Steven M. Bellovin

Percy K. and Vida L.W. Hudson Professor Emeritus of Computer Science

smb@cs.columbia.edu
https://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

2025–now Senior Affiliate Scholar, Institute for Technology Law & Policy, Georgetown University.

2025–now Percy K. and Vida L.W. Hudson Professor Emeritus of Computer Science and former affiliate law faculty, Columbia University.

2017–2025 Affiliate faculty member, Columbia University Law School.

2014–2025 Percy K. and Vida L.W. Hudson Professor of Computer Science, Columbia University.

2018-2019 On sabbatical, Center for Law and Information Policy, Fordham University School of Law

2016 Technology Scholar, Privacy and Civil Liberties Oversight Board.

2005–2014 Professor of Computer Science, Columbia University.

2012–2013 Chief Technologist, Federal Trade Commission.

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

2005–2012 AT&T, consultant

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

2023 Usenix Lifetime Achievement Award ("The Flame"), along with Matt Blaze and Susan Landau, for our "profound and lasting impact on Computer Science, Computer Security, Law, and Public Policy through their groundbreaking research, their influential publications, and their dedication to advancing knowledge that informs public policy."

2019 "Test of Time" award for Bellovin and Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks"

2016 ESORICS Outstanding Research Award

2016 EFF Pioneer Award (co-winner with the other authors of the "Keys Under Doormats" paper)

2015 J.D. Falk Award (co-winner with the other authors of the "Keys Under Doormats" paper)

2014 Elected to the Cybersecurity Hall of Fame

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 Usenix Lifetime Achievement Award ("The Flame"), along with Tom Truscott and Jim Ellis, "for their work in creating USENET."

Books and Chapters

- Steven M. Bellovin, Susan Landau, and Herbert S. Lin. Limiting the undesired impact of cyber weapons: Technical requirements and policy implications. In Herbert Lin and Amy Zegart, editors, *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, pages 265–288. Brookings Institution Press, Washington, DC, 2018.

- Steven M. Bellovin. *Thinking Security: Stopping Next Year's Hackers*. Addison-Wesley, Boston, 2016.

- 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.

- 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.

- Network security issues. In Peter Denning and Dorothy Denning, editors, *Internet Besieged: 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, 1st edition edition, 1994.

Papers and Articles

- Steven M. Bellovin. Computer science and the law. *Communications of the ACM*, 68(8):19–21, June 2025. "Inside RISKS" column.
- Steven M. Bellovin. Rethinking privacy regulation. *GWU Journal of Law and Technology*, 1(1):1, 2025.
- Steven M. Bellovin. Privacy-preserving age verification—and its limitations. Submission to the IAB/W3C Workshop on Age-Based Restrictions on Content Access, August 2025.
- Steven M. Bellovin. Compression, correction, confidentiality, and comprehension: A modern look at telegraph codebooks. *Cryptologia*, 2025.
- Steven M. Bellovin. Netnews: The origin story. *IEEE Annals of the History of Computing*, 47(1):7–21, 2025.
- Panel on Assessment of the National Institute of Standards and Technology (NIST) Information Technology Laboratory. *An Assessment of Selected Divisions of the National Institute of Standards and Technology Information Technology Laboratory*. National Academies Press, Washington, DC, 2025.
- Steven M. Bellovin. Who coined the phrase "data shadow"? *Ohio State Technology Law Journal*, 20(2):317, May 2024.
- Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague, and Carmela Troncoso. Bugs in our pockets: The risks of client-side scanning. *Journal of Cybersecurity*, 10(1), 2024.
- Steven M. Bellovin. The antiquity of algorithmic patents. *Ohio State Technology Law Journal*, 20(2):365, May 2024.

