Bibliography

[1] ISO/IEC 27001: Information technology - Security techniques - Information security management systems - Requirements, 2005. URL http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103.

[2] American National Standards Institute (ANSI). Role Based Access Control. Technical Report ANSI INCITS 359-2004, American National Standards Institute, 2004.

[3] Dana Al Kukhun. *Steps towards adaptive situation and context-aware access: A contribution to the extension of access control mechanums within Pervasive Information Systems.* PhD thesis, Universite de Toulouse, 2012. URL http://www.irit.fr/publis/SIG/These_Dana_Al_Kukhun.pdf.

[4] Ja'far Alqatawna, Erik Rissanen, and Babak Sadighi. Overriding of access control in XACML. In *Proceedings of the Eight* IEEE *International Workshop on Policies for Distributed Systems and Networks*, POLICY '07, pages 87–95. IEEE Computer Society, 2007. ISBN 0-7695-2767-1. DOI: 10.1109/POLICY.2007.31.

[5] Claudio A. Ardagna, Sabrina De Capitani di Vimercatia, Sara Forestia, Tyrone W. Grandison, Sushil Jajodiac, and Pierangela Samaratia. Access control for smarter healthcare using policy spaces. *Computers & Security*, 29(8):848–858, 2010. DOI: 10.1016/j.cose.2010.07.001.

[6] Michael Backes, Günter Karjoth, Walid Bagga, and Matthias Schunter. Efficient comparison of enterprise privacy policies. In *Proceedings of the 2004* ACM *symposium on Applied computing*, SAC '04, pages 375–382. ACM Press, 2004. ISBN 1-58113-812-1. DOI: 10.1145/967900.967983.

[7] Lee Badger. Providing a flexible security override for trusted systems. In *Proceedings Computer Security Foundations Workshop III*, pages 115–121. IEEE Computer Society, 1990. ISBN 0-8186-2071-4. DOI: 10.1109/CSFW.1990.128192.

H. Petritsch, *Break-Glass,* DOI 10.1007/978-3-658-07365-7,

[8] Olav Bandmann, Babak Sadighi Firozabadi, and Mads Dam. Constrained delegation. In *Proceedings of the 2002* IEEE *Symposium on Security and Privacy*, pages 131–140. IEEE Computer Society, 2002. ISBN 0-7695-1543-6. DOI: 10.1109/SECPRI.2002.1004367.

[9] Ezedin Barka and Ravi Sandhu. Framework for role-based delegation models. In *Proceedings of the 16th Annual Computer Security Applications Conference*, ACSAC '00, pages 168–176. IEEE Computer Society, 2000. ISBN 0-7695-0859-6. DOI: 10.1109/ACSAC.2000.898870.

[10] Steve Barker. The next 700 access control models or a unifying meta-model? In *Proceedings of the 14th ACM symposium on Access control models and technologies*, SACMAT '09, pages 187–196. ACM Press, 2009. ISBN 978-1-60558-537-6. DOI: 10.1145/1542207.1542238.

[11] Steffen Bartsch. A calculus for the qualitative risk assessment of policy override authorization. In *Proceedings of the 3rd international conference on Security of information and networks*, SIN '10, pages 62–70. ACM Press, 2010. ISBN 978-1-4503-0234-0. DOI: 10.1145/1854099.1854115.

[12] Basel Committee on Banking Supervision. Basel II: International convergence of capital measurement and capital standards. Technical report, Bank for International Settlements, Basel, Switzerland, 2004. URL http://www.bis.org/publ/bcbsca.htm.

[13] David A. Basin, Jürgen Doser, and Torsten Lodderstedt. Model driven security: From UML models to access control infrastructures. ACM *Transactions on Software Engineering and Methodology*, 15(1):39–91, 2006. ISSN 1049-331X. DOI: 10.1145/1125808.1125810.

[14] Moritz Y. Becker. A formal security policy for an NHS electronic health record service. Technical Report 628, University of Cambridge, 2005. URL http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-628.html.

[15] D. Elliott Bell and Leonard J. La Padula. Secure computer systems: Mathematical foundations. Technical Report MTR-2547, Volume I, MITRE, 1973.

[16] D. Elliott Bell and Leonard J. La Padula. Secure computer system: Unified exposition and multics interpretation. Technical Report MTR-2997, Rev. 1, MITRE, 1976.

[17] D. Elliott Bell and Leonard J. LaPadula. Secure computer systems: A mathematical model, volume II. In *Journal of Computer Security 4*, pages 229–263, 1996. An electronic reconstruction of *Secure Computer Systems: Mathematical Foundations*, 1973.

[18] David Elliott Bell. Looking back at the bell-la padula model. In *Proceedings of the 21st Annual Computer Security Applications Conference*, ACSAC '05, pages 337–351. IEEE Computer Society, 2005. ISBN 0-7695-2461-3. DOI: 10.1109/CSAC.2005.37.

[19] Berliner Beauftragter für Datenschutz und Informationsfreiheit. Datenschutz und Informationsfreiheit, 2009. URL http://www.datenschutz-berlin.de/attachments/669/Jahresbericht_2009.pdf.

[20] Elisa Bertino, Piero Andrea Bonatti, and Elena Ferrari. TRBAC: A temporal role-based access control model. ACM *Transactions on Information and System Security*, 4(3):191–233, August 2001. ISSN 1094-9224. DOI: 10.1145/501978.501979.

[21] Elisa Bertino, Barbara Catania, Maria Luisa Damiani, and Paolo Perlasca. GEO-RBAC: a spatially aware RBAC. In *Proceedings of the tenth* ACM *symposium on Access control models and technologies*, SACMAT '05, pages 29–37. ACM Press, 2005. ISBN 1-59593-045-0. DOI: 10.1145/1063979.1063985.

