Fred Schneider Bio:

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, since 2000.
Chief Scientist, Griffiss Institute, January 2003–January 2004.
Chief Scientist, NST TRUST Science and Technology Center, May 2005–present.

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, March 1994–present (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–present, (Co-managing editor since October 1992).
ACM Computing Surveys, March 1995–present.
IEEE Transactions on Dependable and Secure Computing, March 2004–present.

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–present.
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–Nov 2000.
JXTA Technical Advisory Council, SUN Microsystems, Nov 2000–Nov 2001.
CIGITAL Technical Advisory Board, Nov 2000–present.
deCode Genetics Security Advisory Board, Feb 2000–March 2002.
Eweb University.Com Board of Advisors, March 2000–March 2002.
FAST ASA Technical Advisory Board, March 2000–present.
Intel Microprocessor Research Lab Advisory Board, Oct 2001–August 2004;
UK Dependability Interdisciplinary Research Collaboration (DIRC),
Steering Committee, March 2001–present;
Chairman, UK International Review of Computer Science, March 2001.
ACM Advisory Committee on Security and Privacy (ACSP), Oct 2001–Nov 2003;
National Research Council Computer Science and Telecommunications Board,
March 2002–present;
NSF/CISE Advisory Committee, May 2002–present.
Co-Chair, Microsoft, Trustworthy Computing Academic Advisory Board,
August 2002–present.
IBM Autonomic Computing Advisory Board, August 2002–May 2004.
Packet General Networks Technical Advisory Board, March 2003–present.
Fortify Software Technical Advisory Board, Feb 2004–present.
Committee on Improving Cybersecurity Research,
Computer Science and Telecommunications Board,
National Research Council, National Academy of Sciences.
Member, Advisory Board, Department of Computer Science, University of Virginia,
July 2005-July 2008

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 (1996–2003).
Daniel M. Lazar Excellence in Teaching Award (2000).
Doctor of Science (*honoris causa*), University of Newcastle, U.K. (May 2003).

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.

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. *TOCS* 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. *TOCS* 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.

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 Semi-*

nar 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.

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 Re-

ports 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. Mullender, 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. On Concurrent Programming. Invited "Inside Risks" column. *Communications of the ACM* 41, 4 (April 1998), 128.
43. Improving Networked Information System Trustworthiness: A Research Agenda. *Proceedings 21st National Information Systems Security Conference* (October 1998, Arlington, Virginia), National Computer Security Center, 766.
44. Toward Trustworthy Networked Information Systems. Invited "Inside Risks" column. *Communications of the ACM* 41, 11 (November 1998), 144.
45. Evolving Telephone Networks. Invited "Inside Risks" column. *Communications of the ACM* 42, 1 (January 1999), 160. With S. Bellovin.
46. 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.
47. Interview with Fred B. Schneider. *Distributed Systems Online.* http://www.computer.org/channels/ds.
48. 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.
49. Editorial: Time for Change. *Distributed Computing* Vol. 13, No. 4 (November 2000), 187.
50. 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.
51. Secure Systems Conundrum. Invited "Inside Risks" column. *Communications of the ACM* 45, 10 (October 2002), 160.
52. 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.

53. Least privilege and more. *Computer Systems: Papers for Roger Needham*, Andrew Herbert and Karen Sparck Jones, eds. Springer-Verlay, New York, 2003, 253–258.
54. The Next Digital Divide. Editorial. *IEEE Security and Privacy* 2, 1 (January/February 2004), 5.
55. Time Out for Station Identification. Editorial. *IEEE Security and Privacy* 2, 1 (September/October 2004), 5.