Development of Digital Access-control Rules is a Two-step Process

# Summary

Creating digital access-control policies in the form of XACML rule-sets has generally be treated as a single-step process. It is better understood as a two-step process: first, creation of a formal representation of text or other natural-language policy source documents; and second, identifying specific user and resource attributes (and values) that are deemed to satisfy the formal policy requirements.

The two steps require different types of analysis. Especially in a multi-enterprise environment, the scope of applicability of the results will be different, and the actors involved in the analysis and in approval of the results will be different.

An operational concept of the two steps and how they are connected is needed, and almost certainly separate tools will be needed to effectively support the two analyses and to flow the output of step 1 into the step 2 analysis.

The potential benefits of this approach are to strengthen confidence in consistent and demonstrable enforcement of the source policies, both for oversight entities and information-sharing partners; and to permit re-use of digital (step 1) policies across the full scope (an industry, a political unit) of the applicable source policies. A less tangible benefit would be to sharpen the focus on cases where the “fit” between policy and available attribute data was weak, and therefore represented increased risk.

# Discussion

XACML policies link data about requestors (users) and data about protected resources (data tags or resource attributes.) The policies refer to specific facts that can be obtained about users, and specific metadata tags that have been determined by resource owners (or custodians) and bound to the protected resource. [Not all XACML policies are written to take into account data tags. Most, perhaps, connect user attributes to a decision to access a specific URL or other resource that is “opaque” in the sense that its access-relevant characteristics are not required to be apparent (from its name) and do not figure explicitly into the determination of the access decision.]

Meanwhile, non-digital policies themselves are most often expressed in terms of concepts, and not specific data facts. In some cases, there is an obvious way to translate the policy into a digital (XACML) policy referencing specific data that can be obtained. For example, if the policy is “alcoholic beverages may not be sold to persons under 21 years of age”, then it would be obviously reasonable to use the birth data on a drivers license to establish compliance and make a “permit” decision. In many cases the mapping between a policy concept and specific data that corresponds to the concept is far from clear. For example: Consider: “break glass only in case of emergency.” What data can be used as evidence of the existence of an “emergency.” Or: “automobile can be searched only if there is probably cause to believe it has been involved in a crime.” Or, “this information can only be accessed by those with a ‘need to know’.” These examples would require some creativity to model in terms of data attributes that actually exist and could be gathered for use in an XACML policy, but they are important real-world use cases.

Some sort of policy authority would have to approve the use of any real—world data that might be used as a proxy for concepts like “need to know” in enforcing information access policy via an IAM system. Even for straightforward mappings between concept and data, questions of what data is acceptable will arise: is the source authoritative? Is the data current and accurate? This a risk decision: “if we provide access to this information based on these data and something bad happens can we show that our reliance was reasonable?”

How can this concept-to-data mapping and approval process be managed better, especially between organizations? After all, a very important promise of ABAC is that it will facilitate sharing sensitive data with partner organizations and customers. At the very least, this means that attributes provisioned to users of one organization must be those required by a partner’s policy-to-data mapping results. At scale, this sort of coordination will be difficult and prohibitively costly if the specific user attribute data requirements of different resource owners is too diverse.

There have been some efforts to standardize user authorization attributes,[[1]](#footnote-1) but very little progress in standardizing and federating digital access-control policies. Even within single enterprises progress has been slow. Although it’s easy to get general agreement that policies should dictate what attributes are required for an access decision, in fact the usual approach has been to use whatever user attributes happen to be handy—things like groups already maintained in the directory, or even domain names (.mil proxying for DOD affiliation.) The relationship between these data and policy rules is often considered “common-sense” and therefore not a priority to make explicit or to implement in an XACML PDP. This avoids the necessity to discover (or write down for the first time!) actual documented policies. It also gets around the inconvenient unavailability of attribute data that might best fit the policy concepts in an actual statute or regulation. Relying on user attributes without explicitly specifying how they relate to an authoritative policy is a bad habit that can lead to a variety of bad consequences. On the other hand these approaches may be inevitable as the “crawl” phase of implementing ABAC. To avoid being stuck in “crawl” until everyone forgets that that isn’t the desired end-state we need to keep focus on the idea that policies should determine useful attributes and not that convenient availability of attributes should constrain policies. To get to “run” we need to get policy creation out in front of attribute selection.

