Specificating and Verifying an Attribute-based Usage Control Approach regarding Open and Dynamic Computing Environments

Christos Grompanopoulos

Department of Applied Informatics

University of Macedonia

This dissertation is submitted for the degree of

Doctor of Philosophy

2014

This Dissertation Advisory Committee (DAC) consists of the following members (listed alphabetically):

- Professor Athanasios Manitsaris

  (Dept. of Applied Informatics, University of Macedonia, Greece.)

- Assistant Professor Christos Georgiadis

  (Dept. of Applied Informatics, University of Macedonia, Greece.)

- Associate Professor Ioannis Mavridis (PhD Supervisor)

  (Dept. of Applied Informatics, University of Macedonia, Greece.)

This Dissertation Defence Committee (DDC) consists of the following members (listed alphabetically):

- TODO

I would like to dedicate this dissertation to my family,

for their love, endless support and encouragement.

Acknowlegements

First and foremost, I would like to express my sincere appreciation and gratitude to my supervisor, Associate Professor Ioannis Mavridis. His guidance and support all these years and during the completion of this dissertation have been invaluable. Even in difficult times, a meeting with him always reinvigorated my enthusiasm and raised my spirits.

I am also extremely grateful to the members of my dissertation committee, Professor Athanasios Manitsaris and Assistant Professor Christos Georgiadis, for their time and dedication in reviewing my work and for their advice throughout my dissertation.

I would also like to thank my colleague and friend Antonios Gouglidis at the Department of Applied Informatics of the University of Macedonia, for sharing his thoughts and feelings during the completion of this laborious but very rewarding journey.

Finally, I would also like to take this opportunity and express my profound gratitude to my parents and all of my family for their continuous support and encouragement.

Abstract

Computing systems are always evolving in order to keep pace with the requirements that are posed by new computing environments. The widespread of networking technologies transformed the standalone computer model into the client-server computer model. Social trends as frequent traveling and social networking, led to the creation of small-sized computing devices that are equipped with sensors to recognize their surrounding environment and adapt accordingly their operations. Therefore, novel computing modes are emerged, as ubiquitous computing and the Internet of Things. The aforementioned type of systems set new requirements in several areas, including also the area of security. Security is an area of great importance in all computing systems. From a computer security, and particularly from an access control point of view the evolution of computing systems induces the creation of Open and Dynamic Computing Environments (ODCE). They are characterized as open since there are no boundaries between the legitimate and illegal users of a system. And dynamic since the configuration of these systems is constantly changing. Despite the importance of access control in ODCE there are a few proposals that addressed their analysis and identification of new requirements. Therefore, also existing access control modes are not able to fully support these requirements.

In this dissertation, we analyze existing access and usage control approaches to identify a number of unique characteristics posed by ODCE. Secondly, we formally define an attribute based usage control model for ODCE that is designed based on the identified requirements. Last but not least, we check the proposed model for its correctness, i.e., the adherence of

the model to its initially defined specifications.

Specifically, we provide information on the RBAC, ABAC and UCON models, which are mostly applicable in the examined case of ODCE. The presented work on the specification of models renders the aforementioned information valuable regarding the modeling of access or usage control systems since it can help in the identification of required specifications of access/usage control models for ODCE, and further, it examines state-of-the-art models and verification techniques to check the correctness of the designed or produced models in respect to their initial specifications. In turn, we highlight through representative usage scenarios the additional requirements that are introduced when attempting to utilize the UCON family of models in modern computing environments. To meet the requirements posed by ODCE, the proposed UseCON model incorporates a number of significant features compared with existing access/usage control models. Firstly, UseCON's extended expressiveness over the existing usage control models is the result of utilizing information originating from either a single or a set of both direct and indirect entities in the creation of the usage allowance decision. Secondly, UseCON inherently supports the utilization of historical information of usages through the automatic management of use entities. We further elaborate on the enhanced expressiveness in UseCON. A number of examples are given to demonstrate the enhanced capabilities of the UseCON model. The simplification of the policy administration process and the support of enhanced policy rules regarding their expressiveness, are included in the advantages of the proposed model. Furthermore, we provide a safety analysis of UseCON's formal TLA+ specification to prove the correctness of the UseCON model. The verification of consistency, safety and liveness properties for the core model and its internal operations for correctness was done by providing a formal specification of the UseCON model in TLA+, and using the TLC model checker. Lastly, we provide information on the declaration of models in TCL and elaborate on some performance metrics and in the internal procedures of the TCL model checker.

