies Press, 2003.

- William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin. *Firewalls and Internet Security; Repelling the Wily Hacker*. Addison-Wesley, Reading, MA, second edition, 2003.
- Stephen T. Kent and Lynette I. Millett, editors. *IDs—Not That Easy: Questions About Nationwide Identity Shystems*. National Academies Press, 2002.
- *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Academies Press, 2002.
- Fred B. Schneider, editor. *Trust in Cyberspace*. National Academy Press, 1999.
- Network security issues. In Peter Denning and Dorothy Denning, editors, *Internet Beseiged: Countering Cyberspace Scofflaws*. ACM Press, 1997.
- Network security issues. In A. Tucker, editor, *CRC Computer Science and Engineering Handbook*. CRC Press, 1996.
- Security and software engineering. In B. Krishnamurthy, editor, *Practical Reusable UNIX Software*. John Wiley & Sons, 1995.
- William R. Cheswick and Steven M. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley, Reading, MA, first edition, 1994.

Papers and Articles

- Steven M. Bellovin, Angelos Keromytis, and Bill Cheswick. Worm propagation strategies in an IPv6 Internet. *;login:*, pages 70–76, February 2006.
- Steven M. Bellovin and Eric K. Rescorla. Deploying a new hash algorithm. In *Procedings of NDSS '06*, 2006.
- Steven M. Bellovin, Matt Blaze, and Susan Landau. The real national-security needs for voip. *Communications of the ACM*, 48(11), November 2005. "Inside RISKS" column.
- Steven M. Bellovin and William R. Cheswick. Privacy-enhanced searches using encrypted Bloom filters, 2004. Draft.
- Steven M. Bellovin. A look back at "Security problems in the TCP/IP protocol suite". In *Annual Computer Security Applications Conference*, December 2004. Invited paper.
- Steven M. Bellovin. Spamming, phishing, authentication, and privacy. *Communications of the ACM*, 47(12), December 2004. "Inside RISKS" column.
- Steven M. Bellovin and Emden R. Gansner. Using link cuts to attack Internet routing, 2003. Draft.

- Steven M. Bellovin. Cybersecurity research needs, July 2003. Testimony before the House Select Committee on Homeland Security, Subcommittee on Cybersecurity, Science, Research, & Development, hearing on "Cybersecurity—Getting it Right".

- Sotiris Ioannidis, Steven M. Bellovin, John Ioannidis, Angelos D. Keromytis, and Jonathan M. Smith. Design and implementation of virtual private services. In *Proceedings of the IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Workshop on Enterprise Security*, Linz, Austria, June 2003.

- Sotiris Ioannidis, Steven M. Bellovin, and Jonathan Smith. Sub-operating systems: A new approach to application security. In *SIGOPS European Workshop*, September 2002.

- John Ioannidis and Steven M. Bellovin. Implementing pushback: Router-based defense aganist DDoS at tacks. In *Proc. Internet Society Symposium on Network and Distributed System Security*, 2002.

- Ratul Mahajan, Steven M. Bellovin, Sally Floyd, John Ioannidis, Vern Paxson, and Scott Shenker. Controlling high bandwidth aggregates in the network. *Computer Communications Review*, 32(3):62–73, July 2002.

- William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. Efficient, DoS-resistant, secure key exchange for internet protocols. In *Proceedings of the ACM Computer and Communications Security (CCS) Conference*, November 2002.

- Steven M. Bellovin. A technique for counting NATted hosts. In *Proc. Second Internet Measurement Workshop*, pages 267–272, Marseille, 2002.

- Peter M. Gleitz and Steven M. Bellovin. Transient addressing for related processes: Improved firewalling by using IPv6 and multiple addresses per host. In *Proceedings of the Eleventh Usenix Security Symposium*,, August 2001.

- Sotiris Ioannidis and Steven M. Bellovin. Building a secure web browser. In *Usenix Conference*, June 2001.

- Steven M. Bellovin. Computer security—an end state? *Communications of the ACM*, 44(3), March 2001.

- S.M. Bellovin and M.A. Blaze. Cryptographic modes of operation for the Internet. In *Second NIST Workshop on Modes of Operation*, August 2001.

- Steven M. Bellovin, C. Cohen, J. Havrilla, S. Herman, B. King, J. Lanza, L. Pesante, R. Pethia, S. McAllister, G. Henault, R. T. Goodden, A. P. Peterson, S. Finnegan, K. Katano, R. M. Smith, and R. A. Lowenthal. Results of the "Security in ActiveX Workshop", December 2000.

