

OT: security of make as authorized_keys command

Source: <http://linux.derkeiler.com/Mailing-Lists/Fedora/2007-12/msg04281.html>

- *From:* "Dave Burns" <tburns@xxxxxxxxxx>
 - *Date:* Sun, 30 Dec 2007 15:19:47 -1000
-

I should probably ask this on an ssh oriented list, but I thought I'd try my luck here first.

I want to do some remote commands securely. I put a key in my `.ssh/authorized_keys` file like so:

```
command="/usr/bin/make $$SSH_ORIGINAL_COMMAND" ssh-rsa AAAAB3NzaC1[etc.etc.]
```

so I can invoke make targets like so:

```
ssh username@host target
```

Assuming the bad guys never get my key, I am fine, even though it is passwordless.

What if a bad guy does get my key? Then I see three possible problems:

- 1) somehow use make's `-F` switch in ssh command to change Makefiles?
- 2) stack overflow of make or ssh?
- 3) Somehow put extra command after make target using `';` or something?

And obviously the bad guy can invoke any of the targets in my makefile, but I've made them pretty innocuous.

So, should I seriously worry about any of these potential problems? Any other holes I haven't thought of?

The motivation for all this is some cron jobs I want to run, obviously calls for a passwordless ssh key, but I want to put some limits on it.

Thanks,
Dave

—

fedora-list mailing list

fedora-list@xxxxxxxxxx

To unsubscribe: <https://www.redhat.com/mailman/listinfo/fedora-list>