

Re: Problems with scp and cron

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-10/0154.html>

From: Simon Tatham (anakin_at_pobox.com)

Date: 10/21/04

Date: 21 Oct 2004 17:34:36 +0100 (BST)

Darren Dunham <ddunham@redwood.taos.com> wrote:

> *Surely that depends on having the settings actually there. I often use*
> *passphraseless keys for automated jobs on machines. They must run even*
> *if the machine has rebooted and I haven't logged into the box to type a*
> *passphrase.*

Quite so. Messing around with long-running ssh-agents just doesn't seem worth it for the trivial security improvement of being safe against someone stealing the machine; for a colocated machine that isn't the likely threat compared to network-based attacks. And a network-based attack gaining access to your account could read decrypted keys out of ssh-agent without much more difficulty than it could read unencrypted ones off disk.

To make my automated jobs secure, I give each one a dedicated SSH key which is heavily restricted at the server end. So if, say, somebody compromises the account which updates a particular set of files in another machine's web space, they only get the ability to update that particular set of files, and don't get full access to my account on the other machine. (Unless, of course, the script I run at the far end has a security hole in it. But that's a risk you take no matter what you do.)

--

Simon Tatham "Imagine what the world would be like if
<anakin@pobox.com> there were no hypothetical situations..."