- Susan Landau, James X. Dempsey, Ece Kamar, Steven M. Bellovin, and Robert Pool. Challenging the machine: Contestability in government AI systems, June 2024.
- Susan Landau, James X. Dempsey, Ece Kamar, and Steven M. Bellovin. Recommendations for government development and use of advanced automated systems to make decisions about individuals, March 2024.
- Janet Zhang and Steven M. Bellovin. Preventing intimate image abuse via privacy-preserving anonymous credentials. *SMU Science and Technology Law Review*, 26:149–215, November 2023.
- Steven M. Bellovin, Adam Shostack, and Tarah Wheeler. Ten questions we hope the Cyber Safety Review Board answers—and three it should ignore. *Lawfare*, February 9, 2022.
- Miranda Christ, Sarah Radway, and Steven M. Bellovin. Differential privacy and swapping: Examining de-identification's impact on minority representation and privacy preservation in the U.S. census. In *IEEE Symposium on Security and Privacy*, May 23, 2022.
- National Academies of Sciences, Engineering, and Medicine. *Fostering Responsible Computing Research: Foundations and Practices*. National Academies Press, 2022.
- Steven Bellovin and Adam Shostack. Finally! A cybersecurity safety review board. *Lawfare*, June 7, 2021.
- John S. Koh, Jason Nieh, and Steven Bellovin. Encrypted cloud photo storage using Google Photo. In *MobiSys 2021*, June 2021.
- National Academies of Sciences, Engineering, and Medicine. *Emerging Areas of Science, Engineering, and Medicine for the Courts: Proceedings of a Workshop in Brief*. National Academies Press, Washington, DC, 2021.
- Steven M. Bellovin. Mail-in ballots are secure, confidential, and trustworthy. *Columbia News*, October 23, 2020.
- Steven M. Bellovin, Matt Blaze, Susan Landau, and Brian Owsley. Seeking the source: Criminal defendants' constitutional right to source code. *Ohio State Technology Law Journal*, 17(1):1–73, December 2020.
- Steven M. Bellovin. Testimony for the New York City Council Committee on Technology hearing on "Benefits and Disadvantages of Cloud-computing Systems", December 15, 2020.
- Steven M. Bellovin. Testimony for the New York City Council Committee on Technology and Committee on Small Business hearing on "Cybersecurity for Small Businesses", February 25, 2020.

- *Safeguarding the Bioeconomy*. National Academies Press, 2020.
- Simha Sethumadhavan, Steven M. Bellovin, Paul Kocher, and Ed Suh. Please disclose security vulnerabilities! February 7, 2019.
- Steven M. Bellovin. Yes, "algorithms" can be biased. Here's why. *Ars Technica*, January 24, 2019.
- Steven M. Bellovin, Preetam K. Dutta, and Nathan Reitinger. Privacy and synthetic datasets. *Stanford Technology Law Review*, 22(1):1–52, 2019.
- John S. Koh, Steven M. Bellovin, and Jason Nieh. Making it easier to encrypt your emails. *;login:*, September, 2019.
- John S. Koh, Steven M. Bellovin, and Jason Nieh. Easy email encryption with easy key management: Why Joanie can encrypt. In *Proc. EuroSys 2019*, Dresden, DE, March 2019.
- Steven M. Bellovin, Susan Landau, and Herbert S. Lin. Limiting the undesired impact of cyber weapons: Technical requirements and policy implications. In Herbert Lin and Amy Zegart, editors, *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, pages 265–288. Brookings Institution Press, Washington, DC, 2018.
- Steven Bellovin and Susan Landau. Encryption by default equals national security. *Lawfare*, October 26, 2018.
- Steven M. Bellovin and Peter G. Neumann. The big picture. *Communications of the ACM*, 61(11), November 2018.
- Steven M. Bellovin, Matt Blaze, Dan Boneh, Susan Landau, and Ronald L. Rivest. Analysis of the CLEAR protocol per the National Academies' framework. Technical Report CUCS-003-18, Department of Computer Science, Columbia University, May 10, 2018.
- Steven M. Bellovin, Matt Blaze, Dan Boneh, Susan Landau, and Ronald L. Rivest. Op-ed: Ray Ozzie's crypto proposal—a dose of technical reality. *Ars Technica*, May 07, 2018.
- Steve Bellovin. Here's how to make sure Hawaii's missile warning fiasco isn't repeated. *Ars Technica*, January 21, 2018.
- Jonathan Bair, Steven Bellovin, Andrew Manley, Blake Reid, and Adam Shostack. That was close! Reward reporting of cybersecurity "near misses". *Colorado Technology Law Journal*, 16(2):327–364, 2018.
- John Koh, Steven M. Bellovin, and Jason Nieh. Easy email encryption with easy key management. Technical Report CUCS-004-18, Department of Computer Science, Columbia University, November 2018.

