BIBLIOGRAPHY

[Abadi88] Abadi, M., and L. Lamport, ''The Existence of Refinement Mappings'', Research Report 29, Digital Equipment Corporation Systems Research Center, August 1988.

[Abadi90a] Abadi, M., ''An Axiomatization of Lamport's Temporal Logic of Actions'', Research Report 65, Digital Equipment Corporation Systems Research Center, October 1990.

[Abadi90b] Abadi, M., and L. Lamport, ''Composing Specifications'', Research Report 66, Digital Equipment Corporation Systems Research Center, October 1990.

[Aho72] Aho, A.V., and J.D. Ullman, *The Theory of Parsing, Translation, and Compiling* , Vol. 1, Prentice-Hall, 1972, p. 113

[Alpern85] Alpern, B., and F. Schneider, ''Defining Liveness'', *Information Processing Letters* , 21(4), October 1985, pp. 181-185.

[Bellare90] Bellare, M., S. Micali, R. Ostovsky, ''The (true) complexity of statistical zero knowledge'', *Proc. 22nd ACM Symp. on Theory of Computing* , 1990, pp. 494-502

[Bell74] Bell, D. Elliot, and Leonard J. LaPadula, *Secure Computer Systems: Mathematical Foundations* , MTR-2547, MITRE Corp., Bedford, MA (March 1973).

[Bertalanffy68] Von Bertalanffy, L., *General System Theory. Foundations, Development, Applications.* New York: George Braziller, 1968

[Boebert85] Boebert, W.E., R.Y. Kain, ''A practical alternative to hierarchical integrity policies'', *Proc. 8th National Computer Security Conference* , Baltimore, Oct. 85, pp. 18-27.

[Burrows88] Burrows, M., M. Abadi, R. Needham, ''Authentication: A Practical Study in Belief and Action'', *Proc. 2nd Conf. on Theoretical Aspects of Reasoning about Knowledge* , IBM Almaden Research Center, Pacific Grove, CA. March, 1988, pp. 325-342.

[Chellas80] Chellas, B., *Modal Logic* . Cambridge University Press, 1980.

[Clark87] Clark, D.D., and Wilson, D.R., ''AComparison of Commercial aand Military Computer Security Policies'', *Proc. of the IEEE Symposium on Security and Privacy* , Oakland, April 1987, pp.184-194.

[Clark88] Clark, D.D., and Wilson, D.R., ''Evolution of a model for computer integrity'', *Proc. 11th National Computer Security Conference* , Baltimore, Oct. 88, addendum.

[Cuppens90] Cuppens, F., ''An epistemic and deontic logic for reasoning about computer security'', *Proc. ESORICS 90*, AFCET, Toulouse, France, Oct. 1990, pp. 135-145.

[CTCPEC90] Canadian System Security Centre, *The Canadian Trusted Computer Product Evaluation Criteria* Version 2.0, Ottawa, Dec 1990.

[CTCPEC92] Canadian System Security Centre, *The Canadian Trusted Computer Product Evaluation Criteria* Version 3.0e, Ottawa, April 1992.

[DiVito88] DiVito, Ben, ''Derived Information Sensitivity as a Modelling Technique'', *Proceedings of the Security Foundations Workshop* , Franconia Inn, Franconia, NH, (June 1988)

[Fagin84] Fagin, R., J. Y. Halpern, M. Y. Vardi, ''A model-theoretic analysis of knowledge: preliminary report'', *Proc. 25th IEEE Symp. on Foundations of Computer Science* , 1984, pp. 268-278.

[Fagin86] Fagin, R., J. Y. Halpern, M. Y. Vardi, ''What can machines know? On the epistemic properties of machines'', *Proc. AAAI* , 1986, pp. 428-434.

[Glasgow88] Glasgow, J., G. MacEwen, and P. Panangaden, ''Reasoning about knowledge and permission in secure distributed systems'', *Proc. Workshop on Foundations of Computer Security* , Franconia, NH, 1988.

[Glasgow89] Glasgow, J., and G. MacEwen, ''Obligation as the basis of integrity specification'', *Proc. Computer Security Foundations Workshop II* , Franconia, NH, June 1989, pp. 64-70.

[Goguen82] Goguen, J.A., and J. Meseguer, ''Security Policies and Security Models'', *Proceedings of the 1982 IEEE Symposium on Security and Privacy* , Oakland, Ca., pp. 11-20.

[Goguen84] Goguen, J. A., and J. Meseguer, ''Unwinding and Inference Control'', *Proceedings of the Symposium on Research in Security and Privacy* , IEEE Computer Society, April 1984, pp. 144-161.

