Hi,

I work for GlusterFS and have done various projects on it. One such interesting project that I am currently working on is setting SELinux context over a fuse mount point. I am the sole developer of this component(under development) and since we have a lot of use cases based on this translator, I find this much more interesting. Currently, setting SELinux context over a FUSE mount point is not possible since (kernel)FUSE does not support it. There are three things that I will try to explain in the perspective of GlusterFS and SELinux and where we stand in accomplishing these tasks.

1) First thing is to make possible for SELinux to check sub-filesystems(fuse.glusterfs). At the moment, SELinux only can check if a filesystem supports SELinux based on the base filesystem. Since, by default FUSE does not support SELinux, sub-filesystems are not able do it as well. A Gluster mount identifies itself as "fuse.glusterfs"(<mainfs>.<subfs>).

Current status : An experimental patch for the kernel has been attached to https://bugzilla.redhat.com/1272868 . May be few improvements to the patch can make it work.

2) We can inform FUSE that the glusterfs sub-file system supports SELinux. Mount options can be passed on to the FUSE(kernel) when mounting takes place. Some options are user-space process specific and can get filtered out, whereas others are passed to FUSE. SELinux mount options are added in /sbin/mount.glusterfs and this is currently supported in GlusterFS. One can do mount -t glusterfs <HOSTNAME>:VOLNAME> -o context="<selinux context>" <mt pt> and pass(set) the SELinux context.

3) When FUSE(kernel) patch gets merged, we will be allowed(able) to set the context from the FUSE mount point which in turn will be reflected in the backend(bricks) as well. For Glusterfs bricks, we will have type as "glusterd_brick_t". Brick processes may only read/write contents in the brick directories that have type 'glusterd_brick_t' which will be enforced by SELinux policy. The client can do a chcon command(chcon <option> context <file>) and can change the security context or a Restorecon command. So, when a client sets/reads a 'security.selinux' extended attribute(simply through ls -Z) over a FUSE mount point, the brick process needs to convert the request to a 'trusted.glusterfs.selinux' xattr. In the brick side, security.selinux xattr is used by the SELinux to prevent unauthorized access to the contents in the brick directories.

How could this be done?

We are designing a SELinux translator on the server side which would convert security.selinux xattr to trusted.glusterfs.selinux. In the setxattr call this is done and we do the vice-versa for the getxattr call, thereby the user could also set his security contexts over the mount point and making brick process secure as well. This is partially implemented here[1] which handles getxattr and setxattr fops. Another thing to note here is that, the translator should also be able to inherit security context from it's parent whenever a new directory(or file) is created or linked. So,

we have to handle other fops like mknod, link, symlink, rename and a few more. We also have issues whenever an add-brick or remove-brick is done(we should take care to set right contexts in the brick directories). This is already handled in a patch which implements SELinux helper hook-scripts[2]. The translator will be enabled by default and there will be an volume set option to disable the translator. Also, by default if no context is set, it would take the default context assigned to it by SELinux. Where exactly should the translator be placed in the server side(Below Marker in the server stack).

[1] http://review.gluster.org/#/c/13762/

[2] http://review.gluster.org/#/c/6630/

Since this project involves developing a whole new translator, it involves communicating with lot of other translators and it is adding a new support to GlusterFS. I find this work of mine as more interesting. My other contributions to GlusterFS can be looked here[3].

[3] http://review.gluster.org/#/q/owner:mselvaga%2540redhat.com

Thanks for reading, please do contact me if you are interested or if you need any clarifications and would like to contribute :-)

--
Thanks & Regards,
Manikandan.
(manikandancs333@gmail.com)
(+91-8098253485)