Privately owned objects

The security script examples given in the Fedora download omit one particular instance that was important to us at the University of Hull; that of a 'privately owned' object. In other words, we wanted a class of objects that was accessible only to their creator and to Fedora administrators.

At first sight, this may seem a simple requirement. We surmised that we should assign them an arbitrary content model of 'User' (a pseudo-model that did not imply a particular internal structure), and for all such objects compare the ownerId property with the user's loginId.

The first 'problem' is that, although it seems to be visible in a number of places, eg the search tool, Fedora (as at 2.1.1) does not actually support the ownerId property. Temporarily we have 'fudged' this for testing purposes by assigning the user's ID to the content model property.

The second 'problem' was the actual comparison of the loginId and the ownerId (or temporarily, contentModel). Neither the Fedora team nor the OASIS documentation provides an example of comparing two variables; always the examples are a variable and a literal. We spent days trying to make this work and eventually posted a 'help!'*message_on_the_Fedora_User_list.*_I_am_indebted_to_Ryan_Scherle,*at_Indiana_University,for_identifying_the_problem.*_" Some_XACML_functions_require_that_you_guarantee_an_argument_is_a_single_value._Because_attributes_can_have_multiple_values, _many_functions_require_an_AttributeDesignator_to_be_wrapped_in_a_one-and-only_function."

The_resulting_rule_goes_like_this:

```
__<Rule_RuleId="1"_Effect="Deny">
____<Condition_FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">
______<Apply_FunctionId="urn:oasis:names:tc:xacml:1.0:function:or">
________<!- Compare object model with loginID (really needs to compare owner) ->
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
<ResourceAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string" AttributeId="urn:fedora:names:fedora:2.1:resource:object:
contentModel"/>
</Apply>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-one-and-only">
<SubjectAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string" AttributeId="urn:fedora:names:fedora:2.1:subject:loginId"/>
</Apply>
</Apply>
<!- OR allow administrative access ->
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of">
<SubjectAttributeDesignator AttributeId="fedoraRole" MustBePresent="false" DataType="http://www.w3.org/2001/XMLSchema#string" />
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">administrator</AttributeValue>
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">fedoraInternalCall-1</AttributeValue>
</Apply>
</Apply>
</Apply>
</Condition>
</Rule>
```

We have requested that the Fedora development team consider implementing, or allowing, an object ownerId property of some sort as soon as possible.

--Richard green 04:08, 25 April 2006 (EDT)