

Re: What can a hacker do with a user private key?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-11/0132.html>

From: Nico Kadel-Garcia (nkadel_at_comcast.net)

Date: 11/19/04

Date: Fri, 19 Nov 2004 09:20:27 -0500

"Richard Lefebvre" <[quasiAROBAS\(@\)videotronPOINT\(.\)ca](mailto:quasiAROBAS(@)videotronPOINT(.)ca)> wrote in message
news:fYmnd.58085\$De5.698715@wagner.videotron.net...

> Hi,

>

> To repeat the subject line, what can a hacker do with a user private key?

> I can try to control security on my computers, but there is nothing I can
> do about users home computer where they keep their private keys. Also is
> there a difference between openssh and ssh.com implementation in that
> regard.

>

> Note: I know it is not the right forum, but what about gnupg private
> key too?

This is a big problem in NFS environments, where user's tend to leave their private keys in their home directories and where lazy people tend to set up password-free keys rather than running an SSH-agent.

If you have someone's private key, you're a big step closer to having access to their account. If it's a password-free key, you have as much access as if you had recorded their private password and have access to every machine that allows key-based access. For a careless admin, this can include root access to the company servers. Leaving such a password free key is as bad as putting the user's password on a Post-It note on their monitor.

ssh.com's code and OpenSSH are identical in this regard.

PGP is similar in providing access to being able to encrypt or authenticate things as if you were that user. But people tend not to leave those without passwords, so it's usually not quite as easy to steal, and it doesn't provide the remote access possibilities that SSH keys do.