

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

2006 Received the 2007 NIST/NSA National Computer Systems Security Award

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

- Salvatore Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Sara Sinclair, Sean Smith, and Shlomo Hershkop, editors. *Insider Attack and Cyber Security: Beyond the Hacker (Advances in Information Security)*. Springer, 2008.

- Seymour E. Goodman and Herbert S. Lin, editors. *Toward a Safer and More Secure Cyberspace*. National Academy Press, 2007.
- 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.
- *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Academies Press, 2002.
- *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Academies Press, 2002.
- Stephen T. Kent and Lynette I. Millett, editors. *IDs—Not That Easy: Questions About Nationwide Identity Systems*. 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

- Maritza Johnson, Steven M. Bellovin, Robert W. Reeder, and Stuart Schechter. Laissez-faire file sharing: Access control designed for individuals at the endpoints, 2009. In submission.
- Mariana Raykova, Binh Vo, Tal Malkin, and Steven M. Bellovin. Secure anonymous database search, 2009. In submission.
- Shaya Potter, Steven M. Bellovin, and Jason Nieh. Two person controller administration: Preventing administrative faults through duplication, 2009. In submission.

- Yuu-Heng Cheng, Mariana Raykova, Alex Poylisher, Scott Alexander, Martin Eiger, and Steve M. Bellovin. The Zodiac policy subsystem: a policy-based management system for a high-security MANET. In *IEEE Policy 2009*, July 2009. To appear.
- Elli Androulaki and Steven M. Bellovin. An anonymous credit card system. In *Trust '09*, September 2009. To appear. A longer version is <http://mice.cs.columbia.edu/getTechreport.php?techreportID=http://mice.%cs.columbia.edu/getTechreport.php?techreportID=590&format=pdf&>.
- Elli Androulaki and Steven M. Bellovin. Anonymous delivery of physical objects. In *Symposium on Privacy-Enhancing Technologies (PET)*, July 2009. To appear.
- S. Bellovin. Guidelines for Specifying the Use of IPsec Version 2. RFC 5406, Internet Engineering Task Force, February 2009.
- Maritza Johnson, Chaitanya Atreya, Adam Aviv, Mariana Raykova, Steven M. Bellovin, and Gail Kaiser. RUST: The reusable security toolkit, 2008. Draft.
- Steven M. Bellovin, Matt Blaze, Whitfield Diffie, Susan Landau, Peter G. Neumann, and Jennifer Rexford. Risking communications security: Potential hazards of the "protect america act. *IEEE Security and Privacy*, 6(1):24–33, January/February 2008.
- Kyle Dent and Steven M. Bellovin. Newspeak: A secure approach for designing web applications. Technical Report CUCS-008-08, Department of Computer Science, Columbia University, February 2008.
- Hang Zhao, Jorge Lobo, and Steven M. Bellovin. An algebra for integration and analysis of ponder2 policies. In *Proceeding of the 9th IEEE Workshop on Policies for Distributed Systems and Networks*, June 2008.
- Maritza Johnson, Chaitanya Atreya, Adam Aviv, Mariana Raykova, Steven M. Bellovin, and Gail Kaiser. RUST: A retargetable usability testbed for website authentication technologies. In *Usenix Workshop on Usability, Psychology, and Security*, April 2008.
- Maritza Johnson and Steven M. Bellovin. Security assurance for web device APIs. In *Security for Access to Device APIs from the Web - W3C Workshop*, December 2008.
- Hang Zhao, Chi-Kin Chau, and Steven M. Bellovin. Rofl: Routing as the firewall layer. In *New Security Paradigms Workshop*, September 2008. A version is available as Technical Report CUCS-026-08.
- Elli Androulaki, Mariana Raykova, Angelos Stavrou, and Steven M. Bellovin. Oponentor: Anonymity as a commodity service. In *Proceedings of the 8th Privacy Enhancing Technologies Symposium*, July 2008.

- Elli Androulaki, Seung Geol Choi, Steven M. Bellovin, and Tal Malkin. Reputation systems for anonymous networks. In *Proceedings of the 8th Privacy Enhancing Technologies Symposium*, July 2008.
- Steven M. Bellovin, Matt Blaze, Whitfield Diffie, Susan Landau, Peter G. Neumann, and Jennifer Rexford. Internal surveillance, external risks. *Communications of the ACM*, 50(12), December 2007.
- Hang Zhao and Steven M. Bellovin. Policy algebras for hybrid firewalls. Technical Report CU-CS-017-07, Department of Computer Science, Columbia University, March 2007. Also presented at the Annual Conference of the ITA, 2007.
- Sotiris Ioannidis, Steven M. Bellovin, John Ioannidis, Angelos D. Keromytis, Kostas Anagnostakis, and Jonathan M. Smith. Coordinated policy enforcement for distributed applications. *International Journal of Network Security*, 4(1):69–80, January 2007.
- Steven M. Bellovin and William R. Cheswick. Privacy-enhanced searches using encrypted Bloom filters. Technical Report CU-CS-034-07, Department of Computer Science, Columbia University, September 2007.
- Elli Androulaki, Mariana Raykova, Angelos Stavrou, and Steven M. Bellovin. Opentor: Anonymity as a commodity service. Technical Report CU-CS-031-07, Department of Computer Science, Columbia University, September 2007.
- Elli Androulaki, Seung Geol Choi, Steven M. Bellovin, and Tal Malkin. Reputation systems for anonymous networks. Technical Report CU-CS-029-07, Department of Computer Science, Columbia University, September 2007.
- S. Bellovin. Key Change Strategies for TCP-MD5. RFC 4808, Internet Engineering Task Force, March 2007.
- Paula Hawthorn, Barbara Simons, Chris Clifton, David Wagner, Steven M. Bellovin, Rebecca Wright, Arnold Rosenthal, Ralph Poore, Lillie Coney, Robert Gellman, and Harry Hochheiser. Statewide databases of registered voters: Study of accuracy, privacy, usability, security, and reliability issues, February 2006. Report commissioned by the U.S. Public Policy Committee of the Association for Computing Machinery.
- Steven M. Bellovin, David D. Clark, Adrian Perrig, and Dawn Song. Workshop report: Clean-slate design for the next-generation secure internet, March 2006. NSF workshop report.
- Steven M. Bellovin, Angelos Keromytis, and Bill Cheswick. Worm propagation strategies in an IPv6 Internet. *login.*, pages 70–76, February 2006.
- Ka-Ping Yee, David Wagner, Marti Hearst, and Steven M. Bellovin. Prerendered user interfaces for higher-assurance electronic voting. In *Usenix/ACCURATE Electronic Voting Technology Workshop*, August 2006. An earlier version appeared as Technical Report UCB/EECS-2006-35.

