

References

- [ABBO76] Abbott, R.P., et al., "Security Analysis and Enhancement of Computer Operating Systems," NBSIR 76-1041, Nat'l Bureau of Standards, ICST, Gaithersburg, Md., Apr. 1976.
- [ABRA87] Abrams, Marshall D., and Harold J. Podell, *Tutorial: Computer and Network Security*, IEEE Computer Society Press, Los Alamitos, Calif., 1987.
- [ABRA90] Abrams, M.D., et al., "A Generalized Framework for Access Control: An Informal Description," *13th Nat'l Computer Security Conf.*, Oct. 1990, pp. 135-143.
- [ADAM89] Adam, Nabil R., and John C. Wortmann, "Security-Control Methods for Statistical Databases: A Comparative Study," *ACM Computing Surveys*, Vol. 21, No. 4, Dec. 1989, pp. 515-556.
- [AFIP79] "Consensus Report, Processors, Operating Systems and Nearby Peripherals," *AFIPS Conf. Proc.*, Theodore M.P. Lee (chairman), Nat'l Computer Conf., June 4-7, 1979.
- [AMER82] *The American Heritage Dictionary*, Second College Edition, Houghton Mifflin, Boston, 1982.
- [AMES83] Ames, S.R., Jr., M. Gasser, and R.R. Schell, "Security Kernel Design and Implementation: An Introduction," *Computer*, Vol. 16, No. 7, July 1983, pp. 14-22.
- [AMOR91] Amoroso, Ed, Thu Nguyen, Jon Weiss (AT&T Bell Laboratories) and John Watson, Pete Lapiska, Terry Starr (GE Aerospace), "Toward an Approach to Measuring Software Trust," *Proc. IEEE Computer Society Symp. Research in Security and Privacy*, IEEE Computer Society Press, Los Alamitos, Calif., May 20-22, 1991, pp. 198-218.
- [ANDE72] Anderson, J.P., "Computer Security Technology Planning Study," ESD-TR-73-51, Vol.1, Hanscom AFB, Mass., 1972 (also available as DTICAD-758206).

[ANDE81] Anderson, J.P., "On the Feasibility of Connecting RECON to an External Network," Tech. Report, James P. Anderson Co., Mar. 1981.

[ANSI91a] X12.58, "Draft Standard for the Trial Use of Managing EDI Security Structures," 1991.

[ANSI91b] X12.42, "Draft Standard for the Trial Use of Managing EDI Cryptographic Service Message Transaction Sets," 1991.

[ANSI91c] "Guideline for Implementing X12.42 & X12.58," 1991.

[ANSI92a] X9.30-199X, "Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry," 1992.

[ANSI92b] X9.31-199X, "Public Key Cryptography Using Reversible Algorithms for the Financial Services Industry," 1992.

[ATTA76] Attanasio, C.R., P.W. Markstein, and R.J. Phillips, "Penetrating an Operating System: A Study of VM/370 Integrity," *IBM Systems J.*, Vol. 15, No. 1, 1976, pp. 102-106.

[BACH86] Bach, Maurice J., *The Design of the Unix Operating System*, Prentice-Hall, Englewood Cliffs, N.J., 1986.

[BALE93] Balenson, D., "Privacy Enhancement for Internet Electronic Mail: Part III — Algorithms, Modes, and Identifiers," RFC 1423, Feb. 1993.

[BAUE88] Bauer, D.S., and M.E. Koblenz, "NIDX — A Real-Time Intrusion Detection Expert System," *Proc. Summer 1988 USENIX Conf.*, June 1988.

[BAUE91] Bauer, R.K., J. Sachs, M. Weidner, and W. Wilson, "A Framework for Developing Accreditable MLS AIS," *Proc. 14th Nat'l Computer Security Conf.*, Oct. 1991.

[BELA74] Belady, L.A., and C. Weissman, "Experiments with Secure Resource Sharing for Virtual Machines," *Proc. Int'l Workshop on Protection in Operating Systems*, IRIA/LABORIA, Rocquencourt, Le Chesnay, France, Aug. 1974.

[BELL73] Bell, D.E., and L.J. LaPadula, "Secure Computer Systems: Mathematical Foundations and Model," M74-244, MITRE Corp., Bedford, Mass., 1973 (also available as DTIC AD-771543).

[BELL75] Bell, D.E., and L.J. LaPadula, "Secure Computer Systems: Unified Exposition and Multics Interpretation," MTR-2997, MITRE Corp., Bedford, Mass., July 1975.

[BELL75a] Bell, D.E., and L.J. LaPadula, "Computer Security Model: Unified Exposition and Multics Interpretation," ESD-TR-75-306, Hanscom AFB, Mass., 1975 (also available as DTIC AD-A023588).

[BELL76] Bell, D.E., and L.J. LaPadula, "Secure Computer Systems: Unified Exposition and Multics Interpretation," MITRE Corp. ESD-TR-75-306, NTIS #AD-A023588, Electronic Systems Division, Air Force Systems Command, Mar. 1976.

[BELL90] Bell, D.E., "Lattices, Policies, and Implementations," *13th Nat'l Computer Security Conf.*, NIST/NCSC, Oct. 1990, pp. 165-171.

[BELL91] Bell, D.E., "Putting Policy Commonalities to Work," *Proc. 14th Nat'l Computer Security Conf.*, Oct. 1991, pp. 456-471.

[BHAR90] Bhargava, Gautam, and Shashi K. Gadia, "The Concept of Error in a Database: An Application of Temporal Database," in *Data Management: Current Trends*, McGraw-Hill, ed., New Delhi, India, Dec. 1990, pp. 106-121.

[BHAR93] Bhargava, Gautam, and Shashi K. Gadia, "Relational Database Systems with Zero Information Loss," *IEEE Trans. Knowledge and Data Eng.*, Vol. 5, No. 1, Feb. 1993, pp. 76-87.

[BIBA77] Biba, K.J., "Integrity Considerations for Secure Computer Systems," ESD-TR-76-372, USAF Electronic Systems Division (also MTR3153, MITRE Corp.), Bedford, Mass., Apr. 1977.

[BIHA90] Biham, E., and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Tech. Report CS90-16, Weizmann Inst. of Science, Dept. of Applied Mathematics and Computer Science, Rehovot, Israel, July 1990.

[BISB78] Bisbey, R., and D. Hollingworth, "Protection Analysis Project Final Report," ISI/RR-78-13, DTIC AD A056816, USC Information Sciences Inst., Marina del Rey, Calif., May 1978.

[BISH82] Bishop, M., "Security Problems with the UNIX Operating System," Computer Science Dept., Purdue Univ., West Lafayette, Ind., Mar. 1982.

[BJOR75] Bjork, L.A., "Generalized Audit Trail Requirements and Concepts for Database Applications," *IBM Systems J.*, Vol. 14, No. 3, 1975, pp. 229-245.

[BLAT90] Blatchford, C.W., "Information Security — The European Perspective," CEN/CENELEC document, CSecG/13/90.

[BLOO90] Bloombecker, B., *Spectacular Computer Crimes*, Dow-Jones-Irwin, Homewood, Ill., 1990.

[BOEB85] Boebert, W.R., and R.Y. Kain, "A Practical Alternative to Integrity Policies," *Proc. 8th Nat'l Computer Security Conf.*, Oct. 1985, pp. 18-27.

[BONY88] Bonyun, David A., "Logging and Accountability in Database Management Systems," *Database Security: Status and Prospects*, Carl E. Landwehr, ed., North-Holland, Amsterdam, 1988, pp. 223-227.

[BOOT81] Booth, K.S., "Authentication of Signatures Using Public Key Encryption," *Comm. ACM*, Vol. 24, No. 11, Nov. 1981, pp. 772-774.

[BORE92] Borenstein, N., and N. Freed, "Multipurpose Internet Mail Extensions," RFC 1341, May 1992.

[BRAN75] Branstad, D.K., "Encryption Protection in Computer Data Communications," *Proc. 4th Data Comm. Symp.*, IEEE, Oct. 7-9, 1975, pp. 8.1-8.7.

[BRAN91] Branstad, M.A., C.P. Pfleeger, D. Brewer, C.S. Jahl, and H. Kurth, "Apparent Differences Between the US TCSEC and the European ITSEC," *Proc. 14th Nat'l Computer Security Conf.*, Oct., 1991, pp. 45-58.

[BREW89] Brewer, D.F.C., and M.J. Nash, "The Chinese Wall Security Policy," *Proc. Symp. Research in Security and Privacy*, May 1989, pp. 206-214.

[BUCZ90] Buczkowski, Leon J., "Database Inference Controller," in *Database Security III: Status and Prospects*, D.L. Spooner and C. Landwehr, eds., North-Holland, Amsterdam, 1990, pp. 311-322.

[BULL91] Bull, A., C.E. Landwehr, J.P. McDermott, and W.S. Choi, "A Taxonomy of Computer Program Security Flaws," Center for Secure Information Technology, Naval Research Laboratory, draft in preparation, 1991.

[BURN89] Burns, R.K., "DBMS Integrity and Secrecy Control," in [NIST89], sec. A.7, pp. 1-4 (1989).

[BURN90] Burns, Rae K., "Referential Secrecy," *Proc. IEEE Symp. Security and Privacy*, Oakland, Calif., May 1990, pp. 133-142.

[CANA92] Canadian System Security Centre, Communication Security Establishment, *The Canadian Trusted Computer Product Evaluation Criteria*, Version 3.0e, Government of Canada, 1992 draft. Note: Version 3.0e was published in Jan. 1993.

[CARL75] Carlstedt, J., R. Bisbey, and G. Popek, "Pattern-Directed Protection Evaluation," ISI/RR-75-31, USC Information Sciences Inst., Marina del Rey, Calif., June 1975.

[CCIT88a] "Data Communications Networks: Message Handling System and Service Overview," CCITT Recommendation X.400, Nov. 1988.

[CCIT88b] "Message Handling Systems: Message Transfer System; Abstract Service Definition and Procedures," CCITT Recommendation X.411, 1988.

[CCIT88c] "The Directory-Authentication Framework," CCITT Recommendation X.509, Nov. 1988.

[CCIT88d] "Specification of Abstract Syntax Notation One (ASN.1)," CCITT Recommendation X.208, Nov. 1988.

[CCIT90] CCITT 1990 X.400 Series of Recommendations, "Message Handling System."

[CCIT92] CCITT X.435 (1991) EDI Messaging SC27/WG1/N131.

[CHAB90] Chabernaud, Christian, and Bernard Vilain, "Telecommunications Services and Distributed Applications," *IEEE Network Magazine*, Nov. 1990, pp. 10-13.

[CHOK92] Chokhani, Santosh, "Trusted Products Evaluations," *Comm. ACM*, Vol. 35, No. 7, July 1992, pp. 64-76.

