

Bruce Schneier

Bruce Schneier (/ˈʃnaɪ.ər/; born January 15, 1963) is an American cryptographer, computer security professional, privacy specialist, and writer. Schneier is a Lecturer in Public Policy at the Harvard Kennedy School^[2] and a Fellow at the Berkman Klein Center for Internet & Society as of November, 2013.^[3] He is a board member of the Electronic Frontier Foundation, Access Now, and The Tor Project; and an advisory board member of Electronic Privacy Information Center and VerifiedVoting.org. He is the author of several books on general security topics, computer security and cryptography and is a squid enthusiast.^[4]

In 2015, Schneier received the EPIC Lifetime Achievement Award from Electronic Privacy Information Center.^[5]

Early life

Bruce Schneier is the son of Martin Schneier, a Brooklyn Supreme Court judge. He grew up in the Flatbush neighborhood of Brooklyn, New York, attending P.S. 139 and Hunter College High School.^[6]

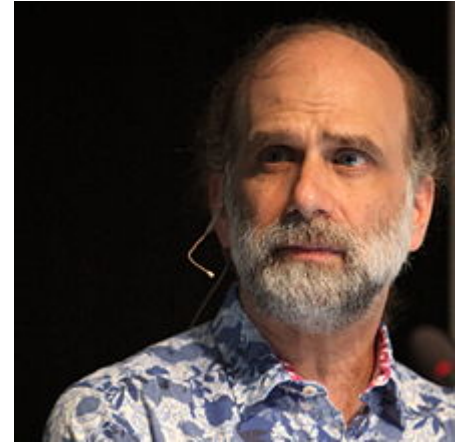
After receiving a physics bachelor's degree from the University of Rochester in 1984,^[7] he went to American University in Washington, D.C., and got his master's degree in computer science in 1988.^[8] He was awarded an honorary Ph.D from the University of Westminster in London, England, in November 2011. The award was made by the Department of Electronics and Computer Science in recognition of Schneier's 'hard work and contribution to industry and public life'.

Schneier was a founder and chief technology officer of Counterpane Internet Security (now BT Managed Security Solutions). He worked for IBM once they acquired Resilient Systems where Schneier was CTO^{[9][10][11]} until he left at the end of June 2019.^[12]

Writings on computer security and general security

In 1991, Schneier was laid off from his job and started writing for computer magazines. Later he decided to write a book on applied cryptography "since no such book existed". He took his articles,

Bruce Schneier



Schneier in 2013

Born	January 15, 1963 ^[1] New York City, US
Alma mater	<u>American University</u> <u>University of Rochester</u>
Known for	<u>Cryptography</u> , <u>security</u>
Scientific career	
Fields	<u>Computer science</u>
Institutions	<u>Harvard University</u> <u>Counterpane Internet Security</u> <u>Bell Labs</u> <u>United States Department of Defense</u> <u>BT Group</u>
Website	<u>www.schneier.com</u> (<u>https://www.schneier.com</u>)
Signature	

wrote a proposal to John Wiley and they bought the proposal.^[13]

In 1994, Schneier published *Applied Cryptography*, which details the design, use, and implementation of cryptographic algorithms.



This book allowed me to write more, to start consulting, to start my companies, and really launched me as an expert in this field, and it really was because no one else has written this book. I wanted to read it so I had to write it. And it happened in a really lucky time when everything started to explode on the Internet.^[13]

In 2010 he published *Cryptography Engineering*, which is focused more on how to use cryptography in real systems and less on its internal design. He has also written books on security for a broader audience. In 2000, Schneier published *Secrets and Lies: Digital Security in a Networked World*; in 2003, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*; in 2012, *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*; and in 2015, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*.^[14]

Schneier writes a freely available monthly Internet newsletter on computer and other security issues, *Crypto-Gram*, as well as a security weblog, *Schneier on Security*.^[15] The blog focuses on the latest threats, and his own thoughts. The weblog started out as a way to publish essays before they appeared in *Crypto-Gram*, making it possible for others to comment on them while the stories were still current, but over time the newsletter became a monthly email version of the blog, re-edited and re-organized.^[16] Schneier is frequently quoted in the press on computer and other security issues, pointing out flaws in security and cryptographic implementations ranging from biometrics to airline security after the September 11 attacks.^[17]

Viewpoints

Blockchain

Schneier warns about misplaced trust in blockchain^[18] and the lack of use cases, calling blockchain a solution in search of a problem.^[19]

What blockchain does is shift some of the trust in people and institutions to trust in technology. You need to trust the cryptography, the protocols, the software, the computers and the network. And you need to trust them absolutely, because they're often single points of failure.