References

1. Gregory D. Abowd and Elizabeth D. Mynatt. Charting past, present, and future research in ubiquitous computing. *ACM Trans. Comput.-Hum. Interact.*, 7(1):29–58, March 2000. ISSN 1073-0516. doi: 10.1145/344949.344988.
2. Gregory D. Abowd, Anind K. Dey, Peter J. Brown, Nigel Davies, Mark Smith, and Pete Steggles. Towards a better understanding of context and context-awareness. In *Proceedings of the 1st International Symposium on Handheld and Ubiquitous Computing*, HUC '99, pages 304–307, London, UK, UK, 1999. Springer-Verlag. ISBN 3-540-66550-1.
3. Abulgader Almutairi and François Siewe. Ca-ucon: A context-aware usage control model. In *Proceedings of the 5th ACM International Workshop on Context-Awareness for Self-Managing Systems*, CASEMANS '11, pages 38–43, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-0877-9. doi: 10.1145/2036146.2036153.
4. ANSI. ANSI INCITS 359-2004, role based access control, 2004.
5. Donovan Artz and Yolanda Gil. A survey of trust in computer science and the semantic web.
6. *Web Semant.*, 5(2):58–71, June 2007. ISSN 1570-8268. doi: 10.1016/j.websem.2007.03.002.
7. Kevin Ashton. That "internet of things" thing. *RFiD Journal*, 22:97–114, 2009.
8. Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787–2805, 2010.
9. Jean Bacon, Ken Moody, and Walt Yao. A model of oasis role-based access control and its support for active security. *ACM Trans. Inf. Syst. Secur.*, 5(4):492–540, November 2002. ISSN 1094-9224. doi: 10.1145/581271.581276.
10. Christel Baier and Joost-Pieter Katoen. *Principles of Model Checking (Representation and Mind Series)*. The MIT Press, 2008. ISBN 026202649X, 9780262026499.
11. Matthias Baldauf, Schahram Dustdar, and Florian Rosenberg. A survey on context-aware systems. *Int. J. Ad Hoc Ubiquitous Comput.*, 2(4):263–277, June 2007. ISSN 1743-8225. doi: 10.1504/IJAHUC.2007.014070.
12. M. Ben-Ari. *Principles of Concurrent and Distributed Programming (2Nd Edition) (Prentice-Hall International Series in Computer Science)*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2006. ISBN 032131283X.
13. Messaoud Benantar. *Access Control Systems: Security, Identity Management and Trust Models*. Springer-Verlag New York, Inc., 2005.
14. Fran Berman, Geoffrey Fox, and Anthony J. G. Hey. *Grid Computing: Making the Global Infrastructure a Reality*. John Wiley & Sons, Inc., New York, NY, USA, 2003. ISBN 0470853190.
15. Azzedine Boukerche and Yonglin Ren. A trust-based security system for ubiquitous and pervasive computing environments. *Comput. Commun.*, 31(18):4343–4351, December 2008. ISSN 0140-3664. doi: 10.1016/j.comcom.2008.05.007.
16. Sabrina Capitani di Vimercati, Sara Foresti, and Pierangela Samarati. Authorization and access control. In Milan Petkovic and Willem Jonker, editors, *Security, Privacy, and Trust in Modern Data Management*, Data-Centric Systems and Applications, pages 39– 53. Springer Berlin Heidelberg, 2007. ISBN 978-3-540-69861-6.
17. Guanling Chen, David Kotz, et al. A survey of context-aware mobile computing research. Technical report, Technical Report TR2000-381, Dept. of Computer Science, Dartmouth College, 2000.
18. H.S. Cheng, Daqing Zhang, and J.G. Tan. Protection of privacy in pervasive computing environments. In *Information Technology: Coding and Computing, 2005. ITCC 2005.*

International Conference on, volume 2, pages 242–247 Vol. 2, April 2005. doi: 10.1109/ITCC.2005.233.