- Steven M. Bellovin. Comments on privacy. LawArXiv, November 2018. Comments submitted to the NTIA request for comments on privacy.
- Steven Bellovin. Replacing social security numbers is harder than you think. *Vice Motherboard*, October 5, 2017.
- Steven M. Bellovin, Susan Landau, and Herbert S. Lin. Limiting the undesired impact of cyber weapons: Technical requirements and policy implications. *Journal of Cybersecurity*, 3(1), 2017.
- Sebastian Zimmeck, Hyungtae Kim, Steven M. Bellovin, and Tony Jebara. A privacy analysis of cross-device tracking. In *Usenix Security*, August 2017.
- Sebastian Zimmeck, Ziqi Wang, Lieyong Zou, Roger Iyengar, Bin Liu, Florian Schaub, Shomir Wilson, Norman Sadeh, Steven M. Bellovin, and Joel Reidenberg. Automated analysis of privacy requirements for mobile apps. In *Proceedings of NDSS '17*, February 2017.
- Steven M. Bellovin. Further information on Miller's 1882 one-time pad. *Cryptologia*, 2017. To appear.
- Steven M. Bellovin. Mysterious checks from Mauborgne to Fabyan. *Cryptologia*, 2017. To appear.
- Lynette I. Millett, Baruch Fischhoff, and Peter J. Weinberger, editors. *Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions*. National Academies Press, 2017.
- Steven M. Bellovin. *Thinking Security: Stopping Next Year's Hackers*. Addison-Wesley, Boston, 2016.
- Steven M. Bellovin. Columbia's riots and rebellions in the 1970s. *Columbia Spectator*, October 13, 2016.
- Steven M. Bellovin, Matt Blaze, Susan Landau, and Stephanie Pell. It's too complicated: How the Internet upends *katz*, *smith*, and electronic surveillance law. *Harvard Journal of Law and Technology*, 30(1):1–101, Fall 2016.
- Steven M. Bellovin, Matt Blaze, and Susan Landau. Insecure surveillance: Technical issues with remote computer searches. *IEEE Computer*, 49(3):14–24, March 2016. An earlier version is available at `https://www.cs.columbia.edu/~smb/papers/rsearch.pdf`.
- Steven M. Bellovin and Adam Shostack. Input to the Commission on Enhancing National Cybersecurity, September 2016.
- Steven M. Bellovin. Comments on "Protecting the privacy of customers of broadband other telecommunications services", July 2016.

- Steven M. Bellovin. Further information on Miller's 1882 one-time pad. Technical Report CUCS-011-16, Department of Computer Science, Columbia University, November 25, 2016.
- Steven M. Bellovin. Vernam, Mauborgne, and Friedman: The one-time pad and the index of coincidence. In Peter Y. A. Ryan, David Naccache, and Jean-Jacques Quisquater, editors, *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Springer, 2016.
- Steven M. Bellovin. Mysterious checks from Mauborgne to Fabyan. Technical Report CUCS-012-16, Department of Computer Science, Columbia University, November 28, 2016. Revised version.
- Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, and Daniel J. Weitzner. Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, 1(1), September 2015.
- Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, Matthew Green, Peter G. Neumann, Susan Landau, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, and Daniel J. Weitzner. Keys under doormats: Mandating insecurity by requiring government access to all data and communications. Technical Report MIT-CSAIL-TR-2015-026, Computer Science and Artificial Intelligence Laboratory, 2015.
- Steven M. Bellovin. The danger of 'exceptional access'. *CNN.com*, November 18, 2015.
- Chris Riederer, Sebastian Zimmeck, Coralie Phanord, Augustin Chaintreau, and Steven M. Bellovin. I don't have a photograph but you can have my footprints—revealing the demographics of location data. In *Proceedings of COSN '15*, 2015.
- Ben A. Fisch, Binh Vo, Fernando Krell, Abishek Kumarasubramanian, Vladimir Kolesnikov, Tal Malkin, and Steven M. Bellovin. Malicious-client security in Blind Seer: A scalable private DBMS. In *IEEE Symposium on Security and Privacy*, May 2015.
- David E. Liddle and Lynette I. Millett, editors. *A Review of the Next Generation Air Transportation System: Implications and Importance of System Architecture*. National Academies Press, Washington, DC, 2015.
- Steven M. Bellovin. The economics of cyberwar. Technical Report CUCS-010-14, Department of Computer Science, Columbia University, April 2014. Presented at the Institute for New Economic Thinking's *Human After All*.
- Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. Lawful hacking: Using existing vulnerabilities for wiretapping on the Internet. *Northwestern Journal of Technology and Intellectual Property*, 12(1):1–64, 2014.

