Bibliography

[Adiron, 2000] Adiron (2000). http://www.adiron.com/.

[Anderson, 1994] Anderson, R. J. (1994). Why cryptosystems fail. *Communications of the ACM*, 37(11):32–40.

[Anderson, 2001] Anderson, R. J. (2001). *Security Engineering*. Wiley.

[Atluri and Huang, 1996] Atluri, V. and Huang, W.-K. (1996). An authorization model for workflows. In *Proc. European Symposium on Research in Computer Security (ESORICS)*, pages 44–64.

[Baldwin, 1990] Baldwin, R. W. (1990). Naming and grouping privileges to simplify security management in large databases. In *Proc. IEEE Symposium on Research in Security and Privacy*, pages 116–132.

[Baskerville, 1993] Baskerville, R. (1993). Information systems security design methods: Implications for information systems development. *ACM Computing Surveys*, 25(4):375–414.

[Bell and LaPadula, 1973] Bell, D. E. and LaPadula, L. J. (1973). Secure computer systems: A mathematical model. Mitre Technical Report 2547, Volume II.

[Blakley, 1998] Blakley, B. (1998). Section 4.3.2 in CORBASEC-FAQ. http://www.bhs.org/IT/Projects/cpr/security/CORBASEC-FAQ/.

[Blakley, 2000] Blakley, B. (2000). *CORBA Security*. Addison–Wesley.

[Blaze et al., 1996] Blaze, M., Feigenbaum, J., and Lacy, J. (1996). Distributed trust management. In *Proc. IEEE Symposium on Security and Privacy*, pages 164–173.

[Booch et al., 1998] Booch, G., Rumbaugh, J., and Jacobson, I. (1998). *The Unified Modeling Language User Guide*. Addison–Wesley.

[Borland, 2000] Borland (2000). GateKeeper Guide, VisiBroker for Java 4.5. http://www.inprise.com/techpubs/books/vbj/vbj45/gatekeeper-guide/title.html.

[Brewer and Nash, 1989] Brewer, D. and Nash, M. (1989). The chinese wall security policy. In *Proc. IEEE Symposium on Security and Privacy*, pages 206–214.

[Brose, 1999] Brose, G. (1999). A view–based access model for CORBA. In Vitek, J. and Jensen, C., editors, *Secure Internet Programming: Security Issues for Mobile and Distributed Objects*, LNCS 1603, pages 237–252. Springer.

[Brose, 2000] Brose, G. (2000). A typed access control model for CORBA. In Cuppens, F., Deswarte, Y., Gollmann, D., and Weidner, M., editors, *Proc. European Symposium on Research in Computer Security (ESORICS)*, LNCS 1895, pages 88–105. Springer.

[Brose, 2001] Brose, G. (2001). Raccoon — An infrastructure for managing access control in CORBA. In *Proc. International Conference on Distributed Applications and Interoperable Systems (DAIS)*. Kluwer.

[Brose et al., 2001a] Brose, G., Kiefer, H., and Noffke, N. (2001a). A CORBA domain management service. In *Proc. Kommunikation in Verteilten Systemen (KiVS)*, pages 233–236. Springer.

[Brose and Löhr, 1999] Brose, G. and Löhr, K.-P. (1999). VPL — Sprachunterstützung für den Entwurf von Zugriffsschutzpolitiken. In Baumgart, R., Rannenberg, K., Wähner, D., and Weck, G., editors, *Verläßliche IT–Systeme, IT–Sicherheit an der Schwelle des neuen Jahrtausends*, DuD–Dachbeiträge, pages 163–185. Vieweg.

[Brose et al., 2001b] Brose, G., Vogel, A., and Duddy, K. (2001b). *Java Programming with CORBA*. John Wiley & Sons, 3rd edition.

[Brüggemann, 1997] Brüggemann, H. H. (1997). *Spezifikation von objektorientierten Rechten*. DUD–Fachbeiträge. Vieweg.

