JYVÄSKYLÄ STUDIES IN COMPUTING

78

Anton Naumenko

Semantics-Based Access Control in Business Networks

JYVÄSKYLÄN YLIOPISTO

JYVÄSKYLÄ STUDIES IN COMPUTING 78

Anton Naumenko

Semantics-Based Access Control in Business Networks

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi yliopiston Agora-rakennuksessa (Ag Aud. 2)
kesäkuun 28. päivänä 2007 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
in the building Agora, Ag Aud. 2, on June 28, 2007 at 12 o'clock noon.

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2007

Semantics-Based Access Control in Business Networks

JYVÄSKYLÄ STUDIES IN COMPUTING 78

Anton Naumenko

Semantics-Based Access Control in Business Networks

UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2007

Editors
Tommi Kärkkäinen
Department of Mathematical Information Technology, University of Jyväskylä
Irene Ylönen, Marja-Leena Tynkkynen
Publishing Unit, University Library of Jyväskylä

URN:ISBN:9789513928759
ISBN 978-951-39-2875-9 (PDF)

ISBN 978-951-39-2866-7 (nid.)
ISSN 1456-5390

Jyväskylä University Printing House, Jyväskylä 2007

ABSTRACT

Naumenko, Anton
Semantics-Based Access Control in Business Networks
Jyväskylä: University of Jyväskylä, 2007, 72 p. (+ included articles)
(Jyväskylä Studies in Computing,
ISSN 1456-5390; 78)
ISBN 978-951-39-2875-9 (PDF), 978-951-39-2866-7 (nid.)
Finnish Summary
Diss.

In business-to-business collaboration, one of the most important issues is privacy and trust. Adequate access control solutions may give a business and its partners the vital possibility to preserve confidentiality, integrity and availability of information and services. This is what businesses need in order to obtain or retain business advantages they derive from the trustful cooperation. Current and emerging information technologies support cooperative business processes across enterprise boundaries. Web-based information systems become more complex, dynamic, heterogeneous, pervasive, nomadic, and open. Conventional security measures fall short to serve both emerging technologies and innovative information systems.

In response to the growing complexity of management of access control for inter-organizational automated business processes, this work aims at the policy-based management of access control in business networks on the abstract conceptual level with authorizations based on semantic relations between concepts, i.e., Semantics-Based Access Control (SBAC). The main contributions of this dissertation are the SBAC conceptual semantics, the SBAC functional semantics, a prototype implementation of the SBAC enforcement function, and initial attempts towards the adoption of SBAC for different technological profiles and in different business domains. Theoretical research results have been aligned with the business needs and critical success factors that are crucial for the applicability of SBAC in real-world settings. This dissertation covers the first full iterative cycle of research on SBAC. It starts chronologically with the case studies in order to derive real-world practical needs, follows with the conceptual-analytical research on the SBAC components, and ends with the qualitative and quantitative evaluation towards justification of initial research ideas. A research framework has been created to coordinate and guide our doctoral research towards SBAC. At the same time, this research framework can organize the future theoretical and practical research on SBAC along the extensible layers of conceptual semantics, functionality, technological profiles, and business domains.

Keywords: access control, Semantic Web, business network, ontology, policy, web service, multi-agent system

ACM Computing Review Categories

D.4.6 OPERATING SYSTEMS: Security and Protection: *Access controls*

H.3.5 INFORMATION STORAGE AND RETRIEVAL: Online Information Services: *Web-based services*

I.2.3 ARTIFICIAL INTELLIGENCE: Deduction and Theorem Proving: *Inference engines*

I.2.4 ARTIFICIAL INTELLIGENCE: Knowledge Representation Formalisms and Methods: *Predicate logic, Representation languages, Semantic networks*

I.2.11 ARTIFICIAL INTELLIGENCE: Distributed Artificial Intelligence: *Intelligent agents, Languages and structures, Multiagent systems*

J.7 COMPUTERS IN OTHER SYSTEMS: *Industrial control*

Author's address

Anton Naumenko
Dept. of Mathematical Information Technology
University of Jyväskylä
P.O.Box 35
FIN-40014 Jyväskylä, Finland
annaumen@cc.jyu.fi

Supervisors

Prof. Dr. Vagan Terziyan
Dept. of Mathematical Information Technology
University of Jyväskylä, Finland

Prof. Dr. Timo Tiihonen
Dept. of Mathematical Information Technology
University of Jyväskylä, Finland

Reviewers

Prof. Dr. Aphrodite Tsalgatidou
Dept. of Informatics and Telecommunications
National & Kapodistrian University of Athens, Greece

Dr. Gregory Levitin
Eng.-Expert,
The Israel Electric Corporation
Haifa, Israel

Opponent

Prof. Dr. Kimmo Salmenjoki
Dept. of Computer Science
University of Vaasa, Finland

ACKNOWLEDGEMENTS

Already at the high school, more than ten years ago I knew that I would head for a Doctoral degree. What I did not know was that I would reach it abroad in such an excellent place as the University of Jyväskylä in Finland. This became possible because of the student exchange programme between the University of Jyväskylä and Kharkov National University of Radioelectronics, Ukraine, that was organized by Dr. Helen Kaykova, Prof. Vagan Terziyan and Prof. Timo Tiihonen.

Later, Professors Vagan Terziyan and Timo Tiihonen have supervised my doctoral research. I thank them for their unwavering guidance for and help with the doctoral research. They managed to make efficient and effective team to ensure my results.

After the supervisors, the reviewers and opponent gave the finishing touch to the whole process. I was lucky enough to get constructive and helpful reviewers, Prof. Aphrodite Tsalgatidou and Dr. Gregory Levitin. I thank them ever so much for playing their important roles and look forward for the scientific debate with the opponent, Prof. Kimmo Salmenjoki.

Cordial thanks go to all the co-authors of the included articles, Prof. Vagan Terziyan, Sergiy Nikitin, Andriy Zharko, Dr. Artem Katasonov, Mirja Pulkkinen, Dr. Kari Luostarinen, Satish Srirama, and Prof. Matthias Jarke.

For the academic financial support I am grateful to the COMAS Graduate School, to the Rector and to the Department of Mathematical Information Technology, University of Jyväskylä.

During the doctoral research I participated to several research projects and highly appreciate the financial support from these projects. The National Technology Agency of Finland (Tekes), Agora Center of the University of Jyväskylä, and cooperating companies (ABB, Metso Automation, TeliaSonera, TietoEnator, and Jyväskylä Science Park) supported activities of the "SmartResource: Proactive Self-Maintained Resources in Semantic Web" research project. The "Mobile Design Patterns and Architectures" (MODPA) research project had been funded by Tekes and industrial partners: Metso Paper, Nokia, SysOpen Digia, SESCA Technologies, Tieturi, and Trusteq. The "SWIMMER: Semantic Web Integrator for Maintenance Management of Enterprise Resources" research and development project is privately funded by Metso Automation. The "Adaptive Services Grid" (ASG) is 6th Framework Integrated Project (EU-IST-004617) funded by the European Commission. The "UBIWARE: Smart Semantic Middleware for Ubiquitous Computing" research project is funded by Tekes and the industrial consortium of ABB, Fingrid, Metso Automation, TeliaSonera, Metso Shared Services, Inno-W, and Hansa Ecura.

I give many thanks to the people behind the above mentioned projects for fun and joyful collaboration. Besides the above mentioned, they are Oleksiy Khriyenko, Oleksandr Kononenko, Dmytro Kovtun, Dr. Jouni Markkula, Dr. Oleksiy Mazhelis, Yaroslav Tsaruk, and Prof. Jari Veijalainen.

Also, I would like to acknowledge the significance of the participation of the following companies and their representatives to my doctoral research, i.e. Dr. Kari Luostarinen from Metso Paper, Dr. Jouni Pyötsiä from Metso Automation, Marko Viitala from ABB, and Vesa Halonen from Trusteq.

Special thanks go to my beloved wife for the ardent inspiration and unstinting support. Also, my parents have always supported my every endeavor related to studies. I wish to be able to repay the same to their grandchildren. Last but not least I am grateful to Ukrainians who have stood by me being good friends and colleagues.

Jyväskylä
June 11, 2007

Anton Naumenko

ACRONYMS

ASG	The “Adaptive Services Grid” research project
DAML	DARPA Agent Markup Language
DAML-S	DAML Services
DL	Description Logic
DRM	Digital Rights Management
EA	Enterprise Architecture
EAC	Enterprise Access Control
EAF	Enterprise Access Control Framework
ERBAC	Enterprise RBAC
ESMS	Enterprise Security Management System
GPRS	General Packet Radio Service
HSCSD	High-Speed Circuit Switched Data
ICT	Information and Communication Technology
IST	Information Society Technologies
IT	Information Technology
JXTA	Opensource-based peer-to-peer infrastructure
KPO	KAoS Policy Ontology
MAC	Mandatory Access Control
MAS	Multi-Agent System
MODPA	The research project: “Mobile Design Patterns and Architectures”
MWS	Mobile Web Service
NIST	National Institute of Standards and Technology
NS	Native System
OREL	Ontology-based Rights Expression Language
OWL	Web Ontology Language
OWL-DL	Description Logic profile of OWL
OWL-S	Semantic Markup for Web Services
P2P	Peer-to-peer
PDM	Product Data Management
PPP	Point-to-Point Protocol
PRBAC	Parameterized RBAC
RAB	Reusable atomic behavior
RBAC	Role-Based Access Control
RDF	Resource Description Framework
RDFS	RDF Schema
ReSIST	The network of excellence: “Resilience for Survivability in IST”
REWERSE	The network of excellence: “Reasoning on the Web”
RMMS	Remote Machinery Maintenance Service
SAC	Semantic Access Control
SACE	Semantic Access Control Enabler

SAML	Security Assertions Markup Language
SBAC	Semantics-Based Access Control
SmartAlliance	The research project proposal: “Ontology-Based Collaboration and Integration Platform for PRINDEX Alliance”
SmartResource	The research project: “Proactive Self-Maintained Resources in Semantic Web”
SOA	Service-Oriented Architecture
SPARQL	SPARQL Protocol and RDF Query Language
SURPAS	Smart Ubiquitous Resource Privacy and Security
SWRL	Semantic Web Rule Language
SWS	Semantic Web Service
SWSF	Semantic Web Services Framework
UBIWARE	The research project proposal: "Smart Semantic Middleware for Ubiquitous Computing"
WLAN	Wireless Local Area Network
WSDL-S	Web Service Semantics
WSMO	Web Service Modeling Ontology
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

LIST OF FIGURES

CONTENTS

LIST OF ORIGINAL ARTICLES

I Naumenko A., Nikitin S., Terziyan V., Zharko A., (2005). Strategic Industrial Alliances in Paper Industry: XML- vs. Ontology-Based Integration Platforms, In: The Learning Organization, Special Issue on: Semantic and Social Aspects of Learning in Organizations, Emerald Publishers, 12(5): 492-514.

II Luostarinen, K., Naumenko, A., Pulkkinen, M., (2006), Identity and Access Management for Remote Maintenance Services in Business Networks, in IFIP International Federation for Information Processing, Project E-Society: Building Bricks, eds. R. Suomi, Cabral, R., Hampe, J. Felix, Heikkilä, A., Järveläinen, J., Koskivaara, E., (Boston: Springer), (226):1-12.

III Naumenko, A., (2006), Contextual rules-based access control model with trust, In Shoniregan C. A. and Logvynovskiy A. (Eds.), Proceedings of the International Conference for Internet Technology and Secured Transactions, ICITST 2006, 11-13 September, London, UK, e-Centre for Infonomics, pp. 68-75.

IV Naumenko A., (2007), Semantics-Based Access Control: Ontologies and Feasibility Study of Policy Enforcement Function , In: J., Filipe, J., Cordeiro, B., Encarnacao, and V., Pedrosa (Eds.), In Proceedings of the 3rd International Conference on Web Information Systems and Technologies (WEBIST-07), Barcelona, Spain - March 3-6, 2007, Volume Internet Technologies, INSTICC Press, pp. 150-155.

V Naumenko, A. and Luostarinen, K., (2006), Access Control Policies in (Semantic) Service-Oriented Architecture, In Schaffert S. and Sure Y. (Eds.), Semantic Systems From Visions to Applications, Proceedings of the SEMANTICS 2006, Austrian Computer Society, Vienna, Austria, pp. 49-62.

VI Naumenko A., Katasonov A., Terziyan V., (2007), A Security Framework for Smart Ubiquitous Industrial Resources, In: Goncalves, R., Müller, J., Mertins K., and Zelm, M., (Eds.), In: Enterprise Interoperability II: New challenges and Approaches, Proceedings of the 3rd International Conference on Interoperability for Enterprise Software and Applications (IESA-07), March 28-30, 2007, Madeira Island, Portugal, Springer, 183-194.

VII Srirama, S., and Naumenko, A., (2007). Secure Communication and Access Control for Mobile Web Service Provisioning, In CD-ROM Preprints of Proceedings of International Conference on Security of Information and Networks (SIN2007), 8-10th May, 2007.

VIII Naumenko, A., Srirama, S., Terziyan, V., and Jarke, M., (2007), Semantics-Based Access Control for Mobile Web Services, International Journal on Semantic Web and Information Systems, Special Issue on Mobile Services and Ontologies, (Submitted for review 2nd of May, 2007).

IX Naumenko, A., (2007), A Research Framework towards Semantics-Based Access Control, International Journal of Network Security, (Submitted for review 2nd of May 2007).

1 INTRODUCTION

Globalization of economy, global and intercultural value chains, large-scale industrial environments, cooperative systems for the international production, logistic, and marketing could hardly be imagined without the rapid evolution of information and communication technologies (ICTs). Moreover, continuous advances of ICTs and their adoption in the industrial world have contributed to the sustainable improvement and efficiency of industrial technologies in the last decades. World Wide Web and Internet technologies have been the drivers and enablers of the most prominent advances in ICTs for industrial collaboration and business networks.

The current Web is evolving towards the Web 2.0, which is an intermediate step towards Semantic Web (Berners-Lee et al., 2001), by adopting new unique advanced features (O'Reilly, 2005). Web-based information systems become more complex, dynamic, heterogeneous, pervasive, and open. Recent advances in networking, sensor and RFID technologies, etc. allow connecting various physical world objects to the information technology (IT) infrastructure. Together with ubiquitous and autonomic computing (Kephart, and Chess, 2003), the ambient intelligence ultimately leads to the "Internet of things". On the other hand, real-world demands for the security have grown increasingly year-by-year. Conventional security measures fall short of serving both emerging Internet technologies and innovative web-based information systems. For example, ambient intelligence and ubiquity of information technologies have brought the digital and physical worlds nearer to such an extent that security becomes the decisive issue in the corresponding environments. The major security implication of these penetrating ICTs is that the risks and negative consequences of security threats become higher than ever.

This dissertation aims to bridge the gap between capabilities of existing access control approaches and growing practical needs of business networks and emerging ICTs to manage access control. This chapter introduces the research area and fundamental concepts of access control, provides an insight into the importance of trust relationships in business networks, briefly describes the Semantic Web standards, and provides the outline of the thesis.

1.1 Fundamentals of access control

Traditional security goals like confidentiality, availability, reliability, integrity, manageability, accountability, responsibility etc., together with conventional measures and mechanisms that support security, do not cover all the needs and threats of new cross-organizational computing environments. Amongst different security measures, access control solutions mainly impact the level of support for confidentiality, integrity, and availability. These are the major security goals in business-to-business relationships.

Confidentiality is an "assurance that information is not disclosed to unauthorized persons, processes, or devices" (INFOSEC 1999). Data integrity is a property of information that is consistently altered, modified or destroyed (INFOSEC 1999). In a wider interpretation, integrity of information systems corresponds to "the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data" (INFOSEC 1999). Availability is a quality of information systems to provide "timely, reliable access to data and information services for authorized users" (INFOSEC 1999).

Access control can be decomposed to two areas – authentication and authorization, i.e., access control refers to the management of admission to system and network resources: "The first part of access control is authenticating the user, which proves the identity of the user or client machine attempting to log on. The second part is granting the authenticated user access to specific resources based on company policies and the permission level assigned to the user or user group."[1] Authentication is a "security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information" (INFOSEC 1999). Authentication is the basis for authorization.

There is a narrower interpretation of access control that mainly encompasses authorization. Access control is seen as "limiting access to information system resources only to authorized users, programs, processes, or other systems" (INFOSEC 1999). Authorization has two distinct meanings relevant to computer security. Authorization is firstly, a right or a permission to use a system resource (INFOSEC 1999) and secondly, it is a process of granting access. The first meaning of authorization relates to the administration function of access control, the second to the enforcement function. The administration function manages user rights and access control policies, also referred to as security policies, which mean laws, rules, conditions, regulations and practices of managing, protecting, and sharing of computing and information assets. A policy can be application or platform specific or can span boundaries of application and enterprise IT infrastructure. The enforcement function consists

[1] "access control." Computer Desktop Encyclopedia. Computer Language Company Inc., 2005. Answers.com 12 .2006. http://www.answers.com/topic/access-control

of access control mechanisms to enforce security policies. An access control mechanism is a “security safeguard designed to detect and deny unauthorized access and permit authorized access” (INFOSEC 1999). It is desirable to use common access control mechanisms for a wide range of policies and to enforce one policy in a wide variety of environments using native access control mechanisms. An access control mechanism implements an access control model. An access control model is a mathematically precise statement of a security policy. It represents the state of a security system and transitions from one state to another state. Thus, access control models mediate security policies and access control mechanisms.

1.2 Trust and privacy in business networks

In response to the modern trends of tightening collaboration in business networks, current and emerging ICTs support cooperative business processes across boundaries of enterprises and organizations (Britton and Bye, 2004; Linthicum 2004). However, this support is limited and there is still space for more sophisticated solutions in order to integrate the information systems of collaborating partners. Currently, one of the most important need-to-be-addressed issues is privacy and trust in business-to-business relations with inter-organizational automated processes. To build trust, one of the first thresholds to overcome is the protection of the information systems and data from unauthorized access. This protection from unauthorized access may give a business and its partners the means to preserve confidentiality, integrity and availability of their business information and business services. This is needed for businesses in order to obtain or retain business advantages they derive from the trustful cooperation. According to the definition of business network by Rosenfeld (1995), a business network is "a group of firms with restricted membership and specific, and often contractual, business objectives likely to result in mutual financial gains… Networks develop more readily within clusters, particularly where multiple business transactions have created familiarity and built trust”.

1.3 Semantic Web standards

Semantic Web has been a vision (Berners-Lee et al., 2001) for the future Web that is now supported by standards, technologies, tools and some success stories. World Wide Web consortium (W3C) launched the Semantic Web Activity as the major standardization process towards “a common framework that allows data to be shared and reused across application, enterprise, and community boundaries”. This is expected to be achieved using a conceptual layer of machine-understandable metadata, making the content available for processing by intelligent software based on that content's semantics. For that, Semantic Web provides standards and tools, based on semantic annotations and ontologies, to deal with the explicit semantics of various Web resources.

In philosophy an ontology is regarded as a systematic account of existence. In computer science the term ontology has another interpretation. According to Gruber (1993), ontology is an explicit specification of conceptualization. An ontological approach allows a shared and common understanding of the domain and facilitates communication between people and heterogeneous and widely spread application systems (Fensel, 2001). A semantic annotation of an entity contains all assertions where this entity appears as the subject.

The Web Ontology Language (OWL) standard defines a language for ontologies (McGuinness and Harmelen, 2004). OWL naturally supports sharing of ontologies, evolution of ontologies, interoperability of ontologies using ontology mapping, detecting inconsistencies in the specification of semantics, balance between expressivity and scalability of reasoning algorithms, a low learning barrier of the language, compatibility to other commonly accepted open standards, internalization of ontology, and other features.