- Steven M. Bellovin, Renée M. Hutchins, Tony Jebara, and Sebastian Zimmeck. When enough is enough: Location tracking, mosaic theory, and machine learning. *NYU Journal of Law and Liberty*, 8(2):555–628, 2014.
- Sebastian Zimmeck and Steven M. Bellovin. Privee: An architecture for automatically analyzing web privacy policies. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 1–16, San Diego, CA, August 2014. USENIX Association.
- Steven M. Bellovin. Position paper: Security and simplicity. In *W3C/IAB Workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)*, March 2014.
- Binh Vo and Steven M. Bellovin. Anonymous publish-subscribe systems. In *SECURECOMM*, Beijing, September 2014.
- Vasilis Pappas, Fernando Krell, Binh Vo, Vladimir Kolesnikov, Tal Malkin, Seung Geol Choi, Wesley George, Angelos Keromytis, and Steven M. Bellovin. Blind Seer: A scalable private DBMS. In *IEEE Symposium on Security and Privacy*, May 2014.
- Steven M. Bellovin, Matt Blaze, and Susan Landau. Comments on proposed remote search rules, October 2014.
- Steven M. Bellovin. By any means possible: How intelligence agencies have gotten their data. *IEEE Security & Privacy*, 12(4), July–August 2014.
- Steven M. Bellovin. Vernam, Mauborgne, and Friedman: The one-time pad and the index of coincidence. Technical Report CUCS-014-14, Department of Computer Science, Columbia University, May 2014.
- David E. Liddle and Lynette I. Millett, editors. *Interim Report of a Review of the Next Generation Air Transportation System Enterprise Architecture, Software, Safety, and Human Factors*. National Academies Press, Washington, DC, 2014.
- Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau. Going bright: Wiretapping without weakening communications infrastructure. *IEEE Security & Privacy*, 11(1):62–72, January–February 2013.
- Steven M. Bellovin. Why healthcare.gov has so many problems. *CNN.com*, October 15, 2013.
- Steven M. Bellovin. Submission to the Privacy and Civil Liberties Oversight Board: Technical issues raised by the Section 215 and Section 702 surveillance programs, July 2013.
- Steven M. Bellovin, Scott O. Bradner, Whitfield Diffie, Susan Landau, and Jennifer Rexford. Can it really work? Problems with extending EINSTEIN 3 to critical infrastructure. *Harvard National Security Journal*, 3:1–38, 2012.

- Carl Landwehr, Dan Boneh, John Mitchell, Steven M. Bellovin, Susan Landau, and Mike Lesk. Privacy and cybersecurity: The next 100 years. *Proceedings of the IEEE*, PP(99):1–15, 2012.

- Maritza Johnson, Serge Egelman, and Steven M. Bellovin. Facebook and privacy: It's complicated. In *Symposium On Usable Privacy and Security (SOUPS)*, July 2012.

- Michelle Madejski, Maritza Johnson, and Steven M. Bellovin. A study of privacy setting errors in an online social network. In *Proceedings of SESOC 2012*, 2012.

- Mariana Raykova, Hang Zhao, and Steven M. Bellovin. Privacy enhanced access control for outsourced data sharing. In *Financial Cryptography and Data Security*, March 2012.

- Mariana Raykova, Ang Cui, Binh Vo, Bin Liu, Tal Malkin, Steven M. Bellovin, and Salvatore J. Stolfo. Usable secure private search. *IEEE Security & Privacy*, 10(5), September-October 2012.

- Steven M. Bellovin, Scott O. Bradner, Whitfield Diffie, Susan Landau, and Jennifer Rexford. As simple as possible—but not more so. *Communications of the ACM*, 2011. Note: this is a shorter version of "Can it really work?".

- Maritza L. Johnson, Steven M. Bellovin, and Angelos D. Keromytis. Computer security research with human subjects: Risks, benefits and informed consent. In *Financial Cryptography and Data Security*, Lecture Notes in Computer Science. Springer Berlin / Heidelberg, 2011.

- Michelle Madejski, Maritza Johnson, and Steven M. Bellovin. The failure of online social network privacy settings. Technical Report CUCS-010-11, Department of Computer Science, Columbia University, February 2011.

- Sal Stolfo, Steven M. Bellovin, and David Evans. Measuring security. *IEEE Security & Privacy*, 9(3):88, May–June 2011.

