

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

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-10/0364.html>

From: UnixFan (gxy1997_at_yahoo.com.au)

Date: 10/29/03

Date: 29 Oct 2003 00:36:29 -0800

Simon Tatham <anakin@pobox.com> wrote in message news:<h8f*3345p@news.chiark.greenend.org.uk>...

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

> > *But in this situation, you also should not assume ssh-agent can
> > provide you the required protection: IMO, ssh-agent is a wrong
> > program which should not exist in security package like SSH: when
> > other programs handling secret keys are trying to shorten the period
> > of unprotected keys in memory, ssh-agent is attracting users to let
> > it to store the unlocked private key in memory for malicious person
> > to retrieve it.*

>

> *The point is, though, that greater and greater security is not
> always a desirable goal. If the greater security comes with greater
> inconvenience, then at some point its cost becomes worse than its
> benefit.*

>

> *Without ssh-agent, it would be very hard to get many people to use
> public keys at all: why would they be willing to type a huge
> passphrase at every login when they had previously been typing a
> short password instead? They would only do that if they _really_
> needed the additional security of PK authentication. (And perhaps
> some people really do; but certainly not everybody.)*

>

> *ssh-agent _can_ be a sensible tradeoff between security and
> convenience, depending on your threat model. For a laptop user in
> particular, it's an obviously sensible option; a major risk to
> laptop users is that their laptop might be stolen and the thief
> might power it up to see what they can find. So ssh-agent makes the
> decrypted private key conveniently accessible to the legitimate user
> of the machine, but if it's stolen while powered down then that key
> is nowhere on the hard disk for the thief to see. (Assuming it
> didn't get swapped out, of course; but encrypting any swap devices
> you've got is doable too.)*

>

> *If someone attacks your already-running machine and gets an
> arbitrary process to run as root or as your UID, then yes, they can
> read the decrypted keys out of your ssh-agent's memory. But once*

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

- > *they've got to that point, they could equally well have replaced*
- > *your ssh-add or your ssh client itself with a trojan which captured*
- > *your password or passphrase, or any number of similar attacks. By*
- > *the time the attacker has arbitrary code running on your system,*
- > *anything else you can throw in their way is basically minor*
- > *inconveniences, and you'd be far better off putting the same effort*
- > *into ensuring that that doesn't happen in the first place.*

Agree with you, ssh-agent does provide some benefits when you are the only user on the machine. But my point is when SSH provides very good value in security for protecting the communication link, many people would assume all programs in the package will give you very good security protection, but in the case of ssh-agent, it's not. As it's not difficult to use debugger to retrieve unlocked private key from ssh-agent, it's not worth the trouble to use ssh-agent to automate SFTP on a development machine.