

Re: Secure file transfer from unix to windows

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-10/0341.html>

From: UnixFan (gxy1997_at_yahoo.com.au)

Date: 10/28/03

Date: 27 Oct 2003 22:59:45 -0800

"Nico Kadel-Garcia" <nkadel@comcast.net> wrote in message
news:<weqdnS6na5Ia9wSiRVn-vQ@comcast.com>...
> "UnixFan" <gxy1997@yahoo.com.au> wrote in message
> news:268fc341.0310231659.182f94e2@posting.google.com...
>> "Nico Kadel-Garcia" <nkadel@comcast.net> wrote in message
> news:<rOidnTDSKfJIUAqiRVn-tg@comcast.com>...
>>> "UnixFan" <gxy1997@yahoo.com.au> wrote in message
>>>> news:268fc341.0310222220.64ec6024@posting.google.com...
>>>>>
>>>>> *We are using a commercial SFTP automation tool called AutoSFTP in our
>>>>> environment. There are other ways for SFTP automation, but if you need
>>>>> good security, AutoSFTP is the best I could find today, and this is
>>>>> the only SFTP automation solution that is allowed by our security and
>>>>> audit department.*
>>>>> *As you are working on a development machine, I would recommend you to
>>>>> use public key authentication and set a null passphrase for the
>>>>> private key.*
>>>>>
>>>>> *BAD-BAD-BAD IDEA! This is much like taping a password to your monitor.*
>>>>> *Unless you can heavily restrict what it has access to, such as using
>>>>> chroot*
>>>>> *cage and preventing shell access, then you are probably better off with
>>>>> a*
>>>>> *plain old FTP access.*
>>>>>
>>>>> *If you need to do this sort of thing, use "ssh-agent" to pre-load a
>>>>> passworded key for the use of the software in question without ever
>>>>> leaving*
>>>>> *an unlocked key around.*
>>>>>
>>>>> *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), and also you must rekey in the passphrase after each system
>>>>> reboot.*
>>>>>
>>>>> *Both are issues, true. But the difference in security between leaving an*

comp.security.ssh: Re: Secure file transfer from unix to windows

- > *unencrypted password key, and having an ssh-agent that you can pull the key*
- > *out of cleverly, is quite large.*
- >
- > *Rekeying is a very important aspect of almost every secured access setup:*
- > *clients generally *shouldn't* have acces after a cold reboot until someone*
- > *contacts them and re-enables the keys. This is true for all sorts of*
- > *authentication key based protocols....*

There is no perfect security: when you worry about the security of unencrypted password key stored on the server with 0600 permission, you do worry about people with root privilege who can read any files, right? But when you can not trust all of them, why don't you worry about them to use system call tracer or use a trojan horse to capture the key when you enter it? With everyone can modify and build up SSH executables, there is really a problem for detecting trojan horse, and that is one of the reason we choose the AutoSFTP from WZIS for our production use: It provides a trojan horse detecting functionality, that will create a checksum certificate for ssh and sftp before you can start to use asftp, such that if later someone changes the ssh or sftp program, asftp will be able to detect the change and refuse to run. Without knowing the certification generation password, even root will not be able to temper the certificate.