[CLAR87] Clark, D.D., and D.R. Wilson, "A Comparison of Commercial and Military Computer Security Policies," *Proc. IEEE Symp. Security and Privacy*, IEEE Computer Society Press, Los Alamitos, Calif., 1987, pp. 184-194.

[CLAR89a] Clark, D.D., and D.R. Wilson, "Comments on the Integrity Model," in [NIST89], sec. 9, pp. 1-6 (1989).

[CLAR89b] Clark, D.D., and D.R. Wilson, "Evolution of a Model for Computer Integrity," in [NIST89], sec. A.2, pp. 1-13 (1989).

[Codd79] Codd, E.F., "Extending the Relational Database Model to Capture More Meaning," *ACM Trans. Database Systems*, Vol. 4, No. 4, 1979.

[CONG74] Congress, US, Privacy Act of 1974, Public Law 92-579, 1974.

[CONG82] Congress, US, Federal Managers' Financial Integrity Act of 1982, Public Law 97-255, Sept. 1982.

[CONG87] Congress, US, Computer Security Act of 1987, Public Law 100-235, Jan. 1988.

[CONG88] Congress, US, Computer Matching and Privacy Protection Act of 1988, Public Law 100-503, Oct. 1988.

[CONG90] Congress, US, Computer Matching and Privacy Protection Amendments of 1990, Public Law 101-508, Nov. 1990.

[COX79] Cox, L.A., and R.R. Schell, "Understanding Computer Related Crime," *Crime Prevention Rev.*, June 1979, pp. 1-10.

[CROC82] Crocker, D., "Standard for the Format of ARPA Internet Text Messages," [Internet] RFC 822, Aug. 1982.

[CSC85] Computer Security Center, "Computer Security Requirements: Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments" (The Yellow Book), CSC-STD-003-85, June 25, 1985.

[CSCD85] *Department of Defense Password Management Guideline*, Dept. of Defense Computer Security Center, CSC-STD-002-85, Apr. 12, 1985.

[CSSC92] Canadian System Security Centre, Communications Security Establishment, *The Canadian Trusted Computer Product Evaluation Criteria*, Government of Canada, Apr. 1992.

[DATE83] Date, C.J., *An Introduction to Database Systems*, Vol. 2, Addison-Wesley, Reading, Mass., 1983.

[DATE86] Date, C.J., *An Introduction to Database Systems*, Vol. 1, fourth edition, Addison-Wesley, Reading, Mass., 1986.

[DCSC83] DoD Computer Security Center, Trusted Computer Security Evaluation Criteria, CSC-STD-001-83, Aug. 15, 1983.

[DENN76] Denning, D.E., "A Lattice Model of Secure Information Flow," *Comm. ACM*, Vol. 19, No. 5, May 1976, pp. 236-243.

[DENN79] Denning, D.E., and Denning, P.J., "Data Security," *ACM Computing Surveys*, Vol. 11, No. 3, 1979, pp. 227-249.

[DENN81] Denning, D.E., and G.M. Sacco, "Time Stamps in Key Distribution Protocols," *Comm. ACM*, Vol. 24, No. 8, Aug. 1981, pp. 533-536.

[DENN82] Denning, Dorothy E., *Cryptography and Data Security*, Addison-Wesley, Reading, Mass., 1982.

[DENN83] Denning, Dorothy E., and Jan Schlorer, "Inference Controls for Statistical Databases," *Computer*, Vol. 16, No. 7, July 1983, pp. 69-82.

[DENN84] Denning, D.E., "Cryptographic Checksums for Multilevel Database Security," *Proc. Symp. Security and Privacy*, IEEE Computer Society Press, Los Alamitos, Calif., 1984, pp. 52-61.

[DENN85] Denning, D.E., "Commutative Filters for Reducing Inference Threats in Multilevel Database Systems," *Proc. Symp. Security and Privacy*, IEEE Computer Society Press, Los Alamitos, Calif., 1985, pp. 134-146.

[DENN86] Denning, Dorothy E., and Matthew Morgenstern, "Military Database Technology Study: AI Techniques for Security and Reliability," SRI tech. report, Aug. 1986.

[DENN86a] Denning, Dorothy E., "A Preliminary Note on the Inference Problem in Multilevel Database Management Systems," *Proc. Nat'l Computer Security Center Invitational Workshop on Database Security*, June 1986.

[DENN86b] Denning, D.E., "An Intrusion-Detection Model," *Proc. IEEE Symp. Security and Privacy*, Oakland, Calif., Apr. 1986, pp. 118-131.

[DENN87] Denning, Dorothy E., Teresa F. Lunt, Roger R. Schell, Mark Heckman, and William R. Shockley, "A Multilevel Relational Data Model," *Proc. IEEE Symp. Security and Privacy*, Apr. 1987, pp. 220-234.

[DENN88a] Denning, Dorothy E., Teresa F. Lunt, Roger R. Schell, William R. Shockley, and Mark Heckman, "The SeaView Security Model," *Proc. IEEE Symp. Security and Privacy*, Apr. 1988, pp. 218-233.

[DENN88b] Denning, Dorothy E., "Lessons Learned from Modeling a Secure Multilevel Relational Database System," in *Database Security: Status and Prospects*, C.E. Landwehr, ed., North-Holland, Amsterdam, 1988, pp. 35-43.

[DIA87] Defense Intelligence Agency (DIA), "Security Requirements for System High and Compartmented Mode Workstations," DDS-2600-5502-87, Nov. 1987.

[DIAS91] Dias, G.V., et al., "DIDS (Distributed Intrusion Detection System) — Motivation, Architecture, and an Early Prototype," *Proc. 14th Nat'l Computer Conf.*, Washington, D.C., Oct. 1991, pp. 167-176.

[DILL86] Dillaway, B.B., and J.T. Haigh, "A Practical Design for a Multi-level Secure Database Management System," *Proc. Second Aerospace Computer Security Conf.*, McLean, Va., Dec. 1986, pp. 44-57.

[DINK90] Dinkel, Charles, ed., *Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols*, Nat'l Inst. of Standards and Technology, US Dept. of Commerce, NISTIR 90-4250, Feb. 1990.

[DITT89] Dittrich, Klaus R., Martin Hartig, and Heribert Pfefferle, "Discretionary Access Control in Structurally Object-Oriented Database Systems," in *Database Security II: Status and Prospects*, Carl E. Landwehr, ed., North-Holland, Amsterdam, 1989, pp. 105-121.

[DOD82] Dept. of Defense, *Department of Defense Privacy Program*, DOD Directive 5400.11, June 1982.

[DOD83] Dept. of Defense, *Military Standard Internet Protocol*, MIL-STD-1777, Aug. 12, 1983.

[DOD85] Dept. of Defense Standard, *Department of Defense Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, GPO 1986-623-963, 643 0, Dec. 26, 1985.

[DOD86] Dept. of Defense Standard, *Department of Defense Trusted Computer System Evaluation Criteria, Information Security Program Regulation*, DOD Regulation 5200.1, May 1986.

[DOD88a] Dept. of Defense, *Military Standard: Defense Systems Software Development*, DOD-STD-2167A, Feb. 29, 1988.

[DOD88b] Dept. of Defense, *Security Requirements for Automated Information Systems*, DOD Directive 5200.28, Mar. 21, 1988.

[DTI92] Dept. of Trade and Industry (DTI), "The UK IT Security Evaluation and Certification Scheme: UKSP 01," "Description of the Scheme; UKSP 06," "UK Certified Product List: Issue 1.4," UKSP01 06, DTI, Mar. 1, 1991; reprinted for the 15th Nat'l Computer Security Conf., Oct. 1, 1992. Note: These publications are updated periodically. For example, "The UK IT Security Evaluation and Certification Scheme" and "Certified Product List" were published together in Oct. 1994.

[ECKM85] Eckmann, S., and R.A. Kemmerer, "INATEST: An Interactive Environment for Testing Formal Specifications," *Software Eng. Notes*, Vol. 10, No. 4, Aug. 1985, pp. 17-18.

[ECKM87] Eckmann, S., "Ina Flo: The FDM Flow Tool," *Proc. 10th Nat'l Computer Conf.*, Baltimore, Sept. 1987, pp. 175-182.

[EDIF91a] Recommendation for UN/EDIFACT Security Joint WG, 1991.

[EDIF91b] Security Framework for EDIFACT (SC27/WG1/N135), 1991.

[EICH89] Eichen, M.W., and J.A. Rochlis, "With Microscope and Tweezers: An Analysis of the Internet Virus of November 1988," *Proc. IEEE Computer Society Symp. Research in Security and Privacy*, IEEE Computer Society Press, Los Alamitos, Calif., May 1-3, 1989, pp. 326-343.

[ELMA89] Elmasri, Ramez, and Shamkant B. Navathe, *Fundamentals of Database Systems*, Benjamin/Cummings, 1989.

[FARM86] Farmer, W.M., D.M. Johnson, and F.J. Thayer, "Towards a Discipline for Developing Verified Software," *9th Nat'l Computer Security Conf.*, Sept. 1986, pp. 91-98.

[FARM90] Farmer, W.M., "A Partial Functions Version of Church's Simple Theory of Types," *J. Symbolic Logic*, Vol. 55, 1990, pp. 1269-1291.

[FARM90a] Farmer, D., and E.H. Spafford, "The COPS Security Checker System," CSD-TR-993, Dept. of Computer Sciences, Purdue Univ., West Lafayette, Ind., 1990 (software available by anonymous ftp from cert@sei.cmu.edu).

[FARM91] Farmer, W.M., J.D. Guttman, and F.J. Thayer, "IMPS: An Interactive Mathematical Proof System," M90-19, MITRE Corp., July 1991.

[FELL87] Fellows, J., J. Hemenway, N. Kalem, and S. Romero, "The Architecture of a Distributed Trusted Computing Base," *Proc. 10th Nat'l Computer Security Conf.*, Sept. 1987, pp. 68-77.

[FELL91] Fellows, J., "Federated Trustworthy Systems," NATO Workshop on Composite Trustworthy Systems, Naval Research Laboratory, Oct. 1991.

[FERN81] Fernandez, Eduardo B., Rita C. Summers, and Christopher Wood, "Database Security and Integrity," Addison-Wesley, Reading, Mass., 1981.

[FERN89] Fernandez, Eduardo B., Ehud Gudes, and Haiyan Song, "A Security Model for Object-Oriented Databases," *Proc. IEEE Symp. Security and Privacy*, May 1989, pp. 110-115.

[FERR91] Ferraiolo, D., and K. Ferraiolo, "Another Factor in Determining Security Requirements for Trusted Computer Applications," *Proc. 14th Nat'l Computer Security Conf.*, Nat'l Computer Security Center, Oct. 1991.

