(mis)Trusting and (ab)Using SSH

Tips and Tricks for Pentesters and Sysadmins

Herman Duarte <hcoduarte@gmail.com>
Bruno Morisson <morisson@genhex.org>

About us

Bruno Morisson

<morisson@genhex.org>
http://genhex.org/~mori/

I do security stuff @ INTEGRITY S.A.

@morisson
http://www.linkedin.com/in/morisson

Herman Duarte

<hcoduarte@gmail.com>

InfoSEC addict @ INTEGRITY S.A.

@hdontwit
http://www.linkedin.com/in/hcoduarte

In the beginning of times...

- Telnet
- r* services (rlogin, rsh)
- Weak (or no) authentication
- Communication in clear

In the beginning of times...

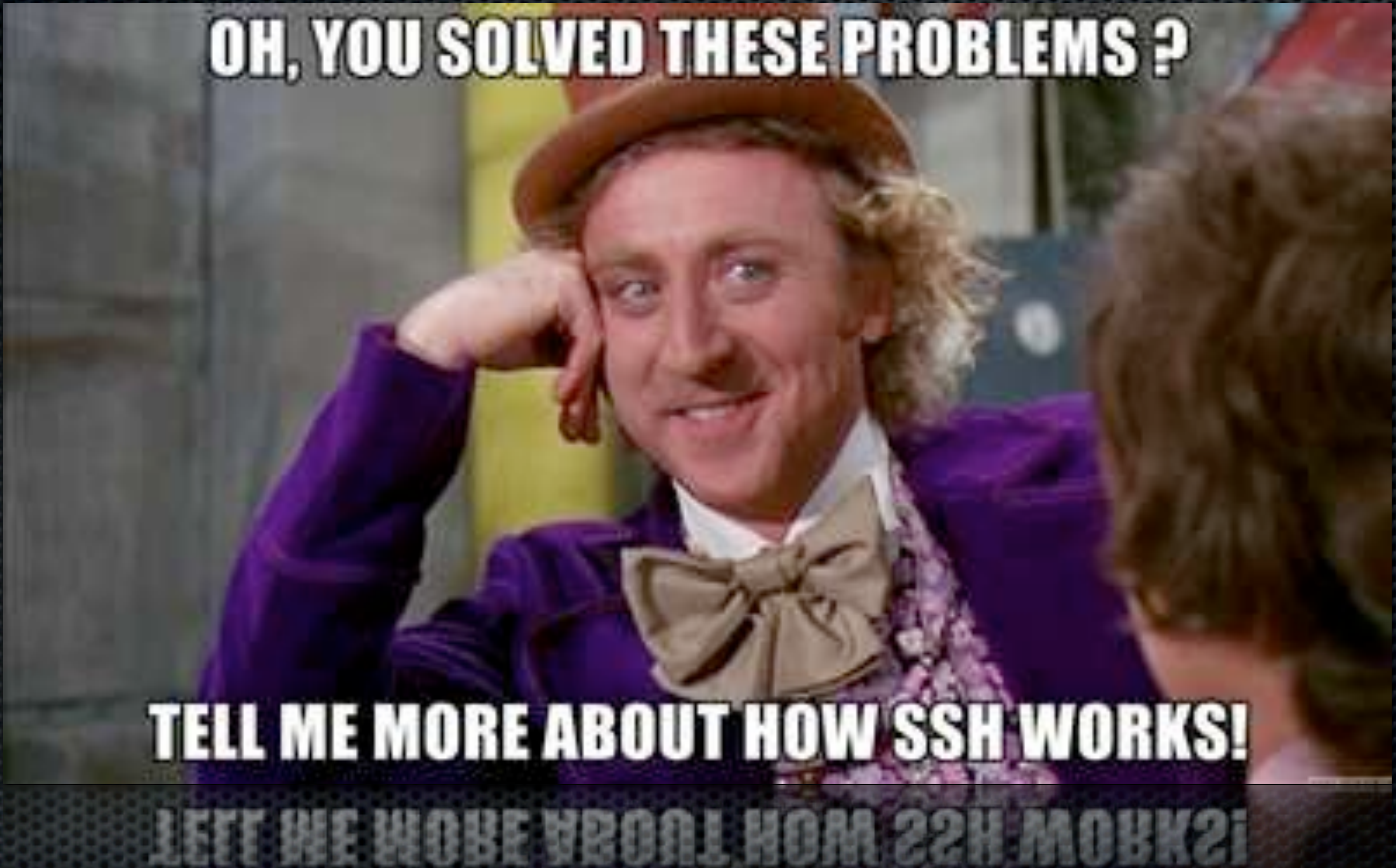
- Sniffing
- Interception
- Hijacking
- Man-In-The-Middle
- ...