I've never seen a legitimate use case for blockchain. I've never seen any system where blockchain provides security in a way that is impossible to provide in any other way.^[20]

He goes on to say that cryptocurrencies are useless and are only used by speculators looking for quick riches.

Cryptography

To Schneier, peer review and expert analysis are important for the security of cryptographic systems.^[21] Mathematical cryptography is usually not the weakest link in a security chain; effective security requires that cryptography be combined with other things.^[22]

The term *Schneier's law* was coined by Cory Doctorow in a 2004 speech.^[23] The law is phrased as:

Any person can invent a security system so clever that she or he can't think of how to break it.

He attributes this to Bruce Schneier, who wrote in 1998: "Anyone, from the most clueless amateur to the best cryptographer, can create an algorithm that he himself can't break. It's not even hard. What is hard is creating an algorithm that no one else can break, even after years of analysis."^[24]

Similar sentiments had been expressed by others before. In *The Codebreakers*, David Kahn states: "Few false ideas have more firmly gripped the minds of so many intelligent men than the one that, if they just tried, they could invent a cipher that no one could break", and in "A Few Words On Secret Writing", in July 1841, Edgar Allan Poe had stated: "Few persons can be made to believe that it is not quite an easy thing to invent a method of secret writing which shall baffle investigation. Yet it may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve."^[25]

Schneier also coined the term "kid sister cryptography", writing in the Preface to *Applied Cryptography*^[26] that:

There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.

Digital rights management

Schneier is critical of digital rights management (DRM) and has said that it allows a vendor to increase lock-in.^[27] Proper implementation of control-based security for the user via trusted computing is very difficult, and security is not the same thing as control.^[27]

Schneier insists that "owning your data is a different way of thinking about data."^[28]

Full disclosure

Schneier is a proponent of full disclosure, i.e. making security issues public.

If researchers don't go public, things don't get fixed. Companies don't see it as a security problem; they see it as a PR problem.^[29]

Homeland security

Schneier has said that homeland security money should be spent on intelligence, investigation, and emergency response.^[30] Defending against the broad threat of terrorism is generally better than focusing on specific potential terrorist plots.^[30] According to Schneier, analysis of intelligence data is difficult but is one of the better ways to deal with global terrorism.^[31] Human intelligence has advantages over automated and computerized analysis, and increasing the amount of intelligence data that is gathered does not help to improve the analysis process.^[31] Agencies that were designed around fighting the Cold War may have a culture that inhibits the sharing of information; the practice of sharing information is more important and less of a security threat in itself when dealing with more decentralized and poorly funded adversaries such as al Qaeda.^[32]

Regarding PETN—the explosive that has become terrorists' weapon of choice—Schneier has written that only swabs and dogs can detect it. He also believes that changes to airport security since 11 September 2001 have done more harm than good and he defeated Kip Hawley, former head of the Transportation Security Administration, in an *Economist* online debate by 87% to 13% regarding the issue.^[33] He is widely credited with coining the term "security theater" to describe some such changes.