OWL relies on the Resource Description Framework (RDF) standard (Hayes, 2004). RDF introduces a formal model of knowledge specification based on assertions in the form of triples. A triple consists of a subject, a predicate and an object of assertion. Subjects, predicates and objects are identified by URI. The OWL and RDF standards use eXtensible Markup Language (XML) (Yergeau et al., 2004). RDF provides a structure for describing and interchanging metadata on the Web (Powers, 2003). RDF is expressive and flexible technology to describe different and arbitrary domains and thus it is widely applicable. There is also a variety of software tools to work with RDF. These include tools for creating RDF triples, for creating a vocabulary for RDF triples called Schema (RDFS), for querying RDF triples, for making an inference based on a defined RDF graph (semantic network), and other.

1.4 Thesis outline

The remainder of the thesis is organized as follows. Chapter 2 presents the research problem, describes the research process, and outlines the employed research methods. Chapter 3 briefly presents all the major results of this research. The related research work and relevant research projects are presented in Chapter 4. Chapter 5 provides a brief overview of the nine original articles, which are included into this thesis, with the description of the author's contribution for the joint publications. The last chapter, Chapter 6, summarizes the contributions of this thesis, and discusses its limitations and future research directions.

2 RESEARCH OBJECTIVES AND RESEARCH APPROACH

The first part of this chapter presents the research problem and its decomposition to the more specific research objectives and research questions. The chapter then describes the research process and research methods.

2.1 Problem statement and research objectives

This work aims at a policy-based management of access control in business networks on the abstract conceptual level with authorizations based on semantic relations between concepts, i.e., Semantics-Based Access Control (SBAC). The major research objectives of this research are the following.

G1 The research must lead to a solid conceptualization that integrates existing knowledge and provides possibilities to facilitate integrating new knowledge.

G2 Qualitative and quantitative evaluations are necessary to provide convincing arguments for the feasibility and rationality of SBAC.

G3 This research should take into account the real-world practical needs of both business networks of commercial companies and emerging ICTs.

Each of the research goals has several research questions. These questions help either to narrow the focus or to determine some important features and qualities of the results.

G1.R1 One has to define what are the most generic concepts and relations in the field of access control. These generic concepts and relations should form the core part of the SBAC conceptual semantics.

G1.R2 The major research question related to the first goal is how to systematically manage the semantics of these generic concepts and relations in SBAC.

G1.R3 Regarding the functionality of SBAC, the question is how to identify and to abstractly design functional access control components for SBAC.

G2.R1 For the qualitative evaluation there should be criteria upon which the SBAC results can be evaluated. Thus it is important to identify what the critical success factors for SBAC are.

G2.R2 Besides the qualitative evaluation, the major practical concern is whether it is feasible to implement SBAC with existing tools and technologies. It is also interesting to check the level of reuse of existing tools.

G2.R3 If SBAC is feasible from the system development point of view, then the next question is whether it is rational from the perspective of performance.

G3.R1 The rationality of SBAC does not only originate from the performance, but it heavily depends on the applicability of SBAC for some real-world practical needs. Thus, the research should explore what the most vital practical business needs for SBAC are.

G3.R2 Subsequently, it is important to see how the SBAC conceptual semantics can be specialized in different domains and for different technologies.

G3.R3 The same is true for the SBAC functionality - how the abstract design of the SBAC can be implemented using the existing paradigms of design of information systems and technologies, and deployed in different domains.

2.2 Research methods and research process

The research on SBAC has used different research methods in order to motivate, elaborate and evaluate it.

2.2.1 Conceptual-analytical research towards theoretical results

The Conceptual-Analytical research (Järvinen, 2004) helped to motivate SBAC and produced the SBAC model, the SBAC ontologies, the SBAC abstract architecture, and the SBAC research framework. We present the historical context for the motivation of this dissertation in this section. The SBAC research framework is presented in the next section. Other theoretical results are discussed in Chapter 3.

The research plan and proposal for SBAC originates from a discussion with the Metso Automation about possible collaborative research and development during 2005-2007, which should aim at a collaboration and integration platform of the industrial alliance for Process Industry Data Exchange (PRINDEX). This discussion resulted in the planning of a research project called SmartAlliance: Ontology-Based Collaboration and Integration Platform for PRINDEX Alliance. The project would have two stages:

1. Design a preliminary architecture of the agent-driven ontology-based alliance platform for collaboration and integration of virtual organizations and partners of strategic alliances. Elaborate ontology-based generic tools for the integration and data exchange which support dynamic nature of domain model and alliance policy.

2. Implement the alliance core ontology and the pilot of the alliance platform for the PRINDEX alliance.

As the above description shows, this project was expected to create an innovative and flexible methodology for inter-organizational management of policies when an ontology-based alliance policy is maintained by a distributed Multi-Agent System (MAS). Despite the fact that this research project application was never submitted for funding, it served as a background for the initial research proposal towards SBAC and for Article I, "Strategic Industrial Alliances in Paper Industry: XML- vs. Ontology-Based Integration Platforms" (Naumenko et al., 2005a).

2.2.2 The SBAC research framework

The SBAC research framework decomposes and shapes the SBAC research and development efforts into research layers and components from more abstract and theoretical to more concrete and practical (Article IX, "A Research Framework towards Semantics-Based Access Control"; Naumenko, 2007b). Each layer has several components. FIGURE 1 illustrates the SBAC research framework.

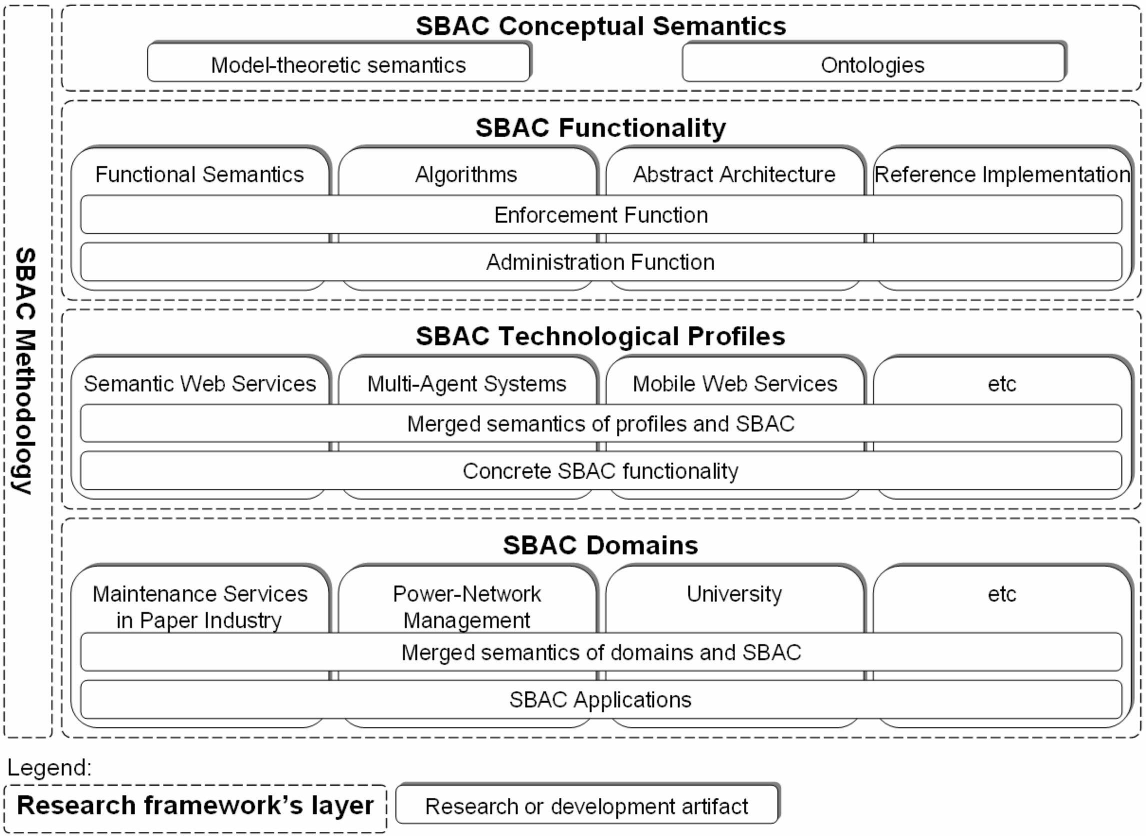

FIGURE 1 The SBAC research framework

The layers and the corresponding components are

– The layer of the conceptual semantics contains the model-theoretic semantics of SBAC and the SBAC ontologies (see Sections 3.1 and 3.2)

– The layer of the functional semantics contains the formal specification of the functionality, algorithms for complex functions and procedures, the abstract architecture and reference implementations (see Section 3.3).

– The layer of the SBAC technological profiles contains the conceptualization and functionality of SBAC with different technologies and paradigms for design of information systems (see Sections 3.5, 3.6 and 3.7).

– The layer of the SBAC adoption domains consolidates research results (e.g. merged semantics, SBAC applications, etc.) related to the real-world domains that were considered for the adoption of SBAC (see Section 3.8, 3.9 and 3.10).

– The SBAC methodology is a formally described system of principles, practices and procedures that guides all stakeholders on how to apply SBAC in concrete cases.

Iterative cycles of research and development according to the design research methodology (Hevner et al., 2004; March and Smith, 1995) were found the most appropriate for the eventual elaboration of SBAC. The process steps of design research methodology (awareness of the problem, development, evaluation, and conclusion) were applied.

2.2.3 System development and feasibility study

The experimental (quantitative) evaluation (Järvinen, 2004) of research ideas employed the System Development research method (Nunamaker et al., 1991) in order to prototype the SBAC enforcement function (Article IV, "Semantics-Based Access Control – Ontologies and Feasibility Study of Policy Enforcement Function"; Naumenko, 2007a). We had to specify the model-theoretic semantics of SBAC in the form of ontologies. Then, the abstract architecture had to be designed towards enforcing access control policies that are represented as ontologies. The feasibility study was based on the prototype of the SBAC enforcement function. The main purpose of this prototype was to make research results tangible for the rationality and feasibility study.

2.2.4 Alignment of results with practice

From the early beginning of our research we always tried to align the research results with practical concerns. Thus, we have been studying real-world business cases and current paradigms of design of information systems in the context of the adoption of SBAC.

Special attention has been paid to the practical motivation of SBAC using results of the Case Study research (Yin, 1994). This involved case studies of real businesses and business networks (see Section 3.8, 3.9 and 3.10 respectively):

1. The case study of Product Data Management (PDM) and Remote Machinery Maintenance Services (RMMSs) in the paper industry cooperating with Metso Automation, Metso Paper, and Trusteq. We studied the information exchange for the PDM process in the paper industry during the SmartResource project (Proactive Self-Maintained Resources in Semantic Web, see http://www.cs.jyu.fi/ai/OntoGroup/SmartResource_details.htm) (Kaykova et al., 2005a, 2005b, 2007). The

results of the case study of the security of RMMSs were initially released as the Case Report, "Metso Paper Oy and Trusteq Oy", in the Mobile Design Patterns and Architectures (MODPA) project (Pulkkinen et al., 2006). Then, the present situation, ongoing initiatives and envisioned long-term situation at Metso Paper were extrapolated into the roadmap (Article II, "Identity and Access Management for Remote Maintenance Services in Business Networks"; Luostarinen et al., 2006). Finally, the roadmap and security issues were revisited from another perspective, focusing the role of Enterprise Architecture (EA) (Lapkin, 2003) as a coordination tool (Pulkkinen et al., 2007).

2. The case study of decentralized network-centric management of power-networks cooperating with ABB (Article VI, "A Security Framework for Smart Ubiquitous Industrial Resources"; Naumenko et al., 2007a). The industrial case of distribution automation in power networks (ABB, Inc) was used in the SmartResource research project and during the preparation of a new research project, UBIWARE (Smart Semantic Middleware for Ubiquitous Computing). See Section 3.6 for details about SmartResource and UBIWARE.
3. The case study of the University of Jyväskylä and of the nation-wide educational network of universities (Virtual University) was conducted last.

The adopting of SBAC for different technological profiles of SBAC, i.e., Semantic Web Services (SWS), MASs and Mobile Web Services (MWS), was based on the case studies, conceptual-analytical research, and qualitative and quantitative evaluation of SBAC.

1. Using the SBAC model, experience from the Adaptive Services Grid (ASG) research project (Naumenko et al., 2005b, Tiitinen et al., 2005) and results of the case studies in the paper industry during the MODPA and SmartResource research projects, the author adopted SBAC for Semantic Web Services (SWSs) (Article V, "Access Control Policies in (Semantic) Service-Oriented Architecture"; Naumenko and Luostarinen, 2006). We motivated and exemplified this research by RMMSs, a domain for paper production machinery. See Section 3.5.
2. Then SBAC was applied for the UBIWARE platform (Article VI, "A Security Framework for Smart Ubiquitous Industrial Resources"; Naumenko et al., 2007a). From the technical perspective, UBIWARE is a MAS that is largely based on the SmartResource platform. We motivated this research by the practical needs in the domain of decentralized network-centric management of power networks. See Section 3.6.
3. Finally, SBAC was applied for MWSs (Article VII, "Secure Communication and Access Control for Mobile Web Service Provisioning", and Article VIII, "Semantics-Based Access Control for Mobile Web Services"; Srirama and Naumenko, 2007; Naumenko et al., 2007b) as a result of cooperation between two research groups of Prof. Dr. Vagan Terziyan and Prof. Dr. Matthias Jarke, on topics related to security of MWS provisioning. See Section 3.7.

3 SEMANTICS-BASED ACCESS CONTROL

This chapter briefly describes the major research and development artifacts that constitute SBAC and are covered by the SBAC research framework.

3.1 The SBAC model-theoretic semantics

We presented the formal conceptual semantics of SBAC in the form of a theoretical model (Article I, “Contextual rules-based access control model with trust”; Naumenko, 2006). This is the preferred style of presentation in the access control research domain. The SBAC conceptual semantics consolidate and formally specify existing knowledge of the access control domain. The model-theoretic semantics of SBAC is an extension of the model-theoretic semantics of the OWL standard (Patel-Schneider et al., 2004). The OWL semantics consists of four parts: formal specification of vocabularies and interpretations, interpretation of embedded constructs, interpretation of axioms and facts, and interpretation of ontologies. SBAC’s compliance to the direct model-theoretic semantics of OWL allows relatively simple introduction of vocabularies and interpretations of concepts of SBAC. This preserves all the features of OWL.

For example, the OWL standard defines the conditions for an abstract OWL interpretation to satisfy an OWL ontology. The definitions of when and how a collection of ontologies and axioms and facts is consistent and entails an ontology or axiom or fact provide background for reasoning and maintaining the integrity of SBAC data. The interpretation of ontologies is the key issue for evolution, consistency, reasoning and organizing features of SBAC; domain knowledge and concrete policies reside in different ontologies with high conceptual granularity for flexible further use (see Section 3.2).

In addition to using the ontological level of Semantic Web stack of layers, SBAC reuses semantics of Semantic Web Rule Language (SWRL) (Horrocks et al., 2004). SWRL rules help to specify semantics that are impossible or inconvenient to capture with the pure OWL language. SWRL is fully based on the direct model-theoretic semantics of OWL. SWRL rules have the form of Horn clauses . These clauses define an implication between two parts of rules – an antecedent and consequent. SWRL adds rules as axioms to the semantics of OWL. For more details, please refer to the specification of SWRL (Horrocks et al., 2004). SWRL allows the specification of domain rules for better formalization of domain knowledge; constraints related to access control in order to shape static and dynamic allocation of rights; conditional access control statements; and context.

The SBAC model defines the following concepts and relations that are partly represented by FIGURE 2.

– *Sets for access control resources and operations*. Access control resources can be subjects or objects of access control. Definition of the resource as a set for subjects and objects gives more flexibility in the specification of access control rights, because it is hard to separate resources to passive and active in environments where artificial resources play active roles and their relations to human users are weak or not present at all. Individual operations could be actions, transactions, access modes, trust predicates for trust statements, etc.

– *Sets of subsets of access control resources and operations*. These sets are partially ordered by the transitive subset relation.

– *Set of access control statements* denotes a many-to-many abstract relation between subject, operation and object of access using the three binary relations described below. This set, with the three binary relations, fixes the generic structure for security-related statements for different purpose. Specializations of this set define concrete semantics in the subdomain ontologies, for example a privilege statement, an obligation statement, a prohibition statement, etc. The main feature of the access control statement semantics and the whole SBAC is that security-related statements mentioned above are specified between sets of subjects, objects and operations instead of individuals.

– *Binary relations subject, operation, and object* are defined between the set of access control statements and the corresponding sets of subsets of resources and operations respectively.

– *Set of privilege statements* is a subset of the set of access control statements. A privilege is an authorization of resources to access other resources using some operations.

– *Set of prohibition statements* is a subset of the set of access control statements. Introducing means for the specification of prohibitions in the SBAC model enhances expressivity of the policy language to make negative authorizations explicit.

– *Set of obligation statements* is a subset of the set of access control statements. There is a need to add the notion of obligations into the SBAC model in order to support a provisional authorization (Jajodia et al., 2000). For provisional authorization, policies define provisional operations that must be executed to fulfill conditionally positive access control decisions or/and to supplement negative decisions.

– *Binary relation of precedence* between sets of access control statements. It is evident that policies with privileges, prohibitions and obligations are not free from conflicts in an arbitrary case. These policies require mechanisms to resolve conflicts and ambiguity for the guarantied decidability. Thus, SBAC policies specify precedence between different kinds of access control statements.

– *Authorization rule*s formally define the decision making functions for policies with only privileges or prohibitions or both with different precedence. According to these rules, the decision of granting or prohibiting depends on membership of resources and operations in sets and on graphs of the binary relations subject, operation and object.

– *Set of security-related rules* are used for the formalization of domain logic and specification of policies. For example, individual abstract statements may automatically gain their specialized interpretations to concrete statements based on conditions as opposite to the static specification without rules. The main benefit from using rules is expected from the possibility to extend the SBAC model with contextual features.

– *Binary relation of context* is defined between access control statements and security-related rules. There is no unified definition or approach for the context. In SBAC, conditions that shape the interpretation and enforcement of access control statements use contextual data. Rules refer to contextual information from atoms of their antecedents. It may be useful to refer back to rules from the statements for which those rules refine the interpretation.

– *Set of trust statements* that denote already established trust relationships. Trust statements comprise trust policies or trust agreements between parties based on commitments formulated and legislated beforehand, for example in the form of contracts like service level agreements. For the integration of trust and access control management, rules can use atoms that refer to trust statements as corresponding contextual data during the specification of conditional trust-based access control statements.

