VITA

FRED B. SCHNEIDER February 20, 2024

Cornell University
Department of Computer Science
422 Gates Hall
107 Hoy Road
Ithaca, New York 14853
(607) 255-9221 (business)
(607) 257-7762 (home)

Date of Birth: December 7, 1953
Citizenship: United States

EDUCATION

1975 B.S., Cornell University, Computer Science and Electrical Engineering.
1977 M.S., SUNY at Stony Brook, Computer Science.
1978 Ph.D., SUNY at Stony Brook, Computer Science.
Thesis: Structure of Concurrent Programs Exhibiting Reproducible Behavior
Advisor: Professor A. J. Bernstein

EXPERIENCE

1978 Assistant Professor, Cornell University, Department of Computer Science.
1984 Associate Professor, Cornell University, Department of Computer Science.
1993 Professor, Cornell University, Department of Computer Science.
Director, AFRL/Cornell Information Assurance Institute, January 2000–July 2008.
Chief Scientist, Griffiss Institute, January 2003–January 2004.
Chief Scientist, NST TRUST Science and Technology Center, May 2005–June 2016.
2009 Appointed *Samuel B. Eckert Professor of Computer Science*, Cornell University.
2014 Chair of Computer Science Department (July 2014 – July 2018).

PROFESSIONAL ACTIVITIES

Editor:

Distributed Computing, Springer-Verlag, October 1984–present,
(Editor-in-chief, January 1989–August 2000).
Information Processing Letters, North-Holland Publishing Company,
March 1987–March 2004.
IEEE Transactions on Software Engineering, April 1992–April 1999.
IEEE Security and Privacy, November 2002–August 2014 (Associate editor-in-chief).
High Integrity Systems, March 1993–December 1996.
Annals of Software Engineering, January 1994–December 2002.
Texts and Monographs in Computer Science, Springer-Verlag,
January 1988–March 2018, (Co-managing editor October 1992–March 2018).
ACM Computing Surveys, March 1995–May 2003.
IEEE Transactions on Dependable and Secure Computing, March 2004–January 2009.
Communications of the ACM, August 2010–August 2013.

Industrial and Professional Advisory:

CSNet Technical Advisory Panel, July 1980–December 1983;
National Research Council Graduate Fellowship Evaluation Panel, February 1981;
IFIP Working Group 2.3 (Programming Methodology), Observer,
September 1982–July 1984; Member, July 1984–April 2007;
College Board Committee for Advanced Placement Computer Science,
July 1983–July 1988;
Committee on Recommendations for U.S. Army Basic Research,
July 1984–June 1988;
Chairman, Information Systems Trustworthiness,
Computer Science and Telecommunications Board,
National Research Council, National Academy of Sciences;
JavaSoft Security Advisory Committee, JavaSoft Inc., June 1997–November 2000;
JXTA Technical Advisory Council, SUN Microsystems, November 2000–November 2001;
CIGITAL Technical Advisory Board, November 2000–June 2004;
deCode Genetics Security Advisory Board, February 2000–March 2002;
Eweb University.Com Board of Advisors, March 2000–March 2002;
FAST ASA Technical Advisory Board, March 2000–March 2008;
Intel Microprocessor Research Lab Advisory Board, October 2001–August 2004;
UK Dependability Interdisciplinary Research Collaboration (DIRC),
Steering Committee, March 2001–January 2007;
Chairman, UK International Review of Computer Science, Fall 2001;
ACM Advisory Committee on Security and Privacy (ACSP), October 2001–November 2003;
National Research Council Computer Science and Telecommunications Board,
July 2002–June 2008; September 2014–January 2024;
NSF/CISE Advisory Committee, May 2002–March 2006;
Co-Chair, Microsoft, Trustworthy Computing Academic Advisory Board,
August 2002–November 2014;
IBM Autonomic Computing Advisory Board, August 2002–May 2004;
Packet General Networks Technical Advisory Board, March 2003–September 2007;
Fortify Software Technical Advisory Board, February 2004–December 2010;
Committee on Improving Cybersecurity Research,
Computer Science and Telecommunications Board,
National Research Council, National Academy of Sciences, June 2004–September 2007,
August 2014–present;
Advisory Board, Department of Computer Science, University of Virginia,
July 2005–February 2017;
PCAST Technical Advisory Group on Networking and Information Technology,
July 2006–January 2009;
Information Security and Privacy Advisory Board, Department of Commerce,
Sept 2006-Sept 2011;
Board of Directors, Computing Research Association, July 2007–June 2016;
Council Member, Computing Community Consortium, July 2007–January 2013;
Member, Computer Science Council, Stony Brook University, December 2009–December 2012;
Member, Defense Science Board, March 2008–December 31, 2012;
Consultant, Lincoln Laboratories, October 2012–present;
Member, Naval Studies Board, National Research Council, March 1, 2013–December 2018;

Chair Emeritus, Forum on Cyber-Resilience, National Research Council, February 2022–present; founding chair August 2014 – January 2022;
Chair, Board of Advisors, ZeroFox, Baltimore Maryland, February 2013–August 2022;
Member, Passages Advisory Board, August 2016–December 2020;
Member, DARPA Microsystems Exploratory Council (MEC), March 2018–September 2019;
Member, National Academies Report Review Committee, April 2023–present;
Consultant, Army Science Board, April 2023–present.

Awards:

IBM Faculty Development Award (1983).
Fellow, American Association for Advancement of Science (1992).
Fellow, Association for Computing Machinery (1995).
Professor-at-Large, University of Tromsoe, Tromsoe, Norway (1996–present).
Daniel M. Lazar Excellence in Teaching Award (2000).
Doctor of Science (*honoris causa*), University of Newcastle, U.K. (May 2003).
ACM SIGOPS Hall of Fame Award (2007).
Fellow, Institute of Electrical and Electronics Engineers (November 2008).
John Swanson '61 ME in honor of his mother, Dorothy G Swanson, Teaching Award (2010).
Member, Norges Tekniske Vitenskapsakademi (Norwegian Academy of Technological Sciences), 2010.
Member, National Academy of Engineering, 2011.
IEEE Emanuel R. Piore Award, 2012.
Service to Computing Research Association Award, 2016.
Jean-Claude Laprie Award in Dependable Computing, June 2017.
Member, American Academy of Arts & Sciences, October 2017.
Edsger W. Dijkstra Prize in Distributed Computing, July 2018.
IEEE Computer Security Foundations Symposium Distinguished Paper, July 2021.
10th Annual NSA Best Scientific Cybersecurity Research Paper Competition for "Verifying Hyperproperties with TLA", January 2023.
Test of Time Award: "Hyperproperties" from 2008 Computer Security Foundations Conference. Presented at 36th IEEE Computer Security Foundations Symposium, July 2023.