[22] John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In IEEE *Symposium on Security and Privacy*, pages 321–334. IEEE Computer Society, 2007. ISBN 0-7695-2848-1. DOI: 10.1109/SP.2007.11.

[23] Claudio Bettini, Sushil Jajodia, Xiaoyang Sean Wang, and Duminda Wijesekera. Obligation monitoring in policy management. In *Proceedings of the 3rd International Workshop on Policies for Distributed Systems and Networks*, POLICY '02, pages 2–12. IEEE Computer Society, 2002. ISBN 0-7695-1611-4. DOI: 10.1109/POLICY.2002.1011288.

[24] K.J. Biba. Integrity considerations for secure computer systems. Technical Report MTR-3153, Rev. 1, MITRE, 1977.

[25] Matthew A. Bishop. *The Art and Science of Computer Security*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2002. ISBN 0201440997.

[26] David F.C. Brewer and Michael J. Nash. The chinese wall security policy. In *Proceedings of the 1989* IEEE *Symposium on Security and Privacy*, pages 206–214. IEEE Computer Society, 1989. ISBN 0-8186-1939-2. DOI: 10.1109/SECPRI.1989.36295.

[27] Achim D. Brucker and Helmut Petritsch. Extending access control models with break-glass. In *Proceedings of the 14th* ACM *symposium on Access control models and technologies*, SACMAT '09, pages 197–206. ACM Press, 2009. ISBN 978-1-60558-537-6. DOI: 10.1145/1542207.1542239.

[28] Achim D. Brucker and Helmut Petritsch. Idea: Efficient evaluation of access control constraints. In *International Symposium on Engineering Secure Software and Systems,* ESSoS *'10*, number 5965 in LNCS, pages 157–165. Springer-Verlag, 2010. ISBN 978-3-642-11746-6. DOI: 10.1007/978-3-642-11747-3_12.

[29] Achim D. Brucker and Helmut Petritsch. A framework for managing and analyzing changes of security policies. In IEEE *International Symposium on Policies for Distributed Systems and Networks*, POLICY '11, pages 105–112. IEEE Computer Society, June 2011. ISBN 978-0-7695-4330-7/11. DOI: 10.1109/POLICY.2011.47.

[30] Achim D. Brucker and Burkhart Wolff. Symbolic test case generation for primitive recursive functions. In *Formal Approaches to Testing of Software*, number 3395 in LNCS, pages 16–32. Springer-Verlag, 2004. ISBN 3-540-25109-X. DOI: 10.1007/b106767.

[31] Achim D. Brucker and Burkhart Wolff. HOL-TestGen: An interactive test-case generation framework. In *Fundamental Approaches to Software Engineering*, number 5503 in LNCS, pages 417–420. Springer-Verlag, 2009. DOI: 10.1007/978-3-642-00593-0_28.

[32] Achim D. Brucker, Helmut Petritsch, and Andreas Schaad. Delegation assistance. In IEEE *International Symposium on Policies for Distributed Systems and Networks*, POLICY '09, pages 84–91. IEEE Computer Society, 2009. ISBN 978-0-7695-3742-9. DOI: 10.1109/POLICY.2009.35.

[33] Achim D. Brucker, Helmut Petritsch, and Stefan G. Weber. Attribute-based encryption with break-glass. In *Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices,* WISTP *2010*, volume 6033 of LNCS, pages 237–244. Springer-Verlag, 2010. ISBN 978-3-642-12367-2. DOI: 10.1007/978-3-642-12368-9_18.

[34] Achim D. Brucker, Lukas Brügger, Paul Kearney, and Burkhart Wolff. An approach to modular and testable security models of real-world health-care applications. In *Proceedings of the 16th* ACM *symposium on Access control models and technologies]*, SACMAT '11, pages 133–142. ACM Press, 2011. ISBN 978-1-4503-0688-1. DOI: 10.1145/1998441.1998461.

[35] Lukas Alexander Brügger. *A Framework for Modelling and Testing of Security Policies.* PhD thesis, ETH Zürich, February 2012.

[36] Jery Bryans. Reasoning about XACML policies using CSP. In *Proceedings of the 2005 workshop on Secure web services*, SWS '05, pages 28–35. ACM Press, 2005. ISBN 1-59593-234-8. DOI: 10.1145/1103022.1103028.

[37] Anna Carlin and Frederick Gallegos. IT audit: A critical business process. *Computer*, 40(7):87–89, July 2007. ISSN 0018-9162. DOI: 10.1109/MC.2007.246.

[38] David Chadwick and Stijn Lievens. Break the glass profile for xacml v2.0 and v3.0 (draft), 2011. URL http://lists.oasis-open.org/archives/xacml/201106/doc00002.doc.

[39] Liang Chen, Jason Crampton, Martin J. Kollingbaum, and Timothy J. Norman. Obligations in risk-aware access control. In *Tenth Annual International Conference on Privacy, Security and Trust*, PST, pages 145–152. IEEE Computer Society, 2012. ISBN 978-1-4673-2323-9. DOI: 10.1109/PST.2012.6297931.

[40] Pau-Chen Cheng, Pankaj Rohatgi, Claudia Keser, Paul A. Karger, Grant M. Wagner, and Angela Schuett Reninger. Fuzzy multi-level security: An experiment on quantified risk-adaptive access control. In *Proceedings of the 2007* IEEE *Symposium on Security and Privacy*, SP '07, pages 222–230. IEEE Computer Society, 2007. ISBN 0-7695-2848-1. DOI: 10.1109/SP.2007.21.