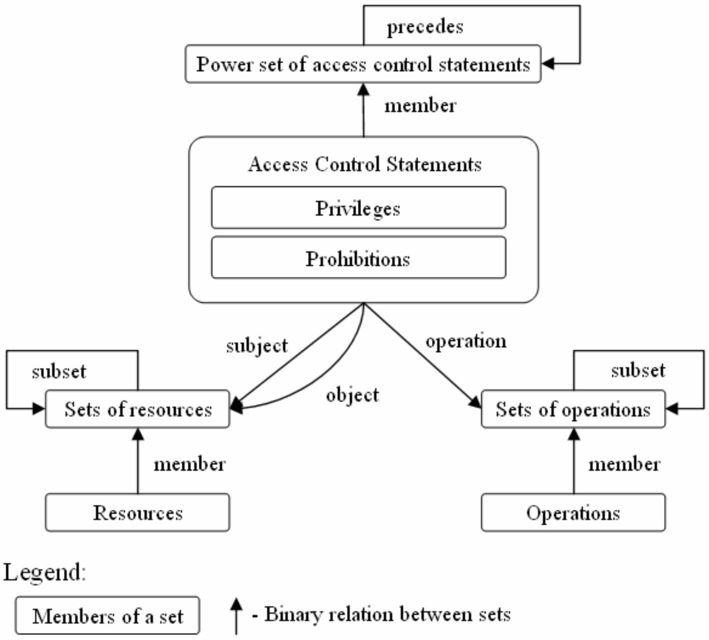

FIGURE 2 The core part of the SBAC model

3.2 The SBAC ontologies

The SBAC ontologies serialize the core part of the SBAC model in a machine-interpretable form. Additionally, we use ontologies to specify policies and domain models. For the specification of the SBAC ontologies we used the abstract syntax of OWL (McGuinness and Harmelen, 2004).

We introduced several ontologies to arrange the different concepts and features of SBAC with a high conceptual granularity. FIGURE 3 illustrates the SBAC ontologies, sample policies and importing mechanism between them.

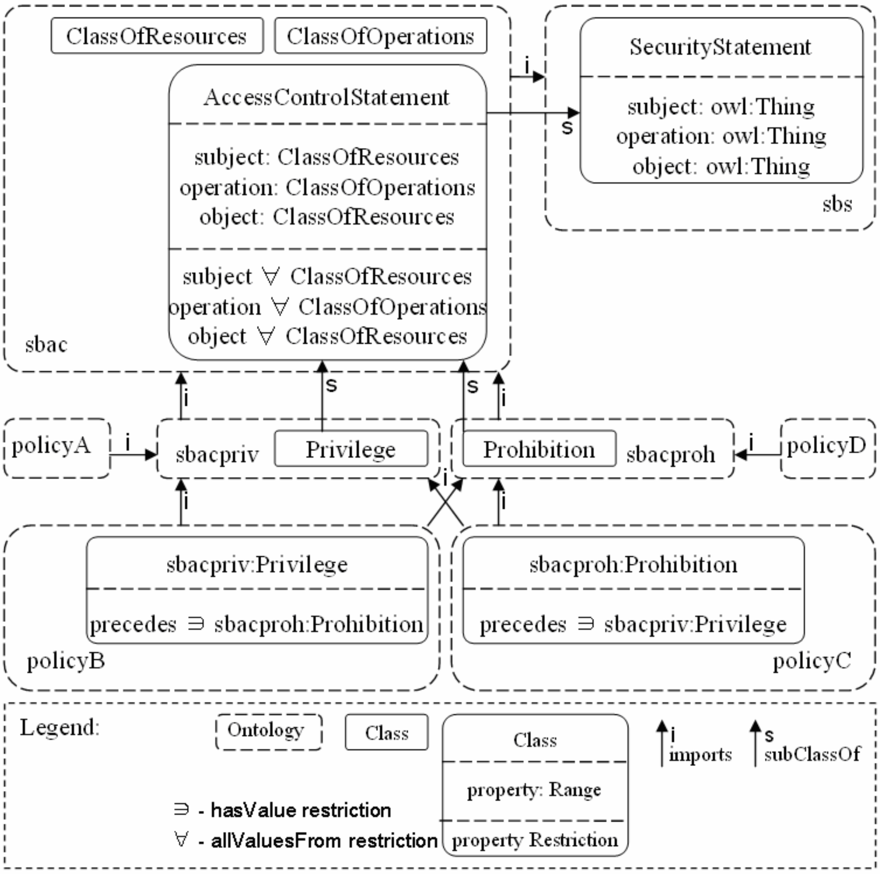

FIGURE 3 The SBAC ontologies and importing mechanism

Semantics-based security (SBS) ontology is an upper ontology. The SBS ontology defines one class and three individual-valued properties The class of security statements and three relations define a generic structure for the specification of statements related to security, e.g., privileges, prohibitions, obligations for access control, trace statements for logging and audit, reputation statements and trust agreement statements for trust management, and other.

The scope of SBAC has encompassed only the semantics of access control statements. Thus, the SBAC ontology imports the SBS ontology in order to allow specialization of the security statement and three relations. The introduced class for access control statements is a subclass of security statements. Subject, operation and object relations of access control statements are subproperties of the corresponding relations of the SBS ontology. The SBAC ontology also defines restrictions on these relations in that their values must be classes of resources and operations, respectively. For this purpose there are two subclasses of the owl:Class concept that denote the set of subsets of resources and the set of subsets of operations. Finally, there is an axiom defining the relation of precedence between specializations of access control statements, like privileges, prohibitions, etc.

The SBAC privilege and the SBAC prohibition ontologies import the SBAC ontology in order to extend it with class axioms that denote the set of privilege statements or the set of prohibition statements, respectively. These classes are subclasses of the abstract class of access control statements.

The sample policies A, B, C and D subscribe to different features of SBAC by importing different collections of SBAC ontologies. Policies A and D can use either privileges or prohibitions respectively. Policies B and C can use both kinds of access control statements, but these policies specify different precedence between privileges and prohibitions.

The issues related to the obligations, security rules, context and trust statements have been left for further consideration and are out of the scope of this research.

3.3 The SBAC abstract architecture

The abstract architecture is an upper view on the components of SBAC and interactions between them. This abstract design captures and reveals only fundamental elements and relations taking into account security patterns (Mazhelis and Naumenko, 2005, 2006). Basically, the abstract architecture is the main bridge between theoretical findings and adoption of SBAC into practice because the abstract architecture integrates the research on theoretical issues with practical concerns and with the development of applications. Another role of the abstract architecture is to ensure interoperability and reusability for SBAC. The abstract architecture consists of abstract design of common or shared characteristics of SBAC that can be formally related to every valid SBAC implementation. Possible concrete designs will be interoperable and will reuse reference implementations because of the shared abstract design.

The abstract architecture is a part of the SBAC functional semantics. In addition to the abstract architecture, the SBAC functional semantics includes other research components, i.e., formal specification of functionality, algorithms and reference implementations. The abstract architecture is closely related to these components. The formal specification of functionality and algorithms provide functional requirements for the design of abstract architecture. Then, the abstract architecture serves as an input to the process of piloting and testing research ideas. Due to the central role of ontologies in SBAC, the abstract architecture should follow Ontology-Driven Architecture (ODA) paradigm

(Tetlow et al., 2006) of software design. ODA is an emerging and immature research target. This is an additional challenge in tackling this research component.

The abstract architecture reflects the SBAC functionality's two main functions: the administrative function and the run-time authorization function, that is also called enforcement function or access control mechanism. The SBAC enforcement function defines an access control policy enforcement mechanism in SBAC. The enforcement function controls run-time access of requestors to protected resources according to ontology-based access control policies, credentials of requestors, attributes of objects and operations using algorithms of SBAC. The SBAC administration function defines mechanisms of manipulation with the SBAC data including semantic annotations of resources and operations, domain ontologies, ontology-based policies, configuration settings for the enforcement function, and other. We concentrated on the SBAC enforcement function during our research.

We identified the common components and characteristics for the SBAC enforcement mechanism. These components are the proactive guard (ProGuard), the policy information retrieval component (PIR), the context information retrieval component (CIR), and the resource information retrieval component (RIR). ProGuard is the proxy and guard for protected resources and information retrieval components. ProGuard enforces an access decision based on the reasoning over the semantically encoded access control policy and the semantic annotations of a subject, an operation, an object and a context of access. ProGuard, driven by results of reasoning, collects all needed semantic annotations and policy rules to make an access decision for communicating with information retrieval components, thus acting proactively. The reasoner interactively provides instructions to get additional data for further reasoning or a decision about access finally. The PIR component provides semantic annotations of access control policies and of trust agreements between cooperative partners. The RIR and CIR components provide unified interfaces to access semantic annotations of resource's attributes and contextual data respectively. FIGURE 4 shows the SBAC abstract architecture of the SBAC enforcement mechanism. FIGURE 5 illustrates a control flow of ProGuard.

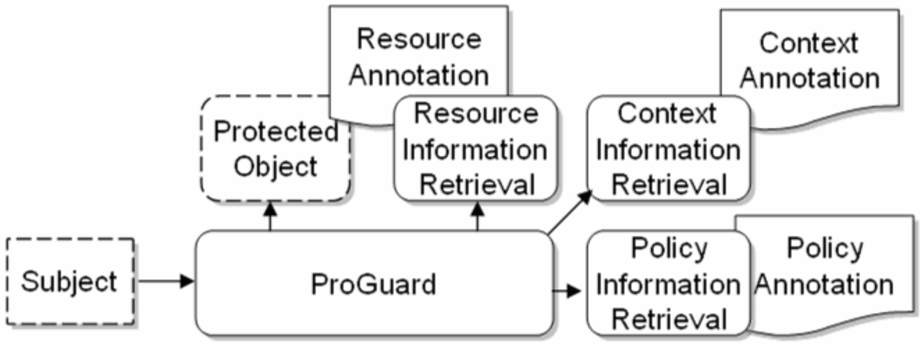
Resource Annotation
Context Annotation
Protected Object
Resource Information Retrieval
Context Information Retrieval
Subject
ProGuard
Policy Information Retrieval
Policy Annotation

FIGURE 4 The abstract architecture of the SBAC enforcement mechanism

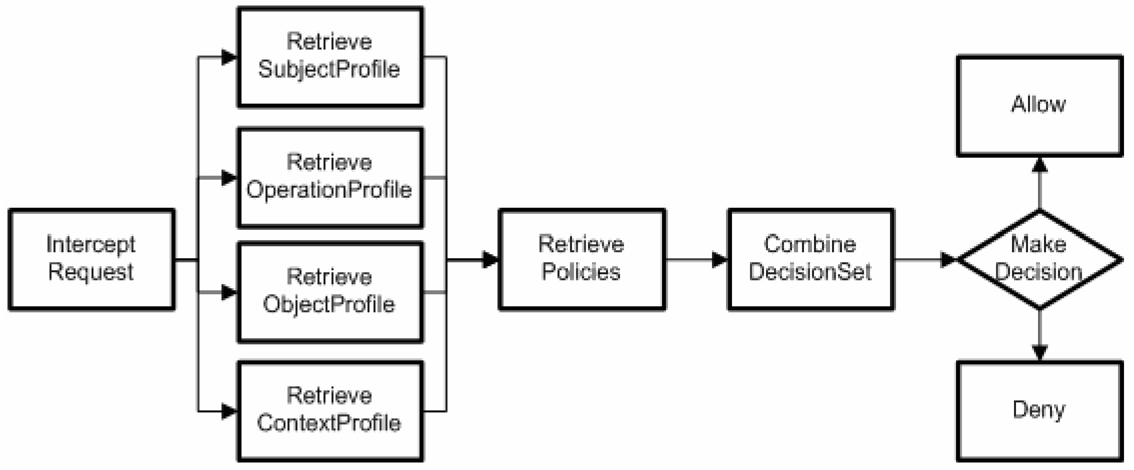

FIGURE 5 The SBAC enforcement procedure

3.4 Prototyping the SBAC enforcement function

After the integration of the revealed components and characteristics in architectural abstractions, the SBAC enforcement mechanism was prototyped for the rationality and feasibility study. FIGURE 6 shows the UML deployment diagram for the prototype.

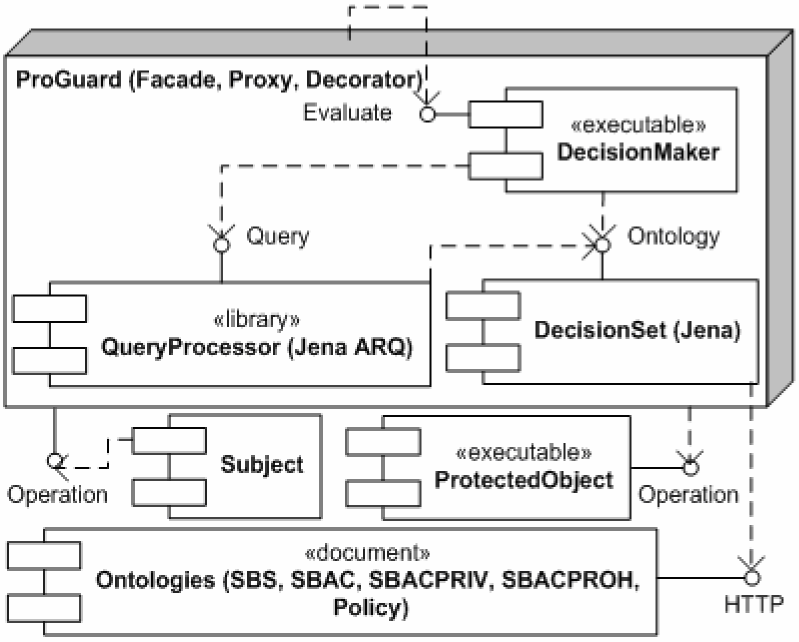

FIGURE 6 The architecture of the prototype

Several existing tools and standards were reused during piloting the SBAC enforcement function for the feasibility study. The SBAC ontologies have been piloted with the Protégé ontology editor (www.protege.stanford.edu). The authorization rule for policies with only privileges was represented with the SPARQL query (Prud'hommeaux and Seaborne, 2006). The use of semantic web framework Jena (http://jena.sourceforge.net/) and of query engine ARQ (http://jena.sourceforge.net/ARQ) allowed rapid prototyping of knowledge base and policy enforcement function. FIGURE 7 shows the components of the development and testing environment.

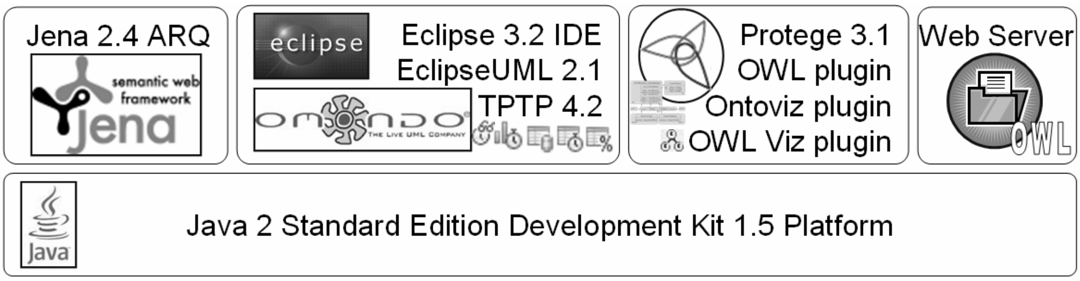

FIGURE 7 The development and testing environment

The development environment contained the following components:

– Java 2 standard edition development kit version 1.5 (java.sun.com/j2se/1.5.0/) is a programming language and platform that was chosen for the prototyping of research ideas

– Eclipse (www.eclipse.org) is an open source community that produces extensible integrated development environment (IDE).

– The Eclipse Test & Performance Tools Platform (TPTP, www.eclipse.org/tptp/) project consists of four subprojects. We used one that provides tools for tracing and profiling java applications for further analysis of performance.

– Web server is a container for SBAC, domain and policy ontologies developed in Protégé that are accessible using HTTP.

The average overall CPU time of the ProGuard start-up process is 12.256 seconds which is mainly due to the start-up of the decision making component (12.141 s). More specifically, it is due to initializing the in-memory decision set. The average overall CPU time of the evaluating process is 0.813 seconds and is fully due to the query execution over the decision set.

This is the fastest response time, because we used the simplest policy and domain ontologies; all data were loaded into the decision set during the start-up process; the SPARQL query corresponded to the authorization rule for policies with only privilege statements. However the results seem promising, and the conclusion is that the SBAC enforcement function is feasible from the perspective of performance.

3.5 SBAC for Semantic Web Services

For adopting SBAC in semantic Service Oriented Architecture (SOA), we merged semantics of SBAC with Web Ontology Language for Services (OWL-S)

(Martin, 2004). Thus, the SWS profile defines what are subjects, operations and objects of access control in (semantic) SOA. FIGURE 8 illustrates the merging of semantics of SBAC, of OWL-S and of domain of maintenance.

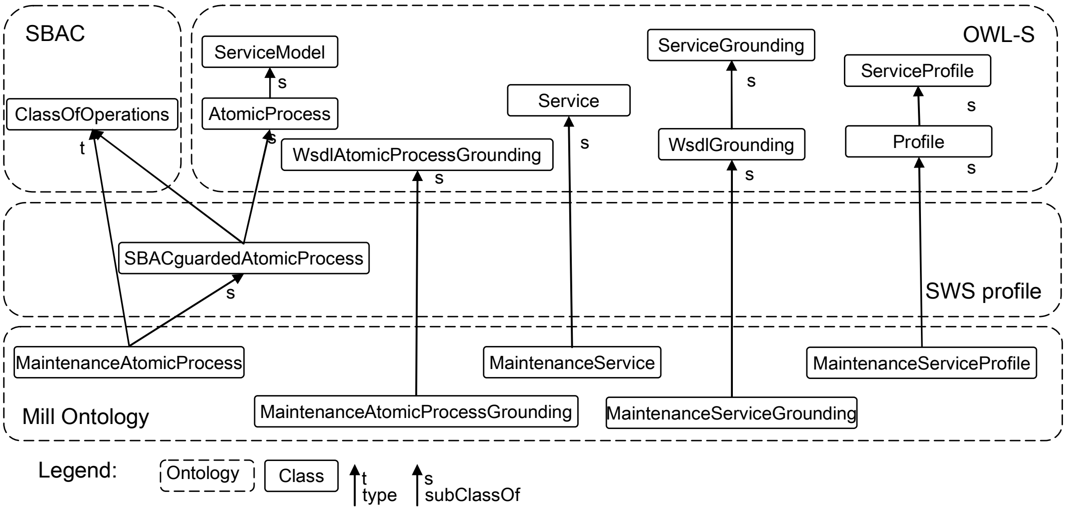

FIGURE 8 The SBAC SWS technological profile ontology

– Humans and intelligent applications are the clients of SWSs. If a Web service has a process specified as its model, then a semantic description of that process may refer to its participants. Clients of a web service comprise only one part of its participants. Moreover, the specification of participants in processes of Web services is optional in the OWL-S. Thus the SWS profile does not dictate the use of classes of participants for the specification of subjects of access control statements. Instead, the SWS profile leaves all the freedom to domain and policy ontologies engineers for classifying resources that are possible subjects of access. However, in most cases there will be an intersection between participants of services and subjects of access. This may result in joint classification hierarchies.

– In OWL-S annotations of service models the smallest level operations are atomic processes. Their modeling follows the metaphor of black box. For Web services, atomic processes correspond to operations of Web Service Description Language (WSDL). These WSDL operations are the lowest granularity level modeling concepts that denote operations used by subjects accessing protected objects in SOA. Thus, the atomic process is the most appropriate concept of OWL-S to be considered as the operation of access control. Thus the SWS profile determines that privileges refer to classes of atomic processes for the specification of authorized operations.

– The essential characteristic of services is that their processes have two distinct types of results. A process can produce some information or/and affect some real world objects as a result of its invocation. Generally, the SBAC must protect objects of the both types. This heterogeneity poses additional difficulties for the specification of access objects. Information objects are outputs of processes. Impacts on the real world state are represented by effects of processes. OWL-S represents effects in annotations as logical formulas and literals. This complicates the specification of objects of access based on the effects to an inappropriate extent. On the other hand, inputs of processes pre-determine results of their invocations – both outputs and effects. Thus authorization of information and real world objects based on inputs is promising and more generic. The proposed approach is limited, because it leaves out of scope the fact that not only inputs pre-determine results of processes but the world state expressed as preconditions in the OWL-S define the outputs and effects as well.