Patents

1. Fault tolerant computer system with shadow virtual processor. United States Patent 5,488,716, January 30, 1996. Co-inventors: E. Balkovich, B. Lampson, and D. Thiel.

2. Transparent fault tolerant computer system. United States Patent 5,802,265, Sept. 1, 1998. Co-inventors: T. C. Bressoud, J. E. Ahern, K. P. Birman, R. C. B. Cooper, B. Glade, and J. D. Service.

3. Transparent fault tolerant computer system. United States Patent 5,968,185, Oct. 19, 1999. Co-inventors: T. C. Bressoud, J. E. Ahern, K. P. Birman, R. C. B. Cooper, B. Glade, and J. D. Service.

4. A method for improving search engine efficiency. Norwegian Patent 327318, June 8, 2009. Co-inventors: Johannes Gehrke and Robbert van Renesse.

PUBLICATIONS

Books

1. *A Logical Approach to Discrete Math.* Springer-Verlag, NY, 1993, 500 pages. With David Gries.
2. *Instructor's Manual for "A Logical Approach to Discrete Math".* D. Gries and F. B. Schneider, Ithaca, NY, 1993. 311 pages. With David Gries.
3. *On Concurrent Programming.* Springer-Verlag, NY, 1997, 473 pages.
4. *Trust in Cyberspace.* (Editor) National Academy Press, December 1998, 331 pages.

Journals

1. Conditions for the equivalence of synchronous and asynchronous operation. *IEEE Transactions on Software Engineering* SE-4, 6 (November 1978), 507–516. With A. J. Bernstein, E. A. Akkoyunlu and A. Silbershatz.
2. Master keys for group sharing. *Information Processing Letters* 12, 1 (February 1981), 23–25. With D. Denning.
3. More on master keys for group sharing. *Information Processing Letters* 13, 3 (December 1981), 125–126. With D. Denning and H. Meijer.
4. Synchronization in distributed programs. *TOPLAS* 4, 2 (April 1982), 125–148.
5. Fail-stop processors: An approach to designing fault-tolerant computing systems. *ACM Transactions on Computer Systems* 1, 3 (August 1983), 222–238. With R. D. Schlichting.
6. User recovery and reversal in interactive systems. *TOPLAS* 6, 1 (January 1984), 1–19. With J. Archer and R. W. Conway.
7. The 'Hoare Logic' of CSP and all that. *TOPLAS* 6, 2 (April 1984), 281–296. With L. Lamport.
8. Fault-tolerant broadcasts. *Science of Computer Programming* 4, 1 (April 1984), 1–15. And D. Gries and R. D. Schlichting.
9. Key exchange using 'Keyless Cryptography'. *Information Processing Letters* 16, 2 (February 1983), 79–82. With B. Alpern.
10. Concepts and notations for concurrent programming. *ACM Computing Surveys* 15, 1 (March 1983), 3–44. With G. Andrews. Reprinted in:
    i. *bit Magazine* (in Japanese),
    ii. *Programming Languages: A Grand Tour*, Third Edition, E. Horowitz (ed.), Computer Science Press,
    iii. *Concurrent Programming*, Narian Gehani and Andrew D. McGettrick (eds.), Addison-Wesley Publishing Company, 1988.
    iv. *Distributed Computer Systems*, H. S. M. Zedan (ed.), Butterworths, London, 1990.
11. Using message-passing for distributed programming: Proof rules and disciplines. *TOPLAS* 6, 3 (July 1984), 402–431. With R. D. Schlichting.

12. Byzantine generals in action: Implementing fail-stop processors. *ACM Transactions on Computer Systems* 2, 2 (May 1984), 145–154.
13. Derivation of a distributed algorithm for finding paths in directed networks. *Science of Computer Programming* 6, 1 (January 1986), 1–9. With R. McCurley.
14. Thrifty execution of task pipelines. *Acta Informatica* 22, 1 (1985), 35–45. With R. W. Conway and D. Skeen.
15. Defining liveness. *Information Processing Letters* 21, 4 (October 1985), 181–185. With B. Alpern.
16. Safety without stuttering. *Information Processing Letters* 23, 4 (November 1986), 177–180. With B. Alpern and A. J. Demers.
17. Recognizing safety and liveness. *Distributed Computing* 2, 3 (1987), 117–126. With B. Alpern.
18. Verifying temporal properties without temporal logic. *TOPLAS* 11, 1 (January 1989), 147–167. With B. Alpern.
19. Implementing fault-tolerant services using the state machine approach: A tutorial. *ACM Computing Surveys* 22, 4 (December 1990), 299–319.
20. Trace-based network proof systems: Expressiveness and completeness. *TOPLAS* 14, 3 (July 1992), 396–416. With J. Widom and D. Gries.
21. Preserving liveness: Comments on "Safety and Liveness from a Methodological Point of View". *Information Processing Letters* 40, 3 (November 1991), 141–142. With M. Abadi, B. Alpern, K. R. Apt, N. Francez, S. Katz, and L. Lamport.
22. A formalization of priority inversion. *Real Time Systems* 5 (1993), 285–303. With O. Babaoglu and K. Marzullo.
23. Proving nondeterministically specified safety properties using progress measures. *Information and Computation* 107, 3 (November 1993), 151–170. With N. Klarlund.
24. A new approach to teaching discrete mathematics. *Primus V* 2 (June 1995), 113–138. With D. Gries.
25. Teaching math more effectively, through the design of calculational proofs. *The Mathematical Monthly* (October 1995), 691–697. With D. Gries.
26. Equational propositional logic. *Information Processing Letters* 53, 3 (February 1995), 145–152. With D. Gries.
27. Verifying programs that use causally-ordered message-passing. *Science of Computer Programming* 24, 2 (1995), 105–128. With S. Stoller.
28. Hypervisor-based fault-tolerance. *ACM Transactions on Computer Systems* 14, 1 (February 1996), 80–107. With T. Bressoud.
29. Adding the everywhere operator to propositional logic. *Journal of Logic and Computation* 8, 1 (February 1998), 119–129. With D. Gries.
30. Building trustworthy systems: Lessons from the PTN and Internet. *IEEE Internet Computing*, 3, 5 (November-December 1999), 64–72. With S. Bellovin and A. Inouye.
31. Enforceable security policies. *ACM Transactions on Information and System Security* 3, 1 (February 2000), 30–50.
32. A TACOMA retrospective. *Software–Practice and Experience 32* (2002), 605–619. With D. Johansen, K. J. Lauvset, R. van Renesse, N. P. Sudmann, and K. Jacobsen.
33. COCA: A secure distributed on-line certification authority. *ACM Transactions on Computer Systems* 20, 4 (November 2002), 329–368. With Lidong Zhou and Robbert van Renesse.
34. Tolerating malicious gossip. *Distributed Computing 16*, 1 (February 2003) 49–68. With