[41] David D. Clark and David R. Wilson. A comparison of commercial and military computer security policies. In IEEE *Symposium on Security and Privacy*, pages 184–194. IEEE Computer Society, 1987. ISBN 0-8186-0771-8. DOI: 10.1109/SP.1987.10001.

[42] Jason Crampton and Hemanth Khambhammettu. Delegation in role-based access control. In *Computer Security – ESORICS 2006*, volume 4189 of LNCS, pages 174–191. Springer-Verlag, 2006. ISBN 978-3-540-44601-9. DOI: 10.1007/11863908_12.

[43] Jason Crampton and Charles Morisset. An auto-delegation mechanism for access control systems. In *Security and Trust Management*, volume 6710 of LNCS, pages 1–16. Springer-Verlag, 2011. ISBN 978-3-642-22443-0. DOI: 10.1007/978-3-642-22444-7_1.

[44] Marnix A. C. Dekker and Sandro Etalle. Audit-based access control for electronic health records. In *Proceedings of the Second International Workshop on Views on Designing Complex Architectures*, volume 168 of *Electronic Notes in Theoretical Computer Science*, pages 221–236. Elsevier Science Publishers, February 2007. DOI: 10.1016/j.entcs.2006.08.028.

[45] Ian Denley and Simon Weston Smith. Privacy in clinical information systems in secondary care. *British Medical Journal (BMJ)*, 318(7194):1328–1331, May 1999. URL http://www.bmj.com/content/318/7194/1328.full.pdf.

[46] Jeremy Dick and Alain Faivre. Automating the generation and sequencing of test cases from model-based specifications. In *Formal Methods Europe 93: Industrial-Strength Formal Methods*, volume 670 of LNCS, pages 268–284. Springer-Verlag, 1993. ISBN 978-3-540-56662-5.

[47] Nathan Dimmock, Andrá Belokosztolszki, David Eyers, Jean Bacon, and Ken Moody. Using trust and risk in role-based access control policies. In *Proceedings of the ninth* ACM *symposium on Access control models and technologies*, SACMAT '04, pages 156–162. ACM Press, 2004. ISBN 1-58113-872-5. DOI: 10.1145/990036.990062.

[48] Sandro Etalle and William H. Winsborough. A posteriori compliance control. In *Proceedings of the 12th ACM symposium on Access control models and technologies*, SACMAT '07, pages 11–20, New York, NY, USA, 2007. ACM. ISBN 978-1-59593-745-2. DOI: 10.1145/1266840.1266843.

[49] David F. Ferraiolo and D. Richard Kuhn. Role-based access controls. In *Proceedings of the 15th National Computer Security Conference*, pages 554–563, 1992.

[50] Ana Ferreira, Ricardo Cruz-Correia, Luis Antunes, Pedro Farinha, E. Oliveira-Palhares, David W. Chadwick, and Altamiro Costa-Pereira. How to break access control in a controlled manner. In *19th* IEEE *International Symposium on Computer-Based Medical Systems*, pages 847–854. IEEE Computer Society, 2006. ISBN 0-7695-2517-1. DOI: 10.1109/CBMS.2006.95.

[51] Ana Ferreira, David Chadwick, Pedro Farinha, Ricardo Correia, Gansen Zao, Rui Chilro, and Luis Antunes. How to securely break into RBAC: The BTG-RBAC model. In *Proceedings of the 2009 Annual Computer Security Applications Conference*, ACSAC '09, pages 23–31. IEEE Computer Society, 2009. ISBN 978-0-7695-3919-5. DOI: 10.1109/ACSAC.2009.12.

[52] Babak Firozabadi and Marek Sergot. Power and permission in security systems. In *Security Protocols*, volume 1796 of LNCS, pages 48–53. Springer-Verlag, 2000. ISBN 978-3-540-67381-1. DOI: 10.1007/10720107_6.

[53] Babak Sadighi Firozabadi, Marek Sergot, and Olav Bandmann. Using authority certificates to create management structures. In *Security Protocols*, volume 2467 of LNCS, pages 134–145. Springer-Verlag, 2002. ISBN 978-3-540-44263-9. DOI: 10.1007/3-540-45807-7_21.

[54] Kathi Fisler, Shriram Krishnamurthi, Leo A. Meyerovich, and Michael Carl Tschantz. Verification and change-impact analysis of access-control policies. In *Proceedings of the 27th international conference on Software engineering*, ICSE '05, pages 196–205. ACM Press, 2005. ISBN 1-58113-963-2. DOI: 10.1145/1062455.1062502.

[55] Ludwig Fuchs, Günther Pernul, and Ravi S. Sandhu. Roles in information security - a survey and classification of the research area. *Computers & Security*, 30(8):748–769, 2011. DOI: 10.1016/j.cose.2011.08.002.

[56] Craig Gentry. *Handbook of Information Security*, volume 2, chapter IBE (Identity-Based Encryption), pages 575–592. John Wiley & Sons, January 2006. ISBN 0-471-64833-7.

[57] Anindya Ghose. Information disclosure and regulatory compliance: Economic issues and research directions. http://ssrn.com/abstract=921770, July 2006.

[58] G. Scott Graham and Peter J. Denning. Protection: principles and practice. In *Proceedings of the spring joint computer conference*, AFIPS '72 (Spring), pages 417–429. ACM Press, 1972. DOI: 10.1145/1478873.1478928.

[59] Lionel Habib, Mathieu Jaume, and Charles Morisset. A formal comparison of the Bell & LaPadula and RBAC models. In *Fourth International Conference on Information Assurance and Security*, ISIAS '08, pages 3–8. IEEE Computer Society, 2008. ISBN 978-0-7695-3324-7. DOI: 10.1109/IAS.2008.18.

