

Re: ssh .vs. rsh

Source: http://www.derkeiler.com/Mailing-Lists/securityfocus/Secure_Shell/2004-01/0083.html

From: Darren Tucker (dtucker_at_zip.com.au)

Date: 01/23/04

Date: Sat, 24 Jan 2004 09:04:43 +1100
To: Steve Bonds <05gekfc02@sneakemail.com>

Steve Bonds wrote:

> *On Wed, 21 Jan 2004, Asif Iqbal iqbala-at-qwestip.net*
> */secureshell@securityfocus.com/ wrote:*
>
>
>> *We have users remotely accessing applications that has GUI in Solaris*
>> *env. It responds real fast if you use rsh, but its pretty slow for*
>> *openssh of any flavor. Is there way we can speed it up ? may be by using*
>> *-c blowfish ?*
>
>
> *If you're looking for better throughput, changing to blowfish will help.*
> *However, it sounds like you're concerned about the response time. There*
> *is significantly more connection setup involved in an SSH connection than*
> *rsh, so it will always be slightly slower. However, if the connection*
> *setup is extremely slow (on the order of several seconds), you might have*
> *a problem.*
>
> *On some other platforms, the process of generating enough entropy for a*
> *secure connection can take a fair amount of time (sometimes over 10*
> *seconds). I didn't think this was a problem for Solaris, but it might be*
> *worth looking into.*
>
> *Some other things to try:*
> *+ run ssh -v and see if one particular step hangs*
> *+ check that your entropy source is running quickly*
> *- if you have /dev/random, be sure sshd is using it and it's not*
> *being fully drained*
> *- check the ssh_prng_cmds to see if any of them are very slow*
> *on your system*
> *+ build a profiling version of sshd and run some tests to see where it*
> *is slow*
>
> *Anyone else have suggestions?*

- Try it with compression on and off.

SecurityFocus Secure Shell: Re: ssh .vs. rsh

- Install the /dev/random patch on both client and server (if you can).
- Try the patch here:
http://bugzilla.mindrot.org/show_bug.cgi?id=769
- Build OpenSSL and OpenSSH with SPARCV8 (or v9) instructions (–mv8 for gcc). The hardware multiply makes a difference to connect time on slow machines.

With those I got the (SSHv2) connect time on my SS5 down to just over 1 sec. Faster machines ought to do better :-)

--

Darren Tucker (dtucker at zip.com.au)

GPG key 8FF4FA69 / D9A3 86E9 7EEE AF4B B2D4 37C9 C982 80C7 8FF4 FA69

Good judgement comes with experience. Unfortunately, the experience usually comes from bad judgement.