[Carzaniga et al., 1998] Carzaniga, A., Fuggetta, A., Hall, R. S., van der Hoek, A., Heimbigner, D., and Wolf, A. L. (1998). A characterization framework for software deployment technologies. Technical Report CU-CS-857-98, Department of Computer Science, University of Colorado.

[CCITT, 1988a] CCITT (1988a). *Recommendation X.500: The Directory: Overview of Concepts, Models and Service*. CCITT.

[CCITT, 1988b] CCITT (1988b). *Recommendation X.509: The Directory — Authentication Framework*. CCITT.

[Chung, 1993] Chung, L. (1993). Dealing with security requirements during the development of information systems. In *Proc. International Conference on Advanced Information Systems Engineering (CAiSE)*.

[Clark and Wilson, 1987] Clark, D. D. and Wilson, D. R. (1987). A comparison of commercial and military computer security policies. In *Proc. IEEE Symposium on Security and Privacy*, pages 184–194.

[Common Criteria, 1999] Common Criteria (1999). *Common Criteria for Information Technology Security Evaluation, Version 2.1, Part 3: Security Assurance Requirements*.

[Concept Five Technologies and Hitachi, 2000] Concept Five Technologies and Hitachi (2000). *Revised Submission to RFP Security Domain Membership Management Service.*

[Coulouris and Dollimore, 1994a] Coulouris, G. and Dollimore, J. (1994a). Requirements for security in cooperative work: two case studies. Technical Report TR 671, Dept. of Computer Science, Queen Mary and Westfield College, University of London.

[Coulouris and Dollimore, 1994b] Coulouris, G. and Dollimore, J. (1994b). A security model for cooperative work. Technical Report TR 674, Dept. of Computer Science, Queen Mary and Westfield College, University of London.

[Coulouris et al., 1998] Coulouris, G., Dollimore, J., and Roberts, M. (1998). Role and task–based access control in the PerDiS groupware platform. In *ACM Workshop on Role–Based Access Control (RBAC)*.

[Damianou et al., 2001] Damianou, N., Dulay, N., Lupu, E., and Sloman, M. (2001). The Ponder policy specification language. In Sloman, M., Lobo, J., and Lupu, E., editors, *Proc. Int. Workshop on Policies for Distributed Systems and Networks (POLICY)*, pages 18–38.

[Dennis and Horn, 1966] Dennis, J. B. and Horn, E. C. V. (1966). Programming semantics for multiprogrammed computations. *Communications of the ACM*, 9(3):143–155.

[Department of Defense, 1985] Department of Defense (1985). Trusted Computer System Evaluation Criteria. DoD 5200.28-STD.

[Devanbu and Stubblebine, 2000] Devanbu, P. T. and Stubblebine, S. (2000). Software engineering for security: A roadmap. In Finkelstein, A., editor, *The Future of Software Engineering*. ACM Press.

[Dijkstra, 2001] Dijkstra, E. W. (2001). The end of computing science? *Communications of the ACM*, 44(3):92.

[Dobson and McDermid, 1989] Dobson, J. E. and McDermid, J. A. (1989). A framework for expressing models of security policy. In *Proc. IEEE Symposium on Security and Privacy*, pages 229–239.

[ECMA, 1996] ECMA (1996). *The ECMA GSS–API mechanism, Standard ECMA–235*. ECMA.

[Edwards, 1996] Edwards, W. K. (1996). Policies and roles in collaborative applications. In *Proc. Computer Supported Cooperative Work (CSCW)*, pages 11–20.

[Ellison et al., 1999b] Ellison, C. M., Frantz, B., Lampson, B., Rivest, R., Thomas, B. M., and Ylönen, T. (1999b). *Simple Public Key Certificate, Internet Draft, draft-ietf-spki-cert-structure-06.txt*.

[Ellison et al., 1999a] Ellison, C. M., Frantz, B., Lampson, B., Rivest, R., Thomas, B. M., and Ylönen, T. (1999a). *SPKI Certificate Theory, RFC 2693*.

