

Re: Does OpenSSH use RCP?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.unix/2006-02/msg00002.html>

- *From:* Dimitri Maziuk <dima@xxxxxxxx>
 - *Date:* Wed, 1 Feb 2006 00:26:29 +0000 (UTC)
-

Volker Birk sez:

```
> Dimitri Maziuk <dima@xxxxxxxx> wrote:
>> Even SSL is often criticized for doing two
>> things -- encryption and authentication -- in one protocol.
>
> I cannot see, why SSL should be criticized for that.
```

Because "one piece does one thing only" is the way we manage complexity and thus reduce the number of implementation bugs.

```
>> And then ssh comes along and crams interactive logins, file
>> transfer and remote command execution into a single protocol,
>
> SSH has the concept of subsystems. And this seems not very dumb to me.
> If you want to, those subsystems are protocols in higher layers for SSH.
```

It's not "if I want to", it's rtrfrc: show me separate protocol definitions for these subsystems in there.

```
>> 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.
>
> If you agree with me, that FTP is ugly, why do you argue?
```

I didn't say FTP was ugly, I said lack of another layer between application and transport in TCP/IP is why FTP doesn't work too well -- in presence of firewalls, without firewalls it works perfectly well.

```
>> One connection - one application model doesn't work, never has.
>
> I cannot see that. There are many protocols beside FTP, which don't
> have this problem.
```

One is enough. As in, to disprove "for all protocols p one connection - one application model works" it's enough to find one p for which it doesn't: discrete math 101.

```
>> Its results are sendmail (see Morris Worm)
>
> You're talking about buggy implementations again.
```

Largely thanks to complexity resulting from trying to fit a peer-to-peer application into "ein client, ein server, eine kleine pipe in between" model. (In this case the fault is more with "one client, one server" part, though.)

Re: Does OpenSSH use RCP?

>> and more recently corba.

>

> What is your problem with IIOP for the matters of this discussion?

Same as FTP: multiple connections per session. Any RPC protocol should have out of band error signalling (read: second connection opened from server back to the client -- exactly like FTP does transfers), when it expands to fully distributed programming system, you get multiple connections from multiple hosts.

Corba traffic does not pass through packet filters. There's only one kind of corba-friendly firewalls and they are application-layer proxies. Why? -- because there's nothing between applications and transport to group multiple related connections into one session.

Dima

--

.... with the exception of January and February 1900, all Microsoft application libraries counted dates the same way.

-- An Interview with Joel Spolsky of JoelonSoftware

.