In addition to the conceptual semantics of the SBAC SWS profile, we also adopted the SBAC abstract architecture and the abstract use case for this technological profile when operations over protected objects are implemented as SWSs. RMMS in the paper industry served as a real-world domain for the adoption of the SBAC abstract architecture. See Section 3.8 for details.

3.6 SBAC for Multi-Agent Systems

For adopting SBAC in MAS, we used UBIWARE that is a new generation middleware platform focused on industrial needs. Generally, UBIWARE integrates ubiquitous computing with the Semantic Web technologies, agent technologies, security, and Enterprise Application Integration. UBIWARE aims at providing support in creation of self-managed interoperable complex industrial systems consisting of mobile, distributed, heterogeneous, shared and reusable resources of different nature. Such middleware enables various components to automatically discover each other and to configure a system with a complex functionality based on the atomic functionalities of the components. FIGURE 9 shows UBIWARE in the role of integrator of heterogeneous industrial resources.

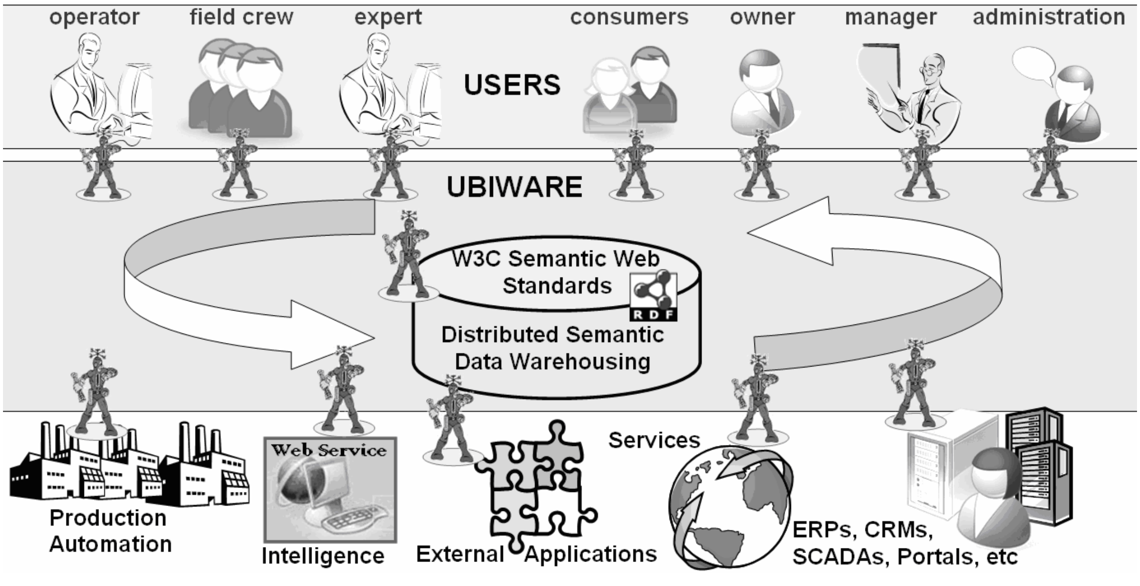

FIGURE 9 The UBIWARE platform and industrial resources

UBIWARE relies on results from the SmartResource project, i.e., the “Smart Resource Technology” for designing complex interoperable software systems. This technology gives every resource in an industrial system a possibility to be smart (by connecting a software agent to it), in a sense that it would be able to proactively sense, monitor and control its own state, communicate with other components, compose and utilize own and external experiences and functionality for self-diagnostics and self-maintenance.

We motivated the adoption of SBAC for UBIWARE based on the analysis of security implications of UBIWARE and scenarios of application of UBIWARE for the decentralized management of power networks (see Section 3.9). The characteristics of UBIWARE that have significant impact on security are *openness, dynamics, heterogeneity, distributed nature, collaborative or social nature, internationality, self-management, mobility, ambient intelligence, ubiquity, and pervasiveness*. Thus the risks and negative consequences of security threats will become higher than ever. The problem is that in new complex industrial environments based on UBIWARE traditional approaches to manage security fall short. Also, emerging security measures for the ubiquitous computing, Semantic Web technologies, agent technologies, etc. are not in a mature stage yet and still require significant elaboration to mitigate associated risks. What is important from the system development point of view is that the security cannot be added to the UBIWARE platform later but that the design decisions regarding security have to be thoroughly correlated with the requirements and design of the platform. Thus, we outlined our long-term vision for the security and privacy management in new emerging types of environments, which we refer to as Smart Ubiquitous Resource Privacy and Security (SURPAS). FIGURE 10 presents the SURPAS research framework.

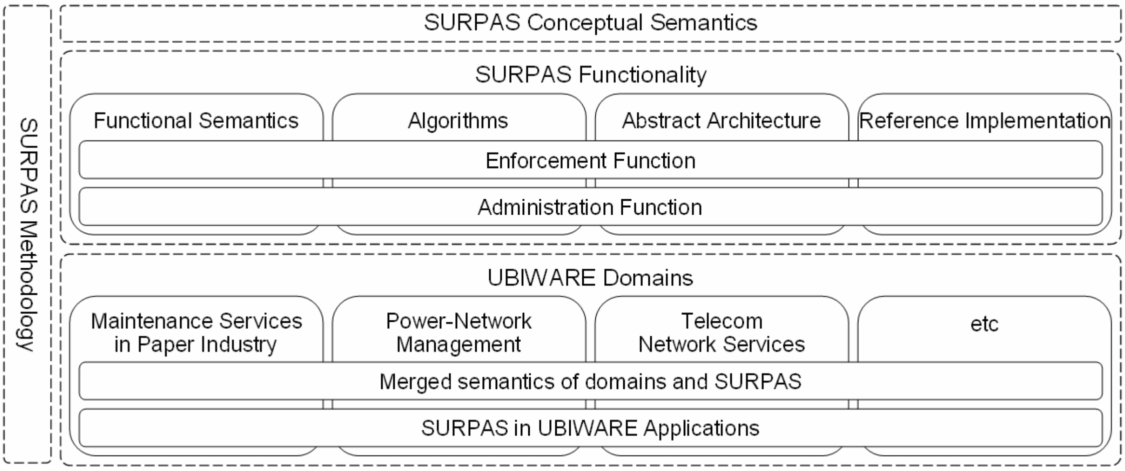

FIGURE 10 The SURPAS research framework

SURPAS is heavily based on SBAC. It extends the focus to the management of privacy, but concentrates on multi-agent systems in general and on the UBIWARE platform in particular. We adopted the SBAC research framework for SURPAS. The SURPAS research framework contains the same theoretical research and development components. It does not have the layer of technological profiles because SURPAS is meant to be used for multi-agent systems. Also, it has business domains of the UBIWARE project.

In addition to the introduction of the SURPAS research framework, we also presented the architecture of secure SmartResource agents. The architecture of SmartResource agents consists of three layers: reusable atomic behaviors (RABs), behavior models corresponding to different roles the agent plays, and the behavior engine. The security components, which SURPAS introduces into the architecture of the SmartResource agent, are the policy enforcement mechanism that is built-in into the behavior engine, and security measures and security policies which can be either provided upon agent's startup or retrieved on demand. FIGURE 11 illustrates the architecture of secure SmartResource agents and external repositories of RABs, roles, policies and security mechanism.

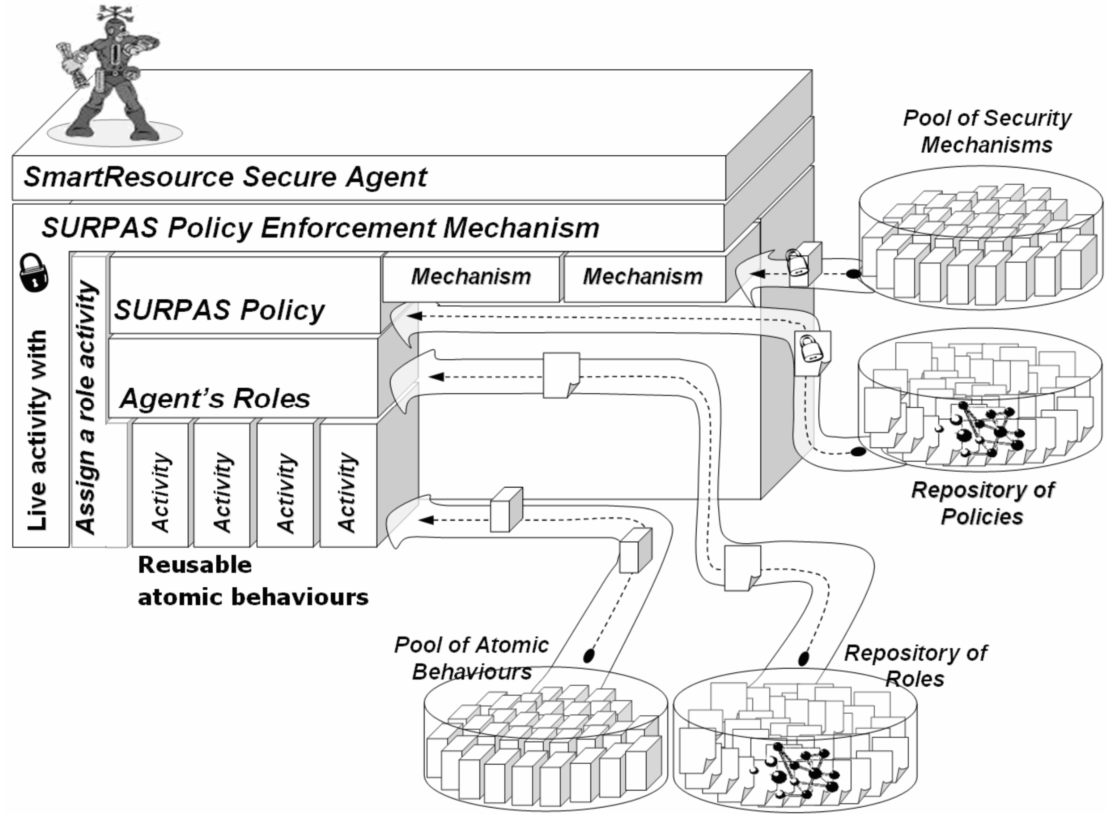

FIGURE 11 The architecture of the secure SmartResource agents

A reusable atomic behavior (RAB) is a piece of code implementing a reasonably atomic function. As the name implies, RABs are assumed to be reusable across different applications, different agents, different roles and different interaction scenarios.

The behavior of an agent is defined by the roles it plays in one or several organizations. A role consists of a set of beliefs representing the knowledge needed for playing the role and a set of behavior rules. Roughly speaking, a behavior rule specifies conditions of (and parameters for) execution of various RABs.

The behavior engine is the same for all the SmartResource agents. The behavior engine consists of the agent core, and the two core activities that we named "assign role" and "live". The AssignRole activity is responsible for parsing roles into the beliefs and behavior rules storages. The Live activity implements the run-time loop of an agent. The Live activity iterates through all the behavior rules, checks them against current beliefs, goals and security policy constraints. After that, it executes RABs together with security mechanisms corresponding to roles and policies, respectively.

The SURPAS policy enforcement mechanism manages security policies and security mechanisms. Its main task is to enforce security policies by interweaving with the Live activity. SURPAS policies are declarative descriptions using expressive and machine-interpretable data formats of Semantic Web. They are reusable over different agents, processes and organizations. Usually, SURPAS policies restrict actions prescribed by roles and enforce use of security mechanisms in addition to normal activities.

Agents access the roles, policies, security mechanisms, and RABs from external repositories, which are assumed to be managed by the organizations which own or hire the agents, or by trusted authorities.

3.7 SBAC for Mobile Web Services

We considered adoption of SBAC for MWS provisioning after adopting SBAC for MAS and SWSs. MWSs and SWSs are web services. The conceptual semantics of the SBAC MWS technological profile is the same as the conceptual semantics of the SBAC SWS technological profile. Thus, our research on SBAC for MWSs concentrated on the proper qualitative justification of SBAC for MWS and proposed to utilize distributed architectures of the SBAC enforcement mechanism as an adequate access control solution for MWS provisioning.

In the wireless environment mobile devices act as both web service clients and providers. The MWS provisioning still complies with the basic standards of SOA. Specifics of MWSs lie in a wider range of technical usage scenarios compared to regular web services. FIGURE 12 illustrates several such scenarios.

1. The mobile TCP/IP connection between the web service client and the MWS is deployed on top of a GPRS (General Packet Radio Service) through the Internet to/from the web service client.
2. In the HSCSD (High-Speed Circuit Switched Data) accessing scenario, a TCP/IP end-to-end connection between the mobile terminal and the dial-in server is established over a HSCSD and PPP (Point-to-Point Protocol) connection through a modem.
3. In a JXTA (peer-to-peer infrastructure) network a virtual P2P network can be established by connecting the mobile device to JXTA superpeers deployed at the base stations. The MWS clients and the providers connect to the JXTA network and can access each other.

4. Provisioning of MWSs in a totally decentralized manner is referred to as pure P2P. Discovery, invocation and integration of web services occur directly between mobile devices without any centralized entities. We have not studied how to provide MWSs according to this kind of technical usage scenario. Bluetooth and WLAN (Wireless Local Area Network) are possible technical solutions.

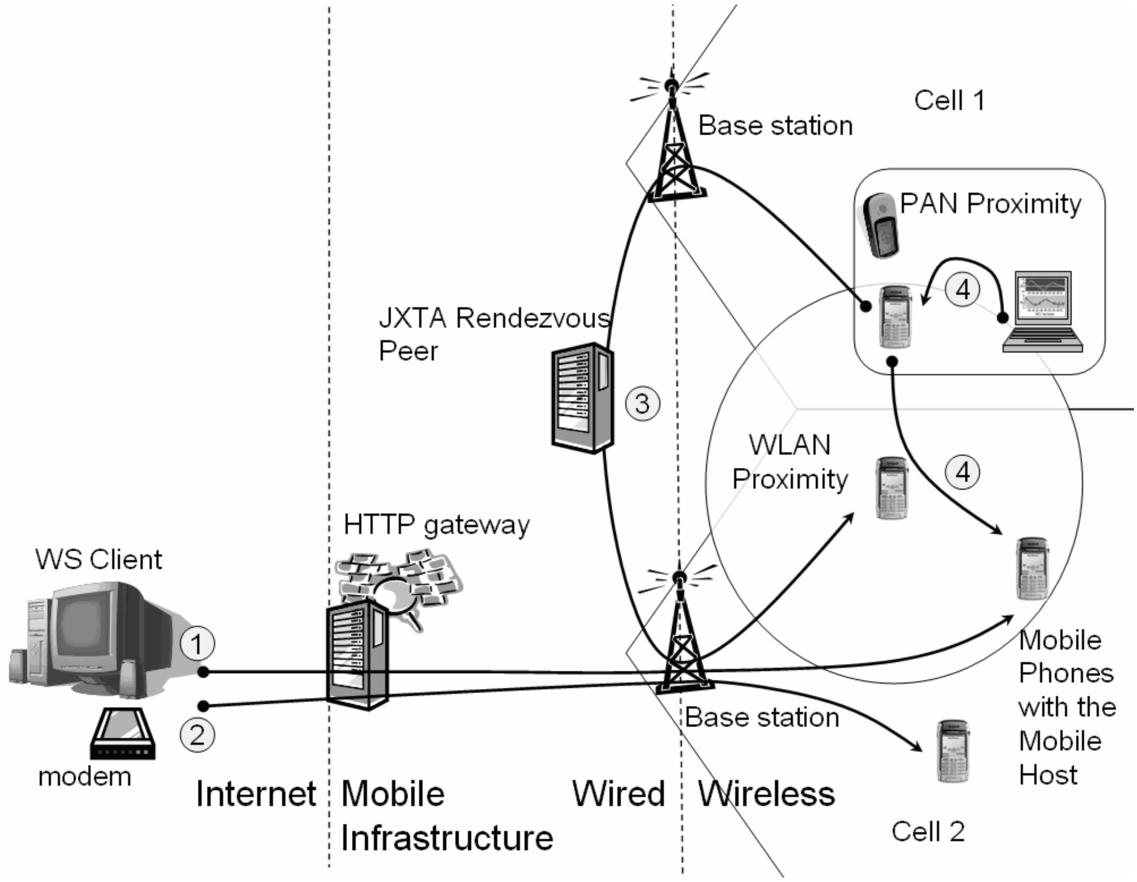

FIGURE 12 Provisioning of mobile web services

Based on these technical usage scenarios, envisioned commercial applications and sample MWSs, we qualitatively evaluated characteristics of MWS provisioning. This included analysis of security threats in mobile environments, review of conventional security requirements for web services, and analysis of security-sensitive characteristics of MWSs. After the evaluation we identified a concise list of ten critical success factors of access control solutions for MWS provisioning: *compatibility, applicability, extensibility, openness, nomadic nature, pervasiveness, context-awareness, usability, flexibility, and self-security*.

Finally, we proposed four options for deployment of the SBAC enforcement mechanism (Article VII, “Secure Communication and Access Control for Mobile Web Service Provisioning”; Srirama and Naumenko, 2007). These options have different implications on the level of security and process of provisioning of MWS. FIGURE 13 shows these four deployment options.

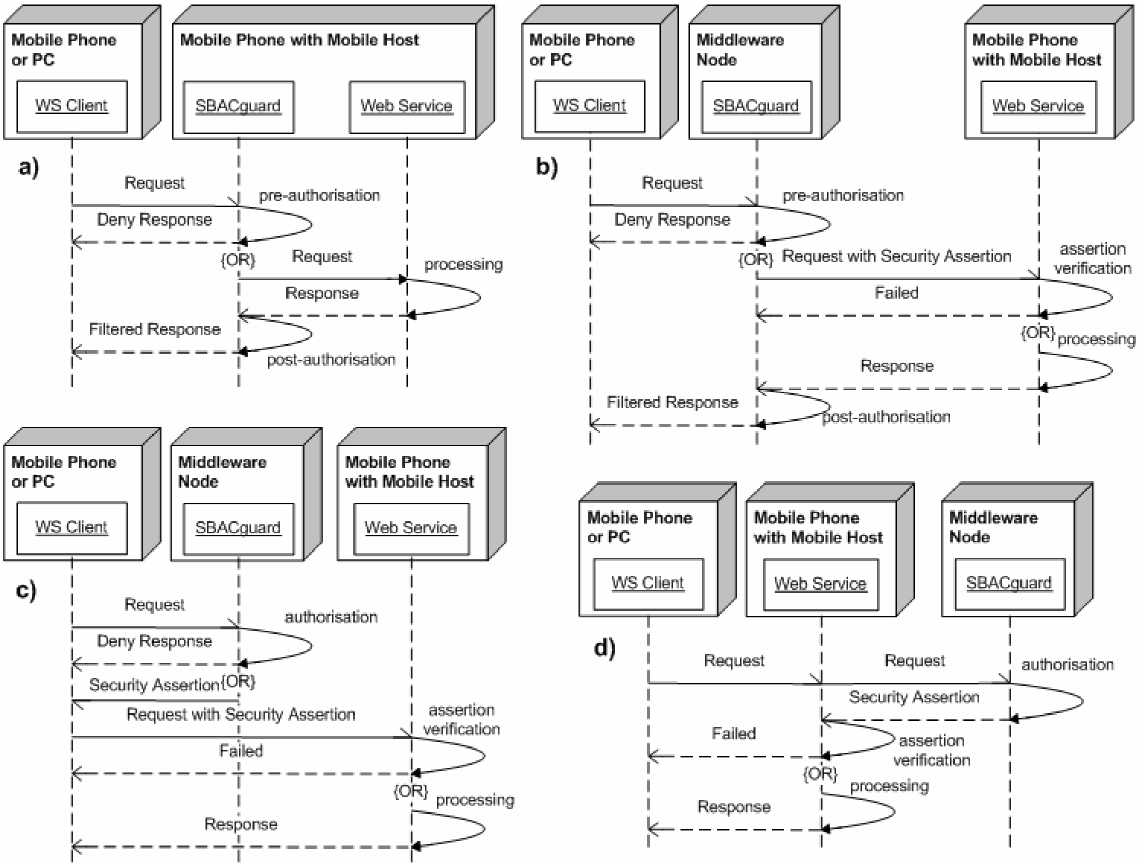

FIGURE 13 The SBAC enforcement for mobile web service provisioning

The embedded guard (option a) is the best applicable option for the pervasive MWS provisioning within the P2P usage scenarios. The clients directly access mobile devices. Interactions between the embedded guard and services do not have delays of wireless or wired asynchronous communication. One crucial advantage of this option is the opportunity to perform post-authorizations, i.e. , procedures of access control that must be performed after service enactment, e.g., filtering of the response. However computational limitations of mobile phones demand nomadic functionality of the guard. This undermines the possibility to use complex semantics-based algorithms for the embedded decision making process.