[Fagin, 1978] Fagin, R. (1978). On an authorization mechanism. *ACM Transactions on Database Systems*, 3(3):310–319.

[Gollmann, 2000] Gollmann, D. (2000). Mergers and principals. In *Proc. International Workshop on Security Protocols*. Springer.

[Gong et al., 1997] Gong, L., Mueller, M., Prafullchandra, H., and Schemers, R. (1997). Going beyond the sandbox: An overview of the new security architecture in the Java Development Kit 1.2. In *Proc. USENIX Symposium on Internet Technologies and Systems*.

[Gosling et al., 1996] Gosling, J., Joy, B., and Steele, G. (1996). *The Java Language Specification*. Addison–Wesley.

[Griffiths and Wade, 1976] Griffiths, P. P. and Wade, B. W. (1976). An authorization mechanism for a relational database system. *ACM Transactions on Database Systems*, 1(3):242–255.

[Hagimont, 1994] Hagimont, D. (1994). Protection in the Guide object–oriented distributed system. In *Proc. European Conference for Object–Oriented Programming (ECOOP)*, LNCS, pages 280–298. Springer.

[Hagimont et al., 1997] Hagimont, D., Huet, O., and Mossière, J. (1997). A protection scheme for a CORBA environment. In *ECOOP '97 Workshop, CORBA: Implementation, Use and Evaluation*.

[Hagimont et al., 1996] Hagimont, D., Mossière, J., Rousset, X., and Saunier, F. (1996). Hidden software capabilities. In *Proc. Int. Conference on Distributed Computing Systems (ICDCS)*, pages 282–288.

[Hailpern and Ossher, 1990] Hailpern, B. and Ossher, H. (1990). Extending objects to support multiple interfaces and access control. *IEEE Transactions on Software Engineering*, 16(11):1247–1257.

[Halfmann and Kühnhauser, 1999] Halfmann, U. and Kühnhauser, W. E. (1999). Embedding security policies into a distributed computing environment. *Operating System Review*, 33(2):51–64.

[Harrison et al., 1976] Harrison, M., Ruzzo, W., and Ullman, J. (1976). Protection in Operating Systems. *Communications of the ACM*, 19(8):461–471.

[Hartmann et al., 2001] Hartmann, B., Flinn, D. J., and Beznosov, K. (2001). *Enterprise Security with EJB and CORBA*. Wiley.

[Herzberg et al., 2000] Herzberg, A., Mass, Y., Mihaeli, J., Naor, D., and Ravid, Y. (2000). Access control meets public key infrastructure, or: Assigning roles to strangers. In *Proc. IEEE Symposium on Security and Privacy*.

[IONA, 2000] IONA (2000). Orbix Wonderwall Administrator's Guide. http://www.iona.com/docs/manuals/orbix/33/pdf/orbixwonderwall33_admin.pdf.

[ISO/IEC, 1992] ISO/IEC (1992). *Database Language SQL*. International Standard, ISO/IEC 9075:1992d. ISO/IEC.

[ISO/IEC, 1996a] ISO/IEC (1996a). *Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Authentication Framework*. International Standard, ISO/IEC 10181–2:1996(E).

[ISO/IEC, 1996b] ISO/IEC (1996b). *Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Access Control Framework*. International Standard, ISO/IEC 10181–3:1996(E).

[ISO/IEC, 1996c] ISO/IEC (1996c). *Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Overview*. International Standard, ISO/IEC 10181–1:1996(E).

[JacORB, 2001] JacORB (2001). http://www.jacorb.org.

[Jajodia et al., 1997] Jajodia, S., Samarati, P., Subrahmanian, V. S., and Bertino, E. (1997). A unified framework for enforcing multiple access control policies. In *Proc. International Conference on Management of Data*, pages 474–485.

[Jones and Liskov, 1978] Jones, A. and Liskov, B. (1978). A language extension for expressing constraints on data access. *Communications of the ACM*, 21(5):358–367.

[Jürjens, 2001] Jürjens, J. (2001). Towards development of secure systems using UMLSec. In Hussmann, H., editor, *Proc. Int. Conference on Fundamental Approaches to Software Engineering (FASE)*, LNCS, pages 187–200. Springer.