- D. Whiting, B. Schneier, and S. Bellovin. AES key agility issues in high-speed IPsec implementations, 2000.
- Steven M. Bellovin, Matt Blaze, David Farber, Peter Neumann, and Gene Spafford. Comments on the Carnivore system technical review draft, December 2000.
- Matt Blaze and Steven M. Bellovin. Open Internet wiretapping, July 2000. Written testimony for a hearing on "Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program" by the Subcommittee on the Constitution, House Judiciary Committee.
- Steven M. Bellovin. Wiretapping the Net. *The Bridge*, 20(2):21–26, Summer 2000.
- Matt Blaze and Steven M. Bellovin. Tapping on my network door. *Communications of the ACM*, 43(10), October 2000.
- Sotiris Ioannidis, Angelos D. Keromytis, Steven M. Bellovin, and Jonathan M. Smith. Implementing a distributed firewall. In *ACM Conference on Computer and Communications Security*, Athens, Greece, November 2000.
- Peter Gregory. Why systems administration is hard. In *Solaris Security*. Prentice-Hall, 1999. (Foreword).
- Steven M. Bellovin. Distributed firewalls. *;login:*, pages 39–47, November 1999.
- J. S. Denker, S. M. Bellovin, H. Daniel, N. L. Mintz, T. Killian, and M. A. Plotnick. Moat: A virtual private network appliance and services platform. In *Proceedings of LISA XIII*, November 1999.
- Fred Schneider, Steven M. Bellovin, and Alan Inouye. Critical infrastructures you can trust: Where telecommunications fits. In *Telecommunications Policy Research Conference*, October 1998.
- William Cheswick and Steven M. Bellovin. How computer security works: Firewalls. *Scientific American*, pages 106–107, October 1998.
- Steven M. Bellovin. Cryptography and the internet. In *Advances in Cryptology: Proceedings of CRYPTO '98*, August 1998.
- Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, and Bruce Schneier. The risks of key recovery, key escrow, and trusted third-party encryption, May 1997. A report by an ad hoc group of cryptographers and computer scientists.
- Yakov Rekhter, Paul Resnick, and Steven M. Bellovin. Financial incentives for route aggregation and efficient address utilization in the Internet. In *Proceedings of Telecommunications Policy Research Conference*, 1997.

- Steven M. Bellovin. Probable plaintext cryptanalysis of the IP security protocols. In *Proceedings of the Symposium on Network and Distributed System Security*, pages 155–160, 1997.
- Bill Cheswick and Steven M. Bellovin. A DNS filter and switch for packet-filtering gateways. In *Proceedings of the Sixth Usenix Unix Security Symposium*, pages 15–19, San Jose, CA, 1996.
- Steven M. Bellovin. Problem areas for the IP security protocols. In *Proceedings of the Sixth Usenix Unix Security Symposium*, pages 205–214, July 1996.
- Uri Blumenthal and Steven M. Bellovin. A better key schedule for DES-like ciphers. In *Proceedings of PRAGOCRYPT '96*, Prague, 1996.
- David A. Wagner and Steven M. Bellovin. A "bump in the stack" encryptor for MS-DOS systems. In *Proceedings of the Symposium on Network and Distributed System Security*, pages 155–160, San Diego, February 1996.
- Steven M. Bellovin. Using the domain name system for system break-ins. In *Proceedings of the Fifth Usenix Unix Security Symposium*, pages 199–208, Salt Lake City, UT, June 1995.
- Steven M. Bellovin. Security and uses of the internet. In *Proceedings of the North American Serials Interest Group*, June 1995.
- Matt Blaze and Steven M. Bellovin. Session-layer encryption. In *Proc. 5th USENIX UNIX Security Symposium*, Salt Lake City, UT, June 1995.
- David A. Wagner and Steven M. Bellovin. A programmable plaintext recognizer, 1994. Unpublished.
- Steven M. Bellovin and Michael Merritt. An attack on the *Interlock Protocol* when used for authentication. *IEEE Transactions on Information Theory*, 40(1):273–275, January 1994.
- Steven M. Bellovin and Michael Merritt. Augmented encrypted key exchange. In *Proceedings of the First ACM Conference on Computer and Communications Security*, pages 244–250, Fairfax, VA, November 1993.
- Steven M. Bellovin. Packets found on an internet. *Computer Communications Review*, 23(3):26–31, July 1993.
- Steven M. Bellovin. A best-case network performance model, 1992. Unpublished.
- Steven M. Bellovin. There be dragons. In *Proceedings of the Third Usenix Unix Security Symposium*, pages 1–16, September 1992.
- Steven M. Bellovin and Michael Merritt. Encrypted key exchange: Password-based protocols secure against dictionary attacks. In *Proc. IEEE Computer Society Symposium on Research in Security and Privacy*, pages 72–84, Oakland, CA, May 1992.