- Steven M. Bellovin and Eric K. Rescorla. Deploying a new hash algorithm. In *Proceedings of NDSS '06*, 2006.
- S. Bellovin and A. Zinin. Standards Maturity Variance Regarding the TCP MD5 Signature Option (RFC 2385) and the BGP-4 Specification. RFC 4278, Internet Engineering Task Force, January 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.
- S. Bellovin and R. Housley. Guidelines for Cryptographic Key Management. RFC 4107, Internet Engineering Task Force, June 2005.
- 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.
- William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. Just fast keying: Key agreement in a hostile Internet. *ACM Transactions on Information and System Security (TISSEC)*, 7(2):1–32, May 2004.
- Steven M. Bellovin. Spamming, phishing, authentication, and privacy. *Communications of the ACM*, 47(12), December 2004. “Inside RISKS” column.
- 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”.
- Steven M. Bellovin and Emden R. Gansner. Using link cuts to attack Internet routing, 2003. Draft.
- 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.
- S. Bellovin. The Security Flag in the IPv4 Header. RFC 3514, Internet Engineering Task Force, April 2003.
- S. Bellovin, J. Ioannidis, A. Keromytis, and R. Stewart. On the Use of Stream Control Transmission Protocol (SCTP) with IPsec. RFC 3554, Internet Engineering Task Force, July 2003.
- S. Bellovin, J. Schiller, and C. Kaufman. Security Mechanisms for the Internet. RFC 3631, Internet Engineering Task Force, December 2003.

- 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.
- John Ioannidis and Steven M. Bellovin. Implementing pushback: Router-based defense against DDoS attacks. In *Proc. Internet Society Symposium on Network and Distributed System Security*, 2002.
- Sotiris Ioannidis, Steven M. Bellovin, and Jonathan Smith. Sub-operating systems: A new approach to application security. In *SIGOPS European Workshop*, September 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.
- Steven M. Bellovin. Computer security—an end state? *Communications of the ACM*, 44(3), March 2001.
- Sotiris Ioannidis and Steven M. Bellovin. Building a secure web browser. In *Usenix Conference*, June 2001.
- 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.
- 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 and Robert G. Moskowitz. Client certificate and key retrieval for IKE. Obsolete Internet draft, November 2000. <http://www.cs.columbia.edu/~smb/papers/draft-ietf-ipsra-getcert-00.txt>.
- Matt Blaze and Steven M. Bellovin. Tapping on my network door. *Communications of the ACM*, 43(10), October 2000.
- Steven M. Bellovin. Wiretapping the Net. *The Bridge*, 20(2):21–26, Summer 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.
- 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.
- Peter Gregory. Why systems administration is hard. In *Solaris Security*. Prentice-Hall, 1999. (Foreword).
- 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.
- S. Bellovin. Report of the IAB Security Architecture Workshop. RFC 2316, Internet Engineering Task Force, April 1998.
- H. Lu, M. Krishnaswamy, L. Conroy, S. Bellovin, F. Burg, A. DeSimone, K. Tewani, P. Davidson, H. Schulzrinne, and K. Vishwanathan. Toward the PSTN/Internet Inter-Networking–Pre-PINT Implementations. RFC 2458, Internet Engineering Task Force, November 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.
- 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.
- Uri Blumenthal and Steven M. Bellovin. A better key schedule for DES-like ciphers. In *Proceedings of PRAGOCRYPT '96*, Prague, 1996.
- S. Bellovin. Defending Against Sequence Number Attacks. RFC 1948, Internet Engineering Task Force, May 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.
- S. Bellovin. Firewall-Friendly FTP. RFC 1579, Internet Engineering Task Force, February 1994.
- S. Bellovin. Security Concerns for IPng. RFC 1675, Internet Engineering Task Force, August 1994.
- S. Bellovin. On Many Addresses per Host. RFC 1681, Internet Engineering Task Force, August 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. Encrypted key exchange: Password-based protocols secure against dictionary attacks, August 1991.
- 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, November 1990. Internal report.
- 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

- 2008** Co-chair, Applied Cryptography and Network Security (ACNS)
- 2006** Chair, Steps Towards Reducing Unwanted Traffic in the Internet (SRUTI)

- 2005-now** Member, Department of Homeland Security Science and Technology Advisory Committee
- 2004-2007** 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

- 7,227,843 Method for reducing congestion in packet-switched networks (2007).
- 7,051,365 Method and apparatus for a distributed firewall (2006).
- 7,035,410 Method and apparatus for enhanced security in a broadband telephony network (2006).
- 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.