[Karjoth, 1998] Karjoth, G. (1998). Authorization in CORBA security. In *Proc. European Symposium on Research in Computer Security (ESORICS)*, pages 143–158.

[Keahey and Gannon, 1997] Keahey, K. and Gannon, D. (1997). PARDIS: A parallel approach to CORBA. In *Proc. 6th IEEE International Symposium on High Performance Distributed Computing*.

[Kiczales et al., 1997] Kiczales, G., Lamping, J., Mendhekar, A., Maeda, C., Lopes, C., Loingiter, J.-M., and Irwin, J. (1997). Aspect–oriented programming. In *Proc. European Conference for Object–Oriented Programming (ECOOP)*, LNCS. Springer.

[Kiefer, 2000] Kiefer, H. (2000). Entwurf und Implementierung eines Domänenverwaltungssystems für CORBA. Master's thesis, Freie Universität Berlin.

[Koch and Brose, 2001] Koch, M. and Brose, G. (2001). Integrating access control policies into the software engineering process. Unpublished manuscript.

[Koch et al., 1996] Koch, T., Krell, C., and Krämer, B. (1996). Policy definition language for automated management of distributed systems. 2nd International Workshop on Systems Management, IEEE Computer Society.

[Koch and Murer, 1999] Koch, T. and Murer, S. (1999). Service architecture integrates mainframes in a CORBA environment. In *Proc. 3rd IEEE conference on Enterprise distributed computing*.

[Kuhn, 1997] Kuhn, D. R. (1997). Mutual exclusion of roles as a means of separation of duty in role–based access control systems. In *Proc. ACM Workshop on Role–Based Access Control (RBAC)*.

[Kühnhauser, 1999] Kühnhauser, W. (1999). *Metapolitiken*. GMD Research Series. GMD.

[Lai et al., 1999] Lai, C., Gong, L., Koved, L., Nadalin, A., and Schemers, R. (1999). User authentication and authorization in the Java platform. In *Proc. Annual Computer Security Conference (ACSAC)*.

[Lampson, 1974] Lampson, B. W. (1974). Protection. *ACM Operating Systems Rev.*, 8(1):18–24.

[Lampson, 2000] Lampson, B. W. (2000). Computer security in the real world. In *Proc. Annual Computer Security Applications Conference (ACSAC)*.

[Lampson et al., 1992] Lampson, B. W., Abadi, M., Burrows, M., and Wobber, E. (1992). Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems*, 10(4):265–310.

[Levy, 1984] Levy, H. M. (1984). *Capability–Based Computer Systems*. Digital Press.

[Linden, 1976] Linden, T. A. (1976). Operating system structures to support security and reliable software. *ACM Computing Surveys*, 8(4):409–445.

[Linn, 1993] Linn, J. (1993). *Generic Security Service Application Program Interface, Internet Official Protocol Standards, RFC 1508*. IETF Network Working Group.

[Linn, 1996] Linn, J. (1996). *The Kerberos Version 5 GSS-API Mechanism, Internet Official Protocol Standards, RFC 1964*. IETF Network Working Group.

[Lupu and Sloman, 1999] Lupu, E. C. and Sloman, M. (1999). Conflicts in policy–based distributed systems management. *IEEE Transactions on Software Engineering*, 25(6):852–896.

[Meyer, 1992] Meyer, B. (1992). *Eiffel: The Language*. Prentice–Hall.

[MICO, 1998] MICO (1998). MICO for the Palm Pilot. http://www.mico.org/pilot/.

[Neumann and Ts'o, 1994] Neumann, B. C. and Ts'o, T. (1994). Kerberos: An authentication service for computer networks. *IEEE Communications Magazine*, 32(9):33–83.

[Noffke, 2001] Noffke, N. (2001). Entwurf und Implementierung eines Rollendienstes für die Zugriffskontrolle in CORBA. Master's thesis, Freie Universität Berlin.

