Bruce Schneier

Contact: Schneier@schneier.com

Background

Bruce Schneier is an internationally renowned security technologist, called a security guru by the *Economist*. He is the author of 14 books -- including the *New York Times* best-seller *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* -- as well as hundreds of articles, essays, and academic papers. His influential newsletter Crypto-Gram and blog Schneier on Security are read by over 250,000 people. Schneier is a fellow at the Berkman Klein Center for Internet and Society at Harvard University, a Lecturer in Public Policy at the Harvard Kennedy School, a board member of the Electronic Frontier Foundation and the Tor Project, and an advisory board member of EPIC and VerifiedVoting.org. He is also a special advisor to IBM Security and the Chief Technology Officer of Resilient: an IBM Company.

Professional Experience

2016+, Chief Technology Officer, Resilient: An IBM Company; and special advisor to IBM Security, Cambridge, MA.

2014–2016, Chief Technology Officer, Resilient Systems, Inc. (formerly called Co3 Systems, Inc.), Cambridge, MA.

2006–2013, Chief Security Technology Officer, British Telecom, London, UK.

1999–2006, Chief Technology Officer, Counterpane Internet Security, Inc., Cupertino, CA.

1993–1999, President, Counterpane Systems, Oak Park, IL and Minneapolis, MN.

1991–1993, Member of Technical Staff, AT&T Bell Labs., Schaumburg, IL.

1990, Director of Operations, Intelligent Resources Information Systems, Inc., Chicago, IL.

1987–1990, Program Manager, Space and Naval Warfare Systems Command, Arlington, VA.

1984–1987, Electronics Engineer, Naval Electronics Systems Security Engineering Center, Washington DC.

Academic Experience

2016+, Lecturer, John F. Kennedy School of Government, Harvard University.

2016+, Research Fellow in the Science, Technology, and Public Policy program at the Belfer Center for Science and International Affairs, Kennedy School of Government, Harvard University.

2013+, Fellow, Berkman Klein Center for Internet and Society, Harvard University.

Board Membership

2016+, Board Member, Tor Project, Cambridge, MA.

2013+, Board Member, Electronic Frontier Foundation, San Francisco, CA.

2004-2013, Board Member, Electronic Privacy Information Center, Washington DC.

Education

M.S. Computer Science, American University, 1986.

B.S. Physics, University of Rochester, 1984.

Books

Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World, WW Norton & Company, 2015.

Carry On: Sound Advice from Schneier on Security, John Wiley & Sons, 2013.

Liars and Outliers: Enabling the Trust that Society Needs to Thrive, John Wiley & Sons, 2012.

Cryptography Engineering (with Niels Ferguson and Tadayoshi Kohno), John Wiley & Sons, 2010.

Schneier on Security, John Wiley & Sons, 2008.

Beyond Fear: Thinking Sensibly about Security in an Uncertain World, Copernicus Books, 2003.

Practical Cryptography (with Niels Ferguson), John Wiley & Sons, 2003

Secrets & Lies: Digital Security in a Networked World, John Wiley & Sons, 2000.

The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance (with David Banisar), John Wiley & Sons, 1997.

Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

The Twofish Encryption Algorithm (with John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson), John Wiley & Sons, 1996.

E-Mail Security, John Wiley & Sons, 1995

Protect Your Macintosh, Peachpit Press, 1994

Applied Cryptography, John Wiley & Sons, 1994.

Academic Publications

J. Quinn and B. Schneier, "A Proportional Voting System for Awards Nominations Resistant to Voting Blocs," *Voting Matters*, n. 31, to appear.

B. Schneier, K. Seidel, S. Vijayakumar, "A Worldwide Survey of Encryption Products," Berkman Center Report, February 11, 2016.

U. Gasser, M. G. Olsen, N. Gertner, D. Renan, J. Goldsmith, J. Sanchez, S. Landau, B. Schneier, J. Nye, L. Schwartztol, D. R. O'Brien, J. Zittrain, "Don't Panic: Making Progress on the 'Going Dark' Debate," Berkman Center Report, February 1, 2016.

