

Re: Agent security (was Re: Secure file transfer from unix to windows)

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-10/0367.html>

From: Neil W Rickert (rickert+nn_at_cs.niu.edu)

Date: 10/29/03

Date: Wed, 29 Oct 2003 13:08:57 GMT

gxy1997@yahoo.com.au (UnixFan) writes:

*> Jacob Nevins <jacobn@chiark.greenend.org.uk> wrote in message
news:<Jas*FIK5p@news.chiark.greenend.org.uk>...*

>> UnixFan <gxy1997@yahoo.com.au> writes:

*>> >ssh-agent does not give you adequate protection (one can use debugger
>> >to retrieve the unlocked private key from ssh-agent: it's not that
>> >difficult provided you know how to use debugger and understand C
>> >code),*

*>> I would have thought that if you're sharing a system with someone who
>> has sufficient privilege to do this, and you don't trust them, then
>> you're doomed in numerous other ways anyway. Is this not the case?*

*>When you don't trust people who can use root account on your system,
>you must not use file system permission as the only way to protect
>your keys. But in this situation, you also should not assume ssh-agent
>can provide you the required protection:*

Then you should also assume that there is a keyboard sniffer logging everything you type. If you cannot trust the machine, be cautious what you do with it.

*> IMO, ssh-agent is a wrong
>program which should not exist in security package like SSH:*

That's a bit severe. You should only use it on trusted machines such as your own single user machine. Likewise you should be cautious about agent forwarding to an untrusted machine.

But I think there isn't really much of a problem here. As best I can tell, very few people use ssh-agent. About the only public key authentications I see in logs are my own, and students doing a homework assignment that requires them to use public key authentication.