The deployment option b) illustrates the middleware guard that is an intermediate web service proxy. This guard provides the same interface as the original MWS, decorates web service invocation with the SBAC policy enforcement mechanism, and delegates authorized requests to the MWS. When the guard is in the Internet, clients are able to access it in the traditional way. Moreover mobile devices receive smaller number of requests or, in other words, only authorized requests. Post-authorization is still possible. The middleware proxy guard can represent several mobile devices and web services. Mobile-to-mobile requests experience delays of wireless communication twice when the guard is not embedded but is a middleware component. An additional component on mobile devices has to validate security assertions of the guard.

The validation of security assertions is necessary in order to check that a security assertion is consistent with a request.

The deployment option c), where the guard is a third-party authorization authority, creates additional inconveniences for clients. They have to get authorization assertions prior to access protected MWSs. Then the component deployed on mobile devices validates security assertions provided with requests like in the previous option. Although this case might look too complex, however this is probably the most applicable option for the industrial, commercial or professional use of MWSs when clients can get security tokens with a long period of validity on the basis of their memberships in or subscriptions to different organizations, social networks, commercial services, etc. This option allows direct multiple requests to MWSs using the same security token over time without the overheads of the authorization decision making a process for each request.

Delegation of authorization of option d) is the last option we considered. MWSs initially receive all requests directly from clients and then outsource the decision making procedure to the middleware guard. While such kind of deployment is possible, it has several significant shortcomings without clear advantages over the above described options. There are the following needs to take care of: to embed the enforcement component for authorization messaging with all possible time overheads; to verify signatures of the guard; to process all requests from clients; and others. One advantage is that the performance demanding SBAC functionality is executed by the middleware guard.

3.8 Case study in the paper industry

The case study in the paper industry involved a series of interviews with representatives from the Metso Automation, Metso Paper and Trusteq commercial companies. We also reviewed different material, e.g., documents, presentations, designs, etc.

The cluster of Metso’s companies, Metso Paper Inc. and Metso Automation Inc., specializes in pulp and paper industry processes, machinery, equipment, control systems, related know-how and after sales services. The Metso Paper's offering extends over the entire life cycle of the process covering new lines, rebuilds and various services. Metso Automation supplies control systems and related ICTs for the products of Metso Paper.

As we mentioned above, during the case study we were concentrating on two areas, namely PDM and RMMSs. The major findings are the following.

– The current level of security for RMMSs is not sufficient for the needs of managing cross-organizational processes. The elaboration of generic authorization enforcement mechanisms in the business network is crucial to handle the heterogeneity and to shift the control over the authorization process from Metso Paper to its customers. FIGURE 14 shows the current architecture for provisioning of RMMSs.

– The inter-organizational information exchange in the paper industry will extensively use the mill model. Currently, there are several research initiatives that try to use Semantic Web standards and technologies in order to develop appropriate solutions for the information exchange for the PDM process. When semantic standards come into use for PDM and RMMSs, then industrial resources for the access control will have semantic descriptions according to the mill ontology. FIGURE 15 illustrates the vision for a future collaborative platform for PDM based on the Semantic Web technologies.

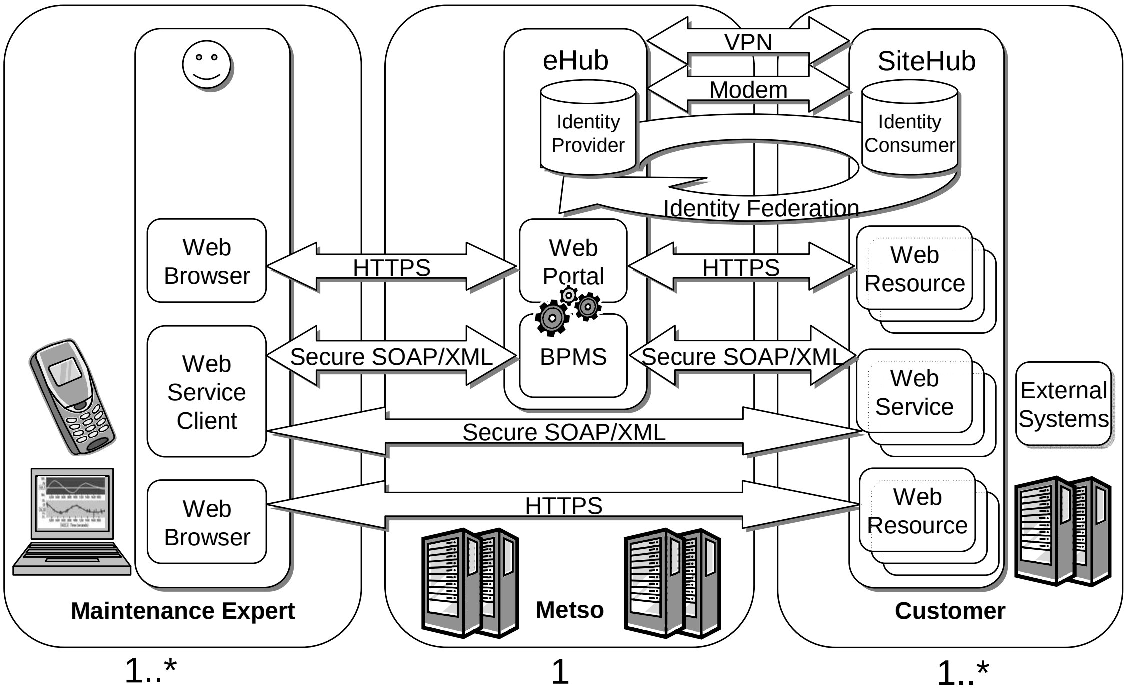

FIGURE 14 The architecture for remote machinery maintenance services

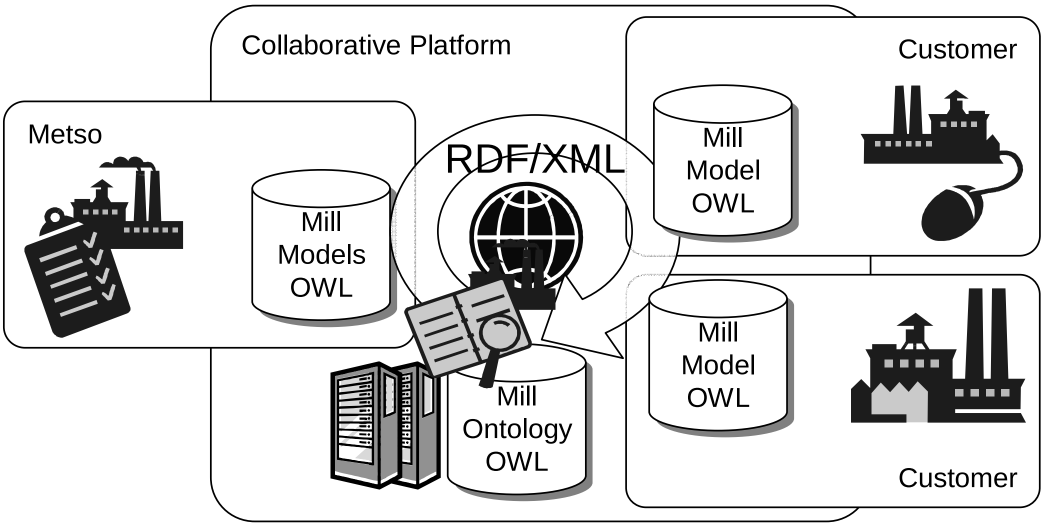

FIGURE 15 The collaborative platform for Product Data Management

After deriving the real-world arguments for motivation of SBAC, we used this case of RMMSs in order to exemplify the adoption of SBAC for the SBAC SWS technological profile. We considered an example of specification of hierarchy of resources, hierarchy of operations, and access control privileges in the industrial maintenance domain. Finally, we adopted the SBAC abstract architecture, where all four components of the architecture of the SBAC enforcement mechanism become SWSs. FIGURE 16 shows the top level architecture and indicates the steps of a possible use case for the SBAC enforcement mechanism.

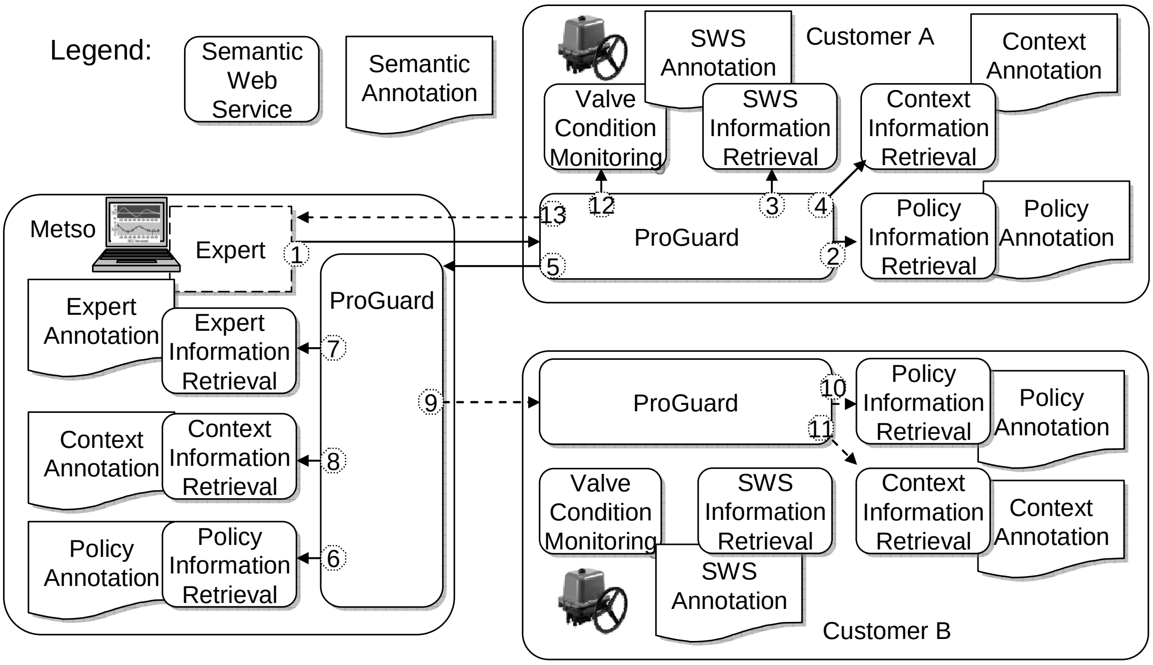
Legend:
Semantic Web Service
Semantic Annotation
Customer A
SWS Annotation
Context Annotation
Valve Condition Monitoring
SWS Information Retrieval
Context Information Retrieval
ProGuard
Policy Information Retrieval
Policy Annotation
Metso
Expert
Expert Annotation
Expert Information Retrieval
Context Annotation
Context Information Retrieval
Policy Annotation
Policy Information Retrieval
ProGuard
1
2
3
4
5
6
7
8
9
10
11
12
13
ProGuard
Policy Information Retrieval
Policy Annotation
Valve Condition Monitoring
SWS Information Retrieval
Context Information Retrieval
Context Annotation
SWS Annotation
Customer B

FIGURE 16 The SBAC use case with maintenance semantic web services

1. Metso's maintenance expert requests status of a valve that is a part of a running production machine of customer A as a countercheck for a predicted fault.
2. ProGuard SWS intercepts the request and retrieves corresponding policy rules based on a policy annotation.
3. Policy rules require some additional information about the expert, valve and context of access for this kind of request. ProGuard retrieves an annotation of the valve from the mill A model ontology.
4. ProGuard retrieves contextual information that is available from a local context annotation.
5. ProGuard of customer A does not have enough information internally, thus it forwards a request for the information about the context and the expert that is the subject of access.
6. Metso's ProGuard intercepts the request 5 and retrieves rules from a trust agreement through PIR of Metso. According to these rules, Metso can provide information about the expert and the context.
7. Metso's ProGuard retrieves the semantic annotation of the expert.

8. Metso's ProGuard retrieves the semantic annotation of relevant context.
9. Based on the annotation of context the reasoner implies that contextual information contains sensitive data, because the maintenance expert predicts a fault based on a history of faults during an operation of a paper production machine of a similar type owned by customer B - the distribution of this information can violate a trust agreement between Metso and customer B. Thus Metso's ProGuard delegates the request to customer B for a decision about a possibility to share sensitive contextual data with customer A.
10. The guard of customer B retrieves rules from its trust agreements with Metso and customer A.
11. ProGuard of customer B retrieves requested contextual information and reasons that customers share information about the condition monitoring and the diagnostics for this type of paper machine. Customer B forwards the decision to Metso Paper. Metso forwards semantic data about the expert and context of access to customer A.
12. ProGuard of customer A based on all collected data makes a positive decision granting access to the valve's status.
13. Alternatively, ProGuard denies access and replies with a rejection of request.

3.9 Case study of decentralized management of power networks

Decentralized management of power networks was studied in order to derive a real-world motivation for SURPAS and UBIWARE. Thus, findings of this case include critical security questions and requirements that justify adoption of SBAC for the UBIWARE-based management of power networks. ABB is a global vendor of hardware and software for power networks. These power networks themselves are owned, controlled and maintained by some local companies. It is noticeable that the control systems of different companies are not integrated. We analyzed four scenarios of potential new applications that could be created based on UBIWARE and revealed several security concerns.

– In Scenario One there is information exchange between sub-networks using UBIWARE. This requires a flexible and expressive framework for the distributed, collaborative and policy-based management of security.

– Scenario Two is a new business model to implement Web-services for certain algorithms, so that the ABB customers can utilize those algorithms online when needed. UBIWARE must handle secure provisioning of (semantic) web services, which is still an open research question.

– Scenario Three is an integration of contextual data with the currently used data, such as the network structure and configuration, feeder relay readings etc. for risk analysis, fault localization, extending operator's view, and other. This requires management of reputation and trust for the external contextual services because these issues influence the confidence in predicted risks, fault locations, etc.

– Scenario Four deals with transferring knowledge of human experts to automated systems, by means of various data mining tools. The privacy concerns of the owners of different sub-networks should be properly managed.

3.10 Case study at the university

Finally, we studied the real-world domain of high education. This case remains the least explored. We overviewed the current situation with authentication and authorization. As in the cases described above, we derived real-world arguments for the motivation of SBAC in this domain. The representative organization was our home university, University of Jyväskylä, in Finland.

The university managed to integrate and provide consolidated authenticating service throughout the organisation. The integration of authentication services between different universities in Finland is deemed solved nowadays as well (Linden, 2005). Regarding authorization, university-wide and cross-organisational access control management is needed. First of all, the university has a variety of information systems and applications for different purposes. All these systems have heterogeneous native access control mechanisms. In addition to the need of university-wide access control management, there are ongoing nation-wide efforts to integrate research, teaching and administration processes of different universities. This is the case, for example, in the National Electronic Library, which is a consortium formed by universities, polytechnics, research institutes, and provincial libraries. National Library’s online services are responsible for managing digital national library resources, and for access control to them in particular (Rouvari, 2004).

Design of university-wide access control solutions is complicated as it requires integration of native platform-dependent access control mechanisms and integration of data representation on the university level. First of all there is a need for common access control model with the support of arbitrary policy types, i.e., the SBAC model. This model should be supported by the language for automated and distributed management of access control policies, i.e., the SBAC ontologies. Finally, there should be a significant support by different software tools for ontological domain modeling, for specification of high-level security policies, for delegation of security-related tasks amongst personnel, for maintenance of organizational process view on access control, for controlled propagation of high-level policies to native mechanisms, for direct enforcement of policies, for verification of consistency and integrity of access control data, and for many others. In order to support consolidated authorization services between universities, the above described components should be open and flexible enough to mitigate heterogeneity and complexity of cross-organizational integration in access control management.

4 RELATED RESEARCH

This chapter presents an overview of related non-semantic access control models, semantic access control, XML-based access control languages, and ongoing research projects and programmes.

4.1 Non-semantic access control models

Traditional models and their elaborations contain many ideas which form the background for and contribute ideas to SBAC.

The ClarkWilson model (Clark and Wilson, 1987) was the first to introduce the access control triple of user, operation and protected data item as the structure for authorizations. SBAC specifies the same structure, but on the level of sets of subjects, operations and objects.

Another, traditional access control model, Mandatory Access Control (MAC) relies on the classification of users and resources to hierarchical security (or clearness, or sensitiveness) levels and domains (or categories) (INFOSEC 1999). For the MAC, the confidentiality is ensured by the Bell-LaPadula rules (Bell and LaPadula, 1973) and the integrity by rules of Biba's model (1977). These rules are defined between hierarchical security levels and domains instead of individual users and resources. Thus, the hierarchy of levels and non-hierarchical categories mediate users and permissions.

The hierarchy of roles from the hierarchical Role-Based Access Control (RBAC) model (Sandhu et al., 1996) provides users with permissions based on the inheritance relation between roles. RBAC roles correspond to individual's positions, duties and activities. Thus the cost reduction is achieved because positions, duties and organizational structures are more stable within enterprises than the positions of the employees. Another great advantage of RBAC is that it is policy neutral. It is possible to configure the RBAC to support a wide variety of traditional and domain specific AC policies.

A lot of research has been done to develop, elaborate and implement RBAC models and their features. The NIST reference model (Ferraiolo et al., 2001) unifies the vision of different parties. RBAC is recognized as a security pattern nowadays (Fernandez and Pan, 2001). There are many extensions to the RBAC model. Parameterized RBAC (PRBAC) (Bacon et al., 2002) is a good example. The access rights a person receives are normally based on a number of factors. These may be organizational unit, position, location or other. Roles must be defined for every valid combination of values of factors. The resulting role hierarchy would obviously be very complex and difficult to maintain. The solution for these problems was found by parameterising the roles. Parameters are binary relations. Thus, the concept of parameter in PRBAC is implemented with a property construct in SBAC.

RBAC has been applied for the enterprise-wide access control as Enterprise Security Management System (ESMS) (Ferraiolo et al., 2003). An Enterprise Access Control (EAC) Framework (EAF) (Ferraiolo et al., 2003) defines components and functionality of ESMS. EAC deals with a variety of access control systems which differ from environment (platform, business application, etc.) to environment. These native systems (NS) have their own implementation of the policy specification (model) and enforcement mechanism. Thus the main challenge of EAF is to integrate native systems to allow administration of access control on a higher level of abstraction.