As a Fellow of Berkman Center for Internet & Society at Harvard University, Schneier is exploring the intersection of security, technology, and people, with an emphasis on power.^[34]

Movie plot threat

"Movie-plot threat" is a term Schneier coined that refers to very specific and dramatic terrorist attack scenarios, reminiscent of the behavior of terrorists in movies, rather than what terrorists actually do in the real world.^[35] Security measures created to protect against movie plot threats do not provide a higher level of real security, because such preparation only pays off if terrorists choose that one particular avenue of attack, which may not even be feasible. Real-world terrorists would also be likely to notice the highly specific security measures, and simply attack in some other way. The specificity of movie plot threats gives them power in the public imagination, however, so even extremely unrealistic security theater countermeasures may receive strong support from the public and legislators. Among many other examples of movie plot threats, Schneier described banning baby carriers from subways, for fear that they may contain explosives.^[36] Starting in April 2006, Schneier has had an annual contest to create the most fantastic movie-plot threat.^[37] In 2015, during the 8th and as of 17 February 2022 the last one, he mentioned that the contest may have run its course.^[38]

System design

Schneier has criticized security approaches that try to prevent any malicious incursion, instead arguing that designing systems to fail well is more important.^[39] The designer of a system should not underestimate the capabilities of an attacker, as technology may make it possible in the future to do things that are not possible at the present.^[21] Under Kerckhoffs's Principle, the need for one or more

parts of a cryptographic system to remain secret increases the fragility of the system; whether details about a system should be obscured depends upon the availability of persons who can make use of the information for beneficial uses versus the potential for attackers to misuse the information.^[40]

Secrecy and security aren't the same, even though it may seem that way. Only bad security relies on secrecy; good security works even if all the details of it are public.^[41]

Cryptographic algorithms

Schneier has been involved in the creation of many cryptographic algorithms.

Hash functions:

- Skein

Stream ciphers:

- Solitaire
- Phelix
- Helix

Pseudo-random number generators:

- Fortuna
- Yarrow algorithm

Block ciphers:

- Blowfish
- Twofish
- Threefish
- MacGuffin

Publications

- Schneier, Bruce. *Applied Cryptography*, John Wiley & Sons, 1994. ISBN 0-471-59756-2
- Schneier, Bruce. *Protect Your Macintosh*, Peachpit Press, 1994. ISBN 1-56609-101-2
- Schneier, Bruce. *E-Mail Security*, John Wiley & Sons, 1995. ISBN 0-471-05318-X
- Schneier, Bruce. *Applied Cryptography*, Second Edition, John Wiley & Sons, 1996. ISBN 0-471-11709-9
- Schneier, Bruce; Kelsey, John; Whiting, Doug; Wagner, David; Hall, Chris; Ferguson, Niels. *The Twofish Encryption Algorithm*, John Wiley & Sons, 1996. ISBN 0-471-35381-7
- Schneier, Bruce; Banisar, David. *The Electronic Privacy Papers*, John Wiley & Sons, 1997. ISBN 0-471-12297-1
- Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons, 2000. ISBN 0-471-25311-1

- Schneier, Bruce. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, Copernicus Books, 2003. ISBN 0-387-02620-7
- Ferguson, Niels; Schneier, Bruce. *Practical Cryptography*, John Wiley & Sons, 2003. ISBN 0-471-22357-3
- Schneier, Bruce. *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons, 2004. ISBN 978-0-471-45380-2
- Schneier, Bruce. *Schneier on Security*, John Wiley & Sons, 2008. ISBN 978-0-470-39535-6
- Ferguson, Niels; Schneier, Bruce; Kohno, Tadayoshi. *Cryptography Engineering*, John Wiley & Sons, 2010. ISBN 978-0-470-47424-2
- Schneier, Bruce. *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*, John Wiley & Sons, 2012. ISBN 978-1-118-14330-8
- Schneier, Bruce. *Carry On: Sound Advice from Schneier on Security*, John Wiley & Sons, 2013. ISBN 978-1118790816
- Schneier, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W. W. Norton & Company, 2015. ISBN 978-0-393-24481-6
- Schneier, Bruce. *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*, W. W. Norton & Company, 2018. ISBN 978-0-393-60888-5
- Schneier, Bruce. *We Have Root: Even More Advice from Schneier on Security*, John Wiley & Sons, 2019. ISBN 978-1119643012
- Schneier, Bruce. *A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend them Back*, W. W. Norton & Company, 2023. ISBN 978-0-393-86666-7