[60] Michael Hafner, Mukhtiar Memon, and Muhammad Alam. Modeling and enforcing advanced access control policies in healthcare systems with SECTET. In *Models in Software Engineering*, volume 5002 of LNCS, pages 132–144. Springer-Verlag, 2008. ISBN 978-3-540-69069-6. DOI: 10.1007/978-3-540-69073-3_15.

[61] Alan R. Hevner, Salvatore T. March, Jinsoo Park, and Sudha Ram. Design science in information systems research. *MIS Quarterly*, 28(1):75–105, March 2004. ISSN 0276-7783. URL http://dl.acm.org/citation.cfm?id=2017212.2017217.

[62] HMISS Analytics. 2012 HMISS analytics report: Security of patient data, 2012. URL http://www.krollcybersecurity.com/media/Kroll-HIMSS_2012_-_Security_of_Patient_Data_040912.pdf.

[63] Vincent C. Hu, David Ferraiolo, Rick Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone. Guide to attribute based access control (ABAC) definition and considerations. Technical Report SP 800-162, National Institute of Standards and Technology (NIST), 2014.

[64] Michael Jackson. The meaning of requirements. *Annals of Software Engineering*, 3:5–21, 1997. ISSN 1022-7091. DOI: 10.1023/A:1018990005598.

[65] Trent Jaeger, Xiaolan Zhang, and Antony Edwards. Policy management using access control spaces. ACM *Transactions on Information and*

*System Security (*TISSEC*)*, 6(3):327–364, August 2003. ISSN 1094-9224. DOI: 10.1145/937527.937528.

[66] Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC). Breakglass: An approach to granting emergency access to healthcare systems. White paper, NEMA, COCIR, and JIRA, 2004.

[67] Jan Kolter, Rolf Schillinger, and Günther Pernul. A privacy-enhanced attribute-based access control system. In *Data and Applications Security XXI*, volume 4602 of LNCS, pages 129–143. Springer-Verlag, 2007. ISBN 978-3-540-73533-5. DOI: 10.1007/978-3-540-73538-0_11.

[68] Leonard J. La Padula and D. Elliott Bell. Secure computer systems: A mathematical model. Technical Report MTR-2547, Volume II, MITRE, 1973.

[69] Butler W. Lampson. Protection. In *Proceedings of the fifth Princeton Symposium on Information Sciences and Systems*, pages 437–443, 1971. Reprinted in Operating Systems Review, 8,1, January 1974, pp. 18–24.

[70] Ninghui Li, Ji-Won Byun, and Elisa Bertino. A critique of the ANSI standard on role-based access control. IEEE *Security and Privacy*, 5(6): 41–49, November 2007. ISSN 1540-7993. DOI: 10.1109/MSP.2007.158.

[71] Dan Lin, Prathima Rao, Elisa Bertino, and Jorge Lobo. An approach to evaluate policy similarity. In *Proceedings of the 12th* ACM *symposium on Access control models and technologies*, SACMAT '07, pages 1–10, 2007. ISBN 978-1-59593-745-2. DOI: 10.1145/1266840.1266842.

[72] Steven B. Lipner. Non-discretionery controls for commercial applications. In IEEE *Symposium on Security and Privacy*, volume 0, page 2. IEEE Computer Society, 1982. ISBN 0-8186-0410-7. DOI: 10.1109/SP.1982.10022.

[73] Jim Longstaff and Tony Howitt. Extensions to sealed envelope and break glass authorization. In AHIC*: Advances in Health Informatics Conference*, 2010. URL http://www.scm.tees.ac.uk/TeesConfidentialityModel/Longstaff_AHIC_apr10.doc.

[74] Jim Longstaff, Mike Lockyer, and John Nicholas. The tees confidentiality model: an authorisation model for identities and roles. In *Proceedings of the eighth* ACM *symposium on Access control models and technologies*, SACMAT '03, pages 125–133. ACM Press, 2003. ISBN 1-58113-681-1. DOI: 10.1145/775412.775428.

[75] J.J. Longstaff, M.A. Lockyer, and M.G. Thick. A model of accountability, confidentiality and override for healthcare and other applications. In *Proceedings of the fifth* ACM *workshop on Role-based access control*, RBAC '00, pages 71–76. ACM Press, 2000. ISBN 1-58113-259-X. DOI: 10.1145/344287.344304.

[76] Srdjan Marinovic, Robert Craven, Jiefei Ma, and Naranker Dulay. Rumpole: a flexible break-glass access control model. In *Proceedings of the 16th* ACM *symposium on Access control models and technologies*, SACMAT '11, pages 73–82. ACM Press, 2011. ISBN 978-1-4503-0688-1. DOI: 10.1145/1998441.1998453.

[77] Srdjan Marinovic, Robert Craven, Jiefei Ma, and Naranker Dulay. Rumpole: a flexible break-glass access control model. In *Proceedings of the 16th ACM symposium on Access control models and technologies*, SACMAT '11, pages 73–82. ACM Press, 2011. ISBN 978-1-4503-0688-1. DOI: 10.1145/1998441.1998453.

[78] Rebecca T. Mercuri. On auditing audit trails. *Communications of the* ACM, 46(1):17–20, January 2003. ISSN 0001-0782. DOI: 10.1145/602421.602436.

[79] OASIS. Core and hierarchical role based access control (RBAC) profile of XACML v2.0, 2005. URL http://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-rbac-profile1-spec-os.pdf.

[80] OASIS. eXtensible Access Control Markup Language (XACML), version 2.0, 2005. URL http://docs.oasis-open.org/xacml/2.0/XACML-2.0-OS-NORMATIVE.zip.

[81] Department of Defense Standard. Trusted computer system evaluation criteria. Technical Report DoD 5200.28-STD, US Department of Defence, 1985. URL http://www.fas.org/irp/nsa/rainbow/std001.htm.