[Goldwasser85] Goldwasser, S., S. Micali, and C. Rackoff, ''The knowledge complexity of interactive proof systems'', *1984 ACM Foundations of Computer Science* , ACM 1985, pp. 291-304.

[Gray90] Gray, J.W.III, ''Probabilistic Interference'', *Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy* , Oakland, Ca., pp. 170-179

[Gray90] Gray, R. M., *Source Coding Theory* , Kluwer Academic Publishers, Dordrecht, Netherlands, 1990.

[Gray91] Gray, J. W., ''Toward a Mathematical Foundation for Information Flow Security'', *Proceedings of the Symposium on Research in Security and Privacy* , IEEE Computer Society, May 1991, pp. 21-34.

[Guttman88] Guttman, J. D., and M. E. Nadel, ''What Needs Securing?'', *Proceedings of the Computer Security Foundations Workshop* , IEEE Computer Society, June 1988, pp. 34-57. June 12-15 1988

[Havender68] Havender J.W., ''Avoiding deadlock in multitasking systems'', *IBM System Journal* , vol. 7 no. 2, 1968, pp. 74-84.

[Hintikka62] Hintikka, J., *Knowledge and belief*, Cornell University Press, 1962.

[Hoare85] Hoare, C.A.R., *Communicating sequential processes*, Prentice-Hall 1985.

[Hopcroft69] Hopcroft, J. E., and J. D. Ullman, *Formal Languages and their Relation to Automata*, Addison-Wesley, Reading, Mass. 1969.

[ISO7498-2] International Organization for Standardization, *OSI Security Architecture*, International Standard ISO 7498 Addendum 2.

[ISO9000] International Organization for Standardization, *Quality Management and Quality Assurance Standards*, International Standard ISO-9000.

[ITSEC89] German Information Security Agency, *Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems*, 1st Version, Bundesanzeiger, Köln, Germany, 1989.

[Jacob88] Jacob J., ''Security specifications'', *Proc. 1988 IEEE Symposium on Security and Privacy*, IEEE 1988, pp. 14-23.

[Johnson88] Johnson, Dale M., and F. Javier Thayer, ''Security and the composition of machines'', *Proceedings of the Security Foundations Workshop*, Franconia Inn, Franconia, NH, June 12-15 1988

[Jueneman89] Jueneman Robert R., ''Integrity controls for military and commercial applications'', *Proc. Invitational Workshop on Data Integrity*, NIST, Jan. 89, sect. A.5

[Klir85] Klir, G.J., *Architecture of Systems Problem Solving*, Plenum Press, New York, 1985

[Kripke63] Kripke, S.A., ''Semantical analysis of modal logic I, normal propositional calculi'', *Zeitschrift fuer mathematische Logik und Grundlagen der Mathematik*, VEB Deutscher Verlag der Wissenschaften, vol. 9 (1963), pp. 67-96.

[Kumar86] Kumar, P.R., and P. Varaiya, *Stochastic Systems: Estimation, Identification, and Adaptive Control* , Prentice-Hall, Englewood Cliffs, NJ (1986)

[Lamport83] Lamport, L., ''Specifying Concurrent Program Modules'', *ACM Transactions on Programming Languages and Systems* , 5(2), April 1983, pp. 190-222.

[Lamport84] Lamport, L., ''Basic concepts'', *Advanced Course on Distributed Systems* , Lecture Notes on Computer Science 190, Berlin-Heidelberg: Springer, 1984

[Lamport89] Lamport, L., ''A Simple Approach to Specifying Concurrent Systems'', *Communications of the ACM* , 32(1), January 1989, pp. 32-45.

[Lamport90] Lamport, L., ''A Temporal Logic of Actions'', Research Report 57, Digital Equipment Corporation Systems Research Center, April 1990.

[Lee88] Lee, T.M.P., ''Using mandatory integrity to enforce commercial security'', *Proc. 1988 IEEE Symposium on Security and Privacy* , Oakland, Apr. 88, pp. 140-146.

[Lipner82] Lipner, S.B., ''Non-discretionary controls for commercial applications'', *Proc. 1982 IEEE Symposium on Security and Privacy* , Oakland, Apr. 82, pp. 2-10.

[Marcus86] Marcus, Leo, and T. Redmond, ''A Semantics of Read'', *Proc. 9th National Computer Security Conference* , Baltimore, MD, National Bureau of Standards, Sept. 1986, pp.184-193

[Marcus88] Marcus, Leo, and Timothy Redmond, ''A model-theoretic approach to specifying, verifying, and hooking up security policies'', *Proceedings IEEE Symposium on Security and Privacy* , IEEE 1988, pp.127-138.

