

Re: PRNGD and ssh-rand-helper

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-05/0336.html>

From: Darren Tucker (dtucker_at_dodgy.net.au)

Date: 05/24/03

Date: Sat, 24 May 2003 01:18:58 GMT

In article <f5fb93bc.0305230621.1156fc86@posting.google.com>, Chad Johnson <cmjohnson@uslec.com> wrote:
>Is there a way to specify to the sshd program to use prngd instead of
>ssh-rand-helper or must I recompile? I would really like to avoid
>having to recompile.
>
>The main problem is performance.

You could make sure both ends have clean name resolution (put then both in each other's hosts file if you have to).

You can use SSH Protocol 1 (eg "ssh -1") which is faster but less secure.

I know you said you didn't want to recompile, but recompiling both openssl and openssh with SPARC v8 instructions (-mcpu=v8 or -mcpu=ultrasparc if you're using gcc) will make a noticeable difference.

--

Darren Tucker (dtucker@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.