Yaron Minsky.

35. Least privilege and more. *IEEE Security and Privacy 1*, 3 (Sept/Oct 2003), 55-59.
36. CODEX: A robust and secure secret distribution system. *IEEE Transactions on Dependable and Secure Computing* 1, 1 (January-March 2003), 34–47. With Michael Marsh.
37. Automated analysis of fault-tolerance in distributed systems. *Formal Methods in System Design* 28, 2 (March 2005), 183–196. With Scott D. Stoller.
38. APSS: Proactive secret sharing in asynchronous systems. *ACM Transactions on Information and System Security* 8, 3 (August 2005), 259–286. With Lidong Zhou and Robbert van Renesse.
39. Implementing trustworthy services using replicated state machines. *IEEE Security and Privacy 3*, 5 (Sept/Oct 2005), 34–43. With Lidong Zhou. Reprinted in:
    Replication Theory and Practice, Bernadette Charron-Bost, Fernando Pedrone, Andre Schiper (eds), Lecture Notes in Computer Science, Volume 5959, Springer-Verlag, New York, 2010, 151–168.
40. Computability classes for enforcement mechanisms. *TOPLAS* 28, 1 (January 2006), 175–205. With Kevin Hamlen and Greg Morrisett.
41. The monoculture risk put into context. *IEEE Security and Privacy 7*, 1 (January/February 2009), 14–17. With Ken Birman.
42. Quantifying Information Flow with Beliefs. *Journal of Computer Security* 17(5), pages 655–701, 2009. With Michael R. Clarkson and Andrew C. Myers.
43. Proactive Obfuscation. *ACM Transactions on Computer Systems* 28, 2 (July 2010), 1–54. With Tom Roeder.
44. Independence from Obfuscation: A Semantic Framework for Diversity. *Journal of Computer Security* 18, 5 (August 2010), 701–749. With Riccardo Pucella.
45. Hyperproperties. *Journal of Computer Security* 18, 6 (September 2010), 1157–1210. With Michael R. Clarkson.
46. Nexus Authorization Logic. *ACM Transactions on Information and System Security* 14, 1 (May 2011), Article 8. And Kevin Walsh, Emin Gun Sirer.
47. Doctrine for Cybersecurity. *Daedalus*. Fall 2011, 70–92. With Deirdre Mulligan
48. Multi-Verifier Signatures. *Journal of Cryptography* 25, 2 (April 2012), 310–348. With Tom Roeder and Rafael Pass.
49. Federated Identity Management Systems: A Privacy-based Characterization. *IEEE Security and Privacy* 11, 5 (September/October 2013), 36–48. With Eleanor Birrell.
50. Quantification of Integrity. *Mathematical Structures in Computer Science* 25 Special Issue 02, (February 2015), 207–258. With Michael R. Clarkson.
51. Vive La Difference: Paxos vs. Viewstamped Replication vs. Zab *IEEE Transactions on Dependable and Secure Computing* 12, 4 (July-Aug. 2015), 472–484. With Robbert van Renesse and Nicolas Schiper.
52. Omni-Kernel: An Operating System Architecture for Pervasive Monitoring and Scheduling. *IEEE Transactions on Parallel & Distributed Systems* 26, 10 (October 2015), 2849–2862. With Age Kvalnes, Dag Johansen, Robbert van Renesse, and Steffen Valvag.
53. Impediments with Policy Interventions to Foster Cybersecurity Investment. *Communications of the ACM*, 61, 3 (March 2018), 36–38.
54. Putting Trust in Security Engineering. *Communications of the ACM*, 61, 5 (May 2018), 37–39.

55. RIF: Reactive Information Flow Labels. *Journal of Computer Security*, Vol 28 (2020), 191–228. With Elisavet Kozyri.
56. Implementing Insider Defenses. *Communications of the ACM*, 64, 5 (May 2021), 60–65. With Eric Grosse and Lynette I. Millett.

