From: Karp, Alan H
To: Comments
Subject: NGAC GOADS Out for Public Review
Date: Monday, June 09, 2014 10:40:04 AM

As you'll see from my comments, I did not study the entire document carefully. In particular, I did not read anything on prohibitions or administrative operations. Based on my previous reviews, I don't have anything substantive to say about them. Also, I only skimmed the Appendices.

I have only two substantive comments, and they are related to item (a) on the page numbered 14.

It appears that capabilities are associated with users rather than processes because the rule refers to Process_User(p). That rule is a violation of the Principle of Least Privilege (LP) and the root cause of many of the problems we currently have with viruses. In effect, it says that every process has all the access rights of the user. One of the strengths of using capabilities is that we can avoid this weakness by giving each process the user starts only the capabilities the process needs to do the job the user wants done. I am prepared to go into great detail on this point if there is interest.

The statement "there exists a privilege" indicates that there is no way to attach a specific privilege to a specific object, which can lead to a confused deputy vulnerability. In particular, a process with privileges p1 and p2 on some object o may wish to denote that a particular operation op is to be carried out with only p1. The "there exists a privilege" rule appears to make this feature unimplementable. Capabilities, in the sense of Dennis and van Horn, provide this functionality by combining designation with authorization. Objects are denoted by the capability, which is independent of the policy. Hence, the process can denote which privileges are available for op by denoting o with a capability authorizing only p1. The policy is used to determine which capabilities are granted to which users, and users enforce LP at finer granularity by giving processes only the privileges the processes need.

Minor points

Page 1: A point I made in previous comments is that RBAC is a policy, not a mechanism. It relies on mechanisms, such as ACLs, to enforce the policy.

Page 1: I can parse "several types of policy policies" but is that what is intended?

Page 14: I think the term "Authorization_Decision" is imprecise. I am making an authorization decision when I add an entry to an ACL. I think a more precise term is "Access_Decision" because we are deciding whether or not to honor the request.

Page 30: "when one of more administrative actions" should read "when one or more administrative actions"

_____
Alan Karp
Principal Scientist
Enterprise Services, Office of the CTO
Hewlett-Packard Company
1501 Page Mill Road
Palo Alto, CA 94304
(650) 857-3967, fax (650) 857-7029
http://www.hpl.hp.com/personal/Alan_Karp