R.M.Needham
Publications

Microsoft Research Limited, Cambridge

Compiled by Karen Spärck Jones, June 2003

with T. Joyce:
'The thesaurus approach to information retrieval', *American Documentation*, 9 (3), 1958, 192-197; reprinted in *Readings in information retrieval*, Ed. K. Spärck Jones and P. Willett, San Francisco, CA: Morgan Kaufmann, 1997.

with M. Masterman and K. Spärck Jones:
'The analogy between mechanical translation and library retrieval', *Proceedings of the International Conference on Scientific Information* (1958), National Academy of Sciences - National Research Council, Washington, DC, 1959, Vol. 2, 917-935.

with A.F. Parker-Rhodes:
'A reduction method for non-arithmetic data, and its application to thesauric translation', *Information Processing: Proceedings of the International Conference on Information Processing* (1959), Paris, 1960, 321-327.

with A.F. Parker-Rhodes:
'The theory of clumps', Cambridge Language Research Unit, Report M.L. 126, 1960.

with A.H.J. Miller and K. Spärck Jones:
'The information retrieval system of the Cambridge Language Research Unit', Cambridge Language Research Unit, Report M.L. 109, 1960.

'The theory of clumps II', Cambridge Language Research Unit, Report M.L. 139, 1961.

Research on information retrieval, classification and grouping 1957-1961, Ph.D. Thesis, University of Cambridge; Cambridge Language Research Unit, Report M.L. 149, 1961.

'A method for using computers in information classification', *Information Processing 62: Proceedings of IFIP Congress 1962*, Ed. C. Popplewell, Amsterdam: North-Holland, 1963, 284-287.

'Automatic classification for information retrieval', in *Information retrieval*, Ed. Serbanescu, I.B.M. European Education Centre, Blaricum, Holland, 1963.

'Automatic classification for information retrieval', lectures given at the NATO Advanced Study Institute on Automatic Document Analysis, Venice, 1963; abstracts published as Cambridge Language Research Unit Report M.L. 166, 1963.

'The exploitation of redundancy in programs', in *The Impact of Users' Needs on the Design of Data Processing Systems*, Conference Proceedings, United Kingdom Automation Council, 1964, 6-7.

with K. Spärck Jones:
'Keywords and clumps', *Journal of Documentation*, 20 (1), 1964, 5-15.

'Information retrieval', *Computing science*, Report to the Science Research Council, Ed. D. Michie, 1965, 92-94.

'Automatic classification - models and problems', in *Mathematics and computer science in biology and medicine*, London: The Medical Research Council, 1965, 111-114.

'Computer methods for classification and grouping', in *The use of computers in anthropology*, Ed. D. Hymes, The Hague: Mouton, 1965, 345-356.

'Applications of the theory of clumps', *Mechanical Translation*, 8 (3/4), 1965, 113-127.

'Semantic problems of machine translation', *Information Processing 65: Proceedings of IFIP Congress 1965*, Ed. W. Kalenich, Washington DC: Spartan Books, 1965, Vol. 1, 65-69.

'Information retrieval and some cognate computing problems', in *Advances in programming and non-numerical computation*, Ed. L. Fox, London: Pergamon Press, 1966, 201-218.

'The termination of certain iterative processes', The Rand Corporation, Santa Monica, Report RM-5188-PR, 1966.

'Automatic classification in linguistics', *The Statistician*, 17 (1), 1967, 45-54.

with D.W. Barron, A.G. Fraser, D.F. Hartley and B. Landy:
'File handling at Cambridge University', *Proceedings of the 1967 Spring Joint Computer Conference*, *AFIPS Conference Proceedings*, Vol. 30, 1967, 163-167.

with K. Spärck Jones:
'Automatic term classifications and retrieval', *Information Storage and Retrieval*, 4 (2), 1968, 91-100.

with M.V. Wilkes:
'The design of multiple-access computer systems: Part 2', *The Computer Journal*, 10, 1968, 315-320.

with D.F. Hartley and B. Landy:
'The structure of a multiprogramming supervisor', *The Computer Journal*, 11, 1968, 247-255.