Enter the Dragon^W**SSH**

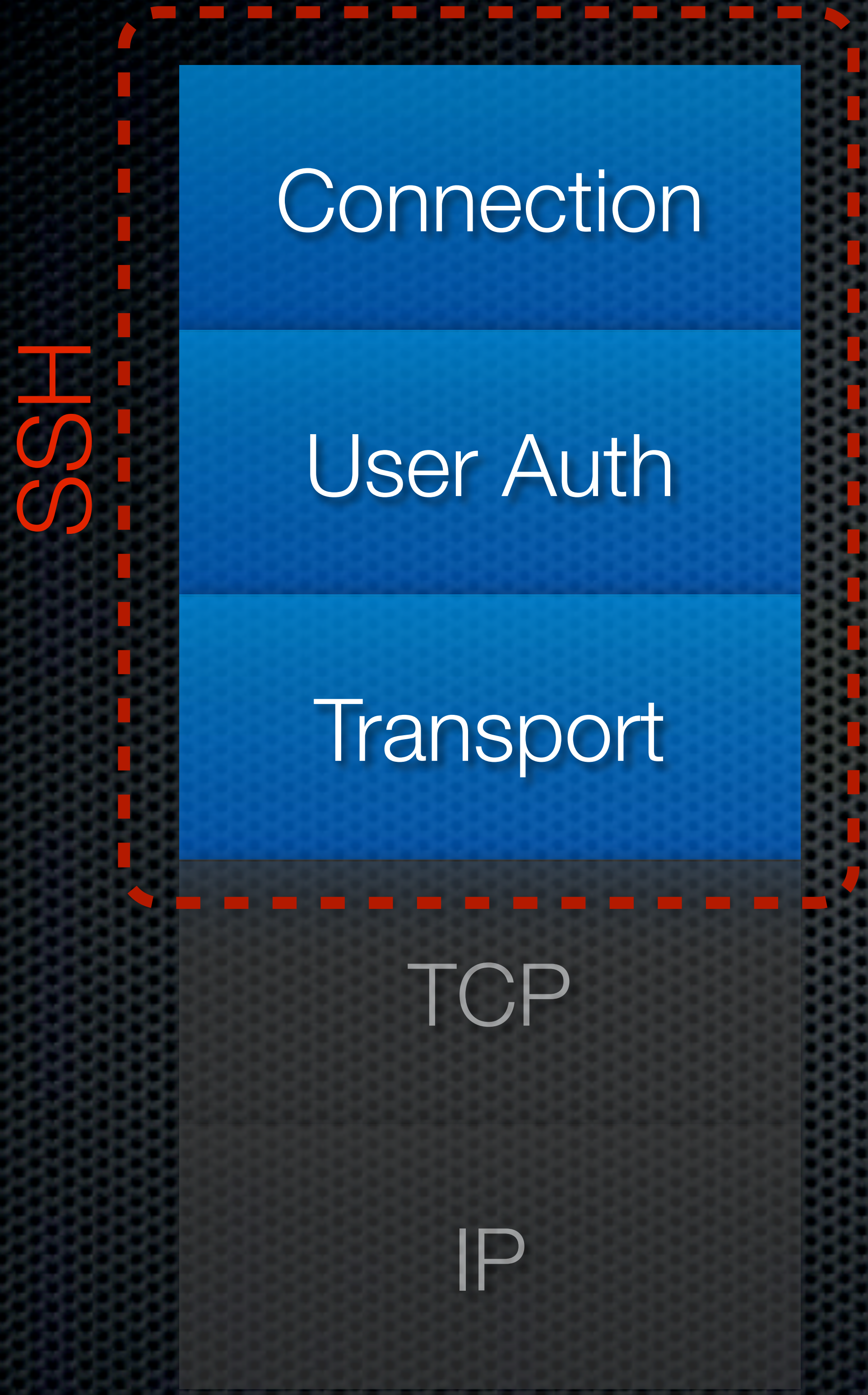
SSH* features

- Key agreement (DH)
- Encrypted communications (C&I from CIA)
- Multiple authentication options (password, public keys, kerberos, etc...)
- Channel Multiplexing
- Port Forwarding
- VPN
- ...and so much more!