Conference Proceedings

1. On language restrictions to ensure deterministic behavior in concurrent systems. *Proc. of Third Jerusalem Conference on Information Technology* (Jerusalem, Israel, August 1978), North-Holland, New York, 537–541. With A. J. Bernstein.
2. Ensuring consistency in a distributed database system by use of distributed semaphores. *Proc. International Symposium on Distributed Databases* (Paris, France, March 1980), North-Holland, New York, 183–189.
3. The master key problem. *Proc. 1980 Symposium on Security and Privacy* (Oakland, California, April 1980), IEEE Computer Society, Oakland, California, 103–107. With D. Denning.
4. Towards fault tolerant process control software. *Proc. of 1981 International Symposium on Fault-Tolerant Computing* (Portland, Maine, June 1981), IEEE Computer Society, Oakland, California, 48–55. And R. D. Schlichting.
5. Understanding and using asynchronous message-passing primitives. *Proc. of ACM Symposium on Principles of Distributed Computing* (Ottawa, Canada, August 1982), ACM, New York, 141–147. With R. D. Schlichting.
6. Fail-Stop processors. (Invited Paper.) *Digest of Papers Spring Compcon '83* (San Francisco, California, March 1983), IEEE Computer Society, Oakland, California, 66–71.
7. Declarations: A uniform approach to aliasing and typing. *Proc. of 12th Annual ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages* (New Orleans, Louisiana, January 1985), ACM, New York, 205–216. With L. Lamport.
8. Inexact agreement: Accuracy, precision, and graceful degradation. *Proc. Fourth Annual SIGACT-SIGOPS Symposium on Principles of Distributed Computing* (Minaki, Ontario, Canada, August 1985), ACM, New York, 237–249. With S. R. Mahaney.
9. Symmetry and Similarity in Distributed Systems. *Proc. Fourth Annual SIGACT-SIGOPS Symposium on Principles of Distributed Computing* (Minaki, Ontario, Canada, August 1985), ACM, New York, 13–22. With R. E. Johnson.
10. Abstractions for fault-tolerance in distributed systems. (Invited Paper.) *Proc. IFIP 10th World Computer Congress, IFIP '86* (Dublin, Ireland, September 1986), 727–733.
11. A paradigm for reliable clock synchronization. (Invited paper.) *Proc. Advanced Seminar on Real-Time Local Area Networks* (Bandol, France, April 1986), INRIA, 85–104.
12. Completeness and incompleteness of trace-based network proof systems. *Proc. of 14th Annual ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages* (Munich, F. R. Germany, January 1987), 27–38. With J. Widom and D. Gries.
13. Proving Boolean combinations of deterministic properties. *Proc. of 2nd Annual Symposium on Logic in Computer Science* (Ithaca, New York, June 1987), 131–137. With B. Alpern.
14. Primary-Backup Protocols: Lower Bounds and Optimal Protocols. *Proc. 3rd IFIP Working Conference on Dependable Computing for Critical Applications* (Sicily, Italy, September 1992), 187–196. With Navin Budhiraja, Keith Marzullo and Sam Toueg.

15. Optimal primary-backup protocols. *Proc. 6th International Workshop, WDAG '92* (Haifa, Israel, November 1992), Lecture Notes in Computer Science, Volume 647, Springer-Verlag, New York, 1992, 362–378. With Navin Budhiraja, Keith Marzullo and Sam Toueg.
16. Reasoning about Programs by exploiting the environment. *Proc. 21st International Colloquium, ICALP '94* (Jerusalem, Israel, July 1994), Lecture Notes in Computer Science, Volume 820, Springer-Verlag, New York, 328–339. With L. Fix.
17. Hybrid verification by exploiting the environment. *Formal Techniques in Real Time and Fault Tolerant Systems* (Luebeck, Germany, September 1994), Lecture Notes in Computer Science, Volume 863, Springer-Verlag, New York, 1–18. With Limor Fix.
18. Teaching logic as a tool. *Proc. 26th SIGCSE Technical Symposium on Computer Science Education* (Nashville, Tennessee, March 1995), SIGCSE Bulletin 27, 1, 384–385. With D. Gries.
19. Operating system support for mobile agents. *Proc. Fifth Workshop on Hot Topics in Operating Systems (HOTOS-V)* (Orcas Island, Washington, May 1995), 42–45. With Dag Johansen and Robbert van Renesse. Reprinted in:
    - *Readings in Agents*, Michael N. Huhns and Munindar P. Singh (eds.), Morgan Kaufman Publishers, San Francisco, California, 1997. 263–266.
    - *Mobility: Processes, Computers, and Agents*, Dejan S. Milojicic, Frederick Douglis, and Richard G. Wheeler (eds.), Addison Wesley and the ACM Press, April 1999, 557–563.
20. Faster possibility detection by combining two approaches. *Proc. 9th International Workshop, WDAG '95* (Le Mont-Saint-Michel, France, September 1995), Lecture Notes in Computer Science, Volume 972, Springer-Verlag, New York, 1995, 318–332. With Scott Stoller.
21. Hypervisor-based Fault Tolerance. *Proc. Fifteenth ACM Symposium on Operating Systems Principles* (Copper Mountain Resort, Colorado, December 1995), Operating Systems Review 29, 5, 1–11. With T. Bressoud.
22. Cryptographic support for fault-tolerant distributed computing. *Proc. of the Seventh ACM SIGOPS European Workshop "System Support for Worldwide Applications"* (Connemara, Ireland, September 1996), ACM, New York, 109–114. With Yaron Minsky, Robbert van Renesse, and Scott D. Stoller.
23. Supporting broad internet access to TACOMA. *Proc. of the Seventh ACM SIGOPS European Workshop "System Support for Worldwide Applications"* (Connemara, Ireland, September 1996), ACM, New York, 55–58. With Dag Johansen and Robbert van Renesse.
24. Automated analysis of fault-tolerance in distributed systems. *Proc. of the First ACM SIGPLAN Workshop on Automated Analysis of Software*, (Paris, France, January 1997), ACM, New York, 33–44. Rance Cleaveland and Daniel Jackson, (eds.). With Scott Stoller.
25. Towards fault-tolerant and secure agentry. *Proc. 11th International Workshop WDAG '97* (Saarbrucken, Germany, September 1997), Lecture Notes in Computer Science, Volume 1320, Springer-Verlag, Heidelberg, 1997, 1–14.
26. Automated stream-based analysis of fault-tolerance. *Formal Techniques in Real-time and Fault-Tolerant Systems (FTRTFT '98)* (Lyngby, Denmark, September 1998), Lecture Notes in Computer Science, Volume 1486, Springer-Verlag, Berlin, 1998, 113–122. With Scott Stoller.