- Steven M. Bellovin and Michael Merritt. Limitations of the Kerberos authentication system. In *USENIX Conference Proceedings*, pages 253–267, Dallas, TX, Winter 1991.
- Steven M. Bellovin and Michael Merritt. Limitations of the Kerberos authentication system. *Computer Communications Review*, October 1990.
- Steven M. Bellovin. Pseudo-network drivers and virtual networks. In *USENIX Conference Proceedings*, pages 229–244, Washington, D.C., January 22-26, 1990.
- Steven M. Bellovin. Towards a commercial IP security option. In *Commercial IPSO Workshop, INTEROP '89*, 1989.
- Steven M. Bellovin. Security problems in the TCP/IP protocol suite. *Computer Communications Review*, 19(2):32–48, April 1989.
- Steven M. Bellovin. The session tty manager. In *Proc. Usenix Conference*, Summer 1988.
- Peter Honeyman and Steven M. Bellovin. PATHALIAS or the care and feeding of relative addresses. In *Proc. Summer Usenix Conference*, 1986.

Major Positions

2006	Chair, Steps Towards Reducing Unwanted Traffic in the Internet (SRUTI)
2005-2006	Member, Department of Homeland Security Science and Technology Advisory Committee
2004-now	Member, National Research Council study committee on cybersecurity research needs.
2002-2004	Member, ICANN DNS Security and Stability Advisory Committee.
2002-2004	Security Area co-director, Internet Engineering Task Force (IETF).
2002	Chair, program committee, IEEE Symposium on Security and Privacy.
2002	Member, Information Technology sub-committee, National Research Council study committee on science and technology against terrorism.
2001-2003	Member, ACM Advisory Committee on Security and Privacy.
2001	Vice-chair, program committee, IEEE Symposium on Security and Privacy.
2001-2003	Member, National Research Council study committee on authentication technologies and their privacy implications.
2000-2002	Chair, IETF ITRACE working group.

2000	Co-chair, Usenix Security Symposium.
1999-2002	IETF representative, ICANN Protocol Supporting Organization
1999-now	Co-chair, IETF SPIRITS working group.
1997-2001	Co-chair, IETF PINT working group.
1996-1998	Member, National Research Council study committee on information systems trustworthiness.
1996-2002	Member, Internet Architecture Board.
1996	Co-chair, Usenix Security Symposium.
1993-1995	Member, IETF IPng Directorate.

U.S. Patents

6,870,845 Method for providing privacy by network address translation (2005).

6,665,299 Method and system for telephony and high speed data access on a broadband access network (2003).

5,958,052 Method and apparatus for restricting access to private information in domain name systems by filtering information (1999).

5,870,557 Method for determining and reporting a level of network activity on a communications network using a routing analyzer and advisor (1999).

5,805,820 Method and apparatus for restricting access to private information in domain name systems by redirecting query requests (1998).

5,440,635 Cryptographic protocol for remote authentication (1995).

5,241,599 Cryptographic protocol for secure communications (1993).

Numerous other patent applications are pending.

I, STEVEN M. BELLOVIN, declare as follows:

1. I am an expert in the area of computer security, retained by the plaintiffs' attorney in the above-captioned litigation. I am a professor of computer science. Attached hereto as Exhibit A is a true and correct copy of my résumé. I have knowledge of the matters stated herein and, if called upon, I could and would competently testify thereto.

2. I have reviewed the Settlement Agreement entered into between the plaintiffs and defendant dated December 28, 2005. I have estimated the impact as follows:

3. An attacker who wishes to take over a computer system faces three problems: initial penetration, concealment of the attack, and (under some circumstances) gaining sufficient privileges on that computer to carry out further attacks or tasks. The XCP software aids in the second of these problems; the MediaMax software aids in the third and in some cases the second. In addition, at least one version of an uninstaller for the XCP software was a significant aid in the first of the attacker's problems.