* for this talk SSH==SSHv2


OH, YOU SOLVED THESE PROBLEMS ?
TELL ME MORE ABOUT HOW SSH WORKS!

SSH 101- The Basics



SSH

Connection

Session Multiplexing, TCP forwarding, socket forwarding, sftp subsystem, etc

User Auth

User Authentication (password, Pubkey, etc)

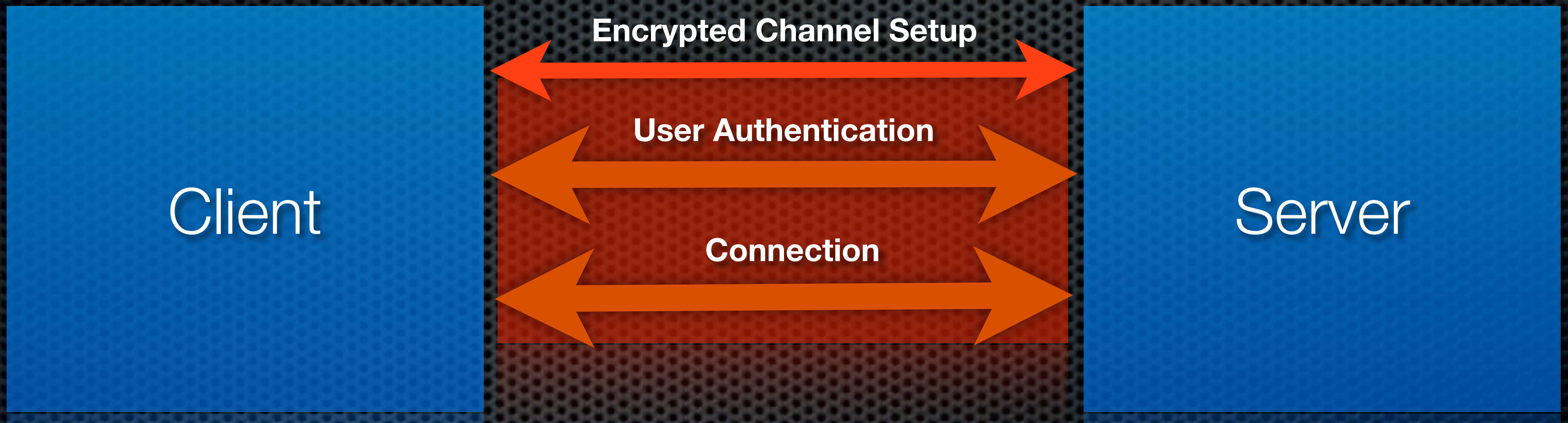
Transport

Key Agreement (DH), Host auth, Integrity, Encryption, Re-Keying

