Why aren’t we using SSH for everything?

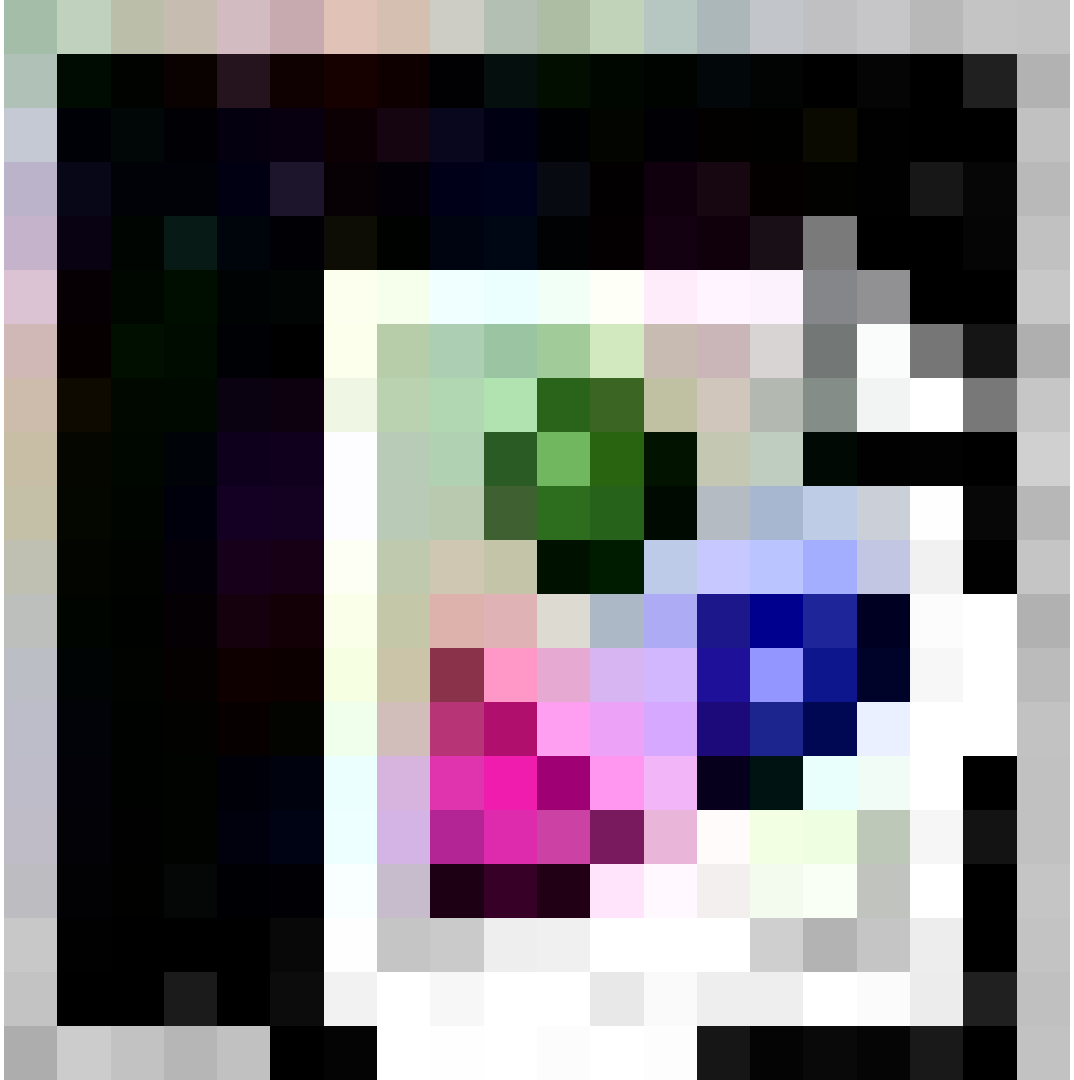
bit.ly/ssh-how-does-it-even

Andrey Petrov (@shazow)

Backstory...

Once upon a time, I built ssh-chat:

```
$ ssh chat.shazow.net
```



```
$ ssh neo@chat.shazow.net
```

```
$ TERM=inator ssh chat.shazow.net
```

```
$ TERM=inator ssh chat.shazow.net
```

** Can send arbitrary variables with the* **SendEnv** *option flag.*

Native Auth

```
$ ls ~/.ssh
id_rsa
id_rsa.pub
```

```
$ ssh chat.shazow.net
 * batman has joined.
```

```
$ ssh chat.shazow.net
The authenticity of host 'chat.shazow.net
(104.236.162.21)' can't be established.
RSA key fingerprint is
e5:d5:d1:75:90:38:42:f6:c7:03:d7:d0:56:7d:6a:db.
Are you sure you want to continue connecting
(yes/no)?
```

```
$ ssh chat.shazow.net
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@       WARNING: POSSIBLE DNS SPOOFING DETECTED!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
The RSA host key for chat.shazow.net has changed,
and the key for the corresponding IP address 104.236.162.21
is unknown. This could either mean that
DNS SPOOFING is happening or the IP address for the host
and its host key have changed at the same time.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
SHA256:HQDLlZsXL3t0lV5CHM0OXeZ5O6PcfHuzkS8cRbbTLBI.
Please contact your system administrator.
Add correct host key in /Users/shazow/.ssh/known_hosts to get rid of this message.
Offending RSA key in /Users/shazow/.ssh/known_hosts:106
RSA host key for chat.shazow.net has changed and you have requested strict checking.
Host key verification failed.
```

```
$ cat ssh-features.md
- SSH is ubiquitous
- Binary protocol
- Mandatory encryption
- Key pinning
- Multiplexing
- Compression
```

```
$ cat ssh-limitations.md
- TCP (every keystroke is a round trip)
- No VHOSTS
- Some implementations have bad defaults
```

```
$ cat ssh-ideas.md
- SSH MUD
- DHT
- Data Streams
- RPC API
- File Server (without scp)
- HTTP over SSH
```

Try it:

```
$ ssh chat.shazow.net
```

Read more:

bit.ly/ssh-how-does-it-even

Follow along:

twitter.com/shazow