[FLIN88] Flink, Charles W., and J.D. Weiss, "System V/MLS Labeling and Mandatory Policy Alternatives," *AT&T Technical J.*, May/June 1988.

[FORC90] Forcht, Karen A., "Ethical Use of Computers," in *Rogue Programs: Viruses, Worms, and Trojan Horses*, Lance J. Hoffman, ed., 1990, pp. 117-120.

[FRAI83] Fraim, L., "SCOMP: A Solution to the Multilevel Security Problem," *Computer*, Vol. 16, No. 7, July 1983, pp. 26-34.

[FROS89] Froscher, Judith N., and Catherine Meadows, "Achieving a Trusted Database Management System Using Parallelism," in *Database Security II: Status and Prospects*, C.E. Landwehr, ed., North-Holland, Amsterdam, 1989.

[GAJN88] Gajnak, G., "Some Results from the Entity/Relationship Multi-level Secure DBMS Project," *Proc. 4th Aerospace Computer Security Applications Conf.*, 1988, pp. 66-71.

[GALI75] Galie, L.M., R.R. Linde, and K.R. Wilson, "Security Analysis of the Texas Instruments Inc. Advanced Scientific Computer," TM-WD-

6505/000/00, System Development Corp., Washington, D.C., June 1975.

[GALI76] Galie, L.M., and R.R. Linde, "Security Analysis of the IBM VS2/R3 Operating System," TM-WD-7203/000/00, System Development Corp., Washington, D.C., Jan. 1976.

[GAMB88] Gambel, D., and S. Walter, "Retrofitting and Developing Applications for a Trusted Computing Base," *Proc. 11th Nat'l Computer Security Conf.*, Nat'l Computer Security Center, Oct. 1988.

[GAO88] US General Accounting Office, "GAO Policy and Procedures Manual for Guidance of Federal Agencies # Title 2, Accounting," Aug. 1987, revised May 1988.

[GARF91] Garfinkel, S., and G. Spafford, *Practical Unix Security*, O'Reilly and Assoc., Sebastopol, Calif., 1991.

[GARV86] C. Garvey, "Multilevel Data Storage Design," TRW Defense Systems Group, 1986.

[GARV88] Garvey, Cristi, and Amy Wu, "ASD-Views," *Proc. IEEE Symp. Security and Privacy*, Oakland, Calif., May 1988, pp. 85-95.

[GARV90] Garvey, Cristi, Thomas Hinke, Nancy Jensen, Jane Solomon, and Amy Wu, "A Layered TCB Implementation Versus the Hinke-Schaefer Approach," in *Database Security III: Status and Prospects*, D.L. Spooner and C.E. Landwehr, eds., North-Holland, Amsterdam, 1990, pp. 151-165.

[GARV91] Garvey, T.D., T.F. Lunt, and M.E. Stickel, "Abductive and Approximate Reasoning Models for Characterizing Inference Channels," *Proc. Computer Security Workshop IV*, June 1991, pp. 118-126.

[GASS87] Gasser, M., *Building a Secure Computer System*, Van Nostrand Reinhold, New York, 1987.

[GASS88] Gasser, M., *Building a Secure Computer System*, Van Nostrand Reinhold, New York, 1988.

[GEMI89] Gemignani, Michael, "Viruses and Criminal Law," *Rogue Programs: Viruses, Worms, and Trojan Horses*, L.J. Hoffman, ed., 1990, pp. 99-103.

[GLIG86] Gligor, V.D., et al., "On the Design and the Implementation of Secure Xenix Workstations," *Proc. Symp. Security and Privacy*, Apr. 1986, pp. 102-117.

[GOGU82] Goguen, J.A., and J. Meseguer, "Security Policies and Security Models," *Proc. Symp. Security and Privacy*, Apr. 1982, pp. 11-20.

[GOGU84] Goguen, Joseph A., and José Meseguer, "Unwinding and Inference Control," *Proc. Symp. Security and Privacy*, Apr. 1984, pp. 75-86.

[GRAN83] Grant, P., and R. Riche, "The Eagle's Own Plume," *US Naval Inst. Proc.*, July 1983.

[GRAU82] Graubart, Richard D., and John P.L. Woodward, "A Preliminary Naval Surveillance DBMS Security Model," *Proc. IEEE Symp. Security and Privacy*, Oakland, Calif., Apr. 1982, pp. 21-37.

[GRAU84] Graubart, Richard D., "The Integrity-Lock Approach to Secure Database Management," *Proc. IEEE Symp. Security and Privacy*, Oakland, Calif., May 1984, pp. 62-74.

[GRAU89] Graubart, Richard D., "A Comparison of Three Secure DBMS Architectures," *Proc. IFIP WG 11.3 Workshop on Database Security*, Monterey, Calif., Sept. 1989.

[GRAU89a] Graubart, Richard, "On the Need for a Third Form of Access Control," *Proc. 12th Nat'l Computer Security Conf.*, NIST/NCSC, Oct. 1989, pp. 296-304.

[GRAU90] Graubart, Richard, "A Comparison of Three Secure DBMS Architectures," in *Database Security III: Status and Prospects*, D.L. Spooner and C.E. Landwehr, eds., North-Holland, Amsterdam, 1990, pp. 109-114.

[GRAY78] Gray, J., "Notes on Data Base Operating Systems," in *Operating Systems — An Advanced Course*, R. Bayer et al., eds., Springer-Verlag, Berlin, 1978, pp. 393-481.

[GRAY86] Gray, J., "Why Do Computers Stop and What Can Be Done About It?" *Proc. IEEE Symp. Reliability in Distributed Software and Database Systems*, 1986, pp. 3-12.

[GRAY89] Gray, James W., Catherine D. Jensen, Nancy L. Kelem, Roberta J. Medlock, LouAnna Notargiacomo, and James P. O'Connor, "Secure Distributed Database Management System: Architecture," final

tech. report, Vols. 1-5, RADC-TR-89-314, Unisys Corp., McLean, Va., Dec. 1989.

[GRAY91] Gray, J.W., "Toward a Mathematical Foundation for Information Flow Security," *Proc. IEEE Symp. Research in Security and Privacy*, IEEE, New York, May 1991, pp. 21-34.

[GRIF76] Griffiths, Patricia P., and Bradford W. Wade, "An Authorization Mechanism for a Relational Database System," *ACM Trans. Database Systems*, Vol. 1, No. 3, Sept. 1976, pp. 242-255.

[GROH76] Grohn, Michael J., "A Model of a Protected Data Management System," ESD-TR-76-289, I.P. Sharp Associates, June 1976.

[GUID83] *Guidelines for Computer Security Certification and Accreditation*, US Dept. of Commerce, Nat'l Bureau of Standards, FIPS PUB 102, Sept. 27, 1983.

[GUID84] Ruthberg, Zella G., and William Neugent, *Overview of Computer Security Certification and Accreditation*, US Dept. of Commerce, Nat'l Bureau of Standards, NBS Special Publication 500-109, Apr. 1984.

[GUID85a] *Password Usage Standard*, US Dept. of Commerce, Nat'l Bureau of Standards, FIPS PUB 112, May 30, 1985.

[GUPTA91] Gupta, S., and V.D. Gligor, "Towards a Theory of Penetration-Resistant Systems and Its Application," *Proc. 4th IEEE Workshop on Computer Security Foundations*, Franconia, N.H., June 1991, pp. 62-78.

[GUPTA92] Gupta, S., and V.D. Gligor, "Experience with a Penetration Analysis Method and Tool," *Proc. 15th Nat'l Computer Security Conf.*, Baltimore, Oct. 1992, pp. 165-183.

[HAFN91] Hafner, Katie, and John Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, Simon and Schuster, New York, 1991.

[HAIG88] Haigh, J.T., "Modeling Database Security Requirements," in *Database Security: Status and Prospects*, North-Holland, Amsterdam, 1988.

[HAIG90] Haigh, J.T., R.C. O'Brien, P.D. Stachour, and D.L. Toups, "The LDV Approach to Database Security," in *Database Security III: Status and Prospects*, D.I. Spooner and C. Landwehr, eds., North-Holland, Amsterdam, 1990.

[HAIG90a] Haigh, J.T., R.C. O'Brien, and D.J. Thomsen, "The LDV Secure Relational DBMS Model," *Proc. IFIP W.G. 11.3 Workshop on Database Security*, Oct. 1990.

[HAIG91] Haigh, J.T., "LOCK Data Views (LDV)," *Lecture Notes for the Short Course Trusted Database Management Systems*, Cristi Garvey, coordinator, Univ. Extension, Univ. of California, Los Angeles, Apr. 2-5, 1991.

[HAIG91a] Haigh, J.T., R.C. O'Brien, and D.J. Thomsen, "The LDV Secure Relational DBMS Model," in *Database Security IV: Status and Prospects*, S. Jajodia and C. Landwehr, eds., North-Holland, Amsterdam, 1991, pp. 265-280.

[HARR76] Harrison, M.A., W.L. Ruzzo, and J.D. Ullman, "Protection in Operating Systems," *Comm. ACM*, Vol. 19, No. 8, Aug. 1976, pp. 461-471.

[HEBB80] Hebbard, B., et al., "A Penetration Analysis of the Michigan Terminal System," *ACM SIGOPS Operating System Rev.*, Vol. 14, No. 1, Jan. 1980, pp. 7-20.

[HINK75] Hinke, Thomas H., and Marvin Schaefer, "Secure Data Management System," Tech. Report RADC-TR-75-266, System Development Corp., Nov. 1975.

[HINK85] Hinke, Thomas H., and Marvin Schaefer, "Secure Data Management System," CARADC-TR-266 (AD-A019201), System Development Corp., Santa Monica, Calif., Nov. 1985.

[HINK88] Hinke, Thomas H., Cristi Garvey, Nancy Jensen, Jackson Wilson, and Amy Wu, "A1 Secure DBMS Design," *Proc. 11th Nat'l Computer Security Conf.: A Postscript*, Baltimore, Oct. 1988, pp. 1-13.

[HINK88a] Hinke, Thomas H., "Inference Aggregation Detection in Database Management Systems," *Proc. IEEE Symp. Research in Security and Privacy*, Apr. 1988, pp. 96-106.

[HINK89] Hinke, Thomas H., "The Trusted Server Approach to Multilevel Security," *Proc. 5th Annual Computer Security Applications Conf.*, Tucson, Ariz., Dec. 1989.

[HINK90] Hinke, Thomas H., "DBMS Trusted Computing Base Taxonomy," originally presented at Workshop on Database Security, IFIP Working Group 11.3, Monterey, Calif., Sept. 1989; published in *Database*

Security III: Status and Prospects, D.L. Spooner and C.E. Landwehr, eds., North-Holland, Amsterdam, 1990.

[HOLL74] Hollingworth, D., S. Glaseman, and M. Hopwood, "Security Test and Evaluation Tools: An Approach to Operating System Security Analysis," P-5298, Rand Corp., Santa Monica, Calif., Sept. 1974.