- Hang Zhao, Jorge Lobo, Arnab Roy, and Steven M. Bellovin. Policy refinement of network services for MANETs. In *The 12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011)*, Dublin, Ireland, May 2011.

- Mariana Raykova, Hang Zhao, and Steven M. Bellovin. Privacy enhanced access control for outsourced data sharing. Technical Report CUCS-039-11, Department of Computer Science, Columbia University, 2011.

- Vasilis Pappas, Mariana Raykova, Binh Vo, Steven M. Bellovin, and Tal Malkin. Private search in the real world. In *Proceedings of the 2011 Annual Computer Security Applications Conference*, December 2011.

- Steven M. Bellovin. Frank Miller: Inventor of the one-time pad. *Cryptologia*, 35(3):203–222, July 2011. An earlier version is available as technical report CUCS-009-11.

- Steven M. Bellovin. Frank Miller: Inventor of the one-time pad. Technical Report CUCS-009-11, Department of Computer Science, Columbia University, March 2011. A revised version appeared in *Cryptologia* 35(3), July 2011.

- Hang Zhao and Steven M. Bellovin. High performance firewalls in MANETs. In *International Conference on Mobile Ad-hoc and Sensor Networks*, pages 154–160, December 2010.

- Shreyas Srivatsan, Maritza Johnson, and Steven M. Bellovin. Simple-VPN: Simple IPsec configuration. Technical Report CUCS-020-10, Department of Computer Science, Columbia University, July 2010.

- Elli Androulaki, Binh Vo, and Steven M. Bellovin. A real-world identity management system with master secret revocation. Technical Report CUCS-008-10, Department of Computer Science, Columbia University, April 2010.

- Elli Androulaki and Steven M. Bellovin. A secure and privacy-preserving targeted ad-system. In *Proceedings of the 1st Workshop on Real-Life Cryptographic Protocols and Standardization*, January 2010.

- Vasilis Pappas, Mariana Raykova, Binh Vo, Steven M. Bellovin, and Tal Malkin. Trade-offs in private search. Technical Report CUCS-022-10, Department of Computer Science, Columbia University, September 2010.

- Elli Androulaki, Binh Vo, and Steven M. Bellovin. Privacy-preserving, taxable bank accounts. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, Athens, September 2010. Longer version issued as Tech Report CUCS-005-10.

- Elli Androulaki, Binh Vo, and Steven M. Bellovin. Privacy-preserving, taxable bank accounts. Technical Report CUCS-005-10, Department of Computer Science, Columbia University, April 2010.

- Maritza Johnson and Steven M. Bellovin. Policy management for e-health records. Usenix HealthSec, August 2010. Position paper.

- National Research Council. *Letter Report for the Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. National Academies Press, Washington, DC, 2010.

- Steven M. Bellovin and Randy Bush. Configuration management and security. *IEEE Journal on Selected Areas in Communications*, 27(3):268–274, April 2009.

- Shaya Potter, Steven M. Bellovin, and Jason Nieh. Two person control administration: Preventing administration faults through duplication. In *LISA '09*, November 2009.

- Maritza Johnson, Steven M. Bellovin, Robert W. Reeder, and Stuart Schechter. Laissez-faire file sharing: Access control designed for individuals at the endpoints. In *New Security Paradigms Workshop*, September 2009.

- Hang Zhao and Steven M. Bellovin. Source prefix filtering in ROFL. Technical Report CUCS-033-09, Department of Computer Science, Columbia University, July 2009.

- Yuu-Heng Cheng, Mariana Raykova, Alex Poylisher, Scott Alexander, Martin Eiger, and Steven M. Bellovin. The Zodiac policy subsystem: a policy-based management system for a high-security MANET. In *IEEE Policy 2009*, July 2009. Longer version issued as CUCS-023-09.

- Yuu-Heng Cheng, Scott Alexander, Alex Poylisher, and Mariana Raykova Steven M. Bellovin. The Zodiac policy subsystem: a policy-based management system for a high-security MANET. Technical Report CUCS-023-09, Department of Computer Science, Columbia University, May 2009.

- Elli Androulaki and Steven M. Bellovin. An anonymous credit card system. In *Proceedings of 6th International Conference on Trust, Privacy & Security in Digital Business (TrustBus)*, September 2009. Longer version issued as Tech Report CUCS-010-09.