27. NAP: Practical Fault-tolerance for Itinerant Computations. *Proc. 19th IEEE International Conference on Distributed Computing Systems* (Austin, Texas, June 1999), IEEE, 180–189. With D. Johansen, K. Marzullo, K. Jacobsen, and D. Zagorodnov.
28. SASI enforcement of security policies: A retrospective. *Proceedings of the New Security Paradigms Workshop* (Caledon Hills, Ontario, Canada, September 1999), Association for Computing Machinery, 87–95. With Ulfar Erlingsson. Reprinted in:
    - *DARPA Information and Survivability Conference and Exposition (DISCEX'00)* (Hilton Head, South Carolina, January 2000) IEEE Computer Society, Los Alamitos, California, 287–295.
29. IRM enforcement of Java stack inspection. *Proceedings 2000 IEEE Symposium on Security and Privacy* (Oakland, California, May 2000), IEEE Computer Society, Los Alamitos, California, 246–255. With Ulfar Erlingsson.
30. Open source in security: Visiting the bizarre. *Proceedings 2000 IEEE Symposium on Security and Privacy* (Oakland, California, May 2000), IEEE Computer Society, Los Alamitos, California, 126–127.
31. A language-based approach to security. *Informatics: 10 Years Back, 10 Years Ahead* (Saarbrucken, Germany, August 2000), Lecture Notes in Computer Science, Volume 2000 (Reinhard Wilhelm, ed.), Springer-Verlag, Heidelberg, 2000, 86-101. And Greg Morrisett, Robert Harper.
32. Language-based Security: What's needed and Why. *Static Analysis, Proceedings 8th International Symposium SAS 2001* (Paris, France, July 2001), Lecture Notes in Computer Science Volume 2126, Springer-Verlag, Heidelberg, 2001, page 374.
33. Lifting reference monitors from the kernel. *Formal Aspects of Security, FASec 2002* (London, United Kingdom, December 2002), Ali E. Abdullah, Peter Ryan, and Steve Schneider (eds.). Lecture Notes in Computer Science, Volume 2629, Springer-Verlag, New York, 2003, 1–2.
34. Chain replication for supporting high throughput and availability. *Sixth Symposium on Operating Systems Design and Implementation* (OSDI '04), (San Francisco, California, December 2004), USENIX Association, 2004, 91–104. With Robbert van Renesse.
35. Peer-to-peer authentication with a distributed single sign-on service. *Peer-to-Peer Systems III, Third International Workshop IPTPS 2204* (La Jolla, CA, February 2004), Lecture Notes in Computer Science, Volume 3279 (G. Voelker and S. Shenker, eds.), Springer-Verlag, Heidelberg, 2004, 250–258. With William Josephson and Emin Gun Sirer.
36. Distributed Blinding for Distributed ElGamel Re-encryption. *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems* (Columbus, OH USA, June, 2005), IEEE Computer Society, 2005, 815–824. With L. Zhou, M.A. Marsh, and A. Redz.
37. Belief in information flow. *Proceedings 18th IEEE Computer Security Foundations Workshop* (Aix-en-Provence, France, June 20-22, 2005), 31–45. With Michael R. Clarkson and Andrew C. Myers.
38. Certified in-lined reference monitoring on .NET. *Proceedings of the 2006 Programming Languages and Analysis for Security Workshop* (Ottawa, Ontario, Canada, June 10, 2006), ACM, 2006, 7–16. With Kevin W. Hamlen and Greg Morrisett.
39. Independence from obfuscation: A semantic framework for diversity. *Proceedings 19th IEEE Computer Security Foundations Workshop* (Venice, Italy, July 2006), IEEE Press, 2006, 230–241. With Riccardo Pucella.

40. The building blocks of consensus. *Proceedings 9th International Conference on Distributed Computing and Networking* ICDCN 08, (Kolkata, India, Jan. 2008), Lecture Notes in Computer Science, Volume 4904 (S. Rao et al, eds.), Springer-Verlag, Heidelberg, 2008, 54–72. With Yee Jiun Song, Robert van Renesse, and Danny Dolev.
41. Device driver safety through a reference validation mechanism. *Proceedings of the 8th USENIX Symposium on Operating Systems Design and Implementation OSDI '08* (San Diego, CA, December 2008), 241–254. With Dan Williams, Patrick Reynolds, Kevin Walsh, and Emin Gun Sirer.
42. Hyperproperties. *Proceedings 21st IEEE Computer Security Foundations Symposium* CSF 2008, (Pittsburgh, PA, June 2008), 51–65. Test of Time Award presented at 36th IEEE Computer Security Foundations Symposium, July 2023. With Michael R. Clarkson.
43. Quantification of Integrity. *Proceedings 23rd IEEE Computer Security Foundations Symposium* CSF 2010, (Edinburgh, UK, July 2010), 28–43. With Michael Clarkson.
44. Logical Attestation: An Authorization Architecture for Trustworth Computing. *SOSP'11 Proceedings of 23rd ACM Symposium on Operating Systems Principles* (Cascais, Portugal, October 2011), 249–264. With Emin Gun Sirer, Willen De Bruijin, Patrick Reynolds, Alan Shieh, Kevin Walsh, and Dan Williams.
45. When not all bits are equal: Incorporating "worth" into information-flow measures. *POST 2014 Principles of Security and Trust* (Grenoble, France, April 2014) Lecture Notes in Computer Science, vol 8414. M. Abadi and S. Kremer Eds. 120—139. With Mario Alvim and Andre Scedrov.
46. Enforcing Privacy Policies with Meta-Code. *6th ACM SIGOPS Asica-Pacific Workshop on Systems*, (Tokyo, Japan, July 2015). With Havard Johansen, Eleanor Birrell, Robbert van Renesse, Magnus Stenhaug, and Dag Johansen.
47. SGX Enforcement of Use-Based Privacy. *Workshop on Privacy in the Electronic Society* WPES 2018. (Toronto, Canada, October 2018), pages 155-167. With Eleanor Birrell, Havard Johansen, Anders Gjerdrum, Dag Johansen, Robbert van Renesse.
48. Beyond Labels: Permissiveness for Dynamic Information Flow Enforcement. *IEEE 32nd Computer Security Foundations Symposium* (CSF) (Hoboken, NJ, July 2019), pages 351–366. With Elisavet Kozyri, Andrew Bedford, Josee Desharnais, and Nadia Tawbi.
49. Ancile: Enhancing Privacy for Ubiquitous Computing with Use-Based Privacy. *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society* (London, England, November 2019), pages 111–124. With Eugene Bagdasaryan, Griffin Berlstein, Jason Waterman, Eleanor Birrell, Nate Foster, and Deborah Estrin.
50. JRIF: Reactive Information Flow Control for Java. *Foundations of Security, Protocols, and Equational Reasoning.* Lecture Notes in Computer Science, Vol 11565, Springer, (April 2019), 70–88. With Elisavet Kozyri, Owen Arden, and Andrew C. Myers.
51. Verifying Hyperproperties with TLA. *34th IEEE Computer Security Foundations Symposium (CSF)* (virtual conference, June 2021), 1–16. With Leslie Lamport. Received CSF Distinguished Paper Award. Also winner, 10th Annual NSA Best Scientific Cybersecurity Research Paper Competition.
52. Causal Network Telemetry. *EuroP4 '22: Proceedings of the 5th International Workshop on P4 in Europe*, (Rome, Italy, December 2022), 46—52. With Yunhe Liu and Nate Foster.
53. Designing a Hardware Root-of-Trust for Zero-Trust Mission Systems. *Proc. GOMACTech-*

24, (Charleston, South Carolina, US.) With Michael Vai, Alice Lee, Eric Simpson, Huy Nguyen, Jeffrey Hughes, John Dean, Gabriel Torres, Jeffery Lim, Ben Nahill, Roger Khazan.