Enterprise RBAC (ERBAC) is an EAC model based on the RBAC reference model. Enterprise role is the main concept of ERBAC (Kern et al., 2002). This role gathers all corresponding roles in native systems and thus collects all their permissions. Enhanced ERBAC introduces advanced features to ERBAC (Kern, 2002). As for PRBAC discussed above, the multiple possibilities to build role hierarchies based on some criteria of role decomposition lead to creation of different role hierarchies which are connected between each other by multiple inheritances. Kern enhanced the ERBAC model in order to parameterize roles by introducing attributes and rules. In such a situation, role to user, user to permission and role-to-role assignments have attributes which specify additional information. User attributes mainly describe personal information, organizational status (unit, position, etc.) and constraints for role assignment. The notion of rules is not defined rigorously, but execution of all functions that manipulate RBAC data should be verified against the corresponding rules.

There have been some efforts to develop representation languages for RBAC data, which work on the level of data structures and syntax definitions (Bacon et al., 2002). Recently, there have also been advances in applying Semantic Web technologies in order to enhance RBAC.

The research on SBAC is mainly based on RBAC. The concept of role serves as an aggregator of and mediator between users and permissions the way the concept of class does in SBAC. We have tried to consider the components of EAF on the level of business networks of enterprises. Also, in this research SBAC serves in a role similar to that of ERBAC in EAC. With respect to policy representation languages, the SBAC ontologies define the language for representation of SBAC policies.

4.2 Semantic access control

This thesis deals with research on the intersection of Semantic Web and access control research areas. There are number of efforts that apply Semantic Web standards to different aspects of access control. This section reviews those that use ontologies or Semantic Web standards instead of access control models or policy languages.

Yagüe et al. introduced Semantic Access Control (SAC) model (Yagüe et al., 2005a) and published results of their research on applying Semantic Web layers (Yagüe et al., 2003b) to access control in different environments, mainly for web services (Yagüe et al., 2005b), digital libraries (Yagüe et al., 2003a) and e-commerce applications. SBAC is similar to SAC in common motivation and theoretical background. However, SBAC differs in its rigorous following of the OWL and Semantic Web stack of standards. The semantics of SAC is based on XML (Yergeau et al., 2004). It is defined as XML Schema, inheriting limitations of XML-based efforts (see Section 4.3).

Concept-level Access Control (Qin and Atluri, 2003) relies on a model based on 4-tuple (object, operation, positive or negative sign, subject) for the specification of authorizations to access Semantic Web data, the main difference from SBAC being that authorizations are defined on the level of individual concepts. Concept-level Access Control uses OWL to express policies.

Ontology-based Rights Expression Language (OREL) for the machine-interpretable representation of access control policies in the field of Digital Rights Management (DRM) has been built on top of OWL (Qu et al., 2004). For DRM, OREL has a copyright ontology which uses the Description Logic (DL) profile of OWL (OWL-DL).

Demiani et al. proposed how to extend existing XML-based policy languages with semantic-aware assertions. They identified the problem of access control based on metadata descriptors of subjects and objects of access; proposed the approach of extending eXtensible Access Control Markup Language (XACML) (Moses, 2005) and Security Assertions Markup Language (SAML, 2005) with RDF (Klyne and Carroll, 2004) statements about subjects and objects; and provided a description for a possible architecture of the security solution.

An access control model, Semantic Based Access Control – SBAC (Javanmardi et al., 2006a, 2006b, 2006c), was recently proposed at the same time as we published our results towards the SBAC model (Naumenko, 2006; Naumenko and Luostarinen, 2006). In addition to the same acronym used, this model is based on OWL and uses SWRL (Horrocks et al., 2004) for enhancing expressivity of OWL with rules. This model contains the ontology base, authorisation base and administrative operations over the authorisation base. The ontology base has subject-ontology, object-ontology, and action-ontology for modelling subjects, objects and actions of access. In our model we do not prescribe disjoint modelling of subjects, objects and actions in different ontologies. Moreover, we generalise the concepts of subjects and objects to more generic concept of resources in order to support the possibility of an individual resource to play the roles of subjects and objects simultaneously. The authorisation base has authorisation statements as a relation between subject, object and action with the positive or negative sign. This relation is slightly different from the structure presented in this dissertation for the specification of access control statements. However, it also allows the specification of privileges and prohibitions on the level of sets of resources instead of individuals. This model formally presents two administrative operations to grant and to revoke access rights. We have not studied systematically the administrative functionality of SBAC so far.

Rei is a rule-based policy expression language represented using RDFS (Brickley and Guha, 2004). Although this language originally was oriented to specify policy rules for individual subjects, targets and actions, it also permits specification of policies based on roles, groups and entities despite the fact that notions for roles, groups and entities have not been specified in the basic Rei ontology (Tonti et al., 2003).

KAoS approach to policy representation language is based on KAoS Policy Ontology (KPO) that uses OWL (Tonti et al., 2003). In this language policies authorize actions that in their annotations restrict subjects and objects of access. Thus the KAoS overstates the importance of actions compared to subjects and objects. Policies may target individual concepts, classes, groups, etc. The use of KAoS is mostly oriented towards agent technologies. However, application of KAoS for SWSs in forms of grid services and of agent services has been reported (Uszok et al., 2004).

Priebe et al. (2006) extended the standard XACML architecture with the retrieval of attributes based on inference over ontologies. However, they leave XACML as the main policy language and use ontologies only as extension mechanisms to capture semantic relationships between attributes. XACML is discussed in Section 4.3 next.

There are some results of applying Semantic Web standards for protecting web services (Shields et al., 2005), resources in grids (Wang et al., 2005), services in MASs (Rao and Sadeh, 2005) and databases (Mitra et al., 2006). These results are generally positive and promising for the whole vision. For example, Agarwal and Sprick have proposed an approach to express access control policies for SWSs (Agarwal and Sprick, 2004). Their access control framework is based on the integration of the credential-based public key infrastructure SPKI/SDSI and DARPA Agent Markup Language (DAML) annotations of web services (DAML-S) (Agarwal et al., 2004). Another example is Semantic Access Control Enabler (SACE) that is a middleware component to enable SAC for information interoperation over syntactically and semantically heterogeneous databases and corresponding RBAC policies (Pan et al., 2006).

4.3 XML-based access control policy languages

Finally, there are number of industrial efforts to produce access control languages and standards based on XML, like XACML (Moses, 2005), Web Services Security (Nadalin et al., 2006), Extensible Rights Markup Language (Wang et al., 2002), etc. Although the proposed XML-based solutions intersect in ideas and concepts with semantics-based approaches, they do not concentrate on semantic features and thus do not fully gain benefits of the Semantic Web technologies. The main limitation of these efforts is that knowledge representation models standardized as part of the Semantic Web activity are much more general and extensible than the representations that are based on tailored XML schemas.

4.4 Research projects and programmes

The international movement[2] towards the Internet of Things recognizes the importance of adequate privacy and security solutions and engages in enormous efforts in response. An excerpt from the Information Society Technologies (IST) Specific Programme[3] for Trust and Security highlights the importance of policy-based management:

"Building and providing trust and confidence in Ambient Intelligence scenarios would imply addressing and meeting specific needs and requirements at all levels … This would mean to consistently express specific security policies (which describe the organizational and technical processes and mechanisms to manage security) at every level as well as to coherently enforce those policies … Enforcing the different security policies would, therefore, need technical capability to (automatically) understand the global security context and to efficiently mediate between the various policies."

The Computer Security Division at NIST, USA (http://csrc.nist.gov/) has a special focus area on Security Research within their Emerging Technologies section.

European Network of Excellence, ReSIST, addresses the strategic objective "Towards a global dependability and security framework" of the Work Programme, and responds to the stated "need for resilience, self-healing, dynamic content and volatile environments".

[2] Conference: FROM RFID TO THE INTERNET OF THINGS, Pervasive Networked Systems, Organised by the European Commission Directorate "Network and Communication technologies", March 2006, Brussels.

[3] European Commission Directorate "Network and Communication Technologies", ICT for Trust and Security, http://cordis.europa.eu/ist/trust-security/programme.htm

European project REWERSE[4] has special working group on developing methodologies, languages, and tools for specifying, enforcing, and integrating heterogeneous policies.

Specifics of security in MASs and Semantic Web have been addressed continuously by international consortiums[5] [6] [7]. A coordination action on ICT vulnerabilities of power systems and the relevant defense methodologies (GRID) is a response to the major recent blackouts over Europe and North America.

[4] REWERSE is a research "Network of Excellence" (NoE) on "Reasoning on the Web" that is funded by the EU Commission and Switzerland under the project reference number 506779.

[5] Virtual Centre of Excellence in Mobile and Personal Communications Ltd, www.mobilevce.com

[6] AgentLink is the European Commission's IST-funded Coordination Action for Agent-Based Computing, www.agentlink.org

[7] Knowledge Web Network of Excellence (FP6-507482), http://knowledgeweb.semanticweb.org

5 OVERVIEW OF THE ORIGINAL ARTICLES

This chapter provides a brief overview of the nine articles which are included into the thesis. Out of these nine papers, three have been published in or submitted for publication to journals. The remaining six papers have been published in conference proceedings. The last section of this chapter describes the author's contribution for the joint publications.

5.1 Article I: "Strategic Industrial Alliances in Paper Industry: XML- vs. Ontology-Based Integration Platforms"

Naumenko A., Nikitin S., Terziyan V., Zharko A., (2005). Strategic Industrial Alliances in Paper Industry: XML- vs. Ontology-Based Integration Platforms, In: The Learning Organization, Special Issue on: Semantic and Social Aspects of Learning in Organizations, Emerald Publishers, 12(5): 492-514.

The primary focus of this paper is integration of enterprises within strategic industrial alliances. Possible challenges for such integration are discussed mainly from a technological point of view. There is a need to manage the alliance strategies, objectives, policies, etc. using a platform for integrated consortium. This platform should not replace existing solutions. On the contrary, this platform should seamlessly integrate current systems and tools in order to manage cross-organizational processes.

The paper aligns theoretical ideas with the practical needs based on a case in the paper industry. The case under consideration is a technological and standardization alliance called PRINDEX (former PaperIXI). This alliance promotes XML-based solutions. This paper motivates applying Semantic Web technologies for alliance platforms of this kind in general, and applying ontologies for the management of alliance policies in particular. The collected arguments in this paper are based on the critical analytical analysis of the proposed PaperIXI platform and other existing XML-based and emerging ontology-based solutions.

This paper triggered the research towards SBAC of this thesis. Specification and management of alliances' policies (rules, restrictions, etc) using Semantic Web technologies and standards is not the main focus of this paper. However, the idea of ontology-based management of alliance policies served as a background for writing the research plan. This paper also determined the orientation of the whole research to business networks. The case of paper industry was revisited several times during the later stages of the research.

5.2 Article II: "Identity and Access Management for Remote Maintenance Services in Business Networks"

Luostarinen, K., Naumenko, A., Pulkkinen, M., (2006), Identity and Access Management for Remote Maintenance Services in Business Networks, in IFIP International Federation for Information Processing, Project E-Society: Building Bricks, eds. R. Suomi, Cabral, R., Hampe, J. Felix, Heikkilä, A., Järveläinen, J., Koskivaara, E., (Boston: Springer), (226):1-12.

The research reported in this paper explores further the paper industry and its business networks. This paper primarily focuses on the security issues and goals of provisioning of RMMSs in a business network around Metso Paper, Inc. Identity and access management for RMMSs was studied with respect to the current situation, the ultimate vision and the roadmap from short-term to long-term goals.

The paper reveals shortcomings within the management of access control and overall security during the inter-organizational information exchange when business processes cross organizational boundaries. The ideal situation was formulated by analyzing and decomposing it in the EA framework of four dimensions: business, information, application and technology architecture. Within the description of the ideal situation, the author collected practical real-world business needs for the management of access control on the level of business networks. Namely,

– The ultimate vision of the business dimension (of the EA) is that trust between parties and privacy of partners should be ensured by a proven high-level built-in pervasive security.

– The business vision has to be supported with the information dimension by adequate languages, and structures and standards of data representation. This is needed for *formal*, *shared*, *flexible*, *expressive*, *distributed*, and *automated* management of access control policies of business networks. *Formal* management refers to the need of having a formal model to mediate access control policies and mechanisms. *Shared* policies have two features. The policy formats have to be interoperable in a business network. Policies should be commonly accepted and understood by partners. *Flexibility* and *expressiveness* of security data structures and standards help to mitigate the heterogeneity and dynamics of businesses, cultures, strategies, visions, approaches, etc. *Automated* management of the access control policy in *centralized*, *distributed* and *mixed* architectures of the business network enables diverse applications and technologies.

– Information systems and applications at the level of the business network have to support the distributed and cooperative management of access control for the business network partners. Security solutions have to be *open* enough to allow easy integration of all possible native implementations of security systems and technologies into a solid security infrastructure.

– In the EA dimension of technologies, we need a new generation of authentication and authorization mechanisms that take into account the distributed and multi-owner nature of the access control management. In addition to authentication and authorization there are many other security technologies that need improvements, e.g., logging for audit.

5.3 Article III: "Contextual rules-based access control model with trust"

Naumenko, A., (2006), Contextual rules-based access control model with trust, In Shoniregan C. A. and Logvynovskiy A. (Eds.), Proceedings of the International Conference for Internet Technology and Secured Transactions, ICITST 2006, 11-13 September, London, UK, e-Centre for Infonomics, pp. 68-75.

In response to the crucial need for a formal specification of access control models, this paper introduced, motivated and described the SBAC model. The model provides means for a policy neutral, flexible, collaborative and distributed access control on the abstract level with authorizations based on semantic relations of access control concepts.

The form of a theoretical model is a preferred style of presentation of new features and ideas in the access control research domain. The SBAC model is mainly based on the model-theoretic semantics of the OWL standard (Patel-Schneider et al. 2004). This enables an ontology-based access control. The model proposes a generic structure for the specification of access control statements. This structure contains fundamental concepts of access control: subjects, operations, and objects. The specification of access control statements relies on classes of subjects, operations, and objects. Additionally, the SBAC model reuses the semantics of rules from SWRL (Horrocks et al. 2004). This enables a rule-based access control and involves specification of conditional access control statements. The model also brings into consideration contextual information, e.g., specified trust relationships between parties.

The use of Semantic Web standards ensures automated reasoning about security policies and thus leads to the elaboration of new more intelligent access control mechanisms. Therefore, the paper discusses the place and role of ontologies in SBAC and presents the upper view on the SBAC policy enforcement mechanism. This upper view encompasses the top level architecture and a possible use case of inter-organizational distributed procedure of access control decision making in a business network.

5.4 Article IV: "Semantics-Based Access Control – Ontologies and Feasibility Study of Policy Enforcement Function "

Naumenko A., (2007), Semantics-Based Access Control: Ontologies and Feasibility Study of Policy Enforcement Function , In: J., Filipe, J., Cordeiro, B., Encarnacao, and V., Pedrosa (Eds.), In Proceedings of the 3rd International Conference on Web Information Systems and Technologies (WEBIST-07), Barcelona, Spain - March 3-6, 2007, Volume Internet Technologies, INSTICC Press, pp. 150-155.

Following the introduction of the SBAC model, the abstract architecture and the possible use case of distributed procedure of access control decision making, this paper introduces the SBAC ontologies and quantitatively evaluates our conceptual research results with the development and testing of the prototype architecture.

SBAC uses ontology-based access control policies and ontologies instead of mathematical access control models and domain models. The SBAC ontologies consolidate and formally specify knowledge of the access control domain in a machine-interpretable form.

The main purpose of prototyping was to test performance of the SBAC enforcement mechanism and to gather information for the feasibility study of the whole vision. The thorough compliance of SBAC with the Semantic Web standards ensured the possibility to reuse several existing Semantic Web tools and applications. Regarding performance, this paper describes two processes which comprise the policy enforcement function. The first process starts up the SBAC guard. The second process continuously evaluates incoming requests. These two processes and their impacts on the overall performance are separately discussed in the paper. The development and experiments with the prototype helped to identify and analyze major factors that influence the performance.

Finally, collected results of quantitative feasibility study illustrate benefits of orientation to the Semantic Web technologies, especially in reusability of tools and expressivity of the SBAC model. In general, the results for performance are quite promising. The automated decision making procedure reasoning over ontologies makes the enforcement mechanism and the whole SBAC intelligent and flexible.

5.5 Article V: "Access Control Policies in (Semantic) Service-Oriented Architecture"

Naumenko, A. and Luostarinen, K., (2006), Access Control Policies in (Semantic) Service-Oriented Architecture, In Schaffert S. and Sure Y. (Eds.), Semantic Systems From Visions to Applications, Proceedings of the SEMANTICS 2006, Austrian Computer Society, Vienna, Austria, pp. 49-62.

This paper briefly describes the SBAC model and introduces the conceptual semantics of the SBAC SWS profile for the specification of access control policies in (semantic) SOA. The real-world industrial case of Metso Paper Inc was again revisited in order to motivate and to exemplify research ideas. The major motivating arguments for adopting SBAC in (semantic) SOA were based on the nature of business-to-business relations in the business network of Metso Paper and on the ongoing initiatives to introduce a semantics-based inter-organizational information exchange. For example, the traditional benefits of SWSs, e.g., dynamic and automatic discovery, integration, composition, invocation, etc., improve the competitiveness of remote maintenance services but they are not more important than the security.

Immature standards and tools in this technological area complicate the elaboration of SBAC for SWSs. For the sake of brevity, the paper specifies the SBAC SWS profile according to the OWL-S specification (Martin 2004). The SBAC SWS Profile is meant to combine semantics of SBAC and SWSs in the form of ontologies. This profile mainly defines what are subjects, operations and objects of access control in (semantic) SOA.

In order to exemplify conceptual ideas, the paper revisits the abstract architecture and the use case of SBAC (Article III). All components of the abstract architecture become SWSs. The abstract use case was rewritten according to the maintenance services for paper machinery. The paper also presents examples of domain ontologies and policies.

5.6 Article VI: "A Security Framework for Smart Ubiquitous Industrial Resources"

Naumenko A., Katasonov A., Terziyan V., (2007), A Security Framework for Smart Ubiquitous Industrial Resources, In: Goncalves, R., Müller, J., Mertins K., and Zelm, M., (Eds.), In: Enterprise Interoperability II: New challenges and Approaches, Proceedings of the 3rd International Conference on

Interoperability for Enterprise Software and Applications (IESA-07), March 28-30, 2007, Madeira Island, Portugal, Springer, pp. 183-194.

The primary focus of this paper is a long-term vision of adoption of SBAC within complex MASs, SURPAS. SURPAS aims at policy-based interoperable pro-active context-aware self-protecting security management in UBIWARE. Generally, UBIWARE is a MAS. It integrates ubiquitous computing with Semantic Web technologies, agent technologies, security, and Enterprise Application Integration.

This paper reports the results of the analysis of the major existing and desired characteristics of UBIWARE-supported environments that impact design decisions for SURPAS. Additionally, we studied the industrial domain of distribution power network management in order to identify the industrial impact of UBIWARE and its business benefits. The case study was conducted in collaboration with ABB, Inc. The analysis of characteristics of UBIWARE-supported environments and the case study provided motivation arguments for SURPAS.

SURPAS follows the general UBIWARE vision – configuring and adding new functionality to the underlying industrial environment on-the-fly by changing high level declarative descriptions. Regarding security, this means that SURPAS is able of smoothly including new, and reconfiguring existing, security mechanisms, for the optimal and secure state of a UBIWARE-based system, in response to the dynamically changing environment.