Activism

Schneier is a board member of the [Electronic Frontier Foundation](#).^[42]

See also

- [Attack tree](#)
- [Failing badly](#)
- [Snake oil \(cryptography\)](#)
- [Alice and Bob](#)

References

1. "Bruce Schneier | Facebook" (<https://www.facebook.com/bruce.schneier>). *Facebook*.
2. "Bruce Schneier" (<https://www.hks.harvard.edu/faculty/bruce-schneier>). *Harvard Kennedy School*. Retrieved December 14, 2021.
3. Bergman, Kristin (October 9, 2014). "Q+A with Bruce Schneier" (<https://cyber.harvard.edu/node/95760>). Retrieved December 14, 2021.
4. "Friday Squid Blogging: Squid Found on Provincetown Sandbar - Schneier on Security" (https://www.schneier.com/blog/archives/2020/07/friday_squid_bl_737.html). *www.schneier.com*. Retrieved November 13, 2020.
5. "EPIC 2015 Champions of Freedom}date=June 1" (<https://web.archive.org/web/20160710014823/https://epic.org/june1/>). *EPIC*. Archived from the original (<https://epic.org/june1/>) on July 10, 2016.

6. Samuel Newhouse (February 9, 2009). "'Schneier on Security;' A Judge's Son Builds a Reputation of Cryptic Fame" (<https://www.schneier.com/news-080.html>). *Brooklyn Daily Eagle*.
7. Drew Amorosi (July 11, 2011). "Interview: BT's Bruce Schneier" (<https://www.schneier.com/news-114.html>). *InfoSecurity*.
8. Mann, Charles C. "Homeland Insecurity" (<https://www.theatlantic.com/magazine/archive/2002/09/homeland-insecurity/302575/>). *The Atlantic*. No. September, 2002. Retrieved December 14, 2021.
9. "Bruce Schneier, CTO of Resilient Systems, Inc" (<https://web.archive.org/web/20150224195700/https://www.resilientsystems.com/company/management-team/bruce-schneier>). Archived from the original (<https://www.resilientsystems.com/company/management-team/bruce-schneier>) on February 24, 2015. Retrieved February 24, 2015.
10. "IBM Security Closes Acquisition of Resilient Systems" (<http://www-03.ibm.com/press/us/en/pressrelease/49472.wss>) (Press release). Armonk, NY, USA: IBM Security. April 6, 2016.
11. Schneier, Bruce (February 29, 2016). "Resilient Systems News: IBM to Buy Resilient Systems" (https://www.schneier.com/blog/archives/2016/02/resilient_syste_2.html). *Schneier on Security*.
12. Schneier, Bruce (June 28, 2019). "I'm Leaving IBM" (https://www.schneier.com/blog/archives/2019/06/im_leaving_ibm.html). *Schneier on Security*.
13. "On starting a career - Special exclusive interview with Bruce Schneier at NoNameCon 2020" (https://www.youtube.com/watch?v=Vn7wL12qjY0&feature=youtu.be&t=226&ab_channel=NoNameCon). *NoNameCon live conference*. September 7, 2020.
14. Austin, Richard (March 12, 2015). "review of *Data and Goliath: The hidden Battles to capture your data and control your world*" (http://www.ieee-security.org/Cipher/BookReviews/2015/Schneier_by_austin.html). *Cipher*. www.ieee-security.org. Retrieved March 18, 2015.
15. "schneier.com" (<https://www.schneier.com/>).
16. Blood, Rebecca (January 2007). "Bruce Schneier" (<http://www.rebeccablood.net/bloggerson/bruce-schneier.html>). *Bloggers on Blogging*. Retrieved April 19, 2007.
17. Severance, Charles (2016). "Bruce Schneier: the security mindset". *Computer*. **49** (2): 7–8. doi:10.1109/MC.2016.38 (<https://doi.org/10.1109%2FMC.2016.38>).
18. SCHNEIER, BRUCE (February 6, 2019). "There's No Good Reason to Trust Blockchain Technology" (<https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/>). *Wired*. ISSN 1059-1028 (<https://www.worldcat.org/issn/1059-1028>). Retrieved February 6, 2019.
19. "Was Bruce Schneier von Blockchain, IoT und Quantencomputern hält" (<https://www.netzwoche.ch/news/2019-02-06/warum-bruce-schneier-keinen-einsatzzweck-fur-die-blockchain-sieht>). *www.netzwoche.ch* (in German). Retrieved February 6, 2019.
20. "On blockchain - Special exclusive interview with Bruce Schneier at NoNameCon 2020" (https://www.youtube.com/watch?v=Vn7wL12qjY0&feature=youtu.be&t=1893&ab_channel=NoNameCon). *NoNameCon live 2020*. Retrieved September 7, 2020.
21. Schneier, Bruce (1997). "Why Cryptography Is Harder Than It Looks" (<https://www.schneier.com/essay-037.html>). Retrieved April 8, 2011.
22. Ferguson, Niels; Schneier, Bruce. "Practical Cryptography: Preface" (<https://www.schneier.com/book-practical-preface.html>). Retrieved April 8, 2011.
23. Cory Doctorow (June 17, 2004). "Microsoft Research DRM talk" (<https://web.archive.org/web/20061202192720/http://www.dashes.com/anil/stuff/doctorow-drm-ms.html>). Archived from the original (<http://www.dashes.com/anil/stuff/doctorow-drm-ms.html>) on December 2, 2006. Retrieved December 31, 2006.
24. "Crypto-gram: October 15, 1998 - Schneier on Security" (<https://www.schneier.com/crypto-gram/archives/1998/1015.html#cipherdesign>). *www.schneier.com*. Retrieved January 26, 2022.
25. ""Schneier's law"" (https://www.schneier.com/blog/archives/2011/04/schneiers_law.html).