[HUMP89a] Humphreys, E.J., "Towards a Secure Messaging Environment," *Proc. European Seminar on Security in Comm. Networks*, London, 1989.

[HUMP89b] Humphreys, E.J., "Open Systems Security and the Impact on Business in Europe," *IT Security in the '90s — Threats and Countermeasures Conf.*, London, Nov. 1989.

[HUMP89c] Humphreys, E.J., "Security Standards for Open Systems," *Proc. Fifth Ann. Computer Security Applications Conf.*, IEEE Computer Society Press, Los Alamitos, Calif., 1989, p. 64 (and graphs used in a presentation).

[HUMP90a] Humphreys, E.J., "Overview of ISO/CCITT Security Standards for Open Systems," Danish Data Society 3rd EDP Conf., Feb. 1990.

[HUMP90b] Humphreys, E.J., "Open Systems Security, Paperless Trading and the Single European Market," *EDI: Letters of the Law Conf.*, Dallas, Feb. 1990.

[HUMP92a] Humphreys, Ted, ed., *Taxonomy of Security Standardisation: Version 2.0*, ITAEGV N69, XISEC Consultants Ltd., Apr. 30, 1992.

[HUMP92b] Open-EDI Security, SC27/WG1/N153, 1992.

[IEEE90] IEEE 802.10 (Editor at the LAN Security Working Group), Standard for Interoperable Local Area Network (LAN) Security (SILS), Part B — Secure Data Exchange, P802.10B/D2, Jan. 23, 1990.

[IRVI91] Irvine, C.E., R.R. Schell, and M.T. Thompson, "Using TNI Concepts for the Near Term Use of High Assurance Database Management Systems," *Proc. Fourth RADC Multilevel Database Security Workshop*, Apr. 22-25, 1991, pp. 107-121.

[ISO89] "Information Processing Systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture," ISO 7498-2, Feb. 1989.

[ISO90] Int'l Standards Organization (ISO), Working Draft on Access Control Framework, ISO/IEC JTC 1/SC 21 N5045, July 1990.

[ISO91a] ISO/IEC JTC 1/SC 27 (Int'l Organization for Standardization/Int'l Electrotechnical Commission, Joint Technical Committee 1 — Information Technology/Subcommittee 27 — Security Techniques), final text of ISO/IEC 9796, "Information Technology — Security Techniques — Digital Signature Scheme Giving Message Recovery," N289, July 7, 1991.

[ISO91b] ISO/IEC JTC 1/SC 27/WG2 (Int'l Organization for Standardization/Int'l Electrotechnical Commission, Joint Technical Committee 1 — Information Technology/Subcommittee 27 — Security Techniques; Working Group 2 — Techniques and Mechanisms), "CD 11166-2 — Banking Key Management by Means of Asymmetric Algorithms Part 2: Approved Algorithms Using the RSA," N102, Nov. 20, 1991.

[ISO91c] ISO/IEC JTC 1/SC 21 (Int'l Organization for Standardization/Int'l Electrotechnical Commission, Joint Technical Committee 1 — Information Technology/Subcommittee 21 — Information Retrieval, Transfer and Management for OSI), "Guide to Open Systems Security," N Project 97.21.9 Q53, Nov. 1991.

[ISO91d] ISO/IEC JTC 1/SC 21 (Int'l Organization for Standardization/Int'l Electrotechnical Commission, Joint Technical Committee 1 — Information Technology/Subcommittee 21 — Information Retrieval, Transfer and Management for OSI), Revised Text of CD 10181-2.2, "Information Technology — Open Systems Interconnection — Security Frameworks in Open Systems — Part 2: Authentication Framework," N5727 (DIS 10181-2), May 13, 1991.

[ISRA87] Israel, H., "Design of Originator Controls in a Computer System: A Trusted Discretionary Access Control Mechanism," *Proc. 3rd Symp. Physical/Electronic Security*, Armed Forces Communications and Electronics Assoc., Philadelphia, Aug. 1987, pp. 3#1-3#6.

[ITAE92a] "Taxonomy of Security Standardisation," Version 2.0, E.J. Humphreys, ed., Apr. 1992.

[ITAE92b] Information Technology Advisory Expert Group on Information Systems Security (ITAEGV), Memorandum M-IT-06 (Draft 2.0) on Taxonomy and Directory of European Standardisation Requirements for Information Systems Security, Oct. 12, 1992.

[ITSE90] "Information Technology Security Evaluation Criteria," Version 1, Der Bundesminister des Innern, Bonn, Germany, May 2, 1990.

[ITSE91] Commission of the European Communities, *Information Technology Security Evaluation Criteria* (ITSEC), Provisional Harmonized Criteria: Version 1.2, Office for Official Publications of the European Communities, Luxembourg, June 1991.

[ITSE92] Commission of the European Communities, *Information Technology Security Evaluation Manual* (ITSEM), Draft V0.2, Directorate — General XIII Telecommunications, Information Industries and Innovation, Directorate F — RACE [Research and Development in Advanced Communications Technology for Europe (for coordination of different systems and advanced communications technologies)] Programme and Development of Advanced Telematic Services, Brussels, Apr. 2, 1992.

[JAJO90] Jajodia, Sushil, and Ravi Sandhu, "Polyinstantiation Integrity in Multilevel Relations," *Proc. IEEE Symp. Research in Security and Privacy*, Oakland, Calif., May 1990.

[JAJO90a] Jajodia, Sushil, and Boris Kogan, "Integrating an Object-Oriented Data Model with Multilevel Security," *Proc. IEEE Symp. Security and Privacy*, Oakland, Calif., May 1990.

[JAJO90b] Jajodia, Sushil, and Boris Kogan, "Transaction Processing in Multilevel-Secure Databases Using Replicated Architecture," *Proc. IEEE Symp. Security and Privacy*, Oakland, Calif., May 1990.

[JAJO90c] Jajodia, Sushil, and Ravi Sandhu, "Polyinstantiation Integrity in Multilevel Relations," *Proc. IEEE Symp. Security and Privacy*, Oakland, Calif., May 1990, pp. 104-115.

[JAJO90d] Jajodia, Sushil, and Ravi Sandhu, "A Formal Framework for Single Level Decomposition of Multilevel Relations," *Proc. IEEE Workshop on Computer Security Foundations*, Franconia, N.H., June 1990, pp. 152-158.

[JAJO90e] Jajodia, Sushil, and Ravi Sandhu, "Database Security: Current Status and Key Issues," *ACM SIGMOD Record*, Vol. 19, No. 4, Dec. 1990, pp. 123-126.

[JAJO90f] Jajodia, Sushil, Ravi Sandhu, and Edgar Sibley, "Update Semantics of Multilevel Relations," *Proc. 6th Annual Computer Security Applications Conf.*, Dec. 1990, pp. 103-112.

[JAJ090g] Jajodia, Sushil, Shashi K. Gadia, Gautam Bhargava, and Edgar H. Sibley, "Audit Trail Organization in Relational Databases," in *Database Security III: Status and Prospects*, D.L. Spooner and C. Landwehr, eds., North-Holland, Amsterdam, 1990, pp. 269-281.

[JAJ091a] Jajodia, Sushil, and Ravi Sandhu, "Polyinstantiation Integrity in Multilevel Relations Revisited," *Database Security IV: Status and Prospects*, S. Jajodia and C.E. Landwehr, eds., North-Holland, Amsterdam, 1991, pp. 297-307.

[JAJ091b] Jajodia, Sushil, and Ravi Sandhu, "A Novel Decomposition of Multilevel Relations into Single-Level Relations," *Proc. IEEE Symp. Security and Privacy*, Oakland, Calif., May 1991, pp. 300-313.

[JAJ091c] Jajodia, Sushil, and Ravi Sandhu, "Toward a Multilevel Secure Relational Data Model," *Proc. ACM SIGMOD Int'l Conf. Management of Data*, Denver, May 29-31, 1991, pp. 50-59.

[JAJ091d] Jajodia, Sushil, and Ravi S. Sandhu, "Enforcing Primary Key Requirements in Multilevel Relations," *Proc. 4th RADC Workshop on Multilevel Database Security*, Little Compton, R.I., Apr. 1991.

[JTC191] "Report on the Open-EDI Conceptual Model JTC1/N1384" (SC27/WG1/N130), 1991.

[KAHN67] Kahn, David, *The Codebreakers*, Macmillan, New York, 1967, pp. 67, 591.

[KALA93] Kalaski, B., "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services," RFC 1424, Feb. 1993.

[KARG74] Karger, P.A., and R.R. Schell, *Multics Security Evaluation: Vulnerability Analysis*, ESD-TR-74-193, Vol. 2, Hanscom AFB, Mass., 1974 (also available as NTIS AD-A001120).

[KARG89] Karger, P.A., "New Methods for Immediate Revocation," *Proc. Symp. Security and Privacy*, IEEE, New York, May 1989, pp. 48-55.

[KARG91] Karger, P.A., M.E. Zurko, D.W. Bonin, A.H. Mason, and C.E. Kahn, "A Retrospective of the VAX VMM Security Kernel," *IEEE Trans. Software Eng.*, Vol. 17, No. 11, Nov. 1991, pp. 1147-1165.

[KEEF88] Keefe, T.F., and W.T. Tsai, "Prototyping the SODA Security Model," *Database Security III: Status and Prospects*, David L. Spooner and Carl Landwehr, eds., North-Holland, Amsterdam, 1990, pp. 211-235.

[KEEF88a] Keefe, T.F., W.T. Tsai, and M.B. Thuraisingham, "A Multilevel Security Model for Object-Oriented System," *Proc. 11th Nat'l Computer Security Conf.*, Oct. 1988, pp. 1-9.

[KEEF89] Keefe, T., W. Tsai, and B. Thuraisingham, "SODA: A Secure Object-Oriented Database System," *Computers and Security*, Vol. 8, Oct. 1990.

[KEMM86] Kemmerer, R.A., "Verification Assessment Study Final Report, Vol. I, Overview, Conclusions, and Future Directions," C3-R01-86, Library No. SW-228, 204, Dept. of Computer Science, Univ. of California, Santa Barbara, Mar. 27, 1986.

[KENS92] Smith, Ken, and Marianne Winslett, "Entity Modeling in the MLS Relational Model," *Proc. 18th Int'l Conf. Very Large Data Bases*, Aug. 1992, pp. 199-210.

[KENT89] Kent, S., and J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part II — Certificate-Based Key Management," [Internet] RFC 1114, Aug. 1989.

[KENT90] Kent, S., and K. Rossen, "E-Mail Privacy for the Internet," *Business Comm. Rev.*, Vol. 20, No. 1, Jan. 1990.