H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. Specter, D. J. Weitzner, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity*, November 2015.

B. Schneier, M. Fredrikson, T. Kohno, T. Ristenpart, "Surreptitiously Weakening Cryptographic Systems," *Cryptology ePrint Archive* Report 2015/097, 2015.

A. Czeskis, D. Mah, O. Sandoval, I. Smith, K. Koscher, J. Appelbaum, T. Kohno, B. Schneier, "DeadDrop/Strongbox Security Assessment," *UW Computer Science and Engineering Technical Report #13-08-02*, August 8, 2013.

B. Schneier, "Schneier on Security: Privacy and Control," *Journal of Privacy and Confidentiality*, v.2, n.1, pp. 3–4, 2010.

N. Ferguson, S. Lucks, B. Schneier, D. Whiting, M. Bellare, T. Kohno, J. Callas, J. Walker, "The Skein Hash Function Family," version 1.2, September 15, 2009.

M. Bellare, T. Kohno, S. Lucks, N. Ferguson, B. Schneier, D. Whiting, J. Callas, J. Walker, "Provable Security Support for the Skein Hash Family," April 29, 2009.

A. Czeskis, D. J. St. Hilaire, K. Koscher, S. D. Gribble, T. Kohno, and B. Schneier, "Defeating Encrypted and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications," 3rd Usenix Workshop on Hot Topics in Security, 2008.

B. Schneier, "The Psychology of Security," *AFRICACRYPT 2008, LNCS 5023*, Springer-Verlag, 2008, pp. 50–79.

R. Anderson and B. Schneier, "Economics of Information Security," *IEEE Security and Privacy* 3 (1), 2005, pp. 12–13.

J. Kelsey and B. Schneier, "Second Preimages on n-bit Hash Functions for Much Less than 2n Work," *Advances in Cryptology: EUROCRYPT 2005 Proceedings*, Springer-Verlag, 2005, pp. 474–490.

D. Whiting, B. Schneier, S. Lucks, and F. Muller, "Phelix: Fast Encryption and Authentication in a Single Cryptographic Primitive," *ECRYPT Stream Cipher Project Report* 2005/027.

N. Ferguson and B. Schneier, "A Cryptographic Evaluation of IPsec," December 2003.

N. Ferguson, D. Whiting, B. Schneier, J. Kelsey, S. Lucks, and T. Kohno, "Helix: Fast Encryption and Authentication in a Single Cryptographic Primitive," *Proceedings of Fast Software Encryption 2003*, pp. 345–362.

K. Jallad, J. Katz, and B. Schneier, "Implementation of Chosen-Ciphertext Attacks against PGP and GnuPG," *Information Security Conference 2002 Proceedings*, Springer-Verlag, 2002.

B. Schneier, "Inside Risks 129: Cyber Underwriters Lab?," *Communications of the ACM*, vol 44, n 4, Apr 2001.

N. Ferguson, J. Kelsey, B. Schneier, M. Stay, D. Wagner, and D. Whiting, "Improved Cryptanalysis of Rijndael," *Seventh Fast Software Encryption Workshop*, Springer-Verlag, 2001, pp. 213–230.

J. Kelsey, T. Kohno, and B. Schneier, "Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent," *Seventh Fast Software Encryption Workshop*, Springer-Verlag, 2001, pp. 7–93.

J. Kelsey and B. Schneier, "The Street Performer Protocol and Digital Copyrights," *First Monday*, v. 45, n. 6 (June 2001).

J. Katz and B. Schneier, "A Chosen Ciphertext Attack against Several E-Mail Encryption Protocols," 9th USENIX Security Symposium, 2000.

B. Schneier, "The Fallacy of Trusted Client Software" (Cryptorhythms column), *Information Security Magazine*, August 2000.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, T. Kohno, M. Stay, "The Twofish Team's Final Comments on AES Selection," May 15, 2000.

