Porter, Rachel

From: James Sellwood <james.sellwood.2010@live.rhul.ac.uk>
Sent: Thursday, February 16, 2017 11:34 AM
To: comments@standards.incits.org
Cc: Porter, Rachel
Subject: Public Review Comments - INCITS 499-201x

To whom it may concern,

I include below comments on "INCITS 499-201x (revision of INCITS 499-2013), Information technology - Next Generation Access Control - Functional Architecture (NGAC-FA)" as part of the public review identified on https://standards.incits.org/apps/group_public/document.php?document_id=83778.

Your faithfully,

James Sellwood

---- Comment Convention ----

To clarify these comments, where a list occurs in a section I have considered that list to be the last part of the paragraph which precedes it.

---- General Comments ----

Role based access control sometimes has each word capitalised and sometimes does not. In some cases there is a hyphen between 'role' and 'based', and other times there is not. Similarly, multi-level security sometimes has each word capitalised and sometimes not.

---- Specific Comments ----

The second sentence of paragraph three in Section 6.2.2.4 (Objects) is incorrect. It looks as though text was removed between ', such as' and 'and references' but the sentence wasn't corrected. I suggest that either the sentence should be corrected to be comparable (but not
identical) to the last sentence of Section 6.2.2.3 (Processes), or the missing text should be inserted.

The second sentence of paragraph four in Section 6.2.4.2 (Assignment) has an end quote character at the start of the quotation "contained by".
This should be a start quote character.

The first sentence of paragraph five in Section 6.2.4.2 (Assignment) is grammatically incorrect and is missing the word 'a' before "container".
It should either be:
Assignments of type (c) in the above list show that an object attribute may be viewed as a "container" of objects.
or:
An assignment of type (c) in the above list shows that an object attribute may be viewed as a "container" of objects.

The last sentence of paragraph five in Section 6.2.4.4 (Prohibition) is ambiguous. It is unclear if it should be read:
Similarly, the exclusive attribute set delineates policy elements that are not ascendants of the attributes in the set and, therefore, are not subject to the prohibition.
or:
Similarly, the exclusive attribute set delineates policy elements that are not ascendants of the attributes in the set and that are subject to the prohibition.

Item b in the third paragraph in Section 6.2.4.5 (Restriction) has an unnecessary semi-colon at the end. Item c in the same list has an unnecessary semi-colon at the end of the third line.

Item b in the fifth paragraph in Section 6.2.4.5 (Restriction) has an unnecessary semi-colon at the end.

Item b in the seventh paragraph in Section 6.2.4.5 (Restriction) has an unnecessary semi-colon at the end.

It is unclear from Section 6.2.4.6 (Obligation) whether the changes made to a PIP's policy information are permanent or transient. Whilst the MLS example in C.3.3 seems to suggest they are transient, there is nothing in the standard which indicates that these changes are reverted, or when and how this occurs.

Paragraph 3 of Section 6.3.2 (Protocols and API Definitions) identifies subsidiary functionality as potentially being required when a protocol is employed but not an API. As such, it seems to suggest that APIs are always trusted, local interfaces whilst protocols are not. Whilst I appreciate the distinction that is trying to be made, it is not commonly the case. Web APIs, for example, are called remotely and usually require the use of similar subsidiary functionality as those listed. I suggest the inclusion of clear definitions of API and protocol to avoid the suggestion that remote APIs are inherently 'safe' in comparison to protocols.

Figure C.2 (Example diagram conventions) indicates the dashed line connecting 'UserAtt3' and 'SAM' is an assignment. This dashed connecting line style is not described above the figure with the other styles. It is not the styling which is identified as being used for an assignment.

The second sentence of paragraph two in Section C.3.1 (Step 6) incorrectly identifies the acronym MLS as 'Multiple Level Security', although elsewhere in the document this is correctly referred to as 'multi-level security' (see above regarding casing inconsistencies). The last sentence of that paragraph has 'associate with his aide' when it should be 'associated with his aide'.

Given the information provided it is unclear that the obligations added in Section C.3.3 (Step 8) are sufficient to support the *-property. They are only sufficient if the PEP's control over object interactions is strict and associated with small atomic operations. Otherwise, a user could submit a request to write to a low classification document (which doesn't trigger any obligations), begin editing the low classification document, submit a request to read from a high classification document (which does trigger an obligation, but the write access is already granted), edit the low classification document to introduce high classification material, close the high classification document, and then close the low classification document.

--

James Sellwood