[KENT93] Kent, S., "Privacy Enhancement for Internet Electronic Mail: Part II — Certificate-Based Key Management," RFC 1422, Feb. 1993.

[KIM89] Kim, Won, and Frederick H. Lochovsky, eds., *Object-Oriented Concepts, Databases, and Applications*, Addison-Wesley, Reading, Mass., 1989.

[KIRK77] Kirkby, G., and M.J. Grohn, "On Specifying the Functional Design of a Protected DMS Tool," I.P. Sharp Associates, Mar. 1977.

[KLEI90] Klein, Daniel V., "Foiling the Cracker: A Survey of, and Improvements to, Password Security," *Proc. UNIX Security Workshop II*, USENIX Assoc., Aug. 1990.

[KNOD88] Knode, Ronald B., and Roger A. Hunt, "Making Database Secure with TRUDATA Technology," *Proc. Fourth Aerospace Computer Security Applications Conf.*, Orlando, Fla., Dec. 1988, pp. 82-90.

[KOH78] Kohnfelder, L.M., "A Method for Certification," MIT Laboratory for Computer Science, Cambridge, Mass., May 1978.

[KRAJ92] Krajewski, M., "Concept for a Smart Card Kerberos," *Proc. 15th Nat'l Computer Security Conf.*, Baltimore, Oct. 1992, pp. 76-83.

[KRAM83] Kramer, S., "The MITRE Flow Table Generator — Vol. I," M83-31, Vol. 1, MITRE Corp., Bedford, Mass., Jan. 1983.

[KURA92] Kurak, C., and J. McHugh, "A Cautionary Note on Image Downgrading," *Proc. Eighth Annual Computer Security Applications Conf.*, IEEE Computer Society Press, Los Alamitos, Calif., Dec. 1992, pp. 153-159.

[LACK74] Lackey, R.D., "Penetration of Computer Systems, an Overview," *Honeywell Computer J.*, Vol. 8, No. 2, 1974.

[LAMP71] Lampson, B.W., "Protection," *Proc. Fifth Princeton Symp. Information Sciences and Systems*, Princeton Univ., Princeton, N.J., Mar. 1971, pp. 437-443, reprinted in *Operating Systems Rev.*, Vol. 8, No. 1, Jan. 1974, pp. 18-24.

[LAMP73] Lampson, B.W., "A Note on the Confinement Problem," *Comm. ACM*, Vol. 16, No. 10, Oct. 1973, pp. 613-615.

[LAMP91] Lampson, B.W., M. Abadi, M. Burrows, and E. Wobber, "Authentication in Distributed Systems: Theory and Practice," *Operating Systems Rev.*, Vol. 25, No. 5, Oct. 1991, pp. 165-182.

[LAND81] Landwehr, Carl E., "Formal Models for Computer Security," *ACM Computing Surveys*, Vol. 13, No. 3, Sept. 1981, pp. 247-278.

[LAND84] Landwehr, Carl E., Connie L. Heitmeyer, and John McLean, "A Security Model for Military Message Systems," *ACM Trans. Computer Systems*, Vol. 2, No. 3, Aug. 1984, pp. 198-222.

[LAPA90] LaPadula, L.J., "Formal Modeling in a Generalized Framework for Access Control," *Proc. IEEE Computer Security Foundations Workshop III*, June 1990, pp. 100-109.

[LAPA91] LaPadula, L.J., "A Rule-Base Approach to Formal Modeling of a Trusted Computer System," M91-021, MITRE Corp., Aug. 1991.

[LEE88] Lee, T.M.P., "Using Mandatory Integrity to Enforce 'Commercial' Security," *Proc. IEEE Computer Society Symp. Security and Privacy*, IEEE Computer Society Press, Los Alamitos, Calif., May 1988, pp. 140-146.

- [LEFK89] Lefkovits, Henry C., et al., "Multilevel Secure Entity-Relationship DBMS, Final Technical Report," RADC-TR-88-310, Jan. 1989.
- [LEVI89] Levin, T.E., S.J. Padilla, and C.E. Irvine, "A Formal Model for UNIX Setuid," *Proc. IEEE Computer Society Symp. Security and Privacy*, IEEE Computer Society Press, Los Alamitos, Calif., May 1989, pp. 73-83.
- [LEVI90] Levin, T.E., A. Tao, and S.J. Padilla, "Covert Storage Channel Analysis: A Worked Example," *Proc. 13th Nat'l Computer Security Conf.*, Oct. 1990, pp. 10-19.
- [LIND75] Linde, R.R., "Operating System Penetration," *Proc. Nat'l Computer Conf.*, Vol. 44, AFIPS Press, Montvale, N.J., 1975.
- [LIND76] Linden, T.A., "Operating System Structures to Support Security and Reliable Software," *ACM Computing Surveys*, Vol. 8, No. 4, 1976, pp. 409-445.
- [LIND76a] Linde, R.R., and R.F. von Buelow, "EXEC-8 Security Analysis," Memo. Report 3205, Naval Research Laboratory, Jan. 1976.
- [LINN86] Linn, J., and S. Kent, "Electronic Mail Privacy Enhancement," *Proc. Second Aerospace Computer Security Conf.*, Dec. 1986.
- [LINN89a] Linn, J., "Privacy Enhancement for Internet Electronic Mail: Part I — Message Encipherment and Authentication Procedures," [Internet] RFC 1113, Aug. 1989.
- [LINN89b] Linn, J., "Privacy Enhancement for Internet Electronic Mail: Part III — Algorithms, Modes, and Identifiers," [Internet] RFC 1115, Aug. 1989.
- [LINN93] Linn, J., "Privacy Enhancement for Internet Electronic Mail: Part I — Message Encipherment and Authentication Procedures," RFC 1421, Feb. 1993.
- [LIPN82] Lipner, S.B., "Non-Discretionary Controls for Commercial Applications," *Proc. IEEE Computer Society Symp. Security and Privacy*, IEEE Computer Society Press, Los Alamitos, Calif., May 1982, pp. 2-10.
- [LUM87] Lum, V., et al., "Designing DBMS Support for the Temporal Dimension," *Proc. ACM SIGMOD Int'l Conf. Management of Data*, May 1987, pp. 115-130.

[LUNT88] Lunt, Teresa F., Roger R. Schell, William R. Schockley, M. Heckman, and B. Warren, "A Near-Term Design for the SeaView Multi-level Database System," *Proc. IEEE Symp. Security and Privacy*, Oakland, Calif., May 1988, pp. 234-244.

[LUNT88a] Lunt, T.F., P.G. Neumann, D.E. Denning, R.R. Schell, M. Heckman, and W.R. Shockley, "Secure Distributed Data Views: Security Policy and Interpretation for Database Management System for a Class A1 DBMS," RADDC-TR-89-313, Vol. 1 of 5, Rome Labs, Griffiss AFB, Rome, N.Y., 1988.

[LUNT88b] Lunt, T.F., D.E. Denning, R.R. Schell, M. Heckman, and W.R. Shockley, "Element-Level Classification with A1 Assurance," *Computers and Security*, Vol. 7, 1988, pp. 73-82.

[LUNT89] Lunt, Teresa F., "Multilevel Security for Object-Oriented Database Systems," *Proc. IFIP WG 11.3 Workshop on Database Security*, Monterey, Calif., Sept. 1989.

[LUNT89a] Lunt, T.F., "Aggregation and Inference: Facts and Fallacies," *Proc. IEEE Symp. Research in Security and Privacy*, May 1989, pp. 102-109.

[LUNT89b] Lunt, Teresa F., and Jonathan K. Millen, "Secure Knowledge-Based Systems," Interim Tech. Report, Computer Science Laboratory, SRI Int'l, Aug. 1989.

[LUNT89c] Lunt, T.F., et al., *Secure Distributed Data Views*, Vols. 1-4, SRI Project 1143, SRI Int'l, 1988-1989.

[LUNT90] Lunt, Teresa F., Dorothy E. Denning, Roger R. Schell, M. Heckman, D. Warren, and William R. Schockley, "The SeaView Security Model," *IEEE Trans. Software Eng.*, Vol. 16, No. 6, June 1990, pp. 593-607.

[LUNT90a] Lunt, Teresa F., Dorothy E. Denning, Roger R. Schell, and William R. Shockley, "The SeaView Security Model," *IEEE Trans. Software Eng.*, Vol. 15, No. 6, June 1990.

[LUNT90b] Lunt, Teresa F., and Donovan Hsieh, "Update Semantics for a Multilevel Relational Database System," *Proc. Fourth IFIP Working Group: 11.3 Workshop on Database Security*, Halifax, U.K., Sept. 1990.

[LUNT90c] Lunt, Teresa F., and Donovan Hsieh, "The SeaView Secure Database System: A Progress Report," *Proc. European Symp. Research on Computer Security (ESORICS 90)*, Toulouse, France, Oct. 1990.

[LUNT90d] Lunt, Teresa F., "Multilevel Security for Object-Oriented Database Systems," in *Database Security III: Status and Prospects*, D.L. Spooner and C. Landwehr, eds., North-Holland, Amsterdam, 1990, pp. 199-210.

[LUNT91] Lunt, Teresa F., and Donovan Hsieh, "Update Semantics for a Multilevel Relational Database System," in *Database Security IV: Status and Prospects*, S. Jajodia and C. Landwehr, eds., North-Holland, Amsterdam, 1991, pp. 281-296.

[LUNT92] Lunt, T.E., et al., "A Real-Time Intrusion Detection Expert System (IDES) — Final Tech. Report," SRI Int'l, Menlo Park, Calif., Feb. 1992.

[MAZU88] Mazumdar, S., D. Stemple, and T. Sheard, "Resolving the Tension between Integrity and Security Using a Theorem Prover," *Proc. ACM Int'l Conf. Management of Data*, ACM, New York, 1988, pp. 233-242.

[MCAU92] McAuliffe, N., "Extending Our Hardware Base: A Worked Example," *Proc. 15th Nat'l Computer Security Conf.*, Baltimore, Oct. 1992, pp. 184-193.

[MCCO90] McCollum, C.J., J.R. Messing, and L. Notargiacomo, "Beyond the Pale of MAC and DAC: Defining New Forms of Access Control," *Proc. IEEE Symp. Research in Security and Privacy*, May 1990, pp. 190-200.

[MCCO91] McCollum, Catherine J., and LouAnna Notargiacomo, "Distributed Concurrency Control with Optional Data Replication," *Proc. IFIP WG 11.3 Workshop on Database Security*, Shepardstown, W.Va., Nov. 1991.

[MCLE85] McLean, J., "A Comment on the 'Basic Security Theorem' of Bell and LaPadula," *Information Processing Letters*, Vol. 20, Feb. 1985, pp. 67-70.

[MCPH74] McPhee, W.S., "Operating System Integrity in OS/VS2," *IBM Systems J.*, No. 3, 1974, pp. 231-252.