[82] U.S. Department of Health and Human Services Office for Civil Rights. HIPAA administrative simplification, 2006.

[83] Oracle. Oracle role manager, 2009. URL http://www.oracle.com/technetwork/articles/oracle-role-manager-wp-1-128095.pdf.

[84] Ken Peffers, Tuure Tuunanen, Marcus Rothenberger, and Samir Chatterjee. A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3):45–77, December 2007. ISSN 0742-1222. DOI: 10.2753/MIS0742-1222240302.

[85] Helmut Petritsch. Exposé zur Anmeldung des Promotionsvorhabens, 2009. URL http://www-sec.uni-regensburg.de/news20/upload/upload__538be2dd87e9be91b66c1bd42eb3657e.pdf.

[86] Matthew Pirretti, Patrick Traynor, Patrick McDaniel, and Brent Waters. Secure attribute-based systems. In *Proceedings of the 13th* ACM *conference on Computer and communications security*, CCS '06, pages 99–112. ACM Press, 2006. ISBN 1-59593-518-5. DOI: 10.1145/1180405.1180419.

[87] Dean Povey. Optimistic security: A new access control paradigm. In *Proceedings of the 1999 workshop on New security paradigms*, NSPW '99, pages 40–45. ACM Press, 1999. ISBN 1-58113-149-6. DOI: 10.1145/335169.335188.

[88] Torsten Priebe, Wolfgang Dobmeier, Björn Muschall, and Günther Pernul. ABAC - ein Referenzmodell für attributbasierte Zugriffskontrolle. In *Sicherheit 2005: Sicherheit - Schutz und Zuverlässigkeit, Beiträge der 2. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.v. (GI)*, volume 62 of *LNI*, pages 285–296. GI, 2005. ISBN 3-88579-391-1.

[89] Erik Rissanen. Towards a mechanism for discretionary overriding of access control (transcript of discussion). In *Security Protocols*, number 3957 in LNCS, pages 320–323, March 2006. DOI: 10.1007/11861386_39.

[90] Erik Rissanen, Babak Firozabadi, and Marek Sergot. Discretionary overriding of access control in the privilege calculus. In *Formal Aspects in Security and Trust*, volume 173 of IFIO *International Federation for Information Processing*, pages 219–232. Springer-Verlag, 2005. ISBN 978-0-387-24050-3. DOI: 10.1007/0-387-24098-5_16.

[91] Lillian Røstad and Ole Edsberg. A study of access control requirements for healthcare systems based on audit trails from access logs. In *Proceedings of the 2006 Annual Computer Security Applications Conferenc*, ACSAC '06, pages 175–186. IEEE Computer Society, 2006. DOI: 10.1109/ACSAC.2006.8.

[92] Amit Sahai and Brent Waters. Fuzzy identity-based encryption. In *Advances in Cryptology* – EUROCRYPT *2005*, number 3494 in LNCS, pages 457–473. Springer-Verlag, 2005. DOI: 10.1007/11426639_27.

[93] Jerome H. Saltzer. Protection and the control of information sharing in multics. *Communications of the* ACM, 17(7):388–402, 1974. ISSN 0001-0782. DOI: 10.1145/361011.361067.

[94] Jerome H. Saltzer and Michael D. Schroeder. The protection of information in computer systems. *Proceedings of the* IEEE, 63(9):1278–1308, 1975. ISSN 0018-9219. DOI: 10.1109/PROC.1975.9939.

[95] Ravi Sandhu and Jaehong Park. Usage control: A vision for next generation access control. In *Computer Network Security*, volume 2776 of LNCS, pages 17–31. Springer-Verlag, 2003. ISBN 978-3-540-40797-3. DOI: 10.1007/978-3-540-45215-7_2.

[96] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. Role-based access control models. *Computer*, 29(2):38–47, February 1996. ISSN 0018-9162. DOI: 10.1109/2.485845.

[97] Ravi S. Sandhu, David F. Ferraiolo, and D. Richard Kuhn. The NIST model for role-based access control: towards a unified standard. In *Proceedings of the fifth* ACM *workshop on Role-based access control*, RBAC '00, pages 47–63. ACM Press, 2000. DOI: 10.1145/344287.344301.

[98] SAP. SAP GRC superuser privilege management, 2006. URL http://scn.sap.com/docs/DOC-1608.

[99] P. Sarbanes, G. Oxley, et al. Sarbanes-Oxley Act of 2002. 107th Congress Report, House of Representatives, 2nd Session, 107–610, 2002.

[100] Andreas Schaad, Jonathan Moffett, and Jeremy Jacob. The role-based access control system of a european bank: a case study and discussion. In *Proceedings of the sixth* ACM *symposium on Access control models and technologies*, SACMAT '01, pages 3–9. ACM Press, 2001. ISBN 1-58113-350-2. DOI: 10.1145/373256.373257.

[101] Sigrid Schefer-Wenzl and Mark Strembeck. A UML extension for modeling break-glass policies. In *Proc. of the 5th International Workshop on Enterprise Modelling and Information Systems Architectures (*EMISA*)*, volume 206 of *Lecture Notes in Informatics (*LNI*)*. Gesellschaft für Informatik, 2012.

[102] Lineke Sneller and Henk Langendijk. Sarbanes oxley section 404 costs of compliance: a case study. *Corporate Governance: An International Review*, 15(2):101–111, 2007. URL http://econpapers.repec.org/RePEc:bla:corgov:v:15:y:2007:i:2:p:101-111.