19. Michael J. Covington, Wende Long, Srividhya Srinivasan, Anind K. Dev, Mustaque Ahamad, and Gregory D. Abowd. Securing context-aware applications using environ- ment roles. In *Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies*, SACMAT '01, pages 10–20, New York, NY, USA, 2001. ACM. ISBN 1-58113-350-2. doi: 10.1145/373256.373258.
20. Jason Crampton and George Loizou. Administrative scope and role hierarchy operations. In *In Proceedings of Seventh ACM Symposium on Access Control Models and Technologies (SACMAT 2002)*, pages 145–154, 2002.
21. Frédéric Cuppens and Nora Cuppens-Boulahia. Modeling contextual security policies. *International Journal of Information Security*, 7(4):285–305, 2008. ISSN 1615-5262. doi: 10.1007/s10207-007-0051-9.
22. Ernesto Damiani, Sabrina De Capitani di Vimercati, and Pierangela Samarati. New paradigms for access control in open environments. In *SIGNAL PROCESSING AND INFORMATION TECHNOLOGY*, pages 540–545, 2005.
23. Pari Delir Haghighi, Shonali Krishnaswamy, Arkady Zaslavsky, and MohamedMedhat Gaber. Reasoning about context in uncertain pervasive computing environments. In Daniel Roggen, Clemens Lombriser, Gerhard Tröster, Gerd Kortuem, and Paul Havinga, editors, *Smart Sensing and Context*, volume 5279 of *Lecture Notes in Computer Science*, pages 112–125. Springer Berlin Heidelberg, 2008. ISBN 978-3-540-88792-8. doi: 10.1007/978-3-540-88793-5_9.
24. Dritsas S., Gritzalis D., Lambrinoudakis C., "Protecting privacy and anonymity in pervasive computing: Trends and perspectives", Telematics and Informatics Journal, Special Issue on Privacy and Anonymity in the Global Village, Vol. 23, No. 3, pp.196-210, 2006, Elsevier Science.
25. Yitao Duan and John Canny. Protecting user data in ubiquitous computing: Towards trustworthy environments. In David Martin and Andrei Serjantov, editors, *Privacy Enhanc- ing Technologies*, volume 3424 of *Lecture Notes in Computer Science*, pages 167–185. Springer Berlin Heidelberg, 2005. ISBN 978-3-540-26203-9. doi: 10.1007/11423409_ 11.
26. David F. Ferraiolo, D. Richard Kuhn, and Ramaswamy Chandramouli. *Role-Based Access Control*. Artech House, Inc., 2003.
27. Foster, Zhao Yong, I. Raicu, and S. Lu. Cloud computing and grid computing 360-degree compared. In *Grid Computing Environments Workshop, 2008. GCE '08*, pages 1–10, 2008.
28. Ian Foster and Carl Kesselman. *The Grid 2: Blueprint for a New Computing Infrastructure*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2003. ISBN 1558609334.
29. Ian Foster, Carl Kesselman, and Steven Tuecke. The anatomy of the grid - enabling scalable virtual organizations. *International Journal of Supercomputer Applications*, 15:2001, 2001.
30. Christos K. Georgiadis, Ioannis Mavridis, George Pangalos, and Roshan K. Thomas. Flex- ible team-based access control using contexts. In *Proceedings of the Sixth ACM Sym- posium on Access Control Models and Technologies*, SACMAT '01, pages 21–27, New York, NY, USA, 2001. ACM. ISBN 1-58113-350-2. doi: 10.1145/373256.373259.
31. Dieter Gollmann. *Computer Security*. John Wiley & Sons, Inc., New York, NY, USA, 1999. ISBN 0-471-97844-2.
32. Antonios Gouglidis and Ioannis Mavridis. On the definition of access control require
33. ments for grid and cloud computing systems. In Anastasios Doulamis, Joe Mam- bretti, Ioannis Tomkos, and Theodora Varvarigou, editors, *Networks for Grid Applica- tions*, volume 25 of *Lecture Notes of the Institute for Computer Sciences, Social In- formatics*