[MEAD88a] Meadows, Catherine, and Sushil Jajodia, "Integrity versus Security in Multi-Level Secure Databases," in *Database Security: Status and Prospects*, C. Landwehr, ed., North-Holland, Amsterdam, 1988, pp. 89-101.

[MEAD88b] Meadows, Catherine, and Sushil Jajodia, "Maintaining Correctness, Availability, and Unambiguity in Trusted Database Management Systems," *Proc. 4th Aerospace Computer Security Applications Conf.*, Dec. 1988, pp. 106-110.

[MEAD90] Meadows, Catherine, "Aggregation Problems: A Position Paper," *Proc. 3rd RADC Workshop in Multilevel Security*, June 1990.

[MEAD90a] Meadows, C.A., "Extending the Brewer-Nash Model to a Multilevel Context," *Proc. IEEE Symp. Research in Security and Privacy*, May 1990, pp. 95-102.

[MEAD92] Meadows, Catherine, and Carl Landwehr, "Designing a Trusted Application in an Object-Oriented Data Model," in *Directions in Database Security*, Teresa Lunt, ed., Springer-Verlag, Berlin, 1992.

[MEND79] Mendelson, E., *Introduction to Mathematical Logic*, D. Van Nostrand, 1979.

[MERK82] Merkle, R.C., *Secrecy, Authentication, and Public Key Systems*, UMI Research Press, Ann Arbor, Mich., 1982.

[MILL84] Millen, J.K., "A1 Policy Modeling," *7th DoD/NBS Computer Security Conf.*, Sept. 1984, pp. 137-145.

[MILL90] Millen, J.K., and D.J. Bodeau, "A Dual-Label Model for the Compartmented Mode Workstation," M90-51, MITRE Corp., Bedford, Mass., Aug. 1990.

[MILL91] Millen, J.K., and D.J. Bodeau, "Report on Computer Security Foundations Workshop IV," *Cipher*, 1991.

[MILL92] Millen, Jonathan K., and Teresa F. Lunt, "Security for Object-Oriented Database Systems," *Proc. IEEE Symp. Research in Security and Privacy*, May 1992.

[MINS87] Minsky, Naftaly H., and David Rozenshtein, "A Law-Based Approach to Object-Oriented Programming," *Proc. Conf. Object-Oriented Programming: Systems, Languages, Applications*, Oct. 1987, pp. 482-493.

[MOFF88] Moffett, J.D., and M.S. Sloman, "The Source of Authority for Commercial Access Control," *Computer*, Vol. 21, No. 2, 1988, pp. 59-69.

[MOOR90] Moore, A.P., "The Specification and Verified Decomposition of System Requirements Using CSP," *IEEE Trans. Software Eng.*, Vol. 16, No. 9, Sept. 1990, pp. 932-948.

[MORG88] Morgenstern, Matthew, "Controlling Logical Inference in Multilevel Database Systems," *Proc. Symp. Security and Privacy*, Apr. 1988, pp. 245-255.

[MUFF4a] Muffett, A.D.E., "Crack Version 4.0a, A Sensible Password Checker for Unix," Computer Unit, Univ. College of Wales, Aberystwyth, Wales (software available by anonymous ftp from cert@sei.cmu.edu).

[MURR87a] Murray, W.H., "Data Integrity in a Business Data Processing System," in [NIST87].

[MURR87b] Murray, W.H., "On the Use of Mandatory," in [NIST87].

[MYER80] Myers, P.A., *Subversion: The Neglected Aspect of Computer Security*, master's thesis, Naval Postgraduate School, Monterey, Calif., 1980.

[NCSC85] Nat'l Computer Security Center, *Dept. of Defense Trusted Computer Security Evaluation Criteria*, DOD 5200.28-STD, Dec. 1985.

[NCSC87a] Nat'l Computer Security Center, *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria*, NCSC-TG-005, July 31, 1987.

[NCSC87b] Nat'l Computer Security Center, *A Guide to Understanding Discretionary Access Control in Trusted Systems*, NCSC-TG-003, Version 1, 1987.

[NCSC88] Nat'l Computer Security Center, *A Guide to Understanding Audit in Trusted Systems*, June 1, 1988.

[NCSC88a] Nat'l Computer Security Center, *Trusted Network, Glossary of Computer Security Terms*, NCSC-TG-004, Oct. 1988.

[NCSC88b] Nat'l Computer Security Center, "Trusted Product Evaluations — A Guide for Vendors," draft, Mar. 1, 1988.

[NCSC88c] Nat'l Computer Security Center, "Trusted Network Testing Guideline," NCSC-TG-010, Version 1, draft, Aug. 1988.

[NCSC89] Nat'l Computer Security Center, *Guidelines for Formal Verification Systems*, Version 1, NCSC-TG-014, Apr. 1989.

[NCSC89a] Nat'l Computer Security Center, *Rating Maintenance Phase — Program Document*, NCSC-TG-013, Version 1, June 23, 1989.

[NCSC91] Nat'l Computer Security Center, *Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria*, NCSC-TG-021, Apr. 1991.

[NCSC91a] Nat'l Computer Security Center, "Integrity in Automated Information Systems," C Tech. Report 79-91, Sept. 1991.

[NCSC91b] Nat'l Computer Security Center, *Final Evaluation Report, SecureWare Incorporated, Compartmented Mode Workstation Plus*, Jan. 1991.

[NCSC92] Nat'l Computer Security Center, *Trusted Product Evaluation Questionnaire*, NCSC-TG-019, Version 2, May 2, 1992.

[NECH91] Nechvatal, James, "Public-Key Cryptography," Special Publication 800-2, Nat'l Inst. of Standards and Technology, US Dept. of Commerce, Apr. 1991.

[NEED78] Needham, R.M., and M.D. Schroeder, "Using Encryption for Authentication in Large Networks of Computers," *Comm. ACM*, Vol. 21, No. 12, Dec. 1978, pp. 993-999.

[NELS91] Nelson, Doug, and Chip Paradise, "Using Polyinstantiation to Develop an MLS Application," *Proc. IEEE 7th Annual Computer Security Applications Conf.*, Dec. 1991, pp. 12-22.

[NEUM89] Neumann, P.G., and D.B. Parker, "A Summary of Computer Misuse Techniques," *Proc. 12th Nat'l Computer Security Conf.*, Oct. 1989, pp. 396-407.

[NIER89] Nierstrasz, Oscar, "A Survey of Object-Oriented Concepts," in *Object-Oriented Concepts, Databases, and Applications*, W. Kim and F.H. Lochovsky, eds., Addison-Wesley, Reading, Mass., 1989, pp. 3-21.

[NIST80] Nat'l Inst. of Standards and Technology, "DES Modes of Operation," Dec. 1980. A companion ISO standard is IS8372.

[NIST87] *Report of the Invitational Workshop on Integrity Policy in Computer Information Systems (WIPCIS)*, S.W. Katzke and Z.G. Ruthberg, eds., Special Publication 500-160, NIST, Jan. 1989.

[NIST89] *Report of the Invitational Workshop on Data Integrity*, Z.G. Ruthberg and W.T. Polk, eds., Special Publication 500-168, NIST, Sept. 1989.

[NIST91] Burr, William E., *Security in ISDN*, Special Publication 500-189, NIST, Sept. 1991.

[NIST92] Nat'l Inst. of Standards and Technology (NIST) and Nat'l Security Agency (NSA), *Federal Criteria for Information Technology Security: Vol. I, Protection Profile Development; Vol. II, Registry of Protection Profiles*, Version 1.0, Dec. 1992.

[OCON88] O'Connor, James P., and James W. Gray, "A Distributed Architecture for Multilevel Database Security," *Proc. 11th Nat'l Computer Security Conf.*, Baltimore, Oct. 1988, pp. 179-187.

[OLSO90] Olson, I.M., and M.D. Abrams, "Computer Access Control Policy Choices," *Computers and Security*, Vol. 9, No. 8, Dec. 1990, pp. 699-714.

[OMB82] Office of Management and Budget, "Internal Control Guidelines: Guidelines for the Evaluation and Improvement of and Reporting on Internal Control Systems in the Federal Government," Dec. 1982.

[OMB84] Office of Management and Budget, "Financial Management Systems," OMB Circular No. A-127, Dec. 1984.

[PADL82] Padlipsky, M.A., TCP-on-a-LAN, RFC 872, M82-48, Sept. 1982.

[PAGE89] Page, J., J. Heaney, M. Adkins, and G. Dolsen, "Evaluation of Security Model Rule Bases," *Proc. Nat'l Computer Security Conf.*, 1989.

[PARK75] Parker, D.B., "Computer Abuse Perpetrators and Vulnerabilities of Computer Systems," Stanford Research Inst., Menlo Park, Calif., Dec. 1975.

[PARK91] Parker, D.B., "An Essay: Restating the Foundation of Information Security," *ISP News*, May/June 1991, pp. 23-27.

[PARN72a] Parnas, D.L., "A Technique for Software Module Specification with Examples," *Comm. ACM*, Vol. 15, No. 5, May 1972, pp. 330-336.

[PARN72b] Parnas, D.L., "On the Criteria to Be Used in Decomposing Systems into Modules," *Comm. ACM*, Vol. 15, No. 12, Dec. 1972, pp. 1053-1058.

[PHIL73] Phillips, R., "VM/370 Penetration Study Final Report," TM(L)-5196/006/00, System Development Corp., Santa Monica, Calif., Oct. 1973.

[POPE79] Popek, G.L., and C.S. Kline, "Encryption and Secure Networks," *ACM Computing Surveys*, Vol. 11, No. 4, Dec. 1979, pp. 331-356.

[POST82] Postel, J., "Simple Mail Transfer Protocol," [Internet] RFC 821, Aug. 1982.

[RABI88] Rabitti, Fausto, Darrell Woelk, and Won Kim, "A Model of Authorization for Object-Oriented and Semantic Databases," *Proc. Conf. Extending Database Technology*, Mar. 1988, pp. 231-250.

[REAG82] Reagan, R.L., Executive Order 12356, US Government Printing Office, Apr. 1982.

[RFC1038] "Revised Internet Protocol Security Options, RIPS0," RFC 1038, Network Information Center. See also RFC 791 and RFC 1108.

[ROCH89] Rochlis, Jon, and Mark Eichen, "With Microscope and Tweezers: The Worm from MIT's Perspective," *Comm. ACM*, June 1989, pp. 689-698.

[ROSE91] Rose, M., "Post Office Protocol: Version 3," [Internet] RFC 1225, May 1991.

[ROUG87] Rougeau, Patricia A., and Edward D. Sturms, "The Sybase Secure Dataserver: A Solution to the Multilevel Secure DBMS Problem," *Proc. 10th Nat'l Computer Security Conf.*, Baltimore, Sept. 1987, pp. 211-215.

