Report on the 9th ACM Symposium on Access Control Models and Technologies (SACMAT'04)

Elena Ferrari

University of Insubria at Como,
Via Valleggio, 11, 22100 Como, Italy
elena.ferrari@uninsubria.it

SACMAT'04 was held on June 2-4, 2004, at Yorktown Heights, New York, USA and was hosted by IBM T.J. Watson Research Center. The symposium, which was co-located with the IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY 2004), continues its tradition of being the premier forum for presentation of research results and experience reports on leading edge issues of access control and related technologies, including models, systems, applications, and theory. SACMAT gives researchers and practitioners a unique opportunity to share their perspectives with others interested in the various aspects of access control.

The call for papers attracted 65 submissions, from all over the world. The program committee selected 18 papers for presentation. The 18 papers, organized in seven sessions, were presented over two and an half days. The selected papers cover a wide range of topics, ranging from next generation access control models, to security analysis, role administration, policy specification and implementation, and access control for distributed environments and XML data. All the accepted papers were included in a volume published by ACM, whereas best papers from the symposium have been invited for possible publication in ACM Transactions on Information and System Security (TISSEC). Besides the technical sessions, this year program included a keynote speech on Access Control for Databases, and a panel on Security for Grid-based Computing Systems.

Keynote speech

The keynote speech: *Access Control in Databases: Developments and Directions*, was given by Bhavani Thuraisingham, program director for Cyber Trust, Data and Application Security, and Sensor and Sensor Networks at the National Science Foundations, USA. Based on her long experience in the field, Dr. Thuraisingham provided a comprehensive overview of the developments in data and application security. Then, she mainly focused on access control, by discussing what has been done so far and which are the current trends. Among them, Dr. Thuraisingham considers, as the most promising, secure data warehousing and e-commerce, XML and RDF security, trust negotiations, privacy preserving data mining, access control for next-generation databases (e.g., dependable and network databases, sensor and stream databases, real-time and embedded databases). The talk ended with an interesting overview of future developments in the field of access control. In particular, Dr. Thuraisingham presented her vision for the Secure Semantic Web and highlighted the need of security mechanisms that cut across all the layers of the Semantic Web architecture. In such a context, interoperability among the devised security mechanisms is an essential need.

Panel

SACMAT'04 included a panel on Security for Grid-based Computing Systems, which is today considered as a prerequisite to really make grid systems usable in a variety of commercial applications. The aim of the panel, moderated by Elisa Bertino, CERIAS, Purdue University, USA, was to discuss which are the challenges and the issues in this field and which are the differences with respect to securing more traditional distributed architectures, with special emphasis on access control. The panelists were Bruno Crispo, Vrije Universiteit, Netherlands, James Joshi, Pittsburgh University, USA, Wengliang (Kevin) Du, Syracuse University, USA, and Ravi Sandhu, George Mason University and NSD Security, USA. The panelists presented their vision, by stressing the need of ad-hoc policy languages for the Grid, and of scalable and adaptive mechanisms for their enforcement. Additional challenges mentioned by the panelists were how to combine scheduling with access control and how to specify and enforce user security requirements in an environment characterized by hosts with different levels of security. The panel was very lively with a lot of discussion and debate among the symposium atten-

dees.

Technical sessions

The technical program included seven sessions. The first session: *Next Generation Access Control Models* dealt with access control for new and emerging environments and applications. The first paper in this section, *A Logical Specification for Usage Control*, by X. Zhang, J. Park, F. Parisi-Presicce, and R. Sandhu provides a logic specification of the UCOn (usage control) model using the Lamport's temporal logic of actions (TLA). TLA provides an elegant formalism, able to model the innovative features of UCON, such as actions, obligations, and conditions. The second paper: *Implementing Access Control to People Location Information*, by U. Hengartner and P. Steenkiste deals with the problem of protecting location information, which is today very relevant due to the widespread use of devices allowing one to localize who is using them. The paper presents an access control model for protecting people location information and the design of a decentralized access control mechanism, which relies on the use of SPKI/SDSI certificates. The last paper of the first session: *Role-based Access Control in Ambient and Remote Space*, by H.F. Wedde and M. Lischka, deals with the management of distributed and mobile access requests, particularly crucial in the era of Ubiquitous Computing. The paper presents a role-based solution, based on previous work by the same authors on Modular Authorizations.

The second session: *Access Control Policy Implementation*, contained three papers focusing on various issues related to access control policies enforcement. In *Towards a Credential-based Implementation of Compound Access Control Policies*, J. Biskup and S. Wortmann present an approach for implementing access control policies using SPKI/SDSI certificates. The considered policies can be composed and specified according to an algebra, able to combine policies of heterogeneous, distributed systems. The paper shows the extensions required to SPKI/SDSI certificates in order to support a relevant fraction of the considered algebra. The second paper, *Succint Specifications of Portable Document Access Policies*, by M. Bykova and M. Atallah, deals with the problem of storing policy information in limited-capacity storage devices, such as cards and sensors. Policies a user satisfies are represented as binary strings. The paper presents an approach for reducing the size of policy strings, and schemes for diminishing the number of false positives (i.e., extra documents that can be accessed even if they are not authorized by any policy, because of the memory constraints on policies storage). Finally, *On the Role of Roles: from Role-based to Role-sensitive Access Control*, by X. Ao and N.H. Minsky analyzes the role of roles in access control. The authors thesis is that an access control mechanism should not be based on any interpretation of the semantics of roles, rather it has to allow the specification of role-based policies as well as of any other useful policies, not based on the concept of role. To support this thesis, the authors show how the LGI mechanism they previously developed can support both role-based policies, even if it does not have any built-in notion of role, and other relevant policies, not directly related to the concept of role.