'Consoles in the cloisters', *Datamation*, January 1969.

with D.F. Hartley:
'Operational experience with the Cambridge multiple-access system', *Computer Science and Technology*, Conference Publication 55, Institution of Electrical Engineers, London, 1969, 255-260.

'Computer operating systems', in *Encyclopedia of linguistics, computation and control*, Ed. A.R. Meetham and R.A. Hudson, London: Pergamon Press, 1969, 57-58.

with D.F. Hartley:
'Theory and practice in operating system design', *2nd ACM Symposium on Operating System Principles*, Princeton, 1969, New York: ACM, 1969, 8-12.

'Software engineering techniques and operating system design and production' and, with D. Aron, 'Software engineering and computer science', in *Software engineering techniques*, Ed. J. Buxton and B. Randell, NATO Scientific Affairs Committee, NATO, Brussels, 1970, 111-113 and 113-114.

'Handling difficult faults in operating systems', *3rd ACM Symposium on Operating System Principles*, Stanford, 1971, New York: ACM, 1971, 55-57.

with B. Landy:
'Software engineering techniques used in the development of the Cambridge multiple access system', *Software - Practice and Experience*, 1 (2), 1971, 167-173.

'Tuning the Titan operating system', in *Operating systems techniques*, Ed. C.A.R. Hoare and R. Perrott, London: Academic Press, 1972, 277-281.

'Protection systems and protection implementations', *Proceedings of the 1972 Fall Joint Computer Conference*, *AFIPS Conference Proceedings*, Vol. 41, 1972, 571-578; reprinted in *The Auerbach Annual, 1972 - Best Computer Papers*, Ed. I.L. Auerbach, Philadelphia, PA: Auerbach (?), 1972.

'Protection - a current research area in operating systems', *Proceedings of the International Computing Symposium 1973*, Ed. G. Gunter, B. Levrat and H. Lipps, Amsterdam: North-Holland, 1974, 123-126.

with M.V. Wilkes:
'Domains of protection and the management of processes', *The Computer Journal*, 17 (2), 1974, 117-120; reprinted in *The Auerbach Annual, 1975 - Best Computer Papers*, Ed. I.L. Auerbach, New York: Petrocelli/Charter, 1975; reprinted in Japanese, 1976.

with R.D.H. Walker:
'Protection and process management in the CAP computer', *Proceedings of the International Workshop on Protection in Operating Systems*, IRIA, Paris, 1974, 155-160.

'The future of central computing services', *Proceedings of the 1976 Computing Services Management Conference*, Ed. D.H. McClain, Inter University Computing Committee, 1976, 74-76.

Articles in *Encyclopedia of computer science*, Ed. A. Ralston and C. Meek, New York: Petrocelli/Charter 1976.

'The CAP project - an interim evaluation', (6th ACM Symposium on Operating System Principles, 1977), *Operating Systems Review*, 11 (5), 1978, 17-22.

with R.D.H. Walker:
'The Cambridge CAP computer and its protection system', (6th ACM Symposium on Computer Operating System Principles, 1977), *Operating Systems Review*, 11 (5), 1978, 1-10.

with A.D. Birrell:
'The CAP filing system', (6th ACM Symposium on Computer Operating System Principles, 1977), *Operating Systems Review*, 11 (5), 1978, 11-16.

with M.D. Schroeder:
'Using encryption for authentication in large networks of computers', Xerox Palo Alto Research Centre, Report CSL-78-4, 1978; *Communications of the ACM*, 21 (12), 1978, 993-999; reprinted in *Advances in computer security*, Ed. R. Turn, Dedham, MA: Artech House, 1988.

with A.D. Birrell:
'An asynchronous garbage collector for the CAP filing system', *Operating Systems Review*, 12 (2), 1978, 31-33.

with A.D. Birrell:
'Character streams', *Operating Systems Review*, 12 (3), 1978, 29-31.

with H.C. Lauer:
'On the duality of operating system structures', (Second International Conference on Operating Systems, 1978), *Operating systems: theory and practice*, Ed. D. Lanciaux, Amsterdam: North-Holland, 1979, 371-384; reprinted in *Operating Systems Review*, 13 (2), 1979, 3-19.