[RSAD91] "Public-Key Cryptography Standards," RSA Data Security Inc., June 1991.

[RUB86] Rub, J.W., "Penetration Handbook," Aerospace Corp., El Segundo, Calif., Jan. 1986.

[SALT75] Saltzer, J.H., and M.D. Schroeder, "The Protection of Information in Computer Systems," *Proc. IEEE*, Vol. 63, No. 9, Sept. 1975, pp. 1278-1308.

[SAND88a] Sandhu, R.S., "The Schematic Protection Model: Its Definition and Analysis for Acyclic Attenuating Schemes," *J. ACM*, Vol. 35, No. 2, 1988, pp. 404-432.

[SAND88b] Sandhu, R.S., "Transaction Control Expressions for Separation of Duties," *4th Aerospace Computer Security Applications Conf.*, 1988, pp. 282-286.

[SAND89] Sandhu, R.S., "Transformation of Access Rights," *Proc. IEEE Symp. Security and Privacy*, 1989, pp. 259-268.

[SAND90] Sandhu, R.S., "Mandatory Controls for Database Integrity," in *Database Security III: Status and Prospects*, D.L. Spooner and C.E. Landwehr, eds., North-Holland, Amsterdam, 1990, pp. 143-150.

[SAND90a] Sandhu, Ravi, Sushil Jajodia, and Teresa Lunt, "A New Polyinstantiation Integrity Constraint for Multilevel Relations," *Proc. IEEE Workshop on Computer Security Foundations*, Franconia, N.H., June 1990, pp. 159-165.

[SAND90b] Sandhu, Ravi, and Sushil Jajodia, "Integrity Mechanisms in Database Management Systems," *Proc. 13th NIST-NCSC Nat'l Computer Security Conf.*, Washington, D.C., Oct. 1990, pp. 526-540.

[SAND91] Sandhu, Ravi, and Sushil Jajodia, "Honest Databases That Can Keep Secrets," *Proc. 14th NIST-NCSC Nat'l Computer Security Conf.*, Washington, D.C., Oct. 1991, pp. 267-282.

[SAND92a] Sandhu, Ravi, Roshan Thomas, and Sushil Jajodia, "Supporting Timing Channel Free Computations in Multilevel Secure Object-Oriented Databases," in *Database Security V: Status and Prospects*, Carl E. Landwehr and Sushil Jajodia, eds., North-Holland, Amsterdam, 1992, pp. 297-314.

[SAND92b] Sandhu, Ravi S., and Sushil Jajodia, "Eliminating Polyinstantiation Securely," *Computers and Security*, Vol. 11, 1992, pp. 547-562.

[SAND92c] Sandhu, Ravi S., and Sushil Jajodia, "Polyinstantiation for Cover Stories," *Proc. European Symp. Research in Computer Security*, Toulouse, France, Lecture Notes in Computer Science, Vol. 648, Springer-Verlag, Berlin, 1992, pp. 307-328.

[SAYD87] Saydjari, O.S., and J.M. Beckman, "Locking Computers Securely," *10th Nat'l Computer Security Conf.*, NCSC/ICST, Sept. 1987, pp. 129-141.

[SC2792] "Guidelines on the Use and Management of Trusted Third Party Services," study document (SC27/WG1/N331), 1992.

[SCHA83] Schaefer, Marvin, ed., *Multilevel Data Management Security*, Air Force Studies Board, Committee on Multilevel Data Management Security, Nat'l Academy Press, Washington, D.C., 1983.

[SCHA84] Schaefer, M., and R.R. Schell, "Toward an Understanding of Extensible Architectures for Evaluated Trusted Computer System Products," *Proc. IEEE Symp. Security and Privacy*, Apr. 1984, pp. 41-49.

[SCHA89] Schaefer, M., "Symbol Security Condition Considered Harmful," *Proc. IEEE Symp. Security and Privacy*, May 1989, pp. 20-46.

[SCHA90] Schaefer, Marvin, "Reflections on Current Issues in Trusted DBMS," in *Database Security IV: Status and Prospects*, S. Jajodia and Carl E. Landwehr, eds., North-Holland, Amsterdam, 1991.

[SCHE74] Schell, R.R., "Effectiveness — The Reason for a Security Kernel," *Proc. Nat'l Computer Conf.*, 1974, pp. 975-976.

[SCHE79] Schell, R.R., "Computer Security: The Achilles' Heel of the Electronic Air Force," *Air Univ. Rev.*, Jan.-Feb. 1979, pp. 16-33.

[SCHE83] Schell, R.R., "A Security Kernel for a Multiprocessor Microcomputer," *Computer*, Vol. 16, No. 7, July 1983, pp. 47-53.

[SCHE84] Schell, R.R., "The Future of Trusted Computer Systems," *Computer Security: A Global Challenge, Proc. Second IFIP Int'l Conf. Computer Security*, J.H. Finch and E.G. Dougall, eds., 1984, pp. 55-67.

[SCHE84a] Schell, R.R., "Security Kernel Design Principles," Auerbach 84-02-07, 1984.

[SCHE85] Schell, R.R., "Position Statement on Network Security Policy and Models," *Proc. Dept. of Defense Computer Security Center Invitational Workshop on Network Security*, Mar. 1985, pp. 2-61-2-70.

[SCHE85a] Schell, R.R., T.F. Tao, and M. Heckman, "Designing the GEMSOS Security Kernel for Security and Performance," *Proc. 8th Nat'l Computer Security Conf.*, 1985, pp. 108-119.

[SCHE86] Schell, R.R., and D.E. Denning, "Integrity in Trusted Database Systems," *Proc. 9th Nat'l Computer Security Conf.*, 1986, pp. 30-36.

[SCHK82] Schkolnick, M., and P. Sorenson, "The Effects of Denormalization on Database Performance," *Australian Computer J.*, Vol. 14, No. 1, Feb. 1982, pp. 12-18.

[SCHN85] Schnackenberg, D.D., "Development of a Multilevel Secure Local Area Network," *Proc. 8th Nat'l Computer Security Conf.*, Oct. 1985, pp. 97-101.

[SCHO87] Shockley, W.D., and R.R. Schell, "TCB Subsets for Incremental Evaluation," *Proc. Third Aerospace Computer Security Conf.*, Orlando, Fla., Dec. 1987, pp. 131-139.

[SCHR72] Schroeder, M.D., and J.H. Saltzer, "A Hardware Architecture for Implementing Protection Rings," *Comm. ACM*, Vol. 15, No. 3, Sept. 1981, pp. 157-170.

[SDC75] "Fujitsu, Ltd., Security/Privacy Report," TM(L)-5593/000/00, System Development Corp., Santa Monica, Calif., Oct. 1975.

[SDC76] "A Security and Integrity Analysis of OS/VS2 Release 3," TM-5662/000/00, System Development Corp., Santa Monica, Calif., Apr. 1976.

[SELI80] Selinger, P.G., "Authorization and Views," in *Distributed Data Bases*, I.W. Draffan and F. Poole, eds., Cambridge Univ. Press, Cambridge, UK, 1980, pp. 233-246.

[SHIR81] Shirley, L.J., and R. Schell, "Mechanism Sufficiency Validation by Assignment," *Proc. IEEE Symp. Security and Privacy*, Apr. 1981, pp. 26-32.

[SHOC87] Shockley, William D., and Roger R. Schell, "TCB Subsets for Incremental Evaluation," *Proc. AIAA/ASIS/IEEE Third Aerospace Computer Security Conf.*, Orlando, Fla., Dec. 1987, pp. 131-139.

[SHOC88] Shockley, W.R., "Implementing the Clark/Wilson Integrity Policy Using Current Technology," *Proc. 11th Nat'l Computer Security Conf.*, Oct. 1988, pp. 29-37.

[SHOC88a] Shockley, W.R., T.F. Tao, and M.F. Thompson, "An Overview of the GEMSOS Class A1 Technology and Application Experience," *Proc. 11th Nat'l Computer Security Conf.*, Oct. 1988, pp. 238-245.

[SHOC88b] Shockley, W.R., R.R. Schell, and M.F. Thompson, "The Importance of High Assurance Computers for Command, Control, Communications, and Intelligence Systems," *Proc. Fourth Aerospace Computer Security Applications Conf.*, Dec. 1988, pp. 331-342.

[SICH83] Sicherman, G.L., W. de Jonge, and R.P. van de Riet, "Answering Queries without Revealing Secrets," *ACM Trans. Database Systems*, Mar. 1983, Vol. 8, No. 1, pp. 41-59.

[SIMP90] Simpact Associates, Inc., "Security in Electronic Messaging: Things You Should Know," 1990.

[SMAH88] Smaha, S.E., "Haystack: An Intrusion Detection System," *Proc. IEEE Fourth Aerospace Computer Security Applications Conf.*, Orlando, Fla., Dec. 1988.

[SMIT88] Smith, G.W., "Identifying and Representing the Security Semantics of an Application," *Proc. IEEE Fourth Aerospace Computer Security Applications Conf.*, Orlando, Fla., Dec. 1988, pp. 125-130.

[SMIT90] Smith, Gary W., "Modeling Security-Relevant Data Semantics," *Proc. IEEE Symp. Research in Security and Privacy*, May 1990, pp. 384-391.

[SMIT90a] Smith, Gary W., *The Modeling and Representation of Security Semantics for Database Applications*, doctoral dissertation, George Mason Univ., Fairfax, Va., 1990.

[SNOD86] Snodgrass, Richard, and Ilsoo Ahn, "Temporal Databases," *Computer*, Vol. 19, No. 3, Sept. 1986, pp. 35-42.

[SNOD87] Snodgrass, Richard, "The Temporal Query Language TQuel," *ACM Trans. Database Systems*, Vol. 12, No. 2, June 1987, pp. 247-298.

[SNYD81] Snyder, L., "Formal Models of Capability-Based Protection Systems," *IEEE Trans. Computers*, Vol. C-30, No. 3, 1981, pp. 172-181.

[SOGI89] Senior Official Group for IT Standards, "Security in Open Networks (SOGITS) Report," Jan. 1989.

[SPAF89] Spafford, E.H., "The Internet Worm: Crisis and Aftermath," *Comm. ACM*, Vol. 32, No. 6, June 1989, pp. 678-688.

[SPAF89a] See [SPAF89].

[SPAF90a] Spafford, Eugene H., Kathleen A. Heaphy, and David J. Ferbrache, "What Is a Computer Virus?" in *Rogue Programs: Viruses, Worms, and Trojan Horses*, Lance J. Hoffman, ed., 1990, pp. 29-42.

[SPAF90b] Spafford, Eugene H., Kathleen A. Heaphy, and David J. Ferbrache, "Further Information on Viruses," in *Rogue Programs: Viruses, Worms, and Trojan Horses*, Lance J. Hoffman, ed., 1990, pp. 173-179.