and Telecommunications Engineering, pages 19–26. Springer Berlin Heidel- berg, 2010. ISBN 978-3-642-11732-9. doi: 10.1007/978-3-642-11733-6_3.
34. Antonios Gouglidis, Ioannis Mavridis, and VincentC. Hu. Security policy verification for multi-domains in cloud systems. *International Journal of Information Security*, pages 1–15, 2013. ISSN 1615-5262. doi: 10.1007/s10207-013-0205-x.
35. Dimitris Gritzalis, M Kandias, V Stavrou, and L Mitrou. History of information: The case of privacy and security in social media. *Proc. of the History of Information Conference*, 2014.
36. Christos Grompanopoulos and Ioannis Mavridis. Towards differentiated utilization of attribute mutability for access control in ubiquitous computing. *Informatics, Panhellenic Conference on*, 0:118–123, 2010. doi: http://doi.ieeecomputersociety.org/10.1109/PCI.2010.45.
37. Christos Grompanopoulos and Ioannis Mavridis. Towards use-based usage control. In Dimitris Gritzalis, Steven Furnell, and Marianthi Theoharidou, editors, *Information Security and Privacy Research*, volume 376 of *IFIP Advances in Information and Communication Technology*, pages 585–590. Springer Boston, 2012a. ISBN 978-3-642-30435-4.
38. Christos Grompanopoulos and Ioannis Mavridis. Challenging issues of ucon in modern computing environments. In *Proceedings of the Fifth Balkan Conference in Informatics*, BCI '12, pages 156–161, New York, NY, USA, 2012b. ACM. ISBN 978-1-4503-1240-0. doi: 10.1145/2371316.2371346.
39. Christos Grompanopoulos, Antonios Gouglidis, and Ioannis Mavridis. A use-based approach for enhancing ucon. In *Security and Trust Management*, pages 81–96. Springer Berlin Heidelberg, 2013.
40. Jinsong Gui, Zhigang Chen, and Xiaoheng Deng. An improved ucona-based authorization policy specification for ubiquitous systems. In Yuanxu Yu, Zhengtao Yu, and Jingying Zhao, editors, *Computer Science for Environmental Engineering and EcoInformatics*, volume 158 of *Communications in Computer and Information Science*, pages 151–158. Springer Berlin Heidelberg, 2011. ISBN 978-3-642-22693-9. doi: 10.1007/ 978-3-642-22694-6_21.
41. Keijo Heljanko. Model checking based software verification, 2006.
42. Chung Tong Hu, David F Ferraiolo, David R Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone. Guide to attribute based access control (abac) defini- tion and considerations. NIST SP - 800-162, 2014.
43. Vincent C Hu, David Ferraiolo, and D Richard Kuhn. *Assessment of access control systems*.
44. US Department of Commerce, National Institute of Standards and Technology, 2006.
45. Michael Huth and Mark Ryan. *Logic in Computer Science: Modelling and Reasoning About Systems*. Cambridge University Press, New York, NY, USA, 2004. ISBN 052154310X.
46. ITU-T. X.812 recommendation, 1995.
47. Helge Janicke, Antonio Cau, and Hussein Zedan. A note on the formalisation of ucon. In *Proceedings of the 12th ACM symposium on Access control models and technologies*, SACMAT '07, pages 163–168, New York, NY, USA, 2007. ACM. ISBN 978-1-59593-745-2.
48. Xin Jin, Ram Krishnan, and Ravi Sandhu. A unified attribute-based access control model covering dac, mac and rbac. In Nora Cuppens-Boulahia, Frédéric Cuppens, and Joaquin Garcia-Alfaro, editors, *Data and Applications Security and Privacy XXVI*, volume 7371 of *Lecture Notes in Computer Science*, pages 41–55. Springer Berlin Heidelberg, 2012. ISBN 978-3-642-31539-8. doi: 10.1007/978-3-642-31540-4_4.
49. A Joshi, T Finin, L Kagal, J Parker, and A Patwardhan. Security policies and trust in ubiquitous computing. *Philos Trans A Math Phys Eng Sci*, 366(1881):3769–3780–, October 2008.
50. L. Kagal, T. Finin, and A. Joshi. Trust-based security in pervasive computing environments. *Computer*, 34(12):154–157, Dec 2001. ISSN 0018-9162. doi: 10.1109/2.970591.