D. Whiting, B. Schneier, S. Bellovin, "AES Key Agility Issues in High-Speed IPsec Implementations," May 15, 2000.

B. Schneier, "The Process of Security," *Information Security Magazine*, April 2000.

N. Ferguson, B. Schneier, and D. Wagner, "Security Weaknesses in Maurer-Like Randomized Stream Ciphers," *Fifth Australasian Conference on Information Security and Privacy* (ACISP 2000), Springer-Verlag, 2000, pp. 234–241.

J. Kelsey and B. Schneier, "MARS Attacks! Preliminary Cryptanalysis of Reduced-Round MARS Variants," *Proceedings of the Third AES Candidate Conference*, April 2000, pp. 169–185.

T. Kohno, J. Kelsey, and B. Schneier, "Preliminary Cryptanalysis of Reduced-Round Serpent," *Proceedings of the Third AES Candidate Conference*, April 2000, pp. 195–211.

B. Schneier and D. Whiting, "A Performance Comparison of the Five AES Finalists," *Proceedings of the Third AES Candidate Conference*, April 2000, pp. 123–135.

N. Ferguson, J. Kelsey, B. Schneier, D. Whiting, "A Twofish Retreat: Related-Key Attacks Against Reduced-Round Twofish," Twofish Technical Report #6, February 14, 2000.

C. Ellison and B. Schneier, "Inside Risks 116: Risks of PKI: Electronic Commerce," *Communications of the ACM*, vol 43, n 2, Feb 2000.

C. Ellison and B. Schneier, "Inside Risks 115: Risks of PKI: Secure E-Mail," *Communications of the ACM*, vol 43, n 1, Jan 2000.

C. Ellison and B. Schneier, "Ten Risks of PKI: What You're Not Being Told about Public Key Infrastructure," *Computer Security Journal*, v 16, n 1, 2000, pp. 1–7.

C. Ellison, C. Hall, R. Milbert, and B. Schneier, "Protecting Secret Keys with Personal Entropy," *Future Generation Computer Systems*, v. 16, 2000, pp. 311–318.

B. Schneier, "Self-Study Course in Block Cipher Cryptanalysis," *Cryptologia*, v.24, n.1, Jan 2000, pp. 18–34.

J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Ciphers," *Journal of Computer Security*, v. 8, n. 2–3, 2000, pp. 141–158.

J. Kelsey and B. Schneier, "Key-Schedule Cryptanalysis of DEAL," *Sixth Annual Workshop on Selected Areas in Cryptography* (SAC 99), Springer Verlag, 2000, pp. 118–134.

J. Kelsey, B. Schneier, and N. Ferguson, "Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator," *Sixth Annual Workshop on Selected Areas in Cryptography* (SAC 99), Springer Verlag, 2000, pp. 13–33.

B. Schneier, "Attack Trees," *Dr. Dobb's Journal*, v. 24, n. 12, Dec 1999, pp. 21–29.

B. Schneier, “The 1999 Crypto Year-in-Review,” *Information Security Magazine*, January 1999.

B. Schneier, “Security in the Real World: How to Evaluate Security Technology,” *Computer Security Journal*, v 15, n 4, 1999, pp. 1–14.

B. Schneier, “A Plea for Simplicity,” *Information Security Magazine*, November 1999.

B. Schneier and Mudge, “Cryptanalysis of Microsoft’s PPTP Authentication Extensions (MS-CHAPv2),” *CQRE ’99*, Springer-Verlag, 1999, pp. 192–203.

B. Schneier, “Inside Risks 112: Risks of Relying on Cryptography,” *Communications of the ACM*, vol 42, n 10, Oct 1999.

B. Schneier, “Inside Risks 111: The Trojan Horse Race,” *Communications of the ACM*, vol 42, n 9, September 1999.

B. Schneier, “International Cryptography,” *Information Security Magazine*, September 1999.

J. Kelsey and B. Schneier, “Minimizing Bandwidth for Remote Access to Cryptographically Protected Audit Logs,” *Second International Workshop on the Recent Advances in Intrusion Detection* (RAID ’99), September 1999.