54. Security-As-A-Service for Embedded Systems. *Proc. MILCOM 2023 – 2023 IEEE Military Communications Conference* (Boston, Mass, November 2023). With Michael Vai, Eric Simpson, Donato Kava, Alice Lee, Huy T Nguyen, Jeffrey Hughes, Gabriel Torres, Jeffery Lim and Ben Nahill.
55. Zero Trust Architecture Approach for Developing Mission Critical Embedded Systems. *Proc. 2023 IEEE High Performance Extreme Computing Conference* (Virtual Conference) With Michael Vai, David Whelihan, Eric Simpson,, Donato Kava, Alice Lee, Huy Nguyen, Jeffrey Hughes, Gabriel Torres, Jeffery Lim, Ben Nahill and, Roger Khazan.

Other Publications

1. Scheduling in Concurrent Pascal. *Operating Systems Review* 12, 2 (April 1978), 15–21. With A. J. Bernstein.
2. Synchronization and concurrent programming. *Handbook of Electrical and Computer Engineering*, John Wiley and Sons, 1983.
3. Abstract data types. *Handbook of Electrical and Computer Engineering*, John Wiley and Sons, 1983.
4. Broadcasts: A paradigm for distributed programs. *Proc. Workshop on Fundamental Issues in Distributed Computing* (Fallbrook, California, December 1980), ACM, New York.
5. Book review: The Practical Guide to Structured Systems Design. *IEEE Spectrum* 18, 3 (March 1981), 92.
6. The fail-stop processor approach. Invited chapter in *Reliability in Distributed Software and Database Systems* (B. Bhargava, ed.), Von Nostrand Reinhold Company, New York, 1987, 370–394.
7. *Distributed Systems—Methods and Tools for Specification.* Lecture Notes in Computer Science, Volume 190, Springer-Verlag, New York, 1985. With M. W. Alford, J. P. Ansart, G. Hommel, L. Lamport, and B. Liskov.
8. A reply to "A Review of the Advanced Course Description in Computer Science of the Educational Testing Service". *Contemporary Education Review* 2, 3. With P. Miller, T. Gill, S. Owicki, B. Presley, and J. Wadkins.
9. Reaching agreement: A fundamental task even in distributed computer systems. *Engineering: Cornell Quarterly* 20, 2 (Fall 1985), 18–22. And O. Babaoglu, K. P. Birman, and S. Toueg.
10. Programming methodology: Making a science out of an art. *Engineering: Cornell Quarterly* 20, 2 (Fall 1985), 23–27. With D. Gries.
11. Concepts for concurrent programming. (Invited Paper.) *Current Trends in Concurrency*, (J. W. de Bakker, W. P. de Roever, and G. Rozenberg, eds.), Lecture Notes in Computer Science, Volume 224, Springer-Verlag, New York, 1986, 669–716. And G. Andrews.
12. The state machine approach: A tutorial. (Invited paper.) *Proc. Workshop on Fault-tolerant Distributed Computing*, (B. Simons and A. Z. Spector, eds.) Lecture Notes in Computer Science, Volume 448, Springer-Verlag, New York, 1990, 18–41.
13. Another position paper on "fairness". *Software Engineering Notes* 13, 3 (July 1988),

1–2. With L. Lamport.

14. Critical (of) issues in real-time systems: A position paper. (Invited paper.) *Real-time systems Newsletter* 4, 2 (Summer 1988), 3–5. Also reprinted in *Distributed Processing Technical Committee Newsletter* 10, 2 (November 1988), 75–77.
15. Cornell's real-time reliable (RR) systems project. *Proc. Foundations of Real-time Computing*, Office of Naval Research Research Initiative Kickoff Workshop, 28–32.
16. Computer Systems. *Computer Science: Achievements and Opportunities*, SIAM Reports on Issues in the Mathematical Sciences, SIAM, Philadelphia, Pennsylvania, 1989, 29–40. With F. Baskett, D. Clark, A. N. Habermann, B. Liskov, and B. Smith.
17. Formal verification of concurrent software. *Proc. of Thirteenth Annual International Computer Software and Applications Conference* (Orlando, Florida, September 1989), 59.
18. Simpler proofs for concurrent reading and writing. *Beauty is Our Business*, Springer-Verlag Texts and Monographs in Computer Science, May 1990, 373–389.
19. Towards derivation of real-time process-control programs. *Proc. of Third Annual Workshop, Foundations of Real-time Computing Initiative* (Washington, DC, October 1990), Office of Naval Research, 373–384. With K. Marzullo.
20. Derivation of sequential, real-time process-control programs. *Foundations of Real-Time Computing: Formal Specifications and Methods*, (A. M. van Tilborg and G. Koob, eds.), Kluwer Academic Publishers, 1991, 39–54. With K. Marzullo and N. Budhiraja.
21. Fault-tolerance support in distributed systems workshop. *ESN Information Bulletin* 91-03 (July 1991), Office of Naval Research European Office, 58–59.
22. The challenge is usability. *2021 AD: Visions of the Future*, National Engineering Consortium, 1991, 50.
23. Putting time into proof outlines. *Proc. of the REX Workshop "Real-Time: Theory in Practice"*, (J. W. de Bakker, C. Huizing, W. P. de Roever, G. Rozenberg, eds.), Lecture Notes in Computer Science, Volume 600, Springer-Verlag, Berlin, 1991, 618–639. And Bard Bloom and Keith Marzullo.
24. Reasoning about real-time actions. *Proc. of Fourth Annual Workshop, Foundations of Real-time Computing Initiative*, (Washington, DC, October 1991), Office of Naval Research, 85–91. And Bard Bloom and Keith Marzullo.
25. Lower bounds for primary-backup implementations of BOFO services. *Proc. of Second Annual Workshop, Ultradependable Multicomputers and Electronic Systems* (Washington, DC, November 1991), Office of Naval Research, 81–86. With Navin Budhiraja, Keith Marzullo, and Sam Toueg.
26. Assertional methods for fault-tolerant, real-time concurrent programs. *Proc. Software Technology Conference 1992* (Los Angeles, California, April 1992) Defense Advanced Research Projects Agency, Software and Intelligent Systems Technology Office and Computing Systems Technology Office, 516–517.
27. Introduction. *Distributed Computing* 6, 1 (June 1992), 1–3.
28. Adding fault-tolerance, virtually. *Proc. of First Annual Workshop on Embedded Systems* (Austin, Texas, January 1993), Office of Naval Research, 41.
29. What good are models and what models are good? Chapter 2, *Distributed Systems*, 2nd Edition (S. Mullender, ed.), Addison Wesley, 1993, 17–25.
30. Replication management using the state machine approach. Chapter 7, *Distributed Systems*, 2nd Edition (S. Mullender, ed.), Addison Wesley, 1993, 169–195.
31. The primary-backup approach. Chapter 8, *Distributed Systems*, 2nd Edition (S. Mul-