'Protection', (Advanced Course on Computing Systems Reliability, Newcastle, 1978); in *Computer systems reliability*, Ed. T. Anderson and B. Randell, Cambridge: Cambridge University Press, 1979, 264-287.

'Protection - theory and practice', *Proceedings of the SEAS Anniversary Meeting 1978*, Vol. 1, 1978, 80-84.

with M.V. Wilkes:
The CAP computer and its operating system, New York: Elsevier North-Holland, 1979.

'Adding capability access to conventional file servers', *Operating Systems Review*, 13 (1), 1979, 3-4.

'Systems aspects of the Cambridge Ring', (7th ACM Symposium on Operating System Principles, 1979), *Operating Systems Review*, 13 (5), 1979, 82-85.

with M.V. Wilkes:
'The Cambridge model distributed system', *Operating Systems Review*, 14 (1), 1980, 21-29.

with A.D. Birrell:
'A universal file server', *IEEE Transactions on Software Engineering*, Vol. SE-6 (5), 1980, 450-453.

with N.H. Garnett:
'An asynchronous garbage collector for the Cambridge file server', *Operating Systems Review*, 14 (4), 1980, 36-40.

with A.J. Herbert:
'Sequencing computation steps in a network', (8th ACM Symposium on Operating System Principles, 1981), *Operating Systems Review*, 15 (5), 1981, 59-63.

'Design considerations for a processing server', *Proceedings of the 8th Annual Symposium on Computer Architecture*, 1981, IEEE, 501-504.

'Capabilities and protection', (Proceedings, GI-10, Saarbrücken, 1980), *GI-10. Jahrestagung*, Ed. R. Wilhelm, Berlin: Springer-Verlag, 1980, 45-53.

with A.D. Birrell, R. Levin and M.D. Schroeder:
'Grapevine: an exercise in distributed computing' (presented at the 8th ACM Symposium on Operating Systems Principles, 1981), *Communications of the ACM*, 25, 1982, 260-274; reprinted in Birrell et al. 'Grapevine: two papers and a report', Xerox Palo Alto Research Centre, Report CSL-83-12, 1983.

with A.J. Herbert:
The Cambridge distributed computing system, Reading, Mass.: Addison-Wesley, 1982.

with M.F. Richardson:
'The Tripos Filing Machine - a front-end to a file server', (9th ACM Symposium on Operating Systems Principles, 1983), *Operating Systems Review*, 17 (5), 1983, 120-128.

with A.J. Herbert and J.G. Mitchell:
'How to connect stable memory to a computer', *Operating Systems Review* 17 (1), 1983, 16.

with M.D. Schroeder and A.D. Birrell:
'Experience with Grapevine: the growth of a distributed system', *ACM Transactions on Computer Systems*, 2 (1), 1984, 3-23; reprinted in Birrell et al. 'Grapevine: two papers and a report', Xerox Palo Alto Research Center, Report CSL-83-12, 1983.

with I.M. Leslie, J.W. Burren and G.C. Adams:
'The architecture of the Universe network', (SIGCOMM 84 Tutorials and Symposium: Communications Architectures and Protocols), *Computer Communications Review*, 14 (2), 1984, 2-9.

with A.G. Waters, C.G. Adams and I.M. Leslie:
'The use of broadcast techniques on the Universe network', (SIGCOMM 84 Tutorials and Symposium: Communications Architectures and Protocols), *Computer Communications Review*, 14 (2), 1984, 52-57.