B. Schneier, “Inside Risks 110: Biometrics: Uses and Abuses,” *Communications of the ACM*, vol 42, n 8, August 1999.

C. Hall, I. Goldberg, and B. Schneier, “Reaction Attacks Against Several Public-Key Cryptosystems,” *Proceedings of Information and Communication Security*, ICICS’99, Springer-Verlag, 1999, pp. 2–12.

B. Schneier and A Shostack, “Breaking Up Is Hard to Do: Modeling Security Threats for Smart Cards,” *USENIX Workshop on Smart Card Technology*, USENIX Press, 1999, pp. 175–185.

J. Kelsey and B. Schneier, “Authenticating Secure Tokens Using Slow Memory Access,” *USENIX Workshop on Smart Card Technology*, USENIX Press, 1999, pp. 101–106.

D. Whiting, J. Kelsey, B. Schneier, D. Wagner, N. Ferguson, and C. Hall, “Further Observations on the Key Schedule of Twofish,” Twofish Technical Report #4, March 16, 1999.

E. Biham, A. Biryukov, N. Ferguson, L. Knudsen, B. Schneier, and A. Shamir, “Cryptanalysis of Magenta,” Second AES Candidate Conference, April 1999.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, “New Results on the Twofish Encryption Algorithm,” Second AES Candidate Conference, April 1999.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, “Performance Comparison of the AES Submissions,” Second AES Candidate Conference, April 1999.

D. Whiting, N. Ferguson, and B. Schneier, "Cryptanalysis of FROG," Second AES Candidate Conference, April 1999.

J. Kelsey, B. Schneier, and D. Wagner, "Key Schedule Weakness in SAFER+," Second AES Candidate Conference, April 1999.

J. Kelsey, B. Schneier, and D. Wagner, "Mod n Cryptanalysis, with Applications Against RC5P and M6, Fast Software Encryption," *Sixth International Workshop Proceedings* (March 1999), Springer-Verlag, 1999, pp. 139–155.

B. Schneier and J. Kelsey, "Secure Audit Logs to Support Computer Forensics," *ACM Transactions on Information and System Security*, v. 2, n. 2, May 1999, pp. 159–176.

B. Schneier, "The 1998 Crypto Year-in-Review," *Information Security Magazine*, January 1999.

J. Riordan and B. Schneier, "A Certified E-Mail Protocol with No Trusted Third Party," *13th Annual Computer Security Applications Conference*, ACM Press, December 1998, pp. 347–351.

B. Schneier, "Cryptographic Design Vulnerabilities," *IEEE Computer*, v. 31, n. 9, Sep 1998, pp. 29–33.

B. Schneier and Mudge, "Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol (PPTP)," *Proceedings of the 5th ACM Conference on Communications and Computer Security*, ACM Press, November 1998, pp. 132–141.

J. Kelsey and B. Schneier, "The Street Performer Protocol," *The Third USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1998.

B. Schneier, "Scrambled Message," *Information Security Magazine*, October 1998.

C. Salter, O.S. Saydjari, B. Schneier, and J. Wallner, "Towards a Secure System Engineering Methodology," *New Security Paradigms Workshop*, September 1998, pp. 2–10.

J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Ciphers," *ESORICS '98 Proceedings*, Springer-Verlag, September 1998, pp. 97–110.

C. Hall, J. Kelsey, V. Rijmen, B. Schneier, and D. Wagner, "Cryptanalysis of SPEED," *Fifth Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, August 1998, 319–338.

D. Wagner, L. Simpson, E. Dawson, J. Kelsey, W. Millan, and B. Schneier, "Cryptanalysis of ORYX," *Fifth Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, August 1998, 296–305.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, and C. Hall, "On the Twofish Key Schedule," Fifth *Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, August 1998, 27–42.

C. Hall, J. Kelsey, B. Schneier, and D. Wagner, "Building Pseudo-Random Functions from Pseudo-Random Permutations," *Advances in Cryptology—CRYPTO '98 Proceedings*, Springer-Verlag, August 98, pp. 370–389.

