

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

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-10/0342.html>

From: UnixFan (gxy1997_at_yahoo.com.au)

Date: 10/28/03

Date: 27 Oct 2003 23:20:24 -0800

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: 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.