51. L. Kagal, T. Finin, Anupam Joshi, and S. Greenspan. Security and privacy challenges in open and dynamic environments. *Computer*, 39(6):89 –91, june 2006. ISSN 0018-9162. doi: 10.1109/MC.2006.207.
52. Lalana Kagal, Tim Finin, and Anupam Joshi. A policy language for a pervasive computing environment. In *Proceedings of the 4th IEEE International Workshop on Policies for Distributed Systems and Networks*, POLICY '03, pages 63–, Washington, DC, USA, 2003. IEEE Computer Society. ISBN 0-7695-1933-4.
53. Ekkart Kindler. Safety and liveness properties: A survey. *Bulletin of the European Association for Theoretical Computer Science*, 53:268–272, 1994.
54. Leanid Krautsevich, Aliaksandr Lazouski, Fabio Martinelli, Paolo Mori, and Artsiom Yautsiukhin. Usage control, risk and trust. In Sokratis Katsikas, Javier Lopez, and Miguel Soriano, editors, *Trust, Privacy and Security in Digital Business*, volume 6264 of *Lecture Notes in Computer Science*, pages 1–12. Springer Berlin Heidelberg, 2010. ISBN 978-3- 642-15151-4. doi: 10.1007/978-3-642-15152-1_1.
55. Devdatta Kulkarni and Anand Tripathi. Context-aware role-based access control in pervasive computing systems. In *Proceedings of the 13th ACM Symposium on Access Control Models and Technologies*, SACMAT '08, pages 113–122, New York, NY, USA, 2008. ACM. ISBN 978-1-60558-129-3. doi: 10.1145/1377836.1377854.
56. Arun Kumar, Neeran Karnik, and Girish Chafle. Context sensitivity in role-based access control. *ACM SIGOPS Operating Systems Review*, 36(3):53–66, 2002.
57. Leslie Lamport. *Specifying Systems: The TLA+ Language and Tools for Hardware and Software Engineers*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2002. ISBN 032114306X.
58. Leslie Lamport, John Matthews, Mark Tuttle, and Yuan Yu. Specifying and verify- ing systems with tla+. In *Proceedings of the 10th workshop on ACM SIGOPS Eu- ropean workshop*, EW 10, pages 45–48, New York, NY, USA, 2002. ACM. doi: 10.1145/1133373.1133382.
59. Butler W. Lampson. Protection. *SIGOPS Oper. Syst. Rev.*, 8:18–24, January 1974. ISSN 0163-5980.
60. Bo Lang, Ian Foster, Frank Siebenlist, Rachana Ananthakrishnan, and Tim Freeman. A flexible attribute based access control method for grid computing. *Journal of Grid Computing*, 7(2):169–180, 2009. ISSN 1570-7873. doi: 10.1007/s10723-008-9112-1.
61. Aliaksandr Lazouski, Fabio Martinelli, and Paolo Mori. Usage control in computer security: A survey. *Computer Science Review*, 4(2):81 – 99, 2010. ISSN 1574-0137.
62. 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, 2007.
63. Jianfeng Lu, Ruixuan Li, Jinwei Hu, and Dewu Xu. Static enforcement of static separation- of-duty policies in usage control authorization models. *IEICE Transactions*, 95-B(5): 1508–1518, 2012.
64. Fabio Martinelli and Paolo Mori. On usage control for grid systems. *Future Gener. Comput. Syst.*, 26(7):1032–1042, July 2010. ISSN 0167-739X. doi: 10.1016/j.future.2009.12.005.
65. Patrick McDaniel. On context in authorization policy. In *Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies*, SACMAT '03, pages 80–89, New York, NY, USA, 2003. ACM. ISBN 1-58113-681-1. doi: 10.1145/775412.775422.
66. Kazuhiro Minami and David Kotz. Secure context-sensitive authorization. In *Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications*, PERCOM '05, pages 257–268, Washington, DC, USA, 2005. IEEE Computer Society. ISBN 0-7695-2299-8. doi: 10.1109/PERCOM.2005.37.
67. Asmund Ahlmann Nyre. Usage control enforcement - a survey. In *Proceedings of the*

