XACML - Questions
March 17, 2005

Dennis Kafura

The XACML Model

Communication

1. How do PDPs and PEPs communicate, is there a standard way to do this, or is it left to the implementation stage to make the decision? (Muhammad Abu-Saqer)

2. The papers talk frequently about how a decision request goes from the PEP to the PDP. Does this imply the pull model of authorization is intrinsic to XACML? (Glenn Fink)

Attributes/Roles

3. The specification states that the term "attribute" is used in place of "group" and "role". Does this mean that XACML has sufficient power to implement a PDP for a full RBAC system? (Glenn Fink)

4. In the XACML paper, the PEP forms a request based on the requester's attribute, the resource in question, the action and other information pertaining to the requester. Is it also possible that the PEP form the request based on user's role, so that it can be used together with RBAC? (Haiyan Cheng)

5. XACML mainly deals with attribute, does that mean XACML is more appropriate to use with attribute based access control than role base access control? Is the find-grained attribute access control works better with XACML? (Haiyan Cheng)

6. How are credentials/attributes presented to the PEP? Does the PEP keep track of all of a user's attributes and provide an authentication service? If this is not the case, then would it be practical to describe a per-user/per-role/per-group access policy in XACML? It seems like such a system of any realistic size would be extremely verbose and difficult to manage. (Lee Smith)

Applicability

7. Is it up to the PEP to figure out what to do with "Not-Applicable" and "Indeterminate" results from the PDP? The specification weakly indicates that these return values should result in denial. (Glenn Fink)

8. Is any further explanation given in the XACML response of Indeterminate about the missing information? Or would returning information about missing values be a security risk? (Corban Rivera)

9. Under what conditions is XACML not appropriate for making access decisions? (Ranjit Randhawa)

10. Is there an problem combining access control and privacy? I would have thought these should be kept separate for security reasons. (Ranjit Randhawa)

The XACML Language

Constructs/Elements

11. I'm not sure I understand why we need the bags concept. They seem to be a waste of resources, since they don't enforce uniqueness in values. What is the advantage of the bag holding duplicates? Why is it a requirement that there needs to be a method for dealing with multi-valued attributes? (Darrell Hyatt)

12. Are XACML functions used in policy evaluation guaranteed to terminate? If not, what would be the effects from the subject user's perspective if an access request did not complete? (Glenn Fink)

13. Can types of attributed be customized? Or it has to be one of the standardized attribute names: Subject, Resource, Action, and Environment.(Haiyan Cheng)

14. What is the XPath query? (Muhammad Abu-Saqer)

15. An example namespace given in the paper is of the form *urn:oasis:names:tc:xacml:1.0:function:string-equal*, why is such a long identifier necessary to describe a function? (Corban Rivera)

Ponder/Java

16. XACML is a "standard policy language and access control decision request/response language." This is similar to Ponder, as it is simply a language and not bound to any implementation. Many of our (the class)'s criticisms of Ponder can therefore be applied to XACML. In particular, Ponder provided a language that is almost too extensible and too powerful for anyone to adopt in a real project. Do these same criticisms apply for XACML, or do you (the class) feel that this language is within the scope of a practical implementation on a real world system? (Craig Bergstrom)

17. Since XACML implementation is built in Java, why or why not XACML don't use or may inherit some of Java properties like inheritance and polymorphism? (Muhammad Abu-Saqer)

18. Can entities like Ponder's refrain and obligation policies be implemented in an XACML system? Does XACML have a different place in the authorization "protocol stack?" (Glenn Fink)

19. Ponder being based on object oriented principles had a very simple way of combining policies and rules in using the principle of inheritance and we had filters for the similar policies. In case of XACML does the Deny-overrides, permit-overrides, first-applicable, only-one-applicable policy generate similar results. (Bharath Ramesh)

Using XACML

Application Considerations

20. Are policies and policy sets stored in LDAP? (Haiyan Cheng)

21. What is an appropriate way to index policy so that the PDP can retrieve the proper policy with minimum time. (Haiyan Cheng)

22. XACML relies heavily on remote functions for things as simple as disjunction and string comparison. Does this make it inappropriate for real-time uses like firewalls, or does some heuristic like caching ameliorate this? (Glenn Fink)

23. In the paper, it says that there're seven standard Combining Algorithms. How to properly choose the algorithm to best reflect the requirement of the access control and how to compare and evaluate each algorithms~~?~~ (Haiyan Cheng)

24. In the paper "different people or groups can manage sub-pieces of policies as appropriate, and XACML knows how to correctly combine the results from these different policies into one decision" What is the XACML uses to achieve consistency between different sub-pieces of policies wrote it by different people? (Muhammad Abu-Saqer)

25. What are the impact of XACML on the speed of development, scalability, portability and other feature how it actually achieves it; some social factors as well such as increased usability in terms of users, developers, administrators, managers and all the user groups? (Muhammad Abu-Saqer)

Relationship to other Systems/Languages

26. Could a similar language developed for WS-Policy ? (Muhammad Abu-Saqer)

27. How XACML Policy work with SAML Request Conditions? (Muhammad Abu-Saqer)

28. Shibboleth is a decentralized middleware security system; one of the potential uses of XACML is distributed environment. The question is how XACML can be use in Shibboleth to achieve a flexible access control and in the same time guarantee the user privacy? (Muhammad Abu-Saqer)

29. Could XACML be used to replace the use of Shibboleth use of Apache's htaccess files (since they are vulnerable and sometimes could not be shared)during the process that the resource site contacts the subject site to request attribute values needed by the policy system.

30. What is the future of XACML? (Muhammad Abu-Saqer)

Standard

31. I understand why XACML was based on XML, but isn't this also to ensure that more people will end up using it compared to another policy language that might be more powerful but needs additional overhead to learn? (Ranjit Randhawa)

32. Comment: XACML claims to be superior because it reuses XML rather than defining a whole new language. I believe this is misleading because while the syntax is XML, the grammar and semantics are completely new. From a human standpoint, XACML is about as hard to learn as Ponder, etc. (Glenn Fink)

33. The introduction to XACML makes the claim that "It [XACML]'s standard". Do they mean that this standard has been widely adopted or simply that it is defined in some standard specification? (Craig Bergstrom)

34. As XACML is now a standard, is there other work going on on policy languages? I read that IBM tried to make EPAL a standard, the problem was that XACML was already a standard. (Ranjit Randhawa)

Tools

35. Currently, are there tools available for working with XACML like debugging policies, visualizing policies etc? (Muhammad Abu-Saqer)

36. How a programming languages like Java could be used in XACML? (Muhammad Abu-Saqer)