4. The XCP software installs a so-called rootkit. The purpose of a rootkit is to conceal other software running on a computer. Rootkits are often used by malware to hide from the system administrator and probably from anti-virus software. In this case, Sony employed the rootkit to hide its own DRM software, presumably to prevent its removal by the system owner administrator. However, there was no mechanism to prevent it from concealing other, more malicious software; according to published reports (*see* http://news.zdnet.co.uk/internet/security/0,39020375,39236720,00.htm and http://www.vnunet.com/vnunet/news/2145874/virus-writers-exploit-sony-drm), at least two pieces of malicious software were modified to do exactly that.

5. The MediaMax software creates a file that is executed any time a protected CD is played. In and of itself, this is not a problem; however, the file is created in such a fashion that any user of the computer, even one without "privileges", can overwrite this file and hence replace it with a modified version. Consider, for example, a home computer where a parent or older child, running on a privileged account, regularly plays protected CDs. A younger child, running on an unprivileged account – one that does not have privileges to modify, say, a protective Internet filter – could use this security hole to gain privileges. This would allow that child to remove filtering software, examine confidential documents such as tax returns, etc.

6. In addition, if there were some system penetration by a mechanism that did not grant full privileges – consider this child inadvertently downloading a worm or visiting a Web site that exploited a browser flaw – the attacker could use this same whole to gain full privileges on the system.

7. Under certain circumstances, the MediaMax software could be abused to help with the initial penetration of the computer. If a consumer were to share a computer's drive over a home network, other computers on that network – perhaps having been penetrated by some other mechanism – could exploit this vulnerability to overwrite that file. The next time the owner played a protected CD, the malicious version of the file will be executed.

8. Some components of the Sony-installed software "phone home," apparently whenever the album is played. Although the apparent purpose is to check for updates to the art work or lyrics (http://www.sysinternals.com/blog/2005/11/more-on-sony-dangerous-decloaking.html), it is also an invasion of privacy. To start, it tells Sony each time the album is played. Beyond that, they learn the IP address of the customer. IP addresses tend to disclose the location of the sender (http://www.zabasearch.com/frames/zaba_location.map.php). Beyond that, IP addresses are

effectively static for many broadband Internet users. Sony can thus build a profile of albums played by customers. They can also correlate this IP address with logs from their other web sites, all without the permission of the customer.

9. It is harder to assess the actual, as opposed to potential, impact. It is, however, well-known that the computer underground values compromised machines for their profit-making potential; *see,* for example, http://news.zdnet.com/2100-1009_22-5772238.html?tag=nl. Machines that are "disinfected" are of no use; accordingly, any mechanism that keeps the "bot" intact, such as a rootkit, is quite valuable.

10. Compromised machines that are turned into bots are used to send spam and to launch denial of service attacks as a form of extortion. If an ISP detects such behavior, its general response is to disable the affected account. The consumer is thus denied all Internet access for some time.

11. It is notoriously difficult to thoroughly disinfect compromised machines. The difficulty is, of course, exacerbated if a rootkit conceals the offending files. The most common advice is to reinstall the operating system; if not done extremely carefully, this can result in a loss of all data and personal files on the machine. A typical reinstallation, including downloading and installing all Microsoft patches and reinstalling all application programs, can take the better part of a day, even if there are no problems. Resolving problems often requires calls to Help Desks and/or costly professional assistance. Microsoft itself has noted the need for reinstallation, especially if the malware is taking advantage of rootkits to conceal its presence (http://www.eweek.com/article2/0,1895,1945808,00.asp).

12. The XCP rootkit is particularly difficult to uninstall. As noted in http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html, errors in uninstalling it can render a system unbootable, disable the CD drive, and more. The author notes

"most users that stumble across the cloaked files with a RKR scan will cripple their computer if they attempt the obvious step of deleting the cloaked files." Indeed, Sony's original uninstaller itself posed very serious security risks (http://www.freedom-to-tinker.com/?p=926). The flaws in it were detected by outsiders, not by Sony itself; for this reason, the provision in the settlement for outside, official review is quite crucial.

13. The total number of infected computers around the world is not known; however, it is very large. A recent Dutch arrest involved a botnet of at least 1.5 million computers (http://news.com.com/Bot+herders+may+have+controlled+1.5+million+PCs/2100-7350_3-5906896.html). As noted above, one of the challenges facing someone who wants to operate a large botnet is concealing the infestation. A rootkit makes this task much easier.

I declare under penalty of perjury that the foregoing is true and correct. Executed this 6th day of April, 2006, at Westfield, New Jersey.

STEVEN M. BELLOVIN

T:\CasesSF\Sony NY\DEC00029673.doc