TCP

IP

SSH 101- The Basics



Client

Encrypted Channel Setup

User Authentication

Connection

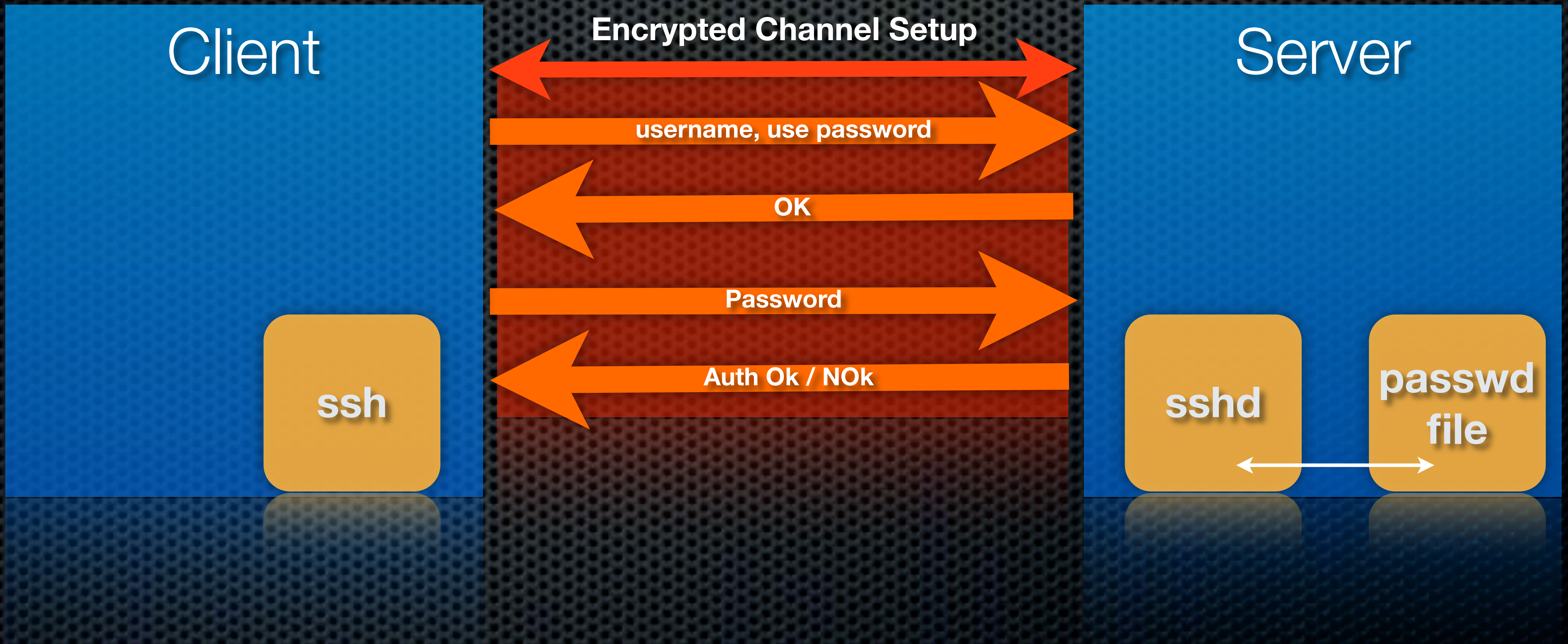
Server

SSH 101- The Basics

User authentication methods:

- GSSAPI
- Host-Based
- Public Key
- Challenge-Response
- Password

Password Authentication

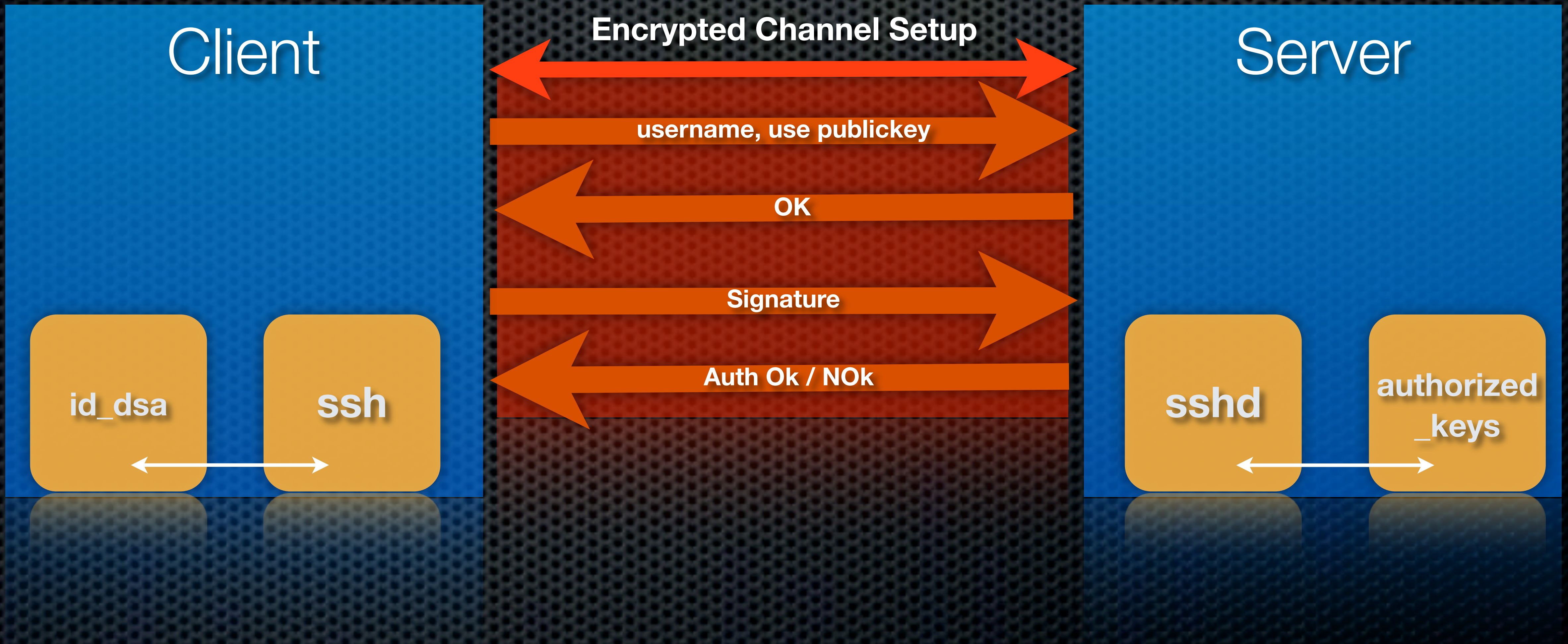


If the server is compromised...