How would separation of the process of developing digital rule sets into two steps work, and how would that help? First, it would recognize that two sets of decisions are needed—decisions on policy, and then decisions on evidence of conformance to the policies. For each, what kinds of activities are involved, what knowledge and authority is required, and who in an organization is best to perform the activities? Given answers to those questions, what kinds of tools would best support the activities?

Making concept-level policy.—Policy requirements come from different sources and have different scopes. One expert [KW] emphasizes a hierarchy of policy sources, starting (in the United States, with the Constitution, then Federal (and State) law, then regulation. We might add to that private contracts and agreements enforceable in the courts; and also case law that provides clarifies or interprets legally enforceable policies. Below that there may be enterprise or business unit policies.

Historically, it has often been assumed that authorization is intrinsically local. That is, only the resource owner knows what access rules should apply (because they are unique to that resource. However, that assumption is questionable. In fact, many of the policies that should be applied for access to a resource are widely applicable: regulations on privacy, fiscal accountability, trade secrets, national security, etc. Moreover, a resource owner may not be particularly well placed in the organization to keep track of them all. Some research indicates [KW & PH for DHS] that local information-resource administrators—the ones who issue application access accounts—are often unable to articulate what policies they apply or how their access decisions related to any valid enterprise policy.[[2]](#footnote-2)

What are the implications if most access policies are not (or at least should not be) “local”? A very important positive implication flows from the observation that the scope of a policy is related to the potential for reuse of the digital policy sets and user attribute data required for attribute-based access control. The Health Insurance Portability and Accountability Act (HIPPA) applies to tens or hundreds of thousands of organizations. A digital representation of HIPPA could also be used by all of these as the starting point for the process of enforcing digital access policy.

Creating a digital representation of a statute or regulation at the concept level is in important ways both simpler and less contentious than creating an XACML rule-set that implements it. It is simpler because it only requires disambiguation of the natural-language version of the source policy document; it does not require the additional step of matching the nouns and verbs of the policy to real-world data elements. It is less contentious because that matching process involves judgments about the appropriateness of the match, and those judgements are in effect risk decisions.

Because the disambiguation of natural-language policies is simpler and less contentious, it seems feasible that a digital representation of a statute or regulation could be developed and widely accepted across the organizations within the scope of the statute or regulation. One might hope to see a cooperative effort among affected organizations to develop an agreed digital representation of the regulation. Depending on the scope of the particular regulation, the effort might be a project of an industry association or perhaps a State Bar Association or the American Bar Association. Ideally, the issuing or enforcement authority of the regulation might undertake to produce an authoritative digital representation of the source document. Access control is not the only motivation for making a digital representation of a natural-language law or regulation—consider the work of the OASIS LegalRuleML TC.[[3]](#footnote-3) Thus access-control would be an additional, rather than the only, motivation for such projects.

Making executable digital rule sets.—

[to be continued]

1. Some “identity federations” have taken on the problem of attribute standardization. The National Identity Exchange Federation (NIEF) and the Transglobal Secure Collaboration Participation (TSCP) are examples. The US Federal Government’s FICAM program is also beginning to serve as a “federation” of Federal agencies, including an effort to standardize user authorization attributes. However, none of these has attempted to formalize the policy rules that are satisfied by the attribute sets the federations approve for use. [↑](#footnote-ref-1)
2. Another limitation of current practice is reliance on resource administrators maintain the databse of authorized users. But just as some or most of the users of a resource are very often not “local” – not in the same business unit, or even company, or even geo/political jurisdiction – a local resource administrator has no practical way to determine initially that users have appropriate access attributes, much less to keep current on changes. [↑](#footnote-ref-2)
3. The LegalRuleML TC aims to produce a rule interchange language for the legal domain. This will enable modelling and reasoning such that implementers can structure, evaluate, and compare legal arguments constructed using the rule representation tools provided. [↑](#footnote-ref-3)