Modelling and Analysing Access Control Policies in XACML 3.0

XACML (eXtensible Access Control Markup Language) is a prominent access control language that is widely adopted both in industry and academia. XACML is an international standard in the field of information security. The problem with XACML is that its specification is described in natural language (c.f. GM03,Mos05,Ris13) and manual analysis of the overall effect and consequences of a large XACML policy set is a very daunting and time-consuming task.

In this thesis we address the problem of understanding the semantics of access control policy language XACML, in particular XACML version 3.0. The main focus of this thesis is modelling and analysing access control policies in XACML 3.0.

There are two main contributions in this thesis. First, we study and formalise XACML 3.0, in particular the Policy Decision Point (PDP). The concrete syntax of XACML is based on the XML format, while its standard semantics is described normatively using natural language. The use of English text in standardisation leads to the risk of misinterpretation and ambiguity. In order to avoid this drawback, we define an abstract syntax of XACML 3.0 and a formal XACML semantics. Second, we propose a logic-based XACML analysis framework using Answer Set Programming (ASP). With ASP we model an XACML PDP that loads XACML policies and evaluates XACML requests against these policies. The expressivity of ASP and the existence of efficient implementations of the answer set semantics provide the means for declarative specification and verification of properties of XACML policies.

Overall, we focus into two different area. The first part focuses on the access control language. More specifically our focus is on the understanding XACML 3.0. The second part focuses on how we use Logic Programming (LP) to model access control policies. We show that there is a relation between XACML and LP through their semantics. We close the thesis by presenting applications in analysing access control properties and a case study. These applications show that these two approaches (AC paradigm and LP paradigm) can be combined together.

We close the thesis by presenting applications in analysing access control properties and a case study. We present access control security policies in a Smart Grid from Smart Meter perspective.
The logic of XACML
We study the international standard XACML 3.0 for describing security access control policies in a compositional way. Our main contributions are (i) to derive a logic that precisely captures the intentions of the standard, (ii) to formally define a semantics for the XACML 3.0 component evaluation, and (iii) to define a semantics for the XACML 3.0 standard combining operators. To guard against modeling artefacts we provide an alternative lattice based way of characterizing the policy combining operators and we formally prove the equivalence of these approaches thereby increasing our faith in either one. We then discuss several ways of extending XACML: one direction is to extend XACML with new combining operators, and another direction is to incorporate the notion of conflict into XACML. We conclude by discussing the possibility of analysing XACML policies for gaps and conflicts.
We present a systematic technique for transforming XACML 3.0 policies in Answer Set Programming (ASP). We show that the resulting logic program has a unique answer set that directly corresponds to our formalisation of the standard semantics of XACML 3.0 from [9]. We demonstrate how our results make it possible to use off-the-shelf ASP solvers to formally verify properties of access control policies represented in XACML, such as checking the completeness of a set of access control policies and verifying policy properties.

Smart Grid Security A Smart Meter-Centric Perspective

The electricity grid is a key infrastructure for our society, therefore its security is a critical public concern. This physical system is becoming more and more complex as it is coupled with a cyber layer carrying information about power usage and control instructions for intelligent appliances, leading to what is known as the Smart Grid. The development of this Cyber-Physical System introduces new security issues, thus calling for efforts in studying possible attacks and devising suitable countermeasures. In this paper, we review a generic model for the Smart Grid, and present possible attacks and countermeasures focusing on a key component of the Smart Grid: the Smart Meter.
The Logic of XACML
We study the international standard XACML 3.0 for describing security access control policy in a compositional way. Our main contribution is to derive a logic that precisely captures the idea behind the standard and to formally define the semantics of the policy combining algorithms of XACML. To guard against modelling artefacts we provide an alternative way of characterizing the policy combining algorithms and we formally prove the equivalence of these approaches. This allows us to pinpoint the shortcoming of previous approaches to formalization based either on Belnap logic or on D-algebra.
Projects:

Conflict Management in Aspect Policies

Department of Applied Mathematics and Computer Science
Period: 01/09/2010 → 21/09/2015
Number of participants: 6
PhD Student:
Ramlı, Carroline Dewi Puspa Kencana (Intern)
Supervisor:
Nielsen, Flemming (Intern)
Main Supervisor:
Nielsen, Hanne Riis (Intern)
Examiner:
Probst, Christian W. (Intern)
Kammüller, Florian (Ekstern)
Karjoth, Günter (Ekstern)

Financing sources
Source: Internal funding (public)
Name of research programme: 1/3 FUU, 1/3 inst 1/3 Andet
Project: PhD