[Nuseibeh and Easterbrook, 2000] Nuseibeh, B. and Easterbrook, S. (2000). Requirements engineering: A roadmap. In Finkelstein, A., editor, *The Future of Software Engineering*. ACM Press.

[Nyanchama and Osborn, 1999] Nyanchama, M. and Osborn, S. (1999). The role graph model and conflict of interest. *ACM Transactions on Information and Systems Security*, 2(1):3–33.

[OMG, 1997] OMG (1997). *CORBAservices: Common Object Services Specification*.

[OMG, 1998a] OMG (1998a). *minimumCORBA*.

[OMG, 1998b] OMG (1998b). *Security Domain Membership Management Service RFP*.

[OMG, 1999a] OMG (1999a). *The Common Object Request Broker: Architecture and Specification, Revision 2.3*.

[OMG, 1999b] OMG (1999b). *Common Secure Interoperability Version 2*.

[OMG, 1999c] OMG (1999c). *CORBA 3.0 New Components Chapters, TC Document ptc/99-10-04*. OMG.

[OMG, 2000a] OMG (2000a). *The Common Object Request Broker: Architecture and Specification, Revision 2.4*.

[OMG, 2000b] OMG (2000b). *OMG Unified Modeling Language Specification, Version 1.3*.

[OMG, 2001a] OMG (2001a). *Common Secure Interoperability (CSIv2)*.

[OMG, 2001b] OMG (2001b). *Security Service Revision 1.7*.

[Osborn and Guo, 2000] Osborn, S. and Guo, Y. (2000). Modeling users in Role–Based Access Control. In *Proc. ACM Workshop on Role–Based Access Control (RBAC)*, pages 31–37.

[Parker and Pinkas, 1995] Parker, T. and Pinkas, D. (1995). *SESAME V4 — Overview*.

[Rabitti et al., 1991] Rabitti, F., Bertino, E., Kim, W., and Woelk, D. (1991). A model of authorization for next–generation database systems. *ACM Transactions on Database Systems*, 16(1):88–131.

[Richardson et al., 1992] Richardson, J., Schwarz, P., and Cabrera, L.-F. (1992). CACL: Efficient fine–grained protection for objects. In *Proc. Conference on Object–Oriented Programming, Languages, Systems, and Applications (OOPSLA)*, pages 263–275.

[Roeckle et al., 2000] Roeckle, H., Schimpf, G., and Weidinger, R. (2000). Process–oriented approach for role–finding to implement role–based security administration in a large industrial organization. In *Proc. ACM Workshop on Role–Based Access Control (RBAC)*, pages 103–110.

[Saltzer and Schroeder, 1975] Saltzer, J. H. and Schroeder, M. D. (1975). The protection of information in computer systems. *Proc. of the IEEE*, 9(63):1278–1308.

[Sandhu, 1992] Sandhu, R. S. (1992). The typed access matrix model. In *Proc. IEEE Symposium on Security and Privacy*, pages 122–136.

[Sandhu et al., 1996] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. (1996). Role–based access control models. *IEEE Computer*, 29(2):38–47.

[Scacchi, 2001] Scacchi, W. (2001). Process models in software engineering. In Marciniak, J., editor, *Encyclopedia of Software Engineering*. Wiley, New York, 2nd edition.

[Scholl et al., 1991] Scholl, M. H., Laasch, C., and Tresch, M. (1991). Updatable views in object–oriented databases. In *Proc. Int. Conference on Deductive and Object–Oriented Databases*, LNCS, pages 189–207. Springer.

[Simon and Zurko, 1997] Simon, R. T. and Zurko, M. E. (1997). Separation of duty in role–based environments. In *Proc. IEEE Computer Security Foundations Workshop (CSFW)*.

[Sloman and Twidle, 1994] Sloman, M. and Twidle, K. (1994). Domains: A framework for structuring management policy. In Sloman, M., editor, *Network and Distributed Systems Management*, chapter 16. Addison–Wesley.