The third session, *Access Control for XML Data*, was devoted to the problem of securing XML data. The first paper, *Specifying Access Control Policies for XML Documents with XPath*, by I. Fundulaki and M. Marx, shows how XPath can be used for specifying the semantics of access control policies for XML documents. The authors consider policies specified by using some of the most relevant access control models for XML documents proposed so far. Additionally, the paper discusses the benefits of using XPath as semantic foundation for access control policies. In the second paper, *A Role-based Approach to Access Control for XML Databases*, J. Whang and S.L. Osborn show how role-based access control and an access control model previously developed for object-oriented databases can be effectively combined and used for protecting XML documents. They also show how the resulting model is very expressive and able to support advanced features such as privilege propagation and propagation exceptions.

The fourth session, *Role Administration*, consisted of three papers. The first, *X-GTRBAC Admin: A Decentralized Administration Model for Enterprise Wide Access Control*, by R. Bhatti, J.B.D. Joshi, E. Bertino, and A. Ghafoor presents an administration model for X-GTRBAC, a role-based temporal access control model previously proposed by the same authors. The administration model is modular designed and simplifies the task of user-role and permission-role assignment. During the presentation, the authors run a demo of the implemented prototype. The second paper; *A Meta Model for Authorisations in Application Security Systems and their Integration into RBAC Administration*, by A. Kern, M. Kuhlmann, R. Kuropka, and A. Ruthert deals with application security. The authors, based on their experience on the administration of policies for large industry application systems, propose a method which integrates application security into RBAC systems, and show the benefit of this in terms of complexity reduction. In the last paper of the session, *Administrative Scope in the Graph-based Framework*, M. Koch, L.V. Mancini, and F. Parisi-Presicce show the benefits of using a graph-based framework for the specification of administration rules in RBAC systems. The main benefits are the possibility of specifying a precise semantics for the operations, and the intuitive and visual representation given by graphs.

The fifth session, *Constraints*, consisted of two papers

focusing on two different kinds of security constraints. The focus of the first paper, *Resolving Constraint Conflicts*, by T. Jaeger, R. Sailer, and X. Zhang, was on constraint conflicts expressing inconsistencies between the specified access control policy and the constraints that may have been specified to limit the policy. The authors propose a formal framework for detecting and solving such conflicts and a set of metrics that can be used during conflict resolution. They use, as case study, a Biba integrity constraint on the SeLinux policy. By contrast, the second and last paper of this session: *Using UML to Visualize Role-Based Access Control Constraints*, by I. Ray, N. Li, R. France, and D.K. Kim, shows how the Unified Modeling Language (UML) can be used to specify RBAC policies and role constraints, thus making them integrated with the application design.

The sixth session, *Security Analysis* was composed by two papers. The first, *Security Analysis in Role-based Access Control*, by N. Li and M.V. Tripunitara, considers the problem of authorization delegation and proposes the use of security analysis techniques for checking the satisfaction of security properties when delegating administrative privileges. The second paper of the session, *Towards a Formal Model for Security Policies Specification and Validation in the SELinux System*, by G. Zanin and L.V. Mancini, presents SELAC, a formal model for the analysis of security policy configurations in SELinux. By using SELAC it is possible to determine, given a set of configuration rules, which accesses can be granted according to these rules and which should be denied.

The seventh and last session of the symposium, *Access Management for Distributed Systems* discussed solutions to manage the complexity of access control in large distributed systems. It consisted of three papers. The first, *Role-based Cascaded Delegation*, by R. Tamassia, D. Yao, and W.H. Winsborough, proposes a model for delegation of authority in trust management systems, based on roles and cascaded delegation. Additionally, it proposes an efficient implementation strategy for such a model, which relies on the use of the Hierarchical Certificate-based Encryption Scheme. In the second paper, *Using Trust and Risk in Role-based Access Control Policies*, N. Dimmock, A. Belokosztolszki, D. Eyers, J. Bacon, and K. Moody present some of the results obtained in the framework of the SECURE project, a European project whose overall goal is to define a trust-based generic decision-making framework to be used in Global Computing. The paper focuses on trust and risk management and shows how the OASIS RBAC system, previously proposed by the same authors, can be extended to deal with trust and risk. Finally, the last paper of this session: *A Composite RBAC Approach for Large, Complex Organizations*, by J.S. Park, K.P. Costello, T.M. Neven, and J.A. Diosomito, focuses on the problem of role management in large and distributed organizations, consisting of many different and heterogeneous systems. The paper claims that a way to manage such complexity is to distinguish between organizational and system roles, and provides a mapping strategy between these two classes of roles.

Conclusions

The success of SACMAT'04 was mainly due to the quality of the selected papers and the lively discussion that took place during all the days of the symposium. More information about SACMAT'04 and the previous editions are available at http://www.sacmat.org. The site also contains the slides of all the presentations given at SACMAT'04.
Next year, SACMAT will be held in Stockolm, Sweden, co-located with the POLICY 2005 Workshop. The Call for Papers and submission instructions will be available at the SACMAT web site.

Acknowledgments. Special thanks are due to Trent Jaeger, the general chair of SACMAT'04, and to the local arrangement committee for their organizative effort. Moreover, I would like to thank the authors, the participants, the speakers, and the panelists of SACMAT'04, as well as all the SACMAT'04 chairs. Finally, I would like to thank the program committee members and external reviewers for the high quality of the proceedings, and our sponsor ACM SIGSAC.