26. Schneier, Bruce (1996). *Applied Cryptography* (<https://www.schneier.com/books/applied-cryptography-2preface/>). John Wiley & Sons. ISBN 978-1-119-09672-6.
27. Schneier, Bruce (February 7, 2008). "With iPhone, 'Security' Is Code for 'Control' " (<https://www.schneier.com/essay-204.html>). Retrieved April 8, 2011.
28. "On owning your data - Special exclusive interview with Bruce Schneier at NoNameCon 2020" (https://www.youtube.com/watch?v=Vn7wL12qjY0&feature=youtu.be&t=2771&ab_channel=NoNameCon). *NoNameCon live conference*. Retrieved September 7, 2020.
29. "After Apple Punishes Researcher, A Complex Relationship Is Tested" (https://www.huffpost.com/entry/charlie-miller-apple-cybersecurity-bug-hacker_n_1095330). *HuffPost*. November 16, 2011. Retrieved January 26, 2022.
30. Schneier, Bruce (September 8, 2005). "Terrorists Don't Do Movie Plots" (<https://www.wired.com/politics/security/commentary/securitymatters/2005/09/68789>). *Wired News*.
31. Schneier, Bruce (January 9, 2004). "Homeland Insecurity" (<https://www.schneier.com/essay-032.html>). Retrieved April 8, 2011.
32. Schneier, Bruce (January 15, 2010). "Fixing intelligence failures – SFGate" (http://articles.sfgate.com/2010-01-15/bay-area/17828460_1_intelligence-homeland-security-organizations). *SFGate*. Retrieved April 8, 2011.
33. "International terrorism: AQAP tries again: Good intelligence work still leaves questions over airport security", *The Economist*, dated 12 May 2012.
34. "Berkman Center Announces 2013–2014 Community" (https://cyber.law.harvard.edu/newsroom/2013_2014_community). Berkman Center for Internet & Society at Harvard University. July 8, 2013. Retrieved July 8, 2013.
35. Ben Makuch (October 8, 2014). "2014 Will Not Be the Year of the First 'Online Murder' " (<http://motherboard.vice.com/read/2014-will-not-be-the-year-of-online-murder>). *Motherboard Vice.com*. Retrieved June 18, 2015.
36. Schneier, Bruce. "Schneier on Security: Exploding Baby Carriages in Subways" (http://www.schneier.com/blog/archives/2005/10/exploding_baby.html). "And if we ban baby carriages from the subways, and the terrorists put their bombs in duffel bags instead, have we really won anything?"
37. Schneier, Bruce. "Schneier on Security: Announcing: Movie-Plot Threat Contest" (http://www.schneier.com/blog/archives/2006/04/announcing_movi.html).
38. Schneier, Bruce. "Eighth Movie-Plot Threat Contest Semifinalists" (https://www.schneier.com/blog/archives/2015/05/eighth_movie-pl.html). *Schneier on Security*. Retrieved February 17, 2022.
39. Homeland Insecurity (<http://charlesmann.org/articles/Homeland-Insecurity-Atlantic.pdf>) Archived (<https://web.archive.org/web/20110928002928/http://charlesmann.org/articles/Homeland-Insecurity-Atlantic.pdf>) September 28, 2011, at the Wayback Machine, *Atlantic Monthly*, September 2002
40. Schneier, Bruce (May 15, 2002). "Crypto-Gram: May 15, 2002" (<http://www.schneier.com/crypto-gram-0205.html>). Retrieved April 8, 2011.
41. Doctorow, Cory. *Little Brother*. New York: Tor Teen, 2008, page 129.
42. Jeschke, Rebecca (June 27, 2013). "Renowned Security Expert Bruce Schneier Joins EFF Board of Directors" (<https://www.eff.org/press/releases/renowned-security-expert-bruce-schneier-joins-eff-board-directors>). Retrieved July 6, 2013.