lender, ed.), Addison Wesley, 1993, 199–215. With Navin Budhiraja, Keith Marzullo, and Sam Toueg.

32. A role for formal methodists. *Fourth International Workshop on Dependable Computing for Critical Applications* (San Diego, California, January 1994), 29–30. Reprinted in *Dependable Computing and Fault-Tolerant Systems* Volume 9, (F. Cristian, G. LeLann, T. Lunt, eds.) Springer-Verlag, 1995, 43–45.
33. Research on fault-tolerant and real-time computing. Software and Systems Program Summary. (Bolling Air Force Base, Washington, DC, September 1994), Air Force Office of Scientific Research, 75–77.
34. Refinement for Fault-Tolerance: An Aircraft Hand-off Protocol. *Foundations of Ultradependable Parallel and Distributed Computing, Paradigms for Dependable Applications*, Kluwer Academic Publishers, 1994, 39–54. With K. Marzullo and J. Dehn.
35. On teaching proof. *Arts & Sciences NewsLetter* 16, 2 (Spring 1995), 3. With D. Gries.
36. Avoiding AAS Mistakes. (Invited paper.) *Proc. of the Air Traffic Management Workshop*, (L. Tobais, M. Tashker, A. Boyle, eds.), NASA Conference Publication 10151, NASA Ames Research Center, February 1995, 133–149.
37. Avoiding the undefined by underspecification. *Computer Science Today Recent Trends and Developments* (Jan van Leeuwen, ed.), Lecture Notes in Computer Science, Volume 1000, Springer-Verlag, 1995, 366–373. With David Gries.
38. On Traditions in Marktoberdorf. *Deductive Program Design* (M. Broy, ed.), ASI Volume F152. Springer-Verlag, Heidelberg, 1–4.
39. Notes on Proof Outline Logic. *Deductive Program Design* (M. Broy, ed.), ASI Volume F152. Springer-Verlag, Heidelberg, 351–394.
40. Report on Dagstuhl Seminar on Time Services, Schloss Dagstuhl, March 11–March 15 1996. *Real-Time Systems* 12, 3 (May 1997), 329–345. With Danny Dolev, Rudiger Reischuk, and H. Raymond Strong.
41. Editorial: New Partnership with ACM. *Distributed Computing* 10, 2 (1997), 63.
42. Improving Networked Information System Trustworthiness: A Research Agenda. *Proceedings 21st National Information Systems Security Conference* (October 1998, Arlington, Virginia), National Computer Security Center, 766.
43. What Tacoma Taught Us. *Mobility: Processes, Computers, and Agents*, Dejan S. Milojicic, Frederick Douglis, and Richard G. Wheeler (eds.), Addison Wesley and the ACM Press, April 1999, 564–566. With Dag Johansen and Robbert van Renesse.
44. Interview with Fred B. Schneider. *Distributed Systems Online.* http://www.computer.org/channels/ds.
45. Formalizations of substitutions of equals for equals. *Millennial Perspectives in Computer Science, Proceedings of the 1999 Oxford-Microsoft Symposium in honour of Professor Sir Antony Hoare*, (Davies, Roscoe, and Woodcock eds.) Palgrave Publishers, Hampshire, England, November 2000, 119–132. With David Gries.
46. A language-based approach to security. *Informatics: 10 Years Back, 10 Years Ahead.* Lecture Notes in Computer Science, Vol. 2000 (Reinhard Wilhelm, editor), Springer Verlag, Heidelberg, 2000, pp. 86-101. And Greg Morrisett, Robert Harper.
47. WAIF: Web of Asynchronous Information Filters. *Future Directions in Distributed Computing* Lecture Notes in Computer Science, Volume 2585 (Schiper, Shvartsman, Weatherspoon, and Zhao, eds.) Springer-Verlag, 2003, 81–86. With Dag Johansen and Robbert van Renesse.
48. Least privilege and more. *Computer Systems: Papers for Roger Needham*, Andrew

Herbert and Karen Sparck Jones, eds. Springer-Verlay, New York, 2003, 253–258.

49. Language-Based Security for Malicious Mobile Code. *Department of Defense Sponsored Information Security Research: New Methods for Protecting Against Cyber Threats.* Wiley Publishing Company, Indianapolis, Indiana, 2007, 477–494. With Dexter Kozen, Greg Morrisett, and Andrew C. Myers.
50. Credentials-Based Authorization: Evaluation and Implementation. Abstract of Plenary Lecture. *Proceedings 34th International Colloquium, ICALP 2007* (Wroclaw, Poland, July 2007), Lars Arge, Christian Cachin, Tomasz Jurdzinski, and Andrzej Tarlecki (eds.). Lecture Notes in Computer Science, Volume 4596, Springer-Verlag, Heidelberg, 2007, 12–14.
51. Mapping the Security Landscape: A Role for Language Techniques. Abstract of Invited Lecture. *Proceedings 18th International Conference ,CONCUR 2007* (Lisbon, Portugal, September 2007), Luis Caires and Vasco T. Vasconcelos (eds.). Lecture Notes in Computer Science, Volume 4703, Springer-Verlag, Heidelberg, 2007, 1.
52. Interview: Silver Bullet Talks with Fred Schneider. *IEEE Security and Privacy Magazine 7*, 6 (November/December 2009), 5–7.
53. Beyond traces and independence. *Dependable and Historic Computing. Essays Dedicated to Brian Randell on the Occassion of His 75th Birthday*, Lecture Notes in Computer Science, Vol. 6875 (Cliff Jones and John Lloyd, eds). Springer Verlag, 2011, 479–485.
54. Computing researchers get 'schooled' on science policy at CCC workshop. *Computing Research News* Volume 24, No. 1 (January 2012). With Peter Harsha.
55. Blueprint for a science of cybersecurity. *The Next Wave* Volume 19, No. 2 (2012), 47–56.
56. Why tags could be it. *Proceedings 16th International Conference, RV 2016* (Madrid, Spain, September 2016), Yiles Falcome and Cesar Sanches (eds), *Lecture Notes in Computer Science*, vol 10012, Springer Verlag, Heidelberg, Sept 2016.
57. History and Context for "Defining Liveness". Distributed Computing Column 72, *ACM SIGACT News*, Vol 49, Issue 4 (December 2018).
58. Policy dimensions of cybersecurity engineering challenges. *The Bridge*, Vol 49, No. 3 (Fall 2019), pages 33–39. With Lynette I. Millett.