- Elli Androulaki and Steven M. Bellovin. An anonymous credit card system. Technical Report CUCS-010-09, Department of Computer Science, Columbia University, February 2009.

- Elli Androulaki and Steven M. Bellovin. Anonymous delivery of physical objects. In *Symposium on Privacy-Enhancing Technologies (PET)*, July 2009.

- Elli Androulaki, Binh Vo, and Steven M. Bellovin. Cybersecurity through identity management. In *Engaging Data: First International Forum on the Application and Management of Personal Electronic Information*, October 2009.

- Elli Androulaki and Steven M. Bellovin. A secure and privacy-preserving targeted ad-system. Technical Report CUCS-044-09, Department of Computer Science, Columbia University, October 2009. A revised version will appear at the 1st Workshop on Real-Life Cryptographic Protocols and Standardization.

- Mariana Raykova, Binh Vo, Tal Malkin, and Steven M. Bellovin. Secure anonymous database search. In *Proceedings of the ACM Cloud Computing Security Workshop*, November 2009.

- Scott Alexander, Yuu-Heng Cheng, Brian Coan, Andrei Ghetie, Vikram Kaul, Bruce Siegell, Steven M. Bellovin, Nicholas Maxemchuk, Henning Schulzrinne, Stephen Schwab, Angelos Stavrou, and Jonathan Smith. The dynamic community of interest and its realization in zodiac. *Communications Magazine, IEEE*, 47:40 – 47, 11 2009.

- 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.

- 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 & 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.

- 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.

- 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.

- Elli Androulaki, Mariana Raykova, Angelos Stavrou, and Steven M. Bellovin. PAR: Payment for anonymous routing. 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.

- Olaf Maennel, Randy Bush, Luca Cittadini, and Steven M. Bellovin. A better approach than carrier-grade-NAT. Technical Report CUCS-041-08, Department of Computer Science, Columbia University, September 2008.

- 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. 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 CUCS-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 CUCS-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 CUCS-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 CUCS-029-07, Department of Computer Science, Columbia University, September 2007.

- Seymour E. Goodman and Herbert S. Lin, editors. *Toward a Safer and More Secure Cyberspace*. National Academy Press, 2007.

- 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, Angelos Keromytis, and Bill Cheswick. Worm propagation strategies in an IPv6 Internet. *;login:*, pages 70–76, February 2006.

- Steven M. Bellovin. Virtual machines, virtual security. *Communications of the ACM*, 49(10), October 2006. "Inside RISKS" column.

- Steven M. Bellovin and Eric K. Rescorla. Deploying a new hash algorithm. In *Proceedings of NDSS '06*, 2006.

- 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, Matt Blaze, Ernest Brickell, Clinton Brooks, Vint Cerf, Whitfield Diffie, Susan Landau, Jon Peterson, and John Treichler. Security implications of applying the Communications Assistance to Law Enforcement Act to Voice over IP, 2006.

- 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, 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. 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.
- 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.
- 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.
- 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". Transcript at https://archive.org/details/gov.gpo.fdsys.CHRG-108hhrg98150.
- Steven M. Bellovin. Access control prefix router advertisement option for IPv6. Obsolete Internet draft, February 2003.
- Steven M. Bellovin, Marcus Leech, and Tom Taylor. ICMP traceback messages. Obsolete Internet draft, February 2003.
- Steven M. Bellovin and Emden R. Gansner. Using link cuts to attack Internet routing, 2003. Draft.
- 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.

- Ratul Mahajan, Steven M. Bellovin, Sally Floyd, John Ioannidis, Vern Paxson, and Scott Shenker. Controlling high bandwidth aggregates in the network. *Computer Communication 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 and Randy Bush. Security through obscurity considered dangerous. Obsolete Internet draft, February 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.
- 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.
- Steven 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. A "Reason" field for ICMP "Administratively Prohibited" messages. Obsolete Internet draft, December 2001.
- Steven M. Bellovin. Using Bloom Filters for authenticated yes/no answers in the DNS. Obsolete Internet draft, December 2001.
- 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, 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 Steven M. 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.
- Steven M. Bellovin and Robert G. Moskowitz. Client certificate and key retrieval for IKE. Obsolete Internet draft, November 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. Distributed firewalls. *;login:*, pages 39–47, November 1999.
- J. S. Denker, Steven 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).
- Steven M. Bellovin, Adam Buchsbaum, and S. Muthukrishnan. TCP compression filter. Obsolete Internet draft, October 1999.
- Steven M. Bellovin, Adam Buchsbaum, and S. Muthukrishnan. TCP filters. Obsolete Internet draft, October 1999.
- Fred B. Schneider, editor. *Trust in Cyberspace*. National Academy Press, 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.
- Network security issues. In Peter Denning and Dorothy Denning, editors, *Internet Besieged: Countering Cyberspace Scofflaws*. ACM Press, 1997.
- 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 *Proc. of the Symposium on Network and Distributed System Security*, pages 155–160, 1997.
- 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.
- Network security issues. In A. Tucker, editor, *CRC Computer Science and Engineering Handbook*. CRC Press, 1996.
- 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.
- Security and software engineering. In B. Krishnamurthy, editor, *Practical Reusable UNIX Software*. John Wiley & Sons, 1995.
- 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.