[Soshi, 2000] Soshi, M. (2000). Safety analysis of the dynamic–typed access matrix model. In Cuppens, F., Deswarte, Y., Gollmann, D., and Weidner, M., editors, *Proc. European Symposium on Research in Computer Security (ESORICS)*, LNCS 1895, pages 106–121. Springer.

[Sterne, 1991] Sterne, D. F. (1991). On the buzzword "security policy". In *Proc. IEEE Symposium on Research in Security and Privacy*, pages 219–230.

[Stiegler, 1979] Stiegler, H. G. (1979). A structure for access control lists. *Software — Practice & Experience*, 9:813–819.

[Sun Microsystems, 1997] Sun Microsystems (1997). *Java Remote Method Invocation Specification*.

[Sun Microsystems, 2000] Sun Microsystems (2000). *Enterprise JavaBeans Specification, Version 2.0, Final Draft*.

[Sun Microsystems, 2001] Sun Microsystems (2001). Java authentication and authorization service (JAAS). http://java.sun.com/products/jaas/.

[Tanenbaum, 1995] Tanenbaum, A. S. (1995). *Distributed Operating Systems*. Prentice–Hall.

[Tanenbaum et al., 1986] Tanenbaum, A. S., Mullender, S., and van Renesse, R. (1986). Using sparse capabilities in a distributed operating system. In *Proc. International Conference on Distributed Computing Systems (ICDCS)*, pages 558–563. IEEE.

[Thomas and Sandhu, 1997] Thomas, R. K. and Sandhu, R. S. (1997). Task–based authorization controls (TBAC): A family of models for active and enterprise–oriented authorization management. In *Proc. IFIP WG 11.3 Workshop on Database Security*.

[Thomsen et al., 1998] Thomsen, D., O'Brien, D., and Bogle, J. (1998). Role based access control framework for network enterprises. In *Proc. Annual Computer Security Applications Conference (ACSAC)*.

[Tidswell and Jaeger, 2000] Tidswell, J. E. and Jaeger, T. (2000). An access control model for simplifying constraint expression. In *Proc. ACM Conference on Computer and Communication Security (CCS)*.

[Tivoli, 2001] Tivoli (2001). http://www.tivoli.com.

[Transarc, 1993] Transarc (1993). *DCE Administration Guide Vol. 2 — Core Services*. Transarc Corp.

[Tu et al., 1997] Tu, M., Griffel, F., Merz, M., and Lamersdorf, W. (1997). Generic policy management for open service markets. In *Proc. International Conference on Distributed Applications and Interoperable Systems (DAIS)*, pages 212–222. Chapman & Hall.

[van de Stadt, 1997] van de Stadt, R. (1997). CyberChair. http://www.cyberchair.org/.

[Vitek and Bokowski, 2001] Vitek, J. and Bokowski, B. (2001). Confined types in Java. *Software Practice & Experience*, 31:507–532.

[W3C, 2000] W3C (2000). *Extensible Markup Language (XML) 1.0*.

[Woo and Lam, 1993] Woo, T. Y. C. and Lam, S. S. (1993). Authorization in distributed systems: A new approach. *Journal of Computer Security*, 2(2–3):107–136.

[Wulf et al., 1974] Wulf, W., Cohen, E., Corwin, W., Jones, A., Levin, R., Pierson, C., and Pollack, F. (1974). HYDRA: the kernel of a multiprocessor operating system. *Communications of the ACM*, 17(6):337–345.

[Xtradyne, 2001] Xtradyne (2001). Domain Boundary Controller. http://www.xtradyne.de/products/boundary.htm.

[Yeong et al., 1995] Yeong, W., Howes, T., and Kille, S. (1995). *Lightweight Directory Access Protocol, Internet Official Protocol Standards*. IETF Network Working Group.

[Zurko et al., 1999] Zurko, M. E., Simon, R., and Sanfilippo, T. (1999). A user–centered, modular authorization service built on an RBAC foundation. In *Proc. IEEE Symposium on Security and Privacy*, pages 57–71.