External links

- Personal website, Schneier.com (<https://www.schneier.com/>)
- Bruce Schneier's books, Schneier.com/books.html (<https://www.schneier.com/books.html>)
- Profile of Bruce Schneier in Politico Magazine (http://www.politico.com/magazine/story/2014/03/bruce-schneier-glenn-greenwald-encryption-104705_full.html) "Glenn Greenwald's Encryption

Guru," by Alex Carp, March 16, 2014

- [Talking security with Bruce Almighty](http://www.itwire.com/opinion-and-analysis/open-sauce/16422-talking-security-with-bruce-almighty) (<http://www.itwire.com/opinion-and-analysis/open-sauce/16422-talking-security-with-bruce-almighty>) Archived (<https://web.archive.org/web/20160304100728/http://www.itwire.com/opinion-and-analysis/open-sauce/16422-talking-security-with-bruce-almighty>) March 4, 2016, at the [Wayback Machine](#)
 - Schneier at the 2009 RSA conference (https://web.archive.org/web/20090428195928/http://media.omegiaweb.com/rsa2009/preview/webcast.htm?id=1_5), video with Schneier participating on the Cryptographer's Panel, April 21, 2009, Moscone Center, San Francisco
 - Bruce Schneier on Real Law Radio (https://web.archive.org/web/20110513061852/http://www.reallawradio.net/podcasts_february-march.html), Bruce talks with Bob DiCello on the legal news talk radio program, Real Law Radio, about the case involving a Philadelphia school that allegedly spied on its students via the webcam on their computers (Podcasts/Saturday February 27, 2010).
 - Roberts, Russ (June 10, 2013). "Schneier on Power, the Internet, and Security" (http://www.econtalk.org/archives/_featuring/bruce_schneier/). *EconTalk*. Library of Economics and Liberty.
 - Bruce Schneier at Google (<https://www.youtube.com/watch?v=m3NJ-Ow2Lvg>), 19 June 2013. Schneier discusses various aspects of Internet computing and global geo-politics including trust, power relations, control, cooperative systems, ethics, laws, and security technologies. (55 minutes)
 - Bruce Schneier interviewed (<http://www.well.com/conf/inkwell.vue/topics/452/Bruce-Schneier-Liar-s-and-Outlier-page01.html>) on [The WELL](#) by Jon Lebkowsky, August 2012
-

Retrieved from "https://en.wikipedia.org/w/index.php?title=Bruce_Schneier&oldid=1169737158"

■