[SPAF90c] Spafford, Eugene H., "The Internet Worm Incident," in *Rogue Programs: Viruses, Worms, and Trojan Horses*, Lance J. Hoffman, ed., 1990, pp. 203-227.

[SPOO89] Spooner, David L., "The Impact of Inheritance on Security in Object-Oriented Database Systems," *Database Security II: Status and Prospects*, Carl E. Landwehr, ed., North-Holland, Amsterdam, 1989, pp. 141-160.

[SSSC91] System Security Study Committee; Computer Science and Telecommunications Board; Commission on Physical Sciences, Mathematics, and Applications; National Research Council, *Computers at Risk: Safe Computing in the Information Age*, Nat'l Academy Press, 1991.

[STAC90] Stachour, Paul D., and Bhavani Thuraisingham, "Design of LDV: A Multilevel Secure Relational Database Management System," *IEEE Trans. Knowledge and Data Eng.*, Vol. 2, No. 2, June 1990, pp. 190-209.

[STEF90] Stefanac, Suzanne, "Mad Macs," in *Rogue Programs: Viruses, Worms, and Trojan Horses*, Lance J. Hoffman, ed., 1990, pp. 180-193.

[STER91] Sterne, D.F., "On the Buzzword 'Security Policy,'" *Proc. IEEE Computer Society Symp. Research in Security and Privacy*, IEEE Computer Society Press, Los Alamitos, Calif., May 1991, pp. 219-230.

[STER91b] Sterne, Daniel F., Martha A. Branstad, Brian S. Hubbard, Barbara A. Mayer, and Dawn M. Wolcott, "An Analysis of Application Specific Security Policies," *Proc. 14th Nat'l Computer Security Conf.*, Nat'l Computer Security Center, Oct. 1991.

[STOL89] Stoll, C., *The Cuckoo's Egg*, Doubleday, New York, 1989.

[STON74] Stonebraker, M., "Implementation of Integrity Constraints and Views by Query Modification," *ACM Nat'l Conf. Proc.*, 1974, pp. 180-186.

[STRA92] Stranger, Jon, "EWOS/ETSI Report," Minutes of Mar. 9-12, 1992, X.400 SIG Meeting, Nat'l Inst. of Standards and Technology OSI Implementers Workshop (NIST OIW), X.400 SIG (Special Interest Group), Mar. 19, 1992.

[SU86] Su, Tzong-An, *Inferences in Databases*, doctoral dissertation, Case Western Reserve Univ., Cleveland, Ohio, 1986.

[SU87] Su, Tzong-An, and Gultekin Ozsoyoglu, "Data Dependencies and Inference Control in Multilevel Relational Database Systems," *Proc. Symp. Security and Privacy*, Apr. 1987, pp. 202-211.

[SU90] Su, Tzong-An, and Gultekin Ozsoyoglu, "Multivalued Dependency Inferences in Multilevel Relational Database Systems," *Database Security III: Status and Prospects*, D.L. Spooner and C. Landwehr, eds., North-Holland, Amsterdam, 1990, pp. 293-300.

[TANE87] Tanenbaum, A.S., *Operating Systems: Design and Implementation*, Prentice-Hall, Englewood Cliffs, N.J., 1987.

[TCSE85] *Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, US Dept. of Defense, Dec. 1985.

[TDI91] *Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria*, NCSC-TG-021, Nat'l Computer Security Center, Apr. 1991.

[TECH85] *Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements — Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments*, CSC-STD-004-85, June 1985, p. 27.

[TEDI91] "Trusted Third Parties and Similar Services" (CEC TEDIS Document), TEDIS Project Report (SC27/WG1/N214), 1991.

[THOM84] Thompson, K., "Reflections on Trusting Trust," *Comm. ACM*, Vol. 27, No. 8, Aug. 1984, pp. 761-763.

[THOM90] Thompson, M.F., R.R. Schell, A. Tao, and T. Levin, "Introduction to the Gemini Trusted Network Processor," *Proc. 13th Nat'l Computer Security Conf.*, Oct. 1990, pp. 211-217.

[THOM90a] Thompson, D.J., "Role-Based Application Design and Enforcement," *Proc. Fourth IFIP WG 11.3 Workshop on Database Security*, Halifax, UK, Sept. 1990.

[THOM90b] Thomas, Rebecca, L.R. Rogers, and J.L. Yates, *Advanced Programmer's Guide to UNIX\254 System V*, Berkeley, Calif., Osborne McGraw-Hill, 1986.

[THUR87] Thuraisingham, Bhavani M., "Security Checking in Relational Database Management Systems Augmented with Inference Engines," *Computers and Security*, Vol. 6, 1987, pp. 479-492.

[THUR89a] Thuraisingham, B.M., "A Multilevel Secure Object-Oriented Data Model," *Proc. 12th Nat'l Computer Security Conf.*, Oct. 1989, pp. 579-590.

[THUR89b] Thuraisingham, B.M., "Mandatory Security in Object-Oriented Database System," *Proc. Conf. Object-Oriented Programming: Systems, Languages, and Applications*, Oct. 1989, pp. 203-210.

[THUR90] Thuraisingham, B., "Recursion Theoretic Properties of the Inference Problem in Database Security," MTP 291, MITRE Corp., Bedford, Mass., May 1990.

[TINT92] Tinto, M., "The Design and Evaluation of INFOSEC Systems: The Computer Security Contribution to the Composition Discussion," C Tech. Report 32-92, Nat'l Security Agency, June 1992.

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

[TRAT76] Trattner, S., "Tools for Analysis of Software Security," ATR-77(2780)-1, Aerospace Corp., El Segundo, Calif., Oct. 1976.

[TSIC82] Tsichritzis, D.C., and F.H. Lochovsky, *Data Models*, Prentice-Hall, Englewood Cliffs, N.J., 1982.

[ULAM76] Ulam, S.M., *Adventures of a Mathematician*, Charles Scribner's Sons, New York, 1976.

[UNIS89] See [GRAY89].

[VETT89] Vetter, Linda, and Gordon Smith, "TCB Subsets: The Next Step," *Proc. Fifth Aerospace Conf.*, Tucson, Ariz., Dec. 1989.

[WALT91] Walter, Michael J., "Getting What You Want," *Optiv: The Business J. for Open Systems* (Corp. for Open Systems Int'l), Vol. 1, No. 1, Fall 1991, pp. 44-45.

[WARE70] Ware, W.H., ed., "Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security,"

DTIC AD-A076-617/0, Rand Corp., Santa Monica, Calif., Feb. 1970, reissued Oct. 1979.

[WEIS73] Weissman, C., "System Security Analysis/Certification Methodology and Results," SP-3728, System Development Corp., Santa Monica, Calif., Oct. 1973.

[WEIS92] Weissman, Clark, "Blacker: Security for the DDN, Examples of A1 Security Engineering Trades," *Proc. 1992 IEEE Computer Society Symp. Research in Security and Privacy*, IEEE Computer Society Press, Los Alamitos, Calif., May 1992, pp. 286-292.

[WEIS92a] Weissman, C., "Security Penetration Testing Guideline, Navy Handbook on Security Certification," TM-8889/000/00 (draft), Paramax Systems Corp., Camarillo, Calif., Dec. 1992.

[WHEE92] Wheeler, T., S. Holsberg, and S. Eckmann, *Ina Go User's Guide*, TM-8613/003, Paramax Systems Corp., Reston, Va., 1992.

[WIED91] Wiederhold, Gio, Sushil Jajodia, and Witold Litwin, "Dealing with Granularity of Time in Temporal Databases," *Lecture Notes in Computer Science*, Vol. 498, R. Anderson et al., eds., Springer-Verlag, New York, 1991, pp. 124-140.

[WILK72] Wilkes, M., *Time-Sharing Computer Systems*, 2nd ed., American-Elsevier, New York, 1972.

[WILK81] Wilkinson, A.L., et al., "A Penetration Analysis of the Burroughs Large System," *ACM SIGOPS Operating Systems Rev.*, Vol. 15, No. 1, Jan. 1981, pp. 14-25.

[WILL90] Williams, J.G., "On the Formalization of Semantic Conventions," *J. Symbolic Logic*, Vol. 55, No. 1, Mar. 1990, pp. 220-243.

[WILL90a] Williams, J., "Stages of Elaboration of Security Requirements for a Trusted Computer System," private communication, Dec. 1990.

[WILL91] Williams, J.G., "Modeling Nondisclosure in Terms of the Subject-Instruction Stream," *Proc. IEEE Symp. Research in Security and Privacy*, IEEE, May 1991.

[WILS88] Wilson, Jackson, "Views as the Security Objects in a Multilevel Secure Relational Database Management System," *Proc. IEEE Symp. Security and Privacy*, Oakland, Calif., May 1988, pp. 70-84.

[WILS89] Wilson, Jackson, "A Security Policy for an A1 DBMS (a Trusted Subject)," *Proc. IEEE Symp. Security and Privacy*, Oakland Calif., May 1989, pp. 116-125.

[WIMB71] Wimbrow, J.H., "A Large-Scale Interactive Administrative System," *IBM Systems J.*, Vol. 10, No. 4, 1971, pp. 260-282.

[WINT74] Winterbotham, F.W., *The Ultra Secret*, Harper and Row, New York, 1974.

[WINK92] Winkler, J.R., and J.C. Landry, "Intrusion and Anomaly Detection: ISOA Update," *Proc. 15th Nat'l Computer Security Conf.*, Baltimore, Oct. 1992, pp. 272-281.

[WISE90] Wiseman, S.R., "On the Problem of Security in Data Bases," in *Database Security III: Status and Prospects*, D.L. Spooner and C.E. Landwehr, eds., North-Holland, Amsterdam, 1990, pp. 143-150.

[WITT90] Wittbold, J.T., and D.M. Johnson, "Information Flow in Nondeterministic Systems," *Proc. IEEE Symp. Research in Security and Privacy*, May 1990, pp. 144-161.

[WOOD87] Woodward, J.P.L., "Exploiting the Dual Nature of Sensitivity Labels," *Proc. IEEE Symp. Security and Privacy*, Apr. 1987, pp. 23-30.

[WOOD88] Wood, A., "The SWORD Model of Multi-Level Secure Databases," RSRE Report 4247, RSRE, Nov. 1988.

[WOOD92] Woodfield, N.K., "An Approach for Evaluating the Security of an Air Force Type Network," *Fifth Annual Computer Security Applications Conf.*, IEEE Computer Society Press, Los Alamitos, Calif., Dec. 1989, pp. 53-62.

[ZDON90] Zdonik, Stanley B., and David Maier, eds., *Readings in Object-Oriented Database Systems*, Morgan Kaufmann, San Mateo, Calif., 1990.