[103] Gunnar Stevens and Volker Wulf. A new dimension in access control: studying maintenance engineering across organizational boundaries. In *Proceedings of the 2002* ACM *conference on Computer supported cooperative work*, CSCW '02, pages 196–205. ACM Press, 2002. ISBN 1-58113-560-2. DOI: 10.1145/587078.587106.

[104] Silvia von Stackelberg, Klemens Böhm, and Matthias Bracht. Embedding 'break the glass' into business process models. Technical report, Faculty of Informatics, Karlsruhe Institute of Technology, 2012. URL http://dbis.ipd.uni-karlsruhe.de/1860.php.

[105] Jacques Wainer, Paulo Barthelmess, and Akhil Kumar. W-RBAC - a workflow security model incorporating controlled overriding of constraints. *International Journal of Cooperative Information Systems*, 12(4):455–485, 2003. DOI: 10.1142/S0218843003000814.

[106] Lingyu Wang, Duminda Wijesekera, and Sushil Jajodia. A logic-based framework for attribute based access control. In *Proceedings of the 2004* ACM *workshop on Formal methods in security engineering*, FMSE '04, pages 45–55. ACM Press, 2004. ISBN 1-58113-971-3. DOI: 10.1145/1029133.1029140.

[107] Janice Warner, Vijayalakshmi Atluri, Ravi Mukkamala, and Jaideep Vaidya. Using semantics for automatic enforcement of access control policies among dynamic coalitions. In *Proceedings of the 12th* ACM *symposium on Access control models and technologies*, SACMAT '07, pages 235–244. ACM Press, 2007. ISBN 978-1-59593-745-2. DOI: 10.1145/1266840.1266877.

[108] Phebe Waterfield and John Casey. The governance of compliance: Putting policies into practice. Yankee Report, April 2005.

[109] Paul Watzlawick. *How real is real? Confusion, disinformation, communication.* Vintage Books, 1977. ISBN 0394722566.

[110] Lei Zhang, Alexander Brodsky, and Sushil Jajodia. Toward information sharing: Benefit and risk access control (barac). In *Seventh* IEEE *International Workshop on Policies for Distributed Systems and Networks*, POLICY 2006, pages 45–53. IEEE Computer Society, 2006. ISBN 0-7695-2598-9. DOI: 10.1109/POLICY.2006.36.

[111] Xinwen Zhang, Sejong Oh, and Ravi Sandhu. PBDM: a flexible delegation model in RBAC. In *Proceedings of the eighth* ACM *symposium on Access control models and technologies*, SACMAT '03, pages 149–157. ACM Press, 2003. ISBN 1-58113-681-1. DOI: 10.1145/775412.775431.

[112] Gansen Zhao, David Chadwick, and Sassa Otenko. Obligations for role based access control. In *21st International Conference on Advanced Information Networking and Applications Workshops*, AINAW '07, pages 424–431. IEEE Computer Society, 2007. ISBN 0-7695-2847-3. DOI: 10.1109/AINAW.2007.267.

[113] Xia Zhao and M. Eric Johnson. Managing information access in data-rich enterprises with escalation and incentives. *International Journal of Electronic Commerce*, 15(1):79–112, 2010. DOI: 10.2753/JEC1086-4415150104.

A Glossary

There are different names and terms for the same or similar concepts in use. We used one term for one concept throughout this thesis wherever possible, i. e., using one common terminology, even when citing and discussing foreign work where other terms are used.

Subject describing the identity executing an access. We will use the term *user* if we explicitly refer to a human.

Resource describing the accessed object.

Action describing a specific task executed on a resource.

Permitted or Authorized are commonly used as equivalents, where *permitted* is commonly used for a concrete access executed by a concrete subject, whereas *authorized* is be used in a rather abstract context.

Permissions vs. Privilege are commonly used as equivalents, however, we use them to express slightly different concepts. We use "permission" to describe a rather technical concept, e. g., a rule in a policy. In contrast, we use "privilege" as the effective right a subject has. For example, permissions can be positive and negative, and a subject may be defined to have some privilege if a positive but no negative rule is found.

Obligation expressing conditions which have to be enforced by the decision-enforcing authority. See subsection 2.2.1 for details.

Policy is used for AC policy defining privileges, e. g., in form of a set of rules. The policy is what is passed as security state σ_{sec} to the ACF. See subsection 2.2.2 for details.

Access Control Function is used as abstraction from concrete AC models, see subsection 2.2.2 for details.

Policy State Assignment describing an assignment within the policy state, see subsection 4.1.3 for details.

Dependency Definition describing the definition of a policy state assignment.

Versioning expressing a concept as introduced in subsection 5.2.1.

H. Petritsch, *Break-Glass,* DOI 10.1007/978-3-658-07365-7,

B Acronyms

ABAC	Attribute Based Access Control
ABE	Attribute-based Encryption
AC	Access Control
ACF	Access Control Function
ACL	Access Control List
ACM	Association for Computing Machinery
ANSI	American National Standards Institute
API	Application Programming Interface
BoD	Binding of Duty
BP	Business Process
BPM	Business Process Model
BTG	Break-the-Glass
CCF	Care Comes First
CDI	Constrained Data Item
DAC	Discretionary Access Control
DOM	Document Object Model
DoS	Denial of Service
DSoD	Dynamic Separation of Duty
IEEE	Institute of Electrical and Electronic Engineers
EHR	Electronic Health Record

H. Petritsch, *Break-Glass,* DOI 10.1007/978-3-658-07365-7,

EMR	Electronic Medical Record
ERP	Enterprise Resource Planning
GRC	Governance, Risk Management, and Compliance
GP	General Practitioner
GUI	Graphical User Interface
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resources
IBAC	Identity Based Access Control
IBE	Identity-based Encryption
ID	Identifier
IDP	Identity Provider
IEEE	Institute of Electrical and Electronics Engineers
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
IVP	Integrity Verification Procedure
LNCS	Lecture Notes in Computer Science
MAC	Mandatory Access Control
MLS	Multi-Level Security
NHS	National Health Service
OASIS	Organization for the Advancement of Structured Information Standards
OS	Operating System
PAP	Policy Administration Point
PCDI	Partially-Constrained Data Item