Finally, the paper presents and discusses the abstract architecture of a secure SmartResource agent that has a central role in UBIWARE. It has four layers: reusable atomic behaviors, behavior models corresponding to different roles the agent plays, SURPAS security policies, and the behavior engine. Roughly speaking, the SURPAS components are the policy enforcement mechanism, security policies and security measures. The SURPAS policy enforcement mechanism is built-in into the behavior engine. The SURPAS security policies follow the SBAC model and ontologies.

5.7 Article VII: "Secure Communication and Access Control for Mobile Web Service Provisioning"

Srirama, S., and Naumenko, A., (2007). Secure Communication and Access Control for Mobile Web Service Provisioning, In CD-ROM Preprints of Proceedings of International Conference on Security of Information and Networks (SIN2007), 8-10th May, 2007.

This article presents our research on securing communication and access control for the MWS provisioning. Both of these issues are addressed in almost equal parts with respect to space. But, our research on securing the communication is in more complete stage.

The paper primarily discusses the security threats and attacks in mobile networks that are relevant for message-level security of MWSs. It later presents the analysis of performance and applicability of different encryption algorithms, signer algorithms and authentication principles for MWS. The detailed performance analysis was based on the developed prototype platform for the MWS provisioning, Mobile Host. Results of tests prove that basic message-level security can be provided, even though not all the standards can be adapted to the MWS communication.

In the second part, this article briefly presents SBAC and the major components of SBAC. The SBAC abstract architecture was presented in the context of mobile environments. Then, the article presents four options of deployment of the SBAC enforcement mechanism with respect to the client and provider of MWS. All four options were found reasonable with different security implications. Rationality of each option is provided with the discussion of advantages and shortcomings.

5.8 Article VIII: "Semantics-Based Access Control for Mobile Web Services"

Naumenko, A., Srirama, S., Terziyan, V., and Jarke, M., (2007), Semantics-Based Access Control for Mobile Web Services, International Journal on Semantic Web and Information Systems, Special Issue on Mobile Services and Ontologies, (Submitted for review 2nd of May, 2007).

This paper concentrates on the application of SBAC for securing MWSs. SBAC was found suitable to handle openness, dynamics, pervasiveness, heterogeneity, and distributed nature of MWS provisioning. The paper consists of three consequent parts.

The first part briefly introduces the concept of MWSs, summarizes the possible technical usage scenarios, and elaborates on the commercial applications and usage scenarios. The commercial applications and usage scenarios section includes the SBAC industrial cases of the business of decentralized network-centric management of power networks and the business of maintenance services in the paper industry.

In order to provide proper qualitative (analytical) justification of research ideas, the second part defines critical success factors for controlling access to MWSs. The analysis of critical success factors takes into account the nature of MWSs, and technical and commercial usage scenarios which were described in the first part.

The third part of the paper describes SBAC and evaluates its components against a list of critical success factors. The SBAC model, policy language and policy enforcement function were analyzed in the context of the MWS provisioning. The major architectural proposal is to utilize distributed architectures of the SBAC enforcement mechanism as an adequate access control solution for the MWS provisioning.

The paper reports results of quantitative (experimental) feasibility study on the performance of the access control decision making procedure. This quantitative feasibility study uses a prototype that was developed to make the research ideas tangible. The quantitative evaluation shows applicability of SBAC for middleware guards of MWSs. Development of the embedded guard following SBAC requires a more robust solution.

5.9 Article IX: "A Research Framework towards Semantics-Based Access Control"

Naumenko, A., (2007), A Research Framework towards Semantics-Based Access Control, International Journal of Network Security, (Submitted for review 2nd of May, 2007).

This paper concludes and summarizes the previous research on SBAC. It describes the SBAC research framework as a coordinating and guiding tool towards SBAC. The SBAC research framework defines major research and development components for the solid but extensible layered structure.

The SBAC layer of conceptual semantics is the main theoretical result of conceptual modelling. It contains the model-theoretic semantics of SBAC and the SBAC ontologies. The model-theoretic specification defines fundamental concepts and relations between them using the theory of sets and extending the direct model-theoretic semantics of OWL. The SBAC ontologies serialize the model-theoretic semantics of SBAC. The formal explicit specification of semantics is an input for the critical analysis of characteristics of suggested features and further elaborations of other components of the SBAC research framework. Taking into account the importance of ontologies, this paper also describes the place and role of ontologies across all layers and components of SBAC.

The SBAC layer of functionality mainly contains the abstract architecture of two access control functions: the administrative function and the policy enforcement function.

The SBAC layer of technological profiles collects cases of adoption of SBAC for different approaches and technologies of software and systems design. This is done to ensure granularity and modularization of SBAC. So far the research on SBAC has explored the adoption of SBAC for SWSs, MASs, and MWSs.

The SBAC layer of real-world application areas consist of different industries, organisations, businesses, etc. These application areas initially are sources of requirements to SBAC. Consequently, these application areas are adoption domains of SBAC. In addition to the previously studied domains of paper industry and power networks, this paper adds the case of high education into the set of SBAC adoption domains.

5.10 About joint publications

The author of this thesis is the sole author of Articles III, IV and IX. In all other articles the author was the principal contributor except Article VII. Regarding Article I, Prof. Vagan Terziyan and Andriy Zharko edited the final draft; Sergiy Nikitin contributed examples into Section 4, "Advantages of OWL over XML". Mirja Pulkkinen supervised and coordinated the research behind Article II, edited the final draft and contributed parts related to EA, Metso Paper, Inc., and introductory material. Dr. Kari Luostarinen commented the final draft and contributed data about Metso Paper, Inc, for Articles II and V. In Article VI, Dr. Artem Katasonov edited the final draft and jointly contributed with Prof. Vagan Terziyan the material about UBIWARE, the industrial case and the architecture of a SmartResource agent. Satish Srirama is a corresponding author of Article VII. Into this paper the author of this thesis contributed Section 4 "Semantics-based access control mechanisms". Regarding Article VIII, Prof. Vagan Terziyan and Prof. Matthias Jarke supervised research and work on this paper; Satish Srirama partly contributed within Sections 2, "Mobile Web Services", and 3, "Criteria for qualitative evaluation of security solutions".

6 CONCLUSIONS

This chapter presents contributions of this thesis, outlines answers to the research questions, summarizes limitations, and describes future research and development targets.

6.1 Contributions

The SBAC research framework, being an important contribution itself, systematically collects and presents the major contributions of this dissertation. These are the SBAC conceptual semantics, the SBAC functional semantics, the prototype implementation of the SBAC enforcement function, the adoption of SBAC for different technological profiles, and the adoption of SBAC in different business domains. The rest of this section describes the significance of each research artifact (Hevner et al., 2004) of the dissertation.

Business needs and *critical success factors* are crucial for the motivation, alignment and applicability of SBAC in real-world settings. The collaborating commercial companies, Metso Automation, Metso Paper, Trusteq and ABB, helped to reveal and to collect practical motivating business needs. The critical success factors of emerging environments and these business needs have determined the directions, emphases and results throughout the research on SBAC.

The SBAC model has significantly impacted other research artifacts in the scope of this dissertation because it is the normative source for referring to the conceptual semantics of SBAC. This theoretical and formal representation of the conceptual semantics has also been important in order to formally extend the Semantic Web standards; to provide the basis for the formal specification of the SBAC functionality; and to conduct further critical analyses of the introduced features using formal methods.

The SBAC ontologies compose the main research proposal. In general, ontologies are the key part of the SBAC research framework. The central role of ontologies determines research decisions and characteristics of SBAC. In particular, the SBAC ontologies create the upper-level machine-interpretable conceptual schema of SBAC. The practical and research implications of the SBAC ontologies are following.

– The abstract architecture and prototyping depend on and directly deal with the SBAC ontologies.

– Domain ontologies and ontologies of the SBAC technological profiles import and extend the SBAC ontologies.

The SBAC abstract architecture is the main bridge between the theoretical findings and the adoption of SBAC into practice. This abstract design captures and organizes SBAC's fundamental elements and their relations. This is needed to ensure compliance and interoperability of different valid specializations and/or implementations of SBAC. For example, SBAC technological profiles and business domains have specialized and adjusted the SBAC abstract architecture. Another example is that, in prototyping for the quantitative testing, the research ideas have been kept in correspondence with the abstract architecture.

The prototype of the SBAC enforcement function has made the research ideas tangible. The process of prototype implementation helped to reflect on the conceptual results from a technical perspective. However, the major role of the prototype has been to justify the initial research proposal based on the quantitative evaluation of its performance. This prototype also proved the high degree of reusability of the existing Semantic Web tools for the implementation of SBAC. Future research on SBAC can use the prototype to decrease the duration of iterations of analytical research and practical evaluation (Hevner et al., 2004). The prototype also facilitates dissemination of SBAC.

Specializations of the SBAC ontologies and abstract architecture in the SBAC technological profiles and business domains exemplify several aspects of how to adopt SBAC into practice. The merged semantics of the SBAC SWS profile has illustrated the way how to merge the SBAC ontologies with the existing ontologies in (semantic) SOA. The engineering of domain ontologies and corresponding SBAC policies for the paper industry has exemplified how to extend the SBAC ontologies. There are also several examples of specialization of the SBAC abstract architecture, i.e., the concrete SBAC architecture and use case using SWSs, diverse deployment options of the SBAC architectural components for the provisioning of MWSs, and the internal architecture of secure SmartResource agents. These all contribute to the knowledge base for the future research and for the assessment of significance of SBAC.

The SBAC research framework has systematically coordinated and guided the research towards SBAC. The research framework has helped to analyze the interrelations and interdependencies between all the above described major contributions. Moreover, it is able to accommodate the existing relevant research contributions of others and to organize results of the future practical research along the extensible layers of technological profiles and business domains.

6.2 Answers to the research questions

At the beginning of this thesis we defined three research questions for each of the three research goals:

G1 *The research must lead to a solid conceptualization that integrates existing knowledge and provides possibilities to facilitate integrating new knowledge.*

G2 *Qualitative and quantitative evaluations are necessary to provide convincing arguments for the feasibility and rationality of SBAC.*

G3 *This research should take into account the real-world practical needs of both business networks of commercial companies and emerging ICTs.*

This section provides concise answers for these research questions which are in a close relation to the above described contributions:

G1.R1 *One has to define what are the most generic concepts and relations in the field of access control. These generic concepts and relations should form the core part of the SBAC conceptual semantics.*

We identified the most generic concepts and relations between them during research on the conceptual semantics of SBAC. The core part contains concepts of subject, operation and object of access. It also includes concepts of resources, different access control statements, rules, context, etc., and relations between these concepts. Section 3.1 of this thesis and Article III, "Contextual rules-based access control model with trust" (Naumenko, 2006), provide more details answering this question.

G1.R2 *The major research question related to the first goal is how to systematically manage the semantics of these generic concepts and relations in SBAC.*

Following the tradition in the research field on access control, we specified the semantics initially in the SBAC model (Article III, "Contextual rules-based access control model with trust", and Article V, "Access Control Policies in (Semantic) Service-Oriented Architecture"; Naumenko, 2006; Naumenko and Luostarinen, 2006). After that we serialized the SBAC model in the form of SBAC ontologies (Article IV, "Semantics-Based Access Control – Ontologies and Feasibility Study of Policy Enforcement Function"; Naumenko, 2007a). The whole research proves that ontology-based management of semantics of access control is the most appropriate for emerging and present computational environments.

G1.R3 *Regarding the functionality of SBAC, the question is how to identify and to abstractly design functional access control components for SBAC.*

The major principle for the design of the SBAC abstract architecture was to reflect only components and relationships that are valid for each concrete implementation of SBAC we might have. Thus, we kept the SBAC abstract architecture free from the specifics of different real-world domains and design of information systems according to different paradigms. Section 3.3 provides a description of the SBAC abstract architecture and refers to the articles where more details can be located.

G2.R1 *For the qualitative evaluation there should be criteria upon which the SBAC results can be evaluated. Thus it is important to identify what the critical success factors for SBAC are.*

The critical success factors for SBAC have been identified in Article VIII, "Semantics-Based Access Control for Mobile Web Services" (Naumenko et al., 2007b). The concise list of these critical success factors can be found in Section 3.7. The same article provides a review of SBAC upon these factors. The case studies collected motivating and justifying arguments for SBAC. In addition, these studies collected real-world practical needs that serve as requirements for SBAC in general and the qualitative evaluation in particular.

G2.R2 *Besides the qualitative evaluation, the major practical concern is whether it is feasible to implement SBAC with existing tools and technologies. It is also interesting to check the level of reuse of existing tools.*

Rapid prototyping of the SBAC enforcement function with the high level of reuse of existing software components proved the feasibility of SBAC from the system development perspective (Article IV, "Semantics-Based Access Control – Ontologies and Feasibility Study of Policy Enforcement Function"; Naumenko, 2007a). Section 3.4 provides a description of the prototype and the process of prototyping.

G2.R3 *If SBAC is feasible from the system development point of view then the next question is whether it is rational from the perspective of performance.*

The performance is important for the SBAC enforcement function because it provides a utility function as part of some business functions. Based on the conducted test for performance of the prototype of the SBAC enforcement function, we concluded that even our research prototype of the SBAC enforcement function has sufficient performance in order to adopt SBAC into practice (Article IV, "Semantics-Based Access Control – Ontologies and Feasibility Study of Policy Enforcement Function"; Naumenko, 2007a). Section 3.4 summarizes the results of the tests.

G3.R1 *The rationality of SBAC does not only originate from the performance, but it heavily depends on the applicability of SBAC for some real-world practical needs. Thus, the research should explore what the most vital practical business needs for SBAC are.*

The case studies in the three real-world domains were conducted mainly to reveal concrete practical needs for the policy-based management of access control in business networks. The vital practical needs were evaluated for the research decisions towards SBAC. Thus the applicability of SBAC originates from the thorough attention to the needs of real-world business networks. Sections 3.8, 3.9, and 3.10 present the results of the case studies.

G3.R2 *Then, it is important to see how the SBAC conceptual semantics can be specialized in different domains and for different technologies.*

Article V, "Access Control Policies in (Semantic) Service-Oriented Architecture" (Naumenko and Luostarinen, 2006), presents the adoption of the SBAC conceptual semantics in semantic SOA for maintenance services in paper industry. We have not adopted the SBAC conceptual semantics for the other two domains. However, Section 3.7 and Article VIII, "Semantics-Based Access Control for Mobile Web Services" (Naumenko et al., 2007b), present the adoption of the SBAC conceptual semantics for MWS provisioning.

G3.R3 *The same is true for the SBAC functionality - how the abstract design of the SBAC can be implemented using the existing paradigms of design of information systems and technologies, and deployed in different domains.*

During our research, the SBAC abstract architecture has been adopted for SWSs, MASs and MWSs. Sections 3.5, 3.6, and 3.7 describe the adoption of the abstract architecture for these emerging technologies. Article V, "Access Control Policies in (Semantic) Service-Oriented Architecture" (Naumenko and Luostarinen, 2006), presents the adoption of the SBAC abstract architecture and use case in real-world domain of maintenance services in paper industry.

6.3 Limitations

There are several critical sections in the research. SBAC relies on the advances of Semantic Web technologies, a great many of which have not been standardized and are being actively discussed and researched. These technologies include rule languages, trust, logic frameworks, inference engines, ontology-driven architecture, and others.

The case studies of practical business needs for SBAC were limited to three real-world cases: two business networks of commercial companies and one educational network for public organizations. Basically, though, the obtained results can be applied for similar settings.

Regarding the SBAC model, the suggested structure of access control statements is disputably universal enough to accommodate privilege, trust, trace, etc statements. This dissertation does not provide any rigorous analysis of rights propagation and secure state of the system that would use the SBAC model. However, it is an important prerequisite to the acceptance and adoption of access control models. The SBAC ontologies specify the concepts using the OWL Full profile. This may cause problems at the stage of practical implementation as long as existing inference engines do not fully support the whole semantics of OWL.

The current prototype implements the access control decision making procedure within the centralized architecture of SBAC. However, other procedures impact the performance as well. The centralized architecture of SBAC is the simplest when compared to both the mixed and distributed architecture. Moreover, the fastest response time of the decision making procedure corresponds to the simplest policy, domain ontology, authorization rule, and to the case where all needed RDF statements of SBAC, domain and policy ontologies are loaded into the decision set during the start-up process. The provided feasibility study illustrates the benefits of orientation to Semantic Web in reusability and expressivity. In general, the performance is quite promising taking into account the non-commercial nature of all the components.

There are limitations in the contributions that are related to the SBAC technological profiles. For example, in the SBAC SWS profile, the theoretical findings were applied to the specification of access control policies for authorizations of web services only corresponding to the OWL-S specifications, despite the existence of other languages and ontologies for SWSs, e.g., Web Service Modeling Ontology (WSMO), Semantic Web Services Framework (SWSF), and Web Service Semantics - WSDL-S. Specifically, there is a weak link between restricted objects of access and classifications of input parameters due to the compliance of OWL-S to the OWL DL profile. Also, the specification of protected objects using the concept of inputs of atomic processes is based on the assumption that inputs pre-determine service invocations which is not always true and does not take into account the world state.

6.4 Further research

SBAC is still an ambitious research and development target. Firstly, further research has to overcome the present limitations of SBAC. Additionally, there are directions of the future research towards new features.

The first research direction is the elaboration of the SBAC conceptual and functional semantics. The SBAC model and ontologies should be improved with the advanced features in order to support semantics-based rules, flexible delegation, expressive constructs for constraints, contextual descriptions, trust management, semantic logging and audit, and other concerns.

Regarding the functional semantics, the specific algorithms require attention to formalize complex tasks and procedures, e.g., semantic annotating of requests, retrieving relevant domain ontologies, taxonomic and faceted classifying of subjects, operations, and objects of access, retrieving relevant policy statements, resolving conflicts in relevant policy statements; access control decision making, and other. The formal specification and reference implementation of the SBAC functionality are important research and development targets for the activities related to the standardization of SBAC.

The second direction, that is more practical, involves adopting SBAC for different technologies and domains. Adoption of SBAC in real-world applications, systems, organizations, industries, etc. can truly assess practical implications and significance of SBAC. The primary target areas are those where Semantic Web emerges and resources have their semantic annotations according to ontologies, e.g., (semantic) SOA and MASs. In addition to the already targeted technological profiles, the promising areas are semantic web portals, information retrieval, social networks, collaborative tools, and other. Regarding the business domains, all businesses, that extensively involve inter-organizational collaboration with high requirements for trust and privacy, can benefit from SBAC.

The third direction encompasses the SBAC methodology that was left out of the scope of this dissertation due to the immature nature of SBAC. However, the contributions of this thesis will hardly make a significant impact without the SBAC methodology. The feedback from case studies of adoption of SBAC for different technologies and business domains and cases themselves can be an important part of the SBAC methodology. They might serve as success stories or best practices depending on their practical and scientific merit.

REFERENCES

Agarwal, S. and Sprick, B., (2004). Access Control for Semantic Web Services, In Proceedings of the IEEE international Conference on Web Services (ICWS'04), IEEE Computer Society, Washington, DC, pp. 770-773.

Agarwal, S., Sprick, B., and Wortmann, S., (2004). Credential based access control for semantic web services, In AAAI Spring Symposium - Semantic Web Services, March 2004, Stanford, California, USA.

Bacon, J., Moody, K., and Yao, W., (2002). A model of OASIS role-based access control and its support for active security, ACM Transactions on Information and System Security (TISSEC), 5(4):492–540.