J. Riordan and B. Schneier, "Environmental Key Generation towards Clueless Agents," *Mobile Agents and Security*, G. Vigna, ed., Springer-Verlag, 1998, pp. 15–24.

C. Hall, J. Kelsey, B. Schneier, and D. Wagner, "Cryptanalysis of SPEED (Extended Abstract)," *Financial Cryptography '98*, Springer-Verlag, 1998, 309–310.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Twofish: A 128-Bit Block Cipher," 15 June 1998.

J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Cryptanalytic Attacks on Pseudorandom Number Generators," *Fast Software Encryption, Fifth International Workshop Proceedings* (March 1998), Springer-Verlag, 1998, pp. 168–188.

D. Coppersmith, D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of TwoPrime," *Fast Software Encryption, Fifth International Workshop Proceedings* (March 1988), Springer-Verlag, 1998, 32–48.

B. Schneier and J. Kelsey, "Cryptographic Support for Secure Logs on Untrusted Machines," *The Seventh USENIX Security Symposium Proceedings*, USENIX Press, January 1998, pp. 53–62.

J. Kelsey, B. Schneier, C. Hall, and D. Wagner, "Secure Applications of Low-Entropy Keys," *1997 Information Security Workshop* (ISW'97), Proceedings (September 1997), Springer-Verlag, 1998, pp. 121–134.

B. Schneier and C. Hall, "An Improved E-mail Security Protocol," *13th Annual Computer Security Applications Conference*, ACM Press, December 1997, pp. 232–238.

C. Hall and B. Schneier, "Remote Electronic Gambling," *13th Annual Computer Security Applications Conference*, ACM Press, December 1997, pp. 227–230.

J. Kelsey, B. Schneier, and D. Wagner, "Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA," *ICICS '97 Proceedings*, Springer-Verlag, November 1997, pp. 233–246.

D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of the Cellular Message Encryption Algorithm," *Advances in Cryptology—CRYPTO '97 Proceedings*, Springer-Verlag, August 1997, pp. 526–537.

N. Ferguson and B. Schneier, "Cryptanalysis of Akelarre," Fourth Annual Workshop on Selected Areas in Cryptography, August 1997, pp. 201–212.

H. Abelson, R. Anderson, S.M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. G. Neumann, R.L. Rivest, J.I. Schiller, and B. Schneier, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," *World Wide Web Journal*, v.2, n.3, 1997, pp. 241–257.

J. Kelsey and B. Schneier, "Conditional Purchase Orders," *4th ACM Conference on Computer and Communications Security*, ACM Press, April 1997, pp. 117–124.

J. Kelsey, B. Schneier, and D. Wagner, "Protocol Interactions and the Chosen Protocol Attack," *Security Protocols, International Workshop April 1997 Proceedings*, Springer-Verlag, 1998, pp. 91–104.

B. Schneier and J. Kelsey, "Remote Auditing of Software Outputs Using a Trusted Coprocessor," *Journal of Future Generation Computer Systems*, v.13, n.1, 1997, pp. 9–18.

B. Schneier, "Why Cryptography is Harder than it Looks," *Information Security Bulletin*, v. 2, n. 2, March 1997, pp. 31–36.

B. Schneier and D. Whiting, "Fast Software Encryption: Designing Encryption Algorithms for Optimal Software Speed on the Intel Pentium Processor," *Fast Software Encryption, Fourth International Workshop Proceedings* (January 1997), Springer-Verlag, 1997, pp. 242–259.

B. Schneier, "Cryptography, Security, and the Future," *Communications of the ACM*, v. 40, n. 1, January 1997, p. 138.

J. Kelsey, B. Schneier, and C. Hall, "An Authenticated Camera," *12th Annual Computer Security Applications Conference*, ACM Press, December 1996, pp. 24–30.

B. Schneier and J. Kelsey, "A Peer-to-Peer Software Metering System," *The Second USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1996, pp. 279–286.

D. Wagner and B. Schneier, "Analysis of the SSL 3.0 Protocol," *The Second USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1996, pp. 29–40.