PDP	Policy Decision Point
PEP	Policy Enforcement Point
PIN	Personal Identification Number
PIP	Policy Information Point
PTP	Partial Transformation Procedure
RBAC	Role Based Access Control
RBAC96	RBAC defined in [96]
REST	Representational State Transfer
ROI	return of investment
SACMAT	Symposium on Access control Models and Technologies
SAML	Security Assertion Markup Language
SAP	www.sap.com
SAT	Boolean Satisfiability Problem
SCIM	System for Cross-domain Identity Management
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SoD	Separation of Duty
SOX	Sarbanes-Oxley Act
SPM	Superuser Privilege Management
SSO	Single Sign On
SSoD	Static Separation of Duty
SUN	Sun Microsystems
SVN	Subversion
TCSEC	Trusted Computer System Evaluation Criteria

TP	Transformation Procedure
TR	Treatment Relationship
UDI	Unconstrained Data Item
UI	User Interface
UML	Unified Modeling Language
URI	Uniform Resource Identifier
US	United States
XACML	eXtensible Access Control Markup Language
XML	Extensible Markup Language
TCM	Tees Confidentiality Model

C Code Samples

C.1 XACML Sample Policy

This Listing C.1 represents the full XACML code from the reduced representation in Listing 2.1 in subsection 2.2.4.

```
<PolicySet
   xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
   PolicySetId="health-record"
   PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:↵
policy-combining-algorithm:permit-overrides">
 <Description>PolicySet for health records</Description>
 <Target>
  <Resources>
   <Resource>
    <ResourceMatch MatchId="urn:custom:uri-starts-with">
     <ResourceAttributeDesignator AttributeId=
        "urn:oasis:names:tc:xacml:1.0:resource:resource-id"
        DataType="http://www.w3.org/2001/XMLSchema#anyURI"
        MustBePresent="true"/>
     <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#anyURI">
        urn:health-record</AttributeValue>
    </ResourceMatch>
   </Resource>
  </Resources>
 </Target>
 <Policy PolicyId="health-record:physician"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:↵
rule-combining-algorithm:first-applicable">
  <Description>Policy for role physician</Description>
  <Target>
   <Subjects>
    <Subject>
     <SubjectMatch MatchId=
       "urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <SubjectAttributeDesignator
        AttributeId="urn:custom:subject:role"
        DataType="http://www.w3.org/2001/XMLSchema#string"/>
      <AttributeValue
         DataType="http://www.w3.org/2001/XMLSchema#string">
```

H. Petritsch, *Break-Glass,* DOI 10.1007/978-3-658-07365-7,

```
36          physician</AttributeValue>
       </SubjectMatch>
      </Subject>
39   </Subjects>
    </Target>
    <VariableDefinition VariableId="treating-physician">
42   <Apply FunctionId=
        "urn:oasis:names:tc:xacml:1.0:function:any-of-any">
      <Function FunctionId=
45      "urn:oasis:names:tc:xacml:1.0:function:string-equal"/>
      <SubjectAttributeDesignator AttributeId=
         "urn:oasis:names:tc:xacml:1.0:subject:subject-id"
48       DataType="http://www.w3.org/2001/XMLSchema#string"
         MustBePresent="true"/>
      <ResourceAttributeDesignator AttributeId=
51       "urn:runEx:patient:treating-subject"
         DataType="http://www.w3.org/2001/XMLSchema#string"/>
     </Apply>
54  </VariableDefinition>
    <Rule Effect="Permit"
       RuleId="health-record:physician:010">
57   <Description>allow read if patient
        gave consent</Description>
     <Target>
60    <Actions>
       <Action>
        <ActionMatch MatchId=
63       "urn:oasis:names:tc:xacml:1.0:function:string-equal">
         <ActionAttributeDesignator AttributeId=
          "urn:oasis:names:tc:xacml:1.0:action:action-id"
66        DataType="http://www.w3.org/2001/XMLSchema#string"/>
         <AttributeValue
          DataType="http://www.w3.org/2001/XMLSchema#string">
69        read</AttributeValue>
        </ActionMatch>
       </Action>
72    </Actions>
     </Target>
     <Condition>
75    <Apply
        FunctionId="urn:oasis:names:tc:xacml:1.0:function:or">
       <!-- check if subject is treating physician -->
78     <VariableReference VariableId="treating-physician"/>
       <!-- check if physician is assigned to a workgoup
            where the patiant has given his consent -->
81     <Apply FunctionId=
          "urn:oasis:names:tc:xacml:1.0:function:any-of-any">
        <Function FunctionId=
84      "urn:oasis:names:tc:xacml:1.0:function:string-equal"/>
        <SubjectAttributeDesignator AttributeId=
```

```
          "urn:runEx:subject:department"
87        DataType="http://www.w3.org/2001/XMLSchema#string"/>
       <ResourceAttributeDesignator AttributeId=
          "urn:runEx:patient:treating-department"
90        DataType="http://www.w3.org/2001/XMLSchema#string"/>
      </Apply>
     </Apply>
93  </Condition>
   </Rule>
  </Policy>
96 <PolicyIdReference>health-record:nurse</PolicyIdReference>
  <Policy PolicyId="health-record:final"
     RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:↵
99 rule-combining-algorithm:first-applicable">
   <Description>Final Deny policy for health records
   </Description>
102 <Target/>
   <Rule Effect="Deny"
      RuleId="health-record:final:010">
105 <Target/>
   </Rule>
  </Policy>
108 </PolicySet>
```

Listing C.1: An XACML policy: physicians are permitted to read a health record if the patient gave his consent to the physician or the physician's department.