IFIP WG 8.4/8.9 International Cross Domain Conference on Availability, Reliability and
68. *Security for Business, Enterprise and Health Information Systems*, ARES'11, pages 38– 49, Berlin, Heidelberg, 2011. Springer-Verlag. ISBN 978-3-642-23299-2.
69. OASIS. Oasis extensible access control markup language (xacml) tc, 2011.
70. Sejong Oh and Ravi Sandhu. A model for role administration using organization structure. In *Proceedings of the seventh ACM symposium on Access control models and technolo- gies*, pages 155–162. ACM, 2002.
71. Jaehong Park and Ravi Sandhu. The ucon abc usage control model. *ACM Trans. Inf. Syst. Secur.*, 7(1):128–174, 2004.
72. Pretschner, M. Hilty, F. Schutz, C. Schaefer, and T. Walter. Usage control enforcement: Present and future. *Security Privacy, IEEE*, 6(4):44–53, July 2008. ISSN 1540-7993. doi: 10.1109/MSP.2008.101.
73. Pretschner, J. Ruesch, C. Schaefer, and T. Walter. Formal analyses of usage control poli- cies. In *Availability, Reliability and Security, 2009. ARES '09. International Conference on*, pages 98–105, 2009. doi: 10.1109/ARES.2009.100.
74. Lili Qiu, Yin Zhang, Feng Wang, Mi Kyung, and Han Ratul Mahajan. Trusted computer system evaluation criteria. In *National Computer Security Center*, 1985.
75. P.V. Rajkumar, S.K. Ghosh, and P. Dasgupta. Concurrent usage control implementation verification using the spin model checker. In Natarajan Meghanathan, Selma Boumer- dassi, Nabendu Chaki, and Dhinaharan Nagamalai, editors, *Recent Trends in Network Security and Applications*, volume 89 of *Communications in Computer and Informa- tion Science*, pages 214–223. Springer Berlin Heidelberg, 2010. ISBN 978-3-642-14477-6. doi: 10.1007/978-3-642-14478-3_22.
76. Ranganathan, J. Al-Muhtadi, and R.H. Campbell. Reasoning about uncertain contexts in pervasive computing environments. *Pervasive Computing, IEEE*, 3(2):62–70, April 2004. ISSN 1536-1268. doi: 10.1109/MPRV.2004.1316821.
77. Kumar Ranganathan. Trustworthy pervasive computing: The hard security problems. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Com- munications Workshops*, PERCOMW '04, pages 117–, Washington, DC, USA, 2004. IEEE Computer Society. ISBN 0-7695-2106-1.
78. Silvio Ranise and Alessandro Armando. On the automated analysis of safety in usage control: A new decidability result. In Li Xu, Elisa Bertino, and Yi Mu, editors, *Net- work and System Security*, volume 7645 of *Lecture Notes in Computer Science*, pages 15–28. Springer Berlin Heidelberg, 2012. ISBN 978-3-642-34600-2. doi: 10.1007/ 978-3-642-34601-9_2.
79. Debashis Saha and Amitava Mukherjee. Pervasive computing: A paradigm for the 21st century. *Computer*, 36(3):25–31, March 2003. ISSN 0018-9162. doi: 10.1109/MC.2003. 1185214.
80. Pierangela Samarati and Sabrina De Capitani di Vimercati. Access control: Policies, mod- els, and mechanisms. In *Revised versions of lectures given during the IFIP WG 1.7 International School on Foundations of Security Analysis and Design on Foundations of Security Analysis and Design: Tutorial Lectures*, FOSAD '00, pages 137–196, London, UK, UK, 2001a. Springer-Verlag. ISBN 3-540-42896-8.
81. Pierangela Samarati and SabrinaCapitani Vimercati. Access control: Policies, models, and mechanisms. In Riccardo Focardi and Roberto Gorrieri, editors, *Foundations of Security Analysis and Design*, volume 2171 of *Lecture Notes in Computer Science*, pages 137–196. Springer Berlin Heidelberg, 2001b. ISBN 978-3-540-42896-1. doi: 10.1007/3-540-45608-2_3.
82. R. Sandhu. The ascaa principles for access control interpreted for collaboration systems. In

Collaborative Technologies and Systems, 2008. CTS 2008. International Symposium on, pages 532–532, May 2008. doi: 10.1109/CTS.2008.4543974.