'Fifth generation computing', in *Information comes of age*, Ed. C. Oppenheim, London: Rossendale, 1984, 71-77.

'Protection', in *Local area networks: an advanced course*, Ed. D. Hutchison, J. Mariani and D. Shepherd, Lecture Notes in Computer Science 184, Berlin: Springer, 1985, 261-281.

with M.D. Schroeder and D.K. Gifford:
'A caching file system for a programmer's workstation', DEC Systems Research Centre, Palo Alto, Report 6; (10th ACM Symposium on Operating Systems Principles, 1985), *Operating Systems Review*, 19 (5), 1985, 25-34.

'Is there anything special about AI?', (Workshop on the Foundations of Artificial Intelligence, 1986), in *The foundations of artificial intelligence: A source book*, Ed. D. Partridge and Y. Wilks, Cambridge: Cambridge University Press, 1990, 269-273.

with A.D. Birrell, B.W. Lampson and M.D. Schroeder:
'A global authentication service without global trust', *Proceedings of the IEEE Symposium on Security and Privacy*, 1986, 223-230.

with D.L. Tennenhouse, I.M. Leslie, C.A. Adams, J.W. Burren and C.S. Cooper:
'Exploiting wideband ISDN: the Unison exchange', *IEEE INFOCOM Conference Proceedings*, San Francisco, 1987, 1018-1026.

with M.D. Schroeder:
'Authentication revisited', *Operating Systems Review*, 21 (1), 1987, 7.

'The Unison experience', *Proceedings of the 23rd Annual Convention of the Computer Society of India*, Ed. S. Raghavan and S. Venkatasubramanian, New Delhi: Macmillan, 1988, 51-57.

with D.K. Gifford and M.D. Schroeder:
'The Cedar file system', *Communications of the ACM*, 31 (3), 1988, 288-298; reprinted, in Japanese, in *Bit*, November 1989, 30-50.

with A. Hopper:
'The Cambridge fast ring networking system', *IEEE Transactions on Computers*, 37 (10), 1988, 1214-1223.

with M. Burrows and M. Abadi:
'Authentication: a practical study of belief and action', *Proceedings of the 2nd Conference on Theoretical Aspects of Reasoning about Knowledge*, Ed. M. Vardi, Los Altos, CA: Morgan Kaufmann, 1988, 325-342.

with M. Burrows:
'Locks in distributed systems - an observation', *Operating Systems Review* 22 (3), 1988, 44.

with M. Burrows and M. Abadi:
'A logic of authentication', DEC Systems Research Centre, Palo Alto, Report 39, 1989; *Proceedings of the Royal Society of London*, Series A, 426, 1989, 233-271; reprinted in *Practical cryptography for data internetworks*, Ed. W. Stallings, Washington DC: IEEE Computer Society Press, 1996.

with M. Burrows and M. Abadi:
'A logic of authentication', (12th ACM Symposium on Operating System Principles, 1989), *Operating Systems Review*, 23 (5), 1989, 1-13; and *ACM Transactions on Computer Systems*, 8 (1), 1990, 18-36. [Refers to the previous Report 39 etc version as fuller.]

with T.M.A. Lomas, L. Gong and J.H. Saltzer:
'Reducing risks from poorly chosen keys', (12th ACM Symposium on Operating System Principles, 1989), *Operating Systems Review*, 23 (5), 1989, 14-18.

'Authentication', in *Safe and secure computing systems*, Ed. T. Anderson, Oxford: Blackwell Scientific, 1989, 189-196.