Editorials

1. On Concurrent Programming. Invited "Inside Risks" column. *Communications of the ACM* 41, 4 (April 1998), 128.
2. Toward Trustworthy Networked Information Systems. Invited "Inside Risks" column. *Communications of the ACM* 41, 11 (November 1998), 144.
3. Evolving Telephone Networks. Invited "Inside Risks" column. *Communications of the ACM* 42, 1 (January 1999), 160. With S. Bellovin.
4. Editorial: Time for Change. *Distributed Computing* Vol. 13, No. 4 (November 2000), 187.
5. Secure Systems Conundrum. Invited "Inside Risks" column. *Communications of the ACM* 45, 10 (October 2002), 160.
6. The Next Digital Divide. Editorial. *IEEE Security and Privacy* 2, 1 (January/February 2004), 5.
7. Time Out for Station Identification. Editorial. *IEEE Security and Privacy* 2, 1

(September/October 2004), 5.

8. The PITAC Report: A Brief Analysis. *IEEE Security and Privacy* 3, 3 (May/June 2005), 10. With Susan Landau and Carl E. Landwehr.
9. It Depends on What You Pay. Editorial. *IEEE Security and Privacy* 3, 3 (May/June 2005), 3.
10. Here Be Dragons. Editorial. *IEEE Security and Privacy* 3, 3 (May/June 2006), 3.
11. Trusted Computing in Context. Editorial. *IEEE Security and Privacy* 5, 2 (March/April 2007), 4-5.
12. Technology Scapegoats and Policy Saviors. Editorial. *IEEE Security and Privacy* 5, 5 (September/October 2007), 3–4.
13. Network Neutrality versus Internet Trustworthiness. Editorial. *IEEE Security and Privacy* 6, 4 (July/August 2008), 3–4.
14. Accountability for Perfection. Editorial. *IEEE Security and Privacy* 7, 2 (March/April 2009), 3–4.
15. Labeling-in Security. Editorial. *IEEE Security and Privacy* 7, 6 (November/December 2009), 3
16. Program Committee Overload in Systems. *Communications of the ACM 52*, 05 (May 2009), 34–37. With Ken Birman.
17. Fumbling the Future, Again. Editorial. *IEEE Security and Privacy* 8, 4 (July/August 2010), 3.
18. A Doctrinal Thesis. Editorial. *IEEE Security and Privacy* 9, 4 (July/August 2011), 3–4. With Deirdre Mulligan
19. Breaking-in Research. Editorial. *IEEE Security and Privacy* 11, 2 (July/August 2013), 3–4.

Policy Documents

1. *Trust in Cyberspace*. Fred Schneider (editor), National Academy Press, Washington, DC, 1998, 331 pages.
2. *Toward a Safer and More Secure Cyberspace*. S Goodman and H. Lin (eds), National Academies Press, Washington, DC, 2007, 328 pages.
3. Security is not a commodity: The road forward for cybersecurity research. Computing Research Initiatives for the 21st Century, Computing Community Consortium. February 2009. With Stefan Savage.
4. Notes for White House 60-day Cyber-Policy Review. E. Lazowska and F.B. Schneider (eds), NSF submission for Cyberspace Policy Review conducted Spring 2009 for the White House.
5. Testimony. United States House of Representatives Committee on Science and Technology, Research and Science Education Subcommittee. Hearing June 10, 2009 on Cyber Security R & D.
6. Testimony. United States House of Representatives Committee on Science and Technology, Technology and Innovation Subcommittee. Hearing October 22, 2009 on Cybersecurity Activities at NIST's Information Technology Laboratory.
7. Fred B Schneider, Elaine M Sedenberg, and Deirdre K. Mulligan. Opinion Piece: Public Cybersecurity and Rationalizing Information Sharing. International Risk Governence Center. IRGC, March 2016.
8. Aaron Burstein and Fred B. Schneider. Trustworthiness as a limitation on network

neutrality. *Federal Communications Law Journal*, Vol. 61 (2009), 591–623.

9. Testimony. United States House of Representatives Armed Services Committee, Terrorism, Unconventional Threats, and Capabilities Subcommitee. Hearing February 25, 2010 on Private Sector Perspectives on Department of Defense Information Technology and Cybersecurity Activities.
10. Deirdre Mulligan and Fred B. Schneider. Doctrine for Cybersecurity. *Daedalus*. Fall 2011, 70–92.
11. Fred B. Schneider. Blueprint for a science of cybersecurity. *The Next Wave* Volume 19, No. 2 (2012), 47–56.
12. Batya Friedman and Fred B. Schneider. Incentivizing Quality and Impact: Evaluating Scholarship in Hiring, Tenure, and Promotion. Best Practices Memo, Computing Research Association, Adopted February 2015.
13. Fred B. Schneider. A computer scientist musinn about the DNC hack. Symposium on Cybersecurity and the Changing International Law of Data, *American Journal of International Law*, volume 110 (Feb 2017) DOI doi.org/10.1017/aju.2017.3
14. Bases for Trust in a Supply Chain. *Lawfare* Feb 1, 2021. `https://www.lawfareblog.com/bases-trust-supply-chain`. With Justin Sherman.