C.2 Lattice Evaluation Algorithm in Java

Listing C.2 represents the lattice evaluation algorithm from Listing 3.3 as implementation for XACML.

```
  public Result combine(EvaluationCtx evalCtx,
                        List<CombinerParameter> combParam,
3                       List<CombinerElement> combElem) {
     /* store the first  deny we get, we will return it in
        case we do not find a permit */
6    Result firstDeny = null;
     /* store the first indeterminate */
     Result firstIndeterminate = null;
9
   /* create a cache where all permits are stored;
      we may need the result itself to get the obligations */
12 Map<String, Result> permitCache =
                               new HashMap<String, Result>();
   /* create a cache where the results of all deny policies
15    are storeddeny policies could be executed several time,
```

```
      i.e., remember both the result and if we executed it */
   Map<String, Result> denyCache =
18                                new HashMap<String, Result>();

   /* get the active policies from the context once */
21 Set<String> activePolicies = getActivePolicies(evalCtx);

   /* create (or get from cache) the policy lattice
24                                        we want to evaluate */
   PolicyLattice lattice =
                    getLattice(evalCtx, combParam, combElem);
27
   /* iterate over the lattice (i.e., level per level) */
   for ( LatticeElem elem : lattice ) {
30  /* check if current element is an active policy */
    if ( isActive(elem, lattice, activePolicies) ) {
     boolean permitted = false, denied = false;
33
     /* store a permit if we find it in this policy */
     Result permit = null;
36   /* first, check for an inherited permit,
                                          then for a permit */
     LatticeElem inhPermit =
39                      getInheritedPermit(elem, permitCache);
     if ( inhPermit != null ) {
      permitted = true;
42   } else if (elem.getPermitPolicy() != null ) {
      /* no inherited permit,
             we have to evaluate the current permit policy */
45    Result res = evaluate(elem.getPermitPolicy(), evalCtx);
      if ( res.getDecision() ==
                             Result.DECISION_INDETERMINATE ) {
48     if ( firstIndeterminate == null ) {
       firstIndeterminate = res;
      }
51     /* this policy will not provide a result,
          go to next */
      continue;
54    } else if ( res.getDecision() ==
                                       Result.DECISION_PERMIT ) {
       /* we found a permit, store it to cache (in the
57        current policy it may be overwritten by a deny) */
       permitCache.put(elem.getIdentifier(), res);
       permit = res;
60     permitted = true;
      } else if ( res.getDecision() == Result.DECISION_DENY
                  && firstDeny == null) {
63     firstDeny = res;
       continue; /* we do not need to evaluate the deny
                    policies if we do not have a permit */
```

```
66      }
       }

69     if ( permitted ) {
        /* check if there is an inherited deny: iterate over
           all extending policies, i.e, downwards */
72      for ( LatticeElem extending : elem.downwards() ) {
         /* check if extending policy
            has a deny policy defined */
75       if ( extending.getDenyPolicy() != null ) {
          Result res;
          /* check if we already evaluated this policy */
78        if ( denyCache.containsKey(
                                 extending.getIdentifier())) {
          res = denyCache.get(extending.getIdentifier());
81        } else {
          /* else, evaluate it and store it into the cache */
          res = evaluate(extending.getDenyPolicy(), evalCtx);
84        denyCache.put(extending.getIdentifier(), res);
         }
         /* check if the current deny policy
87          denies this request */
         if ( res.getDecision() ==
                               Result.DECISION_INDETERMINATE ) {
90        if ( firstIndeterminate == null ) {
           firstIndeterminate = res;
          }
93        } else if ( res.getDecision() ==
                                        Result.DECISION_DENY ) {
          denied = true;
96        if ( firstDeny == null ) {
           firstDeny = res;
          }
99        break; /* we have found a deny,
                    do not need to look further */
         }
102     }
       }
       /* we end up here only if we found a permit,
105       check if we also found a deny */
       if ( ! denied) {
        /* if we did not find a permit for this policy */
108     if ( permit == null ) {
         /* we got an inherited permit: we have to remove the
            lattice obligations from this permit and attach
111         the lattice obligations of the current policy */
         permit = permitCache.get(inhPermit.getIdentifier());
         AbstractPolicy curPolicy =
114                    (AbstractPolicy) elem.getPermitPolicy();
         AbstractPolicy inhPolicy =
```

```
                    (AbstractPolicy) inhPermit.getPermitPolicy();
117         Set<Obligation> obligations = permit.getObligations();

            /* remove obligations defined by inhPolicy */
120         for ( Obligation oblgRm : inhPolicy.getObligations()){
             for ( Obligation oblg : obligations ) {
              if ( oblg.getId().equals(oblgRm) ) {
123            obligations.remove(oblg);
               break;
              }
126           }
            }
            /* add obligations from current policy */
129         for ( Obligation oblg : curPolicy.getObligations() ) {
             obligations.add(oblg.evaluate(evalCtx));
            }
132         permit = new Result(permit.getDecision(),
                                          evalCtx, obligations);
            }
135        return permit;
          }
         }
        }
141     if ( firstIndeterminate != null ) {
         return firstIndeterminate;
       } else if ( firstDeny != null ) {
         return firstDeny;
144    } else {
         return new Result(Result.DECISION_DENY, evalCtx);
       }
147  }
```

Listing C.2: The lattice evaluation algorithm implemented as XACML policy combining algorithm in Java; full Java code for Listing 3.3.