'Names' and 'Using cryptography for authentication', (Arctic 88; Fingerlakes 89: Advanced Courses on Distributed Systems), in *Distributed systems*, Ed. S. Mullender, New York: ACM Press and Addison-Wesley, 1989, 89-101 and 103-116.

with J.M. Bacon and I.M. Leslie:
'Distributed computing with a processor bank', Technical Report 168, Computer Laboratory, University of Cambridge, 1989.

with M. Burrows and M. Abadi:
'The scope of a logic of authentication', *Proceedings of the DIMACS Workshop on Distributed Computing and Cryptography* (1989), Ed. J. Feigenbaum and M. Merritt, New York: American Mathematical Society, 1991, 119-126.

with A. Herbert:
'Report on the Third European SIGOPS Workshop, "Autonomy or Interdependence in Distributed Systems" ', *Operating Systems Review*, 23 (2), 1989, 3-19.

with L. Gong and R. Yahalom:
'Reasoning about belief in cryptographic protocols', *Proceedings of the 1990 IEEE Symposium on Security and Privacy*, 1990, 234-248.

with M. Burrows and M. Abadi:
'Rejoinder to Nessett', *Operating Systems Review*, 24 (2), 1990, 39-40.

'Capabilities and security', in *Security and Persistence: Proceedings of the International Workshop on Computer Architectures to Support Security and Persistence of Information*, Ed. J. Rosenberg and J. Keedy, Bremen, Germany, 1990, 1-8.

with M.D. Schroeder and others:
'Autonet: a high-speed, self-configuring local area network using point-to-point links', DEC Systems Research Centre, Palo Alto, Report 59, 1990; *IEEE Journal on Selected Areas in Communications*, 9 (8), 1991, 1318-1335.

'What next? Some speculations', in *Operating systems of the 90s and beyond*, Ed. A.I. Karshmer and J. Nehmer, Berlin: Springer Verlag, 1991, 220-222.

'Later developments at Cambridge: Titan, CAP, and the Cambridge Ring', *IEEE Annals of the History of Computing*, 14 (4), 1992, 57-58.

with A. Nakamura:
'An approach to real-time scheduling - but is it really a problem for multimedia?', (NOSSDAV 92), in *Network and Operating System Support for Digital Audio and Video*, Ed. P. Venkat Randan, Lecture Notes in Computer Science 712, Berlin: Springer-Verlag, 1992, 32-39.

'Names' and 'Cryptography and secure channels', in *Distributed systems*, Ed. S. Mullender, 2nd ed., Reading, MA: Addison-Wesley, 1993, 315-326 and 531-541.

with M.A. Lomas, L. Gong and J.H. Saltzer:
'Protecting poorly chosen secrets from guessing attacks', *IEEE Journal on Selected Areas in Communications*, 11 (5), 1993, 648-656. Abraham Award for Best Paper in the Journal for 1993.

'Denial of service', *Proceedings of the 1st ACM Conference on Communications and Computing Security*, 1993, 151-153.

'Distributed computing', Guest Editorial, *The Computer Bulletin*, 6 (2), 1994, 2.

with M. Abadi:
'Prudent engineering practice for cryptographic protocols', *Proceedings of the 1994 IEEE Symposium on Security and Privacy*, 1994, 122-136. Outstanding paper award.

'Computers and communications', *Computer Science and Informatics*, (Computer Society of India), 23 (4), 1993, 1-6.

'Denial of service: an example', expanded version of 1993 paper, *Communications of the ACM* 37 (11), 1994, 42-46.

with M. Abadi:
'Prudent engineering practice for cryptographic protocols', expanded version of 1994 IEEE Symposium paper, DEC Systems Research Centre, Palo Alto, Report 125, 1994; *IEEE Transactions on Software Engineering*, 22 (1), 1996, 6-15.

with A. Nakamura:
'The dependency protocol for real-time synchronisation', *RTESA 94, Proceedings of the First International Workshop on Real-Time Computing Systems and Applications*, IEEE, Seoul, 1994.

with D. Wheeler:
'Two cryptographic notes', Technical Report 355, Computer Laboratory, University of Cambridge, 1994.

