

Re: sudo without password

Source: <http://linux.derkeiler.com/Mailing-Lists/Ubuntu/2006-06/msg01496.html>

- *From:* ubuntu@xxxxxx
 - *Date:* Fri, 09 Jun 2006 10:53:56 -0400
-

Luis wrote:

Just wanted to say that I agree with this post. Software is meant to evolve just like everything else.

There is no way a human being can anticipate all possible outcomes for a problem. The people who did the original specs for UNIX were just that, humans. And as such, they did a very good job at designing a system that survived for 30 or so years!

Now is time for us, the new generation that actually use this system, to improve it and come out with equally visionary (and clever) ways to improve the system overall. Security, performance, ease of use being top of the list in my own mental goals -- and roughly in that order.

Then again, this is simply an opinion. Nothing else.

p.s. I use "human" for two obvious reasons. This is the Ubuntu's way of letting us know that we are part of a larger group as well as the niche of engineers who develop software. And, that only machines are meant to formulate answers to existing problems in a linear way. Humans tend to be more holistic about things.

As I recall, UNIX specifically chose it's current security model because the more secure ones (like access lists) required far more time and effort, and therefore are more likely to have holes left by the operators.

It's the human component, as you say. If your security model is too much of a pain in the rear to set up and maintain, it will fall apart. Quite often, the simpler the solution, the more secure it will be in the long run.

The threats these days, are quite different from age past. Originally, the worry was all these users with shell accounts on your system. These days, nobody just gives out shell accounts to critical servers, unless those people are specifically administering them.

Re: sudo without password

I just first tried Ubuntu for the first time with the release of Dapper, and I was rather surprised it did not install a host–firewall by default. I understand Ubuntu's take of "we don't install anything that listens", but that quickly falls apart when the user starts installing things like NFS that require portmap, for instance.

Ubuntu seems to be taking the Debian approach of "We're doing things minimally, so if you install something insecure, it's your own damn fault." As a distro targeted at desktops, I'd like to see Ubuntu be a bit more forward–looking. A veteran sysadmin has no problem with the Debian way, but a novice desktop user probably does. And a novice will install those security problematic packages. One of window's major problems is users installing every silly program, widget, screensaver, or other stupidity that they run across on–line, each of which installs another piece of adware, spyware, or trojan. Eventually, the system simply becomes unusable. Just because the user is now trying out linux doesn't mean they've kicked that habit.

As an aside, another interesting notion, I think, was released with SuSE 10.1: AppArmor. The idea is to restrict programs, rather than users. Effectively, you create access lists of what a particular program is allowed to access. Much the same deal as chroot, but with far less hassle. (Since you don't actually have to copy it all into a single path)

The trick is to maintain effective security without it becoming too much of a burden. The human component is the biggest factor.

—

ubuntu–users mailing list

ubuntu–users@xxxxxxxxxxxxxxxxxx

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