

# Re: Linux security

---

*Source:* <http://linux.derkeiler.com/Mailing-Lists/Ubuntu/2006-05/msg00028.html>

---

- *From:* Alan McKinnon <[alan@xxxxxxxxxxxxxxxxxxxxxx](mailto:alan@xxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Sun, 30 Apr 2006 23:24:47 +0200
- 

On Sunday 30 April 2006 02:54, Michael T. Richter wrote:

On Sat, 2006-29-04 at 21:29 +0200, Alan McKinnon wrote:

Another bolding. I just downloaded the acl utilities from universe. Where's the "write-append" access? Even with the acl extensions in place you still can't match the functionality that is in Windows NT-based systems out of the box.

Why do you want that fine level of control? I've yet to see a valid case where such fine control on a file system is truly indicated.

I have a log file, say, that a cluster of applications writes to as an audit trail. I want only those applications to access it. (SELinux provides me with that level of control.) And I want those applications to be able to write to the end of the log file, but not be able to read the file nor alter any contents once written.

You can hack a solution around that, but any such solution is just that: a hack.

Hmmmm, you have a point. I missed that one.

Historically the solution would be to have 600 permissions on those files, owned by root and root makes damn sure that syslog does what he wants it to do. A valid case can be made that current-day systems have outgrown this usage pattern.

I see what you are getting at – being able to allow/disallow specific actions on file by file basis. But keep in mind that each new combination of facility/control doubles the number of settings, and this very quickly gets out of hand and becomes a maintenance headache. Witness the number of Windows boxen where

## Re: Linux security

the user runs as an admin just to get their work done. Yes I know there are ways to avoid this, but how many people really do it? Reading between the lines I suspect you do, but that'll make you one of a very few that I know of to have made that claim.

I find the sudden backpedal amusing. (Not you, but of the community as a whole.) Not that many messages ago it was all braggadocio about how "Linux offers finer-grained control over security" and now it's suddenly "why would you want that fine a level of control over security?"

Let's face it – security is hard. Really, really, fscking, OMG how many things to I have to track? \*hard\*. I've thought up a bunch of conceptual security ideas in my time, but quickly realized each one would create a huge admin burden.

I can cope nicely with the ideas behind say TCP wrappers: fine grained control over who can connect to what port. But there are usually less than 10 incoming ports I'm interested in, and less than 10 hosts in total across all those ports. So I can block access to sshd for all, except two specific hosts. I can keep this info in my head, and once I set it up it stays static – I don't create new port-opening apps several times a day.

In contrast, a file system is a different beast altogether. 'find / -print | wc -l' on this box returns over a million files. There's no way I can track fine-grained control over this lot, so I trust the packagers to do something sensible. I can't even keep the ownerships and permissions on /mnt/share straight (that's a shared partition where I keep data to be shared across several users and OSes).

I believe in the right tool for the right job, but there comes a point where complexity out-weighs usefulness. For me, network apps are under that bar, and filesystems (all of them) are way over it. Databases ride the fence depending on what goes in them.

This cuts to the heart of the whole anti-Windows crowd's problem: they don't actually know the platform they're criticising. I hear claims made here on this mailing list alone which are absolutely, stunningly breathtaking in their sheer ignorance. Usually from the same people who shout "FUD!" at the top of their lungs whenever anybody says anything negative about Linux, ironically enough.

That's not an Ubuntu trait, it's a human one.

A large chunk of this list's users seem to be the under-25 crowd, with heaps of idealism and not much experience. Think back to when you

Re: Linux security

were that age. I just did, and you have no idea how thankful I am that Google wasn't around when I was 25...

If you think this list is bad, try listen to the Ferrari/Mclaren/Williams/Renault/Toyota fanboys on Sunday afternoons :-)

Here's my gentle proposal to people (and not you, I stress Alan -- you seem to know enough about the Windows platform to have an informed opinion): learn what you're critiquing so that those of us who actually do know it can't throw your absolutely staggering ignorance back in your face with a sardonic laugh.

Hmmm, you might want to tone down the harshness there just a wee bit :-) Those same young fanboys would benefit more from a patient explanation than from a flame, even though they will task your patience to the limit.

Very fine grained control is very useful in a database for example, where the data domain being stored is narrowly defined. But in something as generic as a file system I don't see it being used much outside of very specialized needs. And just because something can be done doesn't mean it should be done.

A file system is essentially a hierarchical database. ;)

or like a hierarchical database where the only data type is a BLOB?

:-)

But yes, just because something can be done doesn't mean it should be. This is why I've used the ultra-fine grained security under Windows NT about five times in twelve years of working with it.

Which raises some harsh horrible questions:

Is yours a typical case? And if so, is it really worth the effort to maintain it?

I can only imagine the code that implements that control, and the amount of QA and testing that has to be done on it. I'd contend that it's only because it's a security feature that that module even still exists in the code base.

## Re: Linux security

(Incidentally this ultra-fine grained security isn't just on files. Another area where Windows NT as a platform is way ahead of stock Linux, with or without fsattr and fsacl utils. I can put that security on sockets, named pipes, synchronisation primitives, etc. — anything with a HANDLE type attached to it.)

Interesting, I didn't know that

But the advisability of it wasn't my point. My point was that total ignoramuses were talking shit about how the UNIX security model is finer-grained than that available under Windows.

I think the fine-grained aspect makes for a (mostly) specious argument. All modern OSes give a reasonable level of control within their design specs. The question is how well is the chosen security model implemented? Amazing fine grained control is worthless if it can be easily subverted. This is far easier to do on Windows than on \*nix. Or put another way, the admin has to work his nuts off on Windows to prevent it, but root can do it with relative ease.

Additionally, the Windows and \*nix security models are fundamentally different – Windows security is largely userID-based and \*nix is traditionally host-based. There is overlap and lately they are converging but at heart a comparison isn't much use. Better to look at infection rates per 1000 machines across the industry and see which culture lends itself to creating secure systems. Currently it looks like \*nix wins this duel, maybe because the admins tend to be individually better informed.

If you want write-append access, ext2 implements an append-only attribute.

Ooh! Now that is interesting. I really do miss write-append. How do I go about using it? (And does Reiser support it since most of my partitions are reiserfs, not ext3fs?)

chattr and lsattr will do it for ext2/3.

AFAIK reiserfs has no equivalent but does do the acl/security label thing. I don't use it myself (see complexity above). I see great promise in reiser4 with arbitrary attributes per node. Maybe, finally we'll have a file system somewhere that can have security that JustWorks.

Re: Linux security

Re: Linux security

There's always WinFS, but given the track record so far on that my money's on Hans

--

If only you and dead people understand hex,  
how many people understand hex?

Alan McKinnon

alan at linuxholdings dot co dot za

+27 82, double three seven, one nine three five

--

ubuntu-users mailing list

ubuntu-users@xxxxxxxxxxxxxxxxxxxx

<https://lists.ubuntu.com/mailman/listinfo/ubuntu-users>