with D.J. Wheeler:
'TEA, a tiny encryption algorithm', *Fast Software Encryption*, 1994, 363-366.

with A. Nakamura:
'The dependency protocol for real-time synchronisation', *Transactions of the Institute of Electronic, Information and Communication Engineers*, Vol. J78-D-I No. 8, 1995, 649-660.

with P.W. Jardetsky and C.J. Sreenan:
'Storage and synchronisation for distributed continuous media', *Multimedia Systems*, 3 (4), 1995, 151-161.

with R.J. Anderson:
'Programming Satan's computer', in *Computer science today*, Ed. J. van Leeuwen, Lecture Notes in Computer Science 1000, Berlin: Springer, 1995, 426-440.

with R.J. Anderson:
'Robustness principles for public key protocols', in *Advances in cryptology - CRYPTO 95*, Ed. D. Coppersmith, Lecture Notes in Computer Science 963, Berlin: Springer, 1995, 236-247.

'Fast communication and slow computers', *Twelfth International Conference on Computer Communication*, Seoul, 1995.

'Computers and communications', in *Computing tomorrow*, Ed. I. Wand and R. Milner, Cambridge: Cambridge University Press, 1996, 284-294.

'The changing environment for security protocols', *IEEE Network*, 11 (3), 1997, 12-15.

'Logic and oversimplification', *Proceedings of the Thirteenth Annual IEEE Symposium on Logic in Cmputer Science*, 1998, 2-3.

with R.J. Anderson and others:
'A new family of authentication protocols', *Operating Systems Review*, 32 (4), 1998, 9-20.

with R.J. Anderson and A. Shamir:
'The steganographic file system', in *Information hiding*, (Second International Workshop on Information Hiding), Ed. D. Aucsmith, Lecture Notes in Computer Science 1525, Berlin: Springer, 1998, 73-84.

'The changing environment', (transcript, with discussion), *Security Protocols*, 7th International Workshop, Cambridge, Ed. B. Christianson et al., Lecture Notes in Computer Science 1796, Berlin: Springer, 1999, 1-5.

'The hardware environment', *Proceedings of the 1999 IEEE Symposium on Security and Privacy*, 1999, 236.

Editor, with K. Spärck Jones and G. Gazdar:
'Computers, language and speech: formal theories and statistical data', *Philosophical Transactions of the Royal Society of London, Series A, Mathematical, Physical and Engineering Sciences*, Vol. 358 No. 1769, 2000, 1225-1431.

with K. Spärck Jones and G. Gazdar:
'Introduction: combining formal theories and statistical data in natural language processing', 'Computers, language and speech: formal theories and statistical data', *Philosophical Transactions of the Royal Society of London, Series A, Mathematical, Physical and Engineering Sciences*, Vol. 358 No. 1769, 2000, 1225-1238.

'Distributed computing: opportunity, challenge, or misfortune?', in *Millennial perspectives in computer science*, (Proceedings of the 1999 Oxford-Microsoft Symposium in honour of Sir Tony Hoare), Ed. J. Davies, B. Roscoe and J. Woodcock, Basingstoke, Hants: Palgrave, 2000, 283-287.

'Mobile computing versus immobile security', (transcript), *Security Protocols*, 9th International Workshop, Cambridge, Ed. B. Christianson et al., Lecture Notes in Computer Science 2467, Berlin: Springer, 2001, 1-3.

'Security - a technical problem or a people problem?', *Proceedings, Information Security Summit*, Prague: Tate International, 2001, 7-9.

'Donald Watts Davies CBE', *Biographical Memoirs of Fellows of the Royal Society*, 48, 2002, 87-96.

'Computer security ?' *Philosophical Transactions of the Royal Society, Series A, Mathematical, Physical and Engineering Sciences*, 361, 2003, 1549-1555; reprinted in *Computer systems: theory, technology and applications*, Ed. A. Herbert and K. Spärck Jones, New York: Springer, 2004, 319-326.