RBAC does not replace DAC

Contributed by Michael Felt

No Looking Back:
Role Based Access Controls
RBAC is a mechanism for Access Control and that is the key to what is wrong

with most implementations using RBAC as an access control. Huh? Isn't RBAC meant to be

the next greatest thing in Access Control? What goes?

Yes. RBAC is meant to be the next step in Access Control - but it's effect as THE controlling mechanism is minimal as long as DAC is still active. DAC?? Discretionary Access Control.

Discretionalry Access Control, also known as DAC, is the traditional access control mechanism for UNIX and Linix based systems (so also OS/X and deep down NT-based systems).
Actually, any access system where the owner of a "object" (file, device, directory, or any other names for "special" something) can modify the access permissions - at whim - is discretionary.

Focusing on UNIX/Linux based permissions there are 9 (nine) permission bits we need to

understand - actually - 3 sets of 3 bits - one each for read, write and execute (rwx). The three sets are referred to as "user", "group" and "other". Some call the "other" bits
by the name "world". In this discussion we shall use the term "other".

On UNIX an identity at any given time is: euid,set of group ids. Normally the euid == ruid
i.e. effective uid == real uid - where ruid is meant to be a login id.
Using DAC mechanisms the OS looks at the active identity (try the command id to see your current identity) and the object permission sets. If the "owner id" and euid match, then those bits determine the current access. If the owner IDs do not match then the system looks at the "group ID" of the object and compares that with the set of active group ids and if there is a match then the group ID permissions are used to determine access control. If neither "owner" nor "group" IDs have a match then the "other" IDs determine access to the object (e.g., file, directory, device).
This is where/why RBAC generally "fails". RBAC has been implemented as an additional access control mechanism - rather than as a replacement.

In other words, RBAC, by default,
is always looking back - providing access the way it has always been done. The behavior is as if the OS is always looking back - determining access based on DAC first, and RBAC as a second thought.

That is all for today - next article I shall discuss how DAC is used to setup selective access control - user DAC being whatever the owner wants for themself - and other access for everyone (non-selective) else. And I'll also explain the command

"find / -group X -exec chmod 0 {} \;"

fully enables RBAC for group .