[Marcus89] Marcus, Leo, ''The search for a unifying framework for computer security'', *Fall '89 CIPHER newsletter* , IEEE Computer Society Technical Committee on Security and Privacy, pp. 55-63.

[McCullough87] McCullough, Daryl, ''Specifications for multi-level security and a hook-up property'', *Proc. 1987 IEEE Symposium on Security and Privacy* , IEEE 1987.

[McCullough88a] McCullough, Daryl, *The Theory of Security* , Technical Report 11-12, Odyssey Research Associates Inc., Ithaca, NY, (1988).

[McCullough88b] McCullough, Daryl, ''Covert Channels and Degrees of Insecurity'', *Proceedings of the Workshop on Foundations of Computer Security* , Franconia, NH, (1988).

[McCullough88c] McCullough, Daryl, ''Noninterference and the composability of security properties'', *Proc. 1988 IEEE Symposium on Security and Privacy* , IEEE 1988, pp. 177-186.

[McLean90] McLean, J., ''Security Models and Information Flow'', *Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy* , Oakland, Ca., pp. 180-187.

[Mesarovic68] Mesarovic, M.J., ''On Some Mathematical Results As Properties of General Systems'' *Mathematical Systems Theory,* Vol 2, No. 3, 1968, pp. 203-222.

[Millen87] Millen, J. K., ''Covert Channel Capacity'', *Proc. 1987 IEEE Symposium on Security and Privacy* , pp. 60-66.

[Millen90] Millen, J., ''Hookup Security for Synchronous Machines'', *Proceedings of the Computer Security Foundations Workshop III* , IEEE Computer Society, June 1990, pp. 84-90.

[Moser89] Moser, L.E., ''Alogic of knowledge and belief for reasoning about computer systems'', *Proc. Computer Security Foundations Workshop II* , Franconia, NH, June 1989, pp. 57-63

[Nyquist24] Nyquist, H., ''Certain factors affecting telegraph speed'', *Bell Syst. Tech. Jour.* , vol. 3, April, 1924, p. 324.

[Pittelli88] Pittelli, Paul A., ''Formalizing integrity using noninterference'', *Proc. 11th National Computer Security Conference* , Baltimore, Oct. 88, pp. 38-42.

[Reiter87] Reiter, R., ''Nonmonotonic reasoning'', *Annual Review of Computer Science* , 1987, pp. 147-186

[Shannon49] Shannon, C. E., ''Communication in the Presence of Noise'', *Proc. of the IRE* , vol. 37, pp. 10-21, January, 1949. Reprinted in *Proc. of the IEEE* , vol. 72, no. 9, pp. 1192-1201, September 1984.

[Solovay77] Solovay, R., and V. Strassen, ''A fast Monte-Carlo test for primality'', *SIAM J. Computing* , vol. 6, no. 4, Dec 1977, pp. 84-85.

[Sutherland86] Sutherland, David, ''A Model of Information'', *Proc. 9th National Computer Security Conference* , National Bureau of Standards, September 1986, pp. 175-183.

[Sutherland89] Sutherland, Ian, S. Perlo, R. Varadarajan, ''Deducibility Security with Dynamic Level Assignment'', *Proceedings of the Second Workshop on Foundations of Computer Security* , Franconia, NH, (1989), pp. 3-8.

[TCSEC85] National Computer Security Center, *Department of Defense Trusted Computer Security Evaluation Criteria* , DOD 5200.28-STD, Dec 1985.

[Thomson88] Thomson, Brian, E.S.Lee, P.I.P. Boulton, M. Stumm, D.M. Lewis, *A Trusted Network Architecture* , Technical Report CSRI-228, Computer Systems Research Institute, University of Toronto, Toronto, Ontario (Oct. 1988)

[Thomson89] Thomson, Brian, E.S.Lee, P.I.P. Boulton, M.Stumm, D.M.Lewis,. ''Deducibility-based Network Security Modelling'', *Proceedings of the First Canadian Computer Security Conference* , Ottawa (1989)

[TNI87] National Computer Security Center, *Trusted Network Interpretation of the Trusted Computer Security Evaluation Criteria* , NCSC-TG-005, July 1987.

[Williams88] Williams, John C., and M. L. Day, ''Sensitivity Labels and Security Profiles'', *Proceedings of the 11th National Computer Security Conference* , National Bureau of Standards, October 1988, pp. 257-266.

[Wittbold90] Wittbold, J.T., and D.M. Johnson, ''Information Flow in Nondeterministic Systems'', *Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy* , Oakland, Ca., pp. 144-161

[Yu88] Yu, C.-F., and V.D. Gligor, ''A formal specification and verification method for the prevention of denial of service'', *Proc. 1988 IEEE Symposium on Security and Privacy* , IEEE 1988, pp. 187-202.