Bell, D. E., and LaPadula, L. J., (1973). Secure Computer Systems: Mathematical Foundations and Model, Bedford, MA: The Mitre Corporation.

Berners-Lee, T., Hendler, J., and Lassila, O., (2001). The Semantic Web. Scientific American, 284(5): 34-43.

Biba, K. J., (1977). Integrity Considerations for Secure Computer Systems, Bedford, MA: The MITRE Corporation.

Brickley, D., and Guha, R. V., (eds.), (2004). RDF Vocabulary Description Language 1.0: RDF Schema, W3C Recommendation, http://www.w3.org/TR/rdf-schema/ (26.02.2007).

Britton, C., and Bye, P., (2004). IT Architectures and Middleware (2nd Edition), Addison-Wesley, Boston.

Clark, D. D., and Wilson., D. R., (1987). A Comparison of Commercial and Military Computer Security Policies, IEEE Symposium of Security and Privacy, pp. 184–194.

Damiani, E., De Capitani di Vimercati, S., Fugazza, C., and Samarati, P., (2004). Extending policy languages to the semantic web, In Proceedings of the 4th International Conference of Web Engineering (ICWE2004), pp. 330--343.

Fensel, D. (2001). Ontologies: Silver Bullet for Knowledge Management and Electronic Commerce. Heidelberg, Springer-Verlag.

Fernandez, E., and Pan, R., (2001). A pattern language for security models, In Proceedings of the 8th Conference on Pattern Languages of Programs, http://hillside.net/plop/plop2001/accepted_submissions/PLoP2001/ebfernandezandrpan0/PLoP2001_ebfernandezandrpan0_1.pdf (26.02.2006)

Ferraiolo, D., Kuhn, D., and Chandramouli, R., (2003). Role-Based Access Control, Artech House.

Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, D., and Chandramouli, R., (2001). Proposed NIST standard for role-based access control, ACM Transactions on Information and Systems Security (TISSEC), 4(3):224–274.

Gruber, T., 1993. A translation approach to portable ontologies. Knowledge Acquisition, 5(2): 199-220.

Hayes, P., (ed.), (2004), RDF Semantics, W3C Recommendation, W3C, http://www.w3.org/TR/rdf-mt/ (26.02.2006)

Hevner, A., March, S., and Park, J., (2004). Design science in information systems research, MIS Quarterly 28(1), 75–105.

Horrocks I., Patel-Schneider P., Boley H., Tabet S., Grosof B. and Dean M., (2004). SWRL: A Semantic Web Rule Language combining OWL and RuleML, W3C Member Submission, W3C, http://www.w3.org/Submission/SWRL/ (26.02.2007).

Jajodia S., Kudo M. and Subrahmanian, V. (2000), Provisional Authorizations, In Proceedings of the Workshop on Security and Privacy in E-commerce, Kluwer Academic Publishers, pp. 133-159.

Javanmardi, S., Amini, M., and Jalili, R., (2006a). An Access Control Model for Protecting Semantic Web Resources, In Proceedings of the 2nd International Semantic Web Policy Workshop (SWPW'06), Nov. 2006, Athens, GA, USA, pp. 32-46.

Javanmardi, S., Amini, M., Jalili, R., and Ganjisaffar, Y., (2006b). SBAC: Semantic Based Access Control, In Proceedings of the 11th Nordic Workshop on Secure IT-systems, Linkping, Sweden, October 2006, pp. 157-168

Javanmardi, S., Hemmati, H., and Jalili, R., (2006c). An Access Control Framework for Pervasive Computing Environments, In Proceedings of the International Conference on Pervasive Systems & Computing, PSC 2006, Las Vegas, Nevada, USA, June 26-29, 2006. CSREA Press 2006, pp 97-103.

Järvinen, P., (2004). On research methods, Tampere: Opinpajan Kirja.

Kaykova O., Khriyenko O., Naumenko A., Terziyan V., Zharko A., (2005a). RSCDF: A Dynamic and Context-Sensitive Metadata Description Framework for Industrial Resources, Eastern-European Journal of Enterprise Technologies, 3(3): 55-78.

Kaykova O., Khriyenko O., Kovtun D., Naumenko A., Terziyan V., Zharko A., (2005b). General Adaption Framework: Enabling Interoperability for Industrial Web Resources, International Journal on Semantic Web and Information Systems, Idea Group, 1(3): 31-63.

Kaykova O., Khriyenko O., Kovtun D., Naumenko A., Terziyan V., Zharko A., (2007). Challenges of General Adaptation Framework for Industrial Semantic Web, A. Sheth and M. Lytras (eds.), Semantic Web-Based Information Systems: State-of-the-Art Applications, Idea Group, Vol. 1, pp. 61-97.

Kephart, O., and Chess, D. M., (2003). The vision of autonomic computing, Computer, 36(1): 41--50.

Kern, A., (2002). Advanced Features for Enterprise-Wide Role-Based Access Control, In Proceedings of the 18th Annual Computer Security Applications Conference, Las Vegas, Nevada, USA, pp. 333–342.

Kern, A., Kuhlmann, M., Schaad, A., and Mofett, J., (2002). Observations on the Role Life-Cycle in the Context of Enterprise Security Management, In Proceedings of the 7th ACM Symposium on Access Control Models and Technologies (SACMAT 2002), Monterey, California, USA, pp. 43–51.

Klyne, G., and Carroll, J., (eds.), (2004). Resource Description Framework (RDF): Concepts and Abstract Syntax, W3C Recommendation, http://www.w3.org/TR/rdf-concepts/ (26.02.2007).

Lapkin, A., (2003). The Gartner Enterprise Architecture Framework, ITXPO Symposium, Gartner Inc.

Linden, M., (2005). Organising federated identity in Finnish higher education, The world of pervasive networking, The 21th Trans European Research and Education Networking Conference, June 6-9, 2005, TERENA, Poznan, Poland.

Linthicum, D., (2004). Next Generation Application Integration: From Simple Information to Web Services, Addison-Wesley, Boston.

Luostarinen, K., Naumenko, A., Pulkkinen, M., (2006), Identity and Access Management for Remote Maintenance Services in Business Networks, in IFIP International Federation for Information Processing, Project E-Society: Building Bricks, eds. R. Suomi, Cabral, R., Hampe, J. Felix, Heikkilä, A., Järveläinen, J., Koskivaara, E., (Boston: Springer), (226):1-12.

March, S. and Smith, G. (1995). Design and Natural Science Research on Information Technology. Decision Support Systems 15 (1995): 251 - 266.

Martin, D., et al., (2004). OWL-S: Semantic Markup for Web Services, W3C Member Submission, http://www.w3.org/Submission/2004/SUBM-OWL-S-20041122/

Mazhelis, O., and Naumenko, A., (2005). Security Patterns in Software Application Design, Technical Report #10, Mobile Design Patterns and Architectures Research Project, Information Technology Research Institute, University of Jyvaskyla, October, 2005.

Mazhelis, O., and Naumenko, A., (2006). The Place and Role of Security Patterns in Software Development Process, In Medina, E.F. and Yagüe, M.I. (Eds.), Security in Information Systems Proceedings of the 4th International Workshop on Security in Information Systems, WOSIS 2006 In conjunction with ICEIS 2006 Paphos, Cyprus, May 2006. INSTICC Press, pp. 91-100.

McGuinness, D., and Harmelen, F., (eds.), (2004). OWL Web Ontology Language Overview, W3C Recommendation, W3C, http://www.w3.org/TR/owl-features/ (26.02.2007)

Mitra, P., Pan, C., Liu, P., and Atluri, V., (2006). Privacy-preserving semantic interoperation and access control of heterogeneous databases, In Proceedings of the 2006 ACM Symposium on information, Computer and Communications Security (Taipei, Taiwan, March 21 - 24, 2006), ASIACCS '06, ACM Press, New York, NY, pp. 66-77.

Moses, T., (ed.), (2005). eXtensible Access Control Markup Language (XACML) Version 2.0. OASIS Standard.

Nadalin, A., Kaler, C., Monzillo, R., and Hallam-Baker, P., (eds.), (2006). Web Services Security: SOAP Message Security 1.1 (WS-Security 2004). OASIS Standard Specification.

INFOSEC – National Information Systems Security Glossary, NSTISSI No. 4009, January 1999 (Revision 1).

Naumenko, A., (2006). Contextual rules-based access control model with trust, In Shoniregan C. A. and Logvynovskiy A. (Eds.), In Proceedings of the International Conference for Internet Technology and Secured Transactions, ICITST 2006, 11-13 September, London, UK, e-Centre for Infonomics, pp. 68-75.

Naumenko A., (2007a), Semantics-Based Access Control – Ontologies and Feasibility Study of Policy Enforcement Function, In: J., Filipe, J., Cordeiro, B., Encarnacao, and V., Pedrosa (Eds.), In Proceedings of the 3rd International Conference on Web Information Systems and Technologies (WEBIST-07), Barcelona, Spain - March 3-6, 2007, Volume Internet Technologies, INSTICC Press, pp. 150-155.

Naumenko, A., (2007b), A Research Framework towards Semantics-Based Access Control, International Journal of Network Security, (Submitted for review 2nd of May, 2007).

Naumenko A., Katasonov A., Terziyan V., (2007a), A Security Framework for Smart Ubiquitous Industrial Resources, In: Goncalves, R., Müller, J., Mertins K., and Zelm, M., (Eds.), In Enterprise Interoperability II: New challenges and Approaches, Proceedings of the 3rd International Conference on Interoperability for Enterprise Software and Applications (IESA-07), March 28-30, 2007, Madeira Island, Portugal, Springer, pp. 183-194.

Naumenko, A. and Luostarinen, K., (2006). Access Control Policies in (Semantic) Service-Oriented Architecture, In Schaffert S. and Sure Y. (Eds.), Semantic Systems From Visions to Applications, Proceedings of the SEMANTICS 2006, Austrian Computer Society, Vienna, Austria, pp. 49-62.

Naumenko A., Nikitin S., Terziyan V., and Zharko A., (2005a). Strategic Industrial Alliances in Paper Industry: XML- vs. Ontology-Based Integration Platforms, In: The Learning Organization, Special Issue on: Semantic and Social Aspects of Learning in Organizations, Emerald Publishers, ISSN: 0969-6474, Vol. 12, No. 5, 2005, pp. 492-514.

Naumenko A., Nikitin S., Terziyan V., Veijalainen J., (2005b). Using UDDI for Publishing Metadata of the Semantic Web, In: V. Terziyan and M. Bramer (Eds.): Proceedings of the 1-st International IFIP/WG12.5 Working Conference on Industrial Applications of Semantic Web, August 25-28, 2005, Jyvaskyla, Finland, Springer, IFIP, pp. 141-159.

Naumenko, A., Srirama, S., Terziyan, V., and Jarke, M., (2007b), Semantics-Based Access Control for Mobile Web Services, International Journal on Semantic Web and Information Systems, Special Issue on Mobile Services and Ontologies, (Submitted for review 2nd of May, 2007).

Nunamaker, J.F., Chen, M. and Purdin, T.D.M., (1991). Systems development in Information Systems research. Journal of Management Information Systems 7(3), 89-106.

O'Reilly T., 2005. What Is Web 2.0 Design Patterns and Business Models for the Next Generation of Software, http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html (26.02.2007).

Pan, C., Mitra, P., and Liu, P., (2006). Semantic access control for information interoperation, In Proceedings of the Eleventh ACM Symposium on Access Control Models and Technologies (Lake Tahoe, California, USA, June 07 - 09, 2006), SACMAT '06. ACM Press, New York, NY, pp. 237-246.

Patel-Schneider P., Hayes P. and Horrocks I., (eds.), (2004). OWL Web Ontology Language Semantics and Abstract Syntax, W3C Recommendation, W3C; www.w3.org/TR/owl-absyn/ (26.02.2007).

Powers, S. (2003). Practical RDF, O'Reilly.

Priebe, T., Dobmeier, W., and Kamprath, N., (2006). Supporting attribute-based access control with ontologies, In Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), IEEE Computer Society, pp. 465-472.

Prud'hommeaux, E., and Seaborne, A. (eds.). (2006). SPARQL Query Language for RDF. W3C Candidate Recommendation, W3C, http://www.w3.org/TR/rdf-sparql-query/ (26.02.2007).

Pulkkinen, M., Naumenko, A., and Luostarinen, K., (2007). Managing Information Security in a Business Network of Machinery Maintenance Services Business - Enterprise Architecture as a Coordination Tool, , In: Sangkyun Kim (Ed.), Special Issue on Methodology of Security Engineering for Industrial Security Management Systems, Journal of Systems and Software, ELSEVIER (in press).

Pulkkinen, M., Naumenko, A., and Nieminen, K., (2006). Metso Paper Oy and Trusteq Oy, Case Report, Mobile Design Patterns and Architectures Research Project, Information Technology Research Institute, University of Jyvaskyla, April, 2006.

Qin, L., and Atluri, V., (2003). Concept-level access control for the Semantic Web, In Proceedings of the 2003 ACM Workshop on XML Security XMLSEC '03, ACM Press, New York, NY, 94-103.

Qu Y.; Zhang, X; Li, H., (2004). OREL: An Ontology-based Rights Expression Language, In Proceedings of the 13th international World Wide Web Conference. ACM Press, pp. 324-325.

Rao, J., and Sadeh, N., (2005). A Semantic Web Framework for Interleaving Policy Reasoning and External Service Discovery, Lecture Notes in Computer Science, Springer, Volume 3791, pp. 56 – 70.

Rosenfeld, S., (1995). Industrial Strength Strategies: Regional Business Clusters and Public Policy. Washington, DC. Aspen Institute.

Rouvari, A., (2004). Scolarly Information Portals. Interoperability: new challenges and solutions 28th Library systems seminar, Trondheim, 9-11 June, 2004, http://www.elag2004.no/papers/Rouvari.pdf (26.02.2007).

Sandhu, R., Coyne, E., Feinstein, H., and Youman, C., (1996). Role-Based Access Control Models, IEEE Computer, 29(2): pp. 38-47.

Security Assertion Markup Language (SAML), (2005), v2.0, OASIS Security Services TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security (26.02.2007).

Srirama, S., and Naumenko, A., (2007). Secure Communication and Access Control for Mobile Web Service Provisioning, In CD-ROM Preprints of

Proceedings of International Conference on Security of Information and Networks (SIN2007), 8-10th May, 2007.

Shields, B., Molloy, O., Lyons, G., and Duggan, J., (2005). Securing Web Services using Semantic Web Technologies, In Proceedings of the 1-st International IFIP/WG12.5 Working Conference on Industrial Applications of Semantic Web IASW-2005. pp. 213 – 225.

Tiitinen, P., Naumenko, A., Nikitin, S., Bartholdt, J., Toma, I., Roman, D., Tausch, B., (2005). Requirements Analysis on Service Registries, Deliverable D2.II-1, Adaptive Services Grid FP6 – 004617, August 2005.

Tonti, G., Bradshaw, J., Jeffers, R., Montanari, R., Suri, R., and Uszok, A., (2003). Semantic web languages for policy representation and reasoning: A comparison of KAoS, Rei, and Ponder, In Proceedings of the International Semantic Web Conference. pp. 419--437.

Uszok, A., Bradshaw, J., Jeffers, R., Johnson, M., Tate A., Dalton, J., and Aitken, S., (2004). Policy and Contract Management for Semantic Web Services, In Proceedings of the AAAI Spring Symposium on Semantic Web Services.

Wang, X., Lao, G., DeMartini, T., Reddy, H., Nguyen, M., and Valenzuela, E., (2002). XrML -- eXtensible rights Markup Language. In Proceedings of the ACM Workshop on XML Security. XMLSEC '02. ACM Press, New York, NY, pp. 71-79.

Wang Xiaopeng, Luo Junzhou, Song Aibo, and Ma Teng, (2005). Semantic access control in grid computing, In Proceedings of 11th International Conference on Parallel and Distributed Systems, pp. 661 - 667 Vol. 1.

Yin, R. K., (1994). Case Study Research - Design and Methods. 2nd edition, Sage Publications: Thousand Oaks, CA.

Yagüe, M., Gallardo, M., and Maña, A. (2005a). Semantic Access Control Model: A Formal Specification, Lecture Notes in Computer Science, Volume 3679, pp. 24 - 43,

Yagüe, M., Maña, A., and López, J. A (2005b). Metadata-based Access Control Model for Web Services. Internet Research Journal: Electronic Networking Applications and Policy, 25(1):99–116.

Yagüe, M., Maña, A., López, J., Pimentel, J., and Troya, J. (2003a). A Secure Solution for Commercial Digital Libraries. Online Information Review Journal, 27(3):147–159.

Yagüe, M., Maña, A., López, J., and Troya, J. (2003b). Applying the Semantic Web Layers to Access Control. In Proc. of the Int. Workshop on Web Semantics, pages 47–63. IEEE Computer Society Press.

Yergeau, F., Bray, T., Paoli, J., Sperberg-McQueen, C., and Maler, E., (2004). Extensible Markup Language (XML) 1.0 (Third Edition). W3C Recommendation, http://www.w3.org/TR/2004/REC-xml-20040204/ (26.02.2007).

YHTEENVETO (FINNISH SUMMARY)

Yksityisyyden ja luottamuksen säilyttäminen on tärkeää liikeyritysten välisessä yhteistyössä. Välitettävien tietojen ja palvelujen luottamuksellisuus, eheys ja saatavuus edellyttävät tarkoituksenmukaisia pääsynhallintaratkaisuja, joiden tuella liiketoiminnallista yhteistyötä syventää ja saavuttaa näin kilpailuetuja. Tietotekniset ratkaisut tukevat enenevässä määrin yritysrajat ylittäviä liiketoimintaprosesseja. WWW-pohjaiset tietojärjestelmät ovat yhä monimutkaisempia, dynaamisempia, heterogeenisempia ja avoimempia. Perinteiset tietoturvaratkaisut eivät enää riitä uusien teknologioiden ja tietojärjestelmien tarpeisiin.

Tässä työssä etsitään ratkaisuja organisaatioiden välisten automatisoitujen liiketoimintaprosessien yhä monimutkaistuvaan pääsynhallintaan tarkastelemalla liiketoimintaverkostoja käsitteellisellä tasolla ja luomalla semanttisiin riippuvuuksiin perustuvaa pääsynhallintaa (SBAC – Semantics Based Access Control). Työn päätulokset ovat SBAC:n käsitteellinen ja toiminnallinen semantiikka, prototyyppitoteutus SBAC politiikkaa toteuttavista toiminnoista sekä hahmotelmat SBAC lähestymistavan soveltamisesta erilaisiin teknologisiin ja liiketoimintaympäristöihin. Liiketoiminnan tarpeet sekä käytännön sovellukset ovat ohjanneet teoreettista tutkimusta ja työ muodostaa ensimmäisen täyden iteraation SBAC-mallin tutkimuksessa. Käytännön toteutusten tarpeita kartoitetaan case-tutkimuksilla. Sen jälkeen rakennetaan käsitemalli SBAC-kokonaisuudesta ja lopuksi arvioidaan niin laadullisesti kuin käytännön testeinkin, miten hyvin alkuperäiset tutkimustavoitteet saavutettiin.

Väitöskirjassa luotu viitekehys on osoittautunut joustavaksi ja laajennuskelpoiseksi. Sen avulla on mahdollista jäsentää tulevaa tutkimusta erotellen mm. käsitteellinen mallinnus, toiminnallisuuksien kehittäminen, teknologiset rajapinnat ja liiketoimintaprosessien tarpeet omiksi tutkimusalueikseen.