B. Schneier, J. Kelsey, and J. Walker, "Distributed Proctoring," *ESORICS 96 Proceedings*, Springer-Verlag, September 1996, pp. 172–182.

J. Kelsey and B. Schneier, "Authenticating Outputs of Computer Software Using a Cryptographic Coprocessor," *Proceedings 1996 CARDIS*, September 1996, pp. 11–24.

J. Kelsey, B. Schneier, and D. Wagner, "Key-Schedule Cryptanalysis of 3-WAY, IDEA, G-DES, RC4, SAFER, and Triple-DES," *Advances in Cryptology—CRYPTO '96 Proceedings*, Springer-Verlag, August 1996, pp. 237–251.

B. Schneier and J. Kelsey, "Automatic Event Stream Notarization Using Digital Signatures," *Security Protocols, International Workshop April 1996 Proceedings*, Springer-Verlag, 1997, pp. 155–169.

B. Schneier and J. Kelsey, "Unbalanced Feistel Networks and Block Cipher Design," *Fast Software Encryption, Third International Workshop Proceedings* (February 1996), Springer-Verlag, 1996, pp. 121–144.

M. Blaze, W. Diffie, R. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Weiner, "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security," January 1996.

M. Jones and B. Schneier, "Securing the World Wide Web: Smart Tokens and their Implementation," *Proceedings of the Fourth International World Wide Web Conference*, December 1995, pp. 397–409.

B. Schneier, "Blowfish—One Year Later," *Dr. Dobb's Journal*, September 1995.

M. Blaze and B. Schneier, "The MacGuffin Block Cipher Algorithm," *Fast Software Encryption, Second International Workshop Proceedings* (December 1994), Springer-Verlag, 1995, pp. 97–110.

B. Schneier, "The GOST Encryption Algorithm," *Dr. Dobb's Journal*, v. 20, n. 1, January 1995, pp. 123–124.

B. Schneier, "A Primer on Authentication and Digital Signatures," *Computer Security Journal*, v. 10, n. 2, 1994, pp. 38–40.

B. Schneier, "Designing Encryption Algorithms for Real People," *Proceedings of the 1994 ACM SIGSAC New Security Paradigms Workshop*, IEEE Computer Society Press, August 1994, pp. 63–71.

B. Schneier, "The Blowfish Encryption Algorithm," *Dr. Dobb's Journal*, v. 19, n. 4, April 1994, pp. 38–40.

B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)," *Fast Software Encryption, Cambridge Security Workshop Proceedings* (December 1993), Springer-Verlag, 1994, pp. 191–204.

B. Schneier, "One-Way Hash Functions," *Dr. Dobb's Journal*, v. 16, n. 9, September 1991, pp. 148–151.

Selected Awards

Business Leader in Cybersecurity Award from Boston Global Forum, December 2015.

Named as one of the 20 top security influencers by *eSecurity Planet*, June 2015.

EPIC Lifetime Achievement Award, June 2015.

Named as one of the top ten information security bloggers of 2014 by the ISO 27001 and ISO 22301 blog, December 2014.

Named as an industry pioneer in information security by *SC Magazine*, December 2014.

Berkman Fellow at the Berkman Center for Internet and Society at Harvard University, 2013–2015 academic years.

Named one of the IFSEC 40: The Most Influential People in Security & Fire, January 2013.

Honorary Doctor of Science (ScD) from University of Westminster, London, December 2011.

CSO Compass Award, May 2010.

Named as one of the top 25 most influential people in the security industry by *Security* magazine, December 2008

Inducted into the Infosecurity Europe Hall of Fame, April 2008.

Computer Professionals for Social Responsibility (CPSR) Norbert Wiener Award, January 2008.

Electronic Frontier Foundation (EFF) Pioneer Award, March 2007.

Dr. Dobb's Journal Excellence in Programming Award, April 2006.

Named as one of the top five influential IT security thinkers by *SC* magazine, December 2005.

Infoworld CTO 25 Award, April 2005.

Secrets and Lies won a Productivity Award in the 13th Annual *Software Development Magazine* Product Excellence Awards, 2000.