83. Ravi Sandhu and Jaehong Park. Usage control: A vision for next generation access control. In *Computer Network Security*, volume 2776, pages 17–31. Springer Berlin / Heidelberg, 2003.
84. Ravi Sandhu and Pierangela Samarati. Authentication, access control, and audit. *ACM Comput. Surv.*, 28(1):241–243, March 1996. ISSN 0360-0300. doi: 10.1145/234313.
85. 234412.
86. Ravi Sandhu, Venkata Bhamidipati, and Qamar Munawer. The arbac97 model for role-based administration of roles. *ACM Trans. Inf. Syst. Secur.*, 2(1):105–135, 1999.
87. Ravi S. Sandhu. Lattice-based access control models, 1993.
88. R.S. Sandhu and P. Samarati. Access control: principle and practice. *Communications Magazine, IEEE*, 32(9):40–48, Sept 1994. ISSN 0163-6804. doi: 10.1109/35.312842.
89. R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman. Role-based access control models. *Computer*, 29(2):38 –47, feb 1996. ISSN 0018-9162. doi: 10.1109/2.485845.
90. Theoharidou M., Papanikolaou N., Pearson S., Gritzalis D., "Privacy risks, security and accountability in the Cloud", in *Proc. of the 5th IEEE Conference on Cloud Computing Technology and Science (CloudCom-2013)*, pp.177-184, IEEE Press, United Kingdom, December 2013
91. R.K. Thomas and R. Sandhu. Models, protocols, and architectures for secure pervasive computing: challenges and research directions. In *Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second IEEE Annual Conference on*, pages 164–168, March 2004. doi: 10.1109/PERCOMW.2004.1276925.
92. Alessandra Toninelli, R. Montanari, L. Kagal, and O. Lassila. Proteus: A semantic context-aware adaptive policy model. In *Policies for Distributed Systems and Networks, 2007. POLICY '07. Eighth IEEE International Workshop on*, pages 129–140, June 2007. doi: 10.1109/POLICY.2007.40.
93. Lingyu Wang, Duminda Wijesekera, and Sushil Jajodia. A logic-based framework for attribute based access control. In *Proceedings of the 2004 ACM Workshop on For- mal Methods in Security Engineering*, FMSE '04, pages 45–55, New York, NY, USA, 2004. ACM. ISBN 1-58113-971-3. doi: 10.1145/1029133.1029140.
94. Mark Weiser. Ubiquitous computing. In *ACM Conference on Computer Science*, page 418, 1994.
95. Mark Weiser. The computer for the 21st century. *SIGMOBILE Mob. Comput. Commun. Rev.*, 3(3):3–11, July 1999. ISSN 1559-1662. doi: 10.1145/329124.329126.
96. Jeannette M. Wing. A specifier's introduction to formal methods. *Computer*, 23(9):8–23, September 1990. ISSN 0018-9162. doi: 10.1109/2.58215.
97. Ran Yang, Chuang Lin, and Fujun Feng. A time and mutable attribute-based access control model. *JCP*, 4(6):510–518, 2009.
98. Eric Yuan and Jin Tong. Attributed based access control (abac) for web services, 2005.
99. G. Zhang and M. Parashar. Dynamic context-aware access control for grid applications. In *Grid Computing, 2003. Proceedings. Fourth International Workshop on*, pages 101–108. IEEE, 2004. ISBN 076952026X.
100. Xinwen Zhang. *Formal Model and Analysis of Usage Control*. PhD thesis, Fairfax, VA, USA, 2006. AAI3221391.
101. Xinwen Zhang, Francesco Parisi-Presicce, Ravi Sandhu, and Jaehong Park. Formal model and policy specification of usage control. *ACM Trans. Inf. Syst. Secur.*, 8:351–387, November 2005. ISSN 1094-9224.
102. Xinwen Zhang, Ravi Sandhu, and Francesco Parisi-Presicce. Safety analysis of usage con- trol authorization models. In *Proceedings of the 2006 ACM Symposium on*

Information, computer and communications security, ASIACCS '06, pages 243–254, New York, NY, USA, 2006. ACM. ISBN 1-59593-272-0.

103. Xinwen Zhang, Masayuki Nakae, Michael J. Covington, and Ravi Sandhu. Toward a usage- based security framework for collaborative computing systems. *ACM Trans. Inf. Syst. Secur.*, 11(1):1–36, 2008.