- William R. Cheswick and Steven M. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*. Addison-Wesley, Reading, MA, 1st edition edition, 1994.
- Steven M. Bellovin and William R. Cheswick. Network firewalls. *IEEE Communications Magazine*, 32(9):50–57, Sept 1994.
- 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.
- David A. Wagner and Steven M. Bellovin. A programmable plaintext recognizer, 1994. Unpublished.
- 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 Communication Review*, 23(3):26–31, July 1993.
- 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 Symposium on Research in Security and Privacy*, pages 72–84, Oakland, CA, May 1992.
- Steven M. Bellovin. A best-case network performance model, 1992. Unpublished.
- 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. Encrypted key exchange: Password-based protocols secure against dictionary attacks, August 1991.
- Steven M. Bellovin and Michael Merritt. Limitations of the Kerberos authentication system. *Computer Communication Review*, 20(5), October 1990.
- Steven M. Bellovin. Pseudo-network drivers and virtual networks. In *USENIX Conference Proceedings*, pages 229–244, Washington, DC, January 1990.
- Steven M. Bellovin. Towards a commercial IP security option. In *Commercial IPSO Workshop, INTEROP '89*, May 1989.
- Steven M. Bellovin. Security problems in the TCP/IP protocol suite. *Computer Communication 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*, pages 126–141, 1986.
- Jacob Gorman, Nikhil Mehta, Marie Nganele, Janet Zhang, and Steven M. Bellovin. Privacy-preserving accountability for non-consensual pornography. In progress.
- Steven M. Bellovin. The prehistory of public key cryptography.

Major Committees

2023–now Member, National Academies Cyber Resilience Forum

2020–2022 Member, National Academies study committee on Fostering Responsible Computing Research: Foundations and Practices

2018–2020 Member, National Academies study committee on Safeguarding the Bioeconomy: Finding Strategies for Understanding, Evaluating, and Protecting the Bioeconomy while Sustaining Innovation and Growth

2013–2015 Member, National Research Council study committee on FAA Next Generation Air Traffic Control System

2012–2018 Member, National Research Council study committee on Cybersecurity Foundations

2010–2020 Member, Computer Science and Telecommunications Board of the National Academies

2009–2012 Member, Technical Guidelines Development Committee of the Elections Assistance Commission

2008 Co-chair, Applied Cryptography and Network Security (ACNS)

2006 Chair, Steps Towards Reducing Unwanted Traffic in the Internet (SRUTI)

2009 Subject matter expert, Department of Homeland Security Data Privacy and Integrity Advisory Committee

2005–2014 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

1999–2003 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

9,392,423 Enhanced communication service for predicting and handling communication interruption

8,798,614 Enhanced communication service for predicting and handling communication interruption

8,676,916 Method and Apparatus for Connection to Virtual Private Networks for Secure Transactions

8,261,069 Privacy-enhanced searches using encryption

8,239,531 Method and Apparatus for Connection to Virtual Private Networks for Secure Transactions

8,145,793 System and Method for Distributed Content Transformation

8,107,479 Method and System for Telephony and High Speed Data Access on a Broadband Access Network

8,037,167 Method for Detecting Hosts behind Network Address Translators

7,907,517 Routing Protocols with Predicted Outage Notification

7,756,008 Routing Protocols with Predicted Outage Notification

7,676,224 Enhanced Communication Service for Predicting and Handling Communication Interruption (2010).

7,558,970 Full-Text Privacy-enhanced searches using encryption

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).