SUDO for AIX - and NOEXEC

Contributed by Michael Felt

I am not a big user of sudo, but I frequently visit customers who are. One issue came up re: why they also installed the program "less" rather than use the AIX default "more".

The issue here is the escape in "more" to open a file with /usr/bin/vi - and then do a shell escape as an elevated user. TA-ta-TA-dah become root with an open shell.

So, my question was - why use "less"? How does this help with NOEXEC?

The answer was simply - less does less (pun) - no built-in shell escape - since the AIX sudo they used did not "honor" the NOEXEC keyword in the sudoers config file they could not use /usr/bin/more and installed and use the program less.

The real issue

The real issue is not whether to use "more" or "less", but to have the ability to use the sudoers keyword NOEXEC. While this is known to work on AIX 5.3 and later the version they had installed did not take advantage of this support.

Whether NOEXEC is supported, or not, comes down to how sudo is packaged (what options are passed to configure) and also how a command such as libtool is set to create a shared library (as a .so file or as a shared object member in an .a archive file.

The current setup is to create a single .so file - and, sadly, my "defaults" for packaging AIXTOOLS - failed.

Tested and failed

I tested my latest (now previous) packaging of sudo (vrmf 1.8.19.20) and it failed. Not because it did not try, but because I had built it as a 64-bit application and the shared library sudo_noexec.so was 64-bit. AIX /usr/bin/more is 32-bit so there was no loadable library.

Resolved!

By repackaging it as 32-bit (http://download.aixtools.net/tools/aixtools.sudo.1.8.19.21.I) the problem was resolved. Now /usr/bin/more loads, but external programs do not load. More acts as if the command was successful and has exited back to more.

p.s.

To see the options I packaged sudo-1.8.19p2 with visit the aixtools wiki page for [sudo] .