

## Re: Does OpenSSH use RCP?

---

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.unix/2006-01/msg00049.html>

---

- *From:* Dimitri Maziuk <[dima@xxxxxxxx](mailto:dima@xxxxxxxx)>
  - *Date:* Tue, 31 Jan 2006 17:08:55 +0000 (UTC)
- 

Volker Birk sez:

> Dimitri Maziuk <[dima@xxxxxxxx](mailto:dima@xxxxxxxx)> wrote:

>> Volker Birk sez:

>> > Casper H.S. Dik <[Casper.Dik@xxxxxxx](mailto:Casper.Dik@xxxxxxx)> wrote:

>> >> >But SFTP is not "FTP over SSH" like FTPs is doing with "FTP over SSL",

>> >> >so I really don't understand, what's wrong with SFTP.

>> >> >Because it would actually have been a better protocol if it had

>> >> >been FTP over SSL :-)

>> >> >I cannot see that.

>> Perhaps you should try reading the fine rfc's and think about them

>> a little?

>

> The idea of FTP to use `_two_` sockets for communication, and that the

> second one is made from server to client, is completely idiotic.

TCP connection can be tuned for optimal performance. FTP command connection is tuned for interactive response, data connection is tuned for maximum throughput. See also "type of service". There's also a provision (that nobody uses AFAIK) of opening a data pipe to 3rd machine.

....It

> makes FTP difficult to handle. Passive mode is not much better – why

> the hell "out of band data", if the underlying protocol is packet

> based?

TCP is connection-based. By your logic, why bother with network stack at all, let's just hand-modulate voltages — that's what's going on on the wire anyway.

> Of course, you can criticise SSH (as a matter of fact, I'm waiting for > yours or Casper's critics), but it is not as ugly as FTP.

The trend has always been to have one piece of the system do one thing only. Even SSL is often criticized for doing two things — encryption and authentication — in one protocol.

And then ssh comes along and crams interactive logins, file transfer and remote command execution into a single protocol,

## Re: Does OpenSSH use RCP?

with authentication, encryption, compression, and what have you thrown in for good measure. There are two versions of that, plus a few bells and whistles: like it must bypass the standard authentication mechanisms, effectively mandating that you create a backdoor on your system. But wait, there's more: there's an existing standard and implementation for encryption and auth., called ssl. Ssh uses it as a library of crypto routines and builds totally different auth. mechanisms on top. Good idea? What colour is the sky on your planet?

Ever seen ssh never close connections? You know why it does that? — Because it's using the same protocol for remote logins and file transfers: stdout is buffered and when remote end exit()s the last line of its output may still be in the buffer. So if you close the connection on return from wait(), you may lose it and end up with corrupt download. So you have to wait for eof on the pipe. How long do you wait? — hard to tell. OpenSSH's answer is "while(1)". D'oh!

> The two-socket-concept is not very good for SSL either. So I really  
> cannot see, why FTP or FTPs should be a good idea. Perhaps you can  
> explain that.

Ever heard of out-of-band signalling? Your OS has a separate stdout and stderr, tuned differently. Every server on your system has separate output and log streams. Etc. In RPC terms that is "two-socket-concept".

The reason it doesn't work with TCP/IP is that stoned Berkeley undergrads back in the 70's didn't see the need for an extra layer on top of transport. (OSI folks did but hey, that standard was developed by a committee so it must be full of crap — what do them suits know.) As a result, we have no place to associate related connections in order to let them pass through firewalls, track http sessions, etc.

One connection – one application model doesn't work, never has. Its results are sendmail (see Morris Worm), problems with ftp and more recently corba. Here's the good news: we're stuck with it.

Dima

—

Yes, Java is so bulletproofed that to a C programmer it feels like being in a straightjacket, but it's a really comfy and warm straightjacket, and the world would be a safer place if everyone was straightjacketed most of the time.

— Mark 'Kamikaze' Hughes

.

- **Follow-Ups:**
  - ◆ **Re: Does OpenSSH use RCP?**  
◇ From: Volker Birk
  - ◆ **Re: Does OpenSSH use RCP?**  
◇ From: tonij67
  
- **References:**
  - ◆ **Does OpenSSH use RCP?**  
◇ From: tonij67
  - ◆ **Re: Does OpenSSH use RCP?**  
◇ From: Casper H . S . Dik
  - ◆ **Re: Does OpenSSH use RCP?**  
◇ From: tonij67
  - ◆ **Re: Does OpenSSH use RCP?**  
◇ From: Volker Birk
  - ◆ **Re: Does OpenSSH use RCP?**  
◇ From: Casper H . S . Dik
  - ◆ **Re: Does OpenSSH use RCP?**  
◇ From: Volker Birk
  - ◆ **Re: Does OpenSSH use RCP?**  
◇ From: Dimitri Maziuk
  - ◆ **Re: Does OpenSSH use RCP?**  
◇ From: Volker Birk
  
- Prev by Date: **Re: Does OpenSSH use RCP?**
- Next by Date: **Re: Does OpenSSH use RCP?**
- Previous by thread: **Re: Does OpenSSH use RCP?**
- Next by thread: **Re: Does OpenSSH use RCP?**
- Index(es):
  - ◆ **Date**
  - ◆ **Thread**