- sshd binary is changed with one that logs passwords
- keylogger is installed on the server

..the password is compromised!

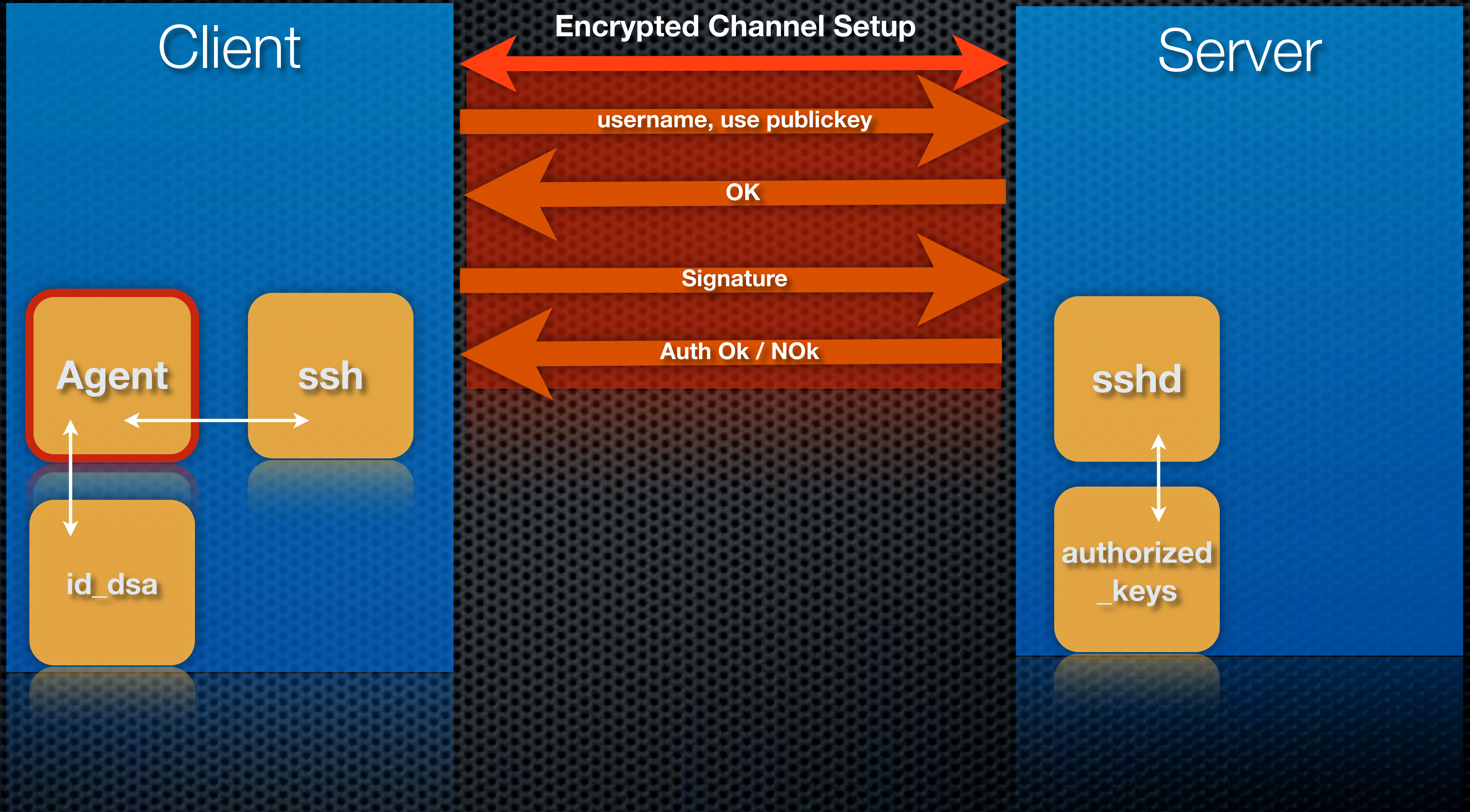
PublicKey Authentication



DEMO

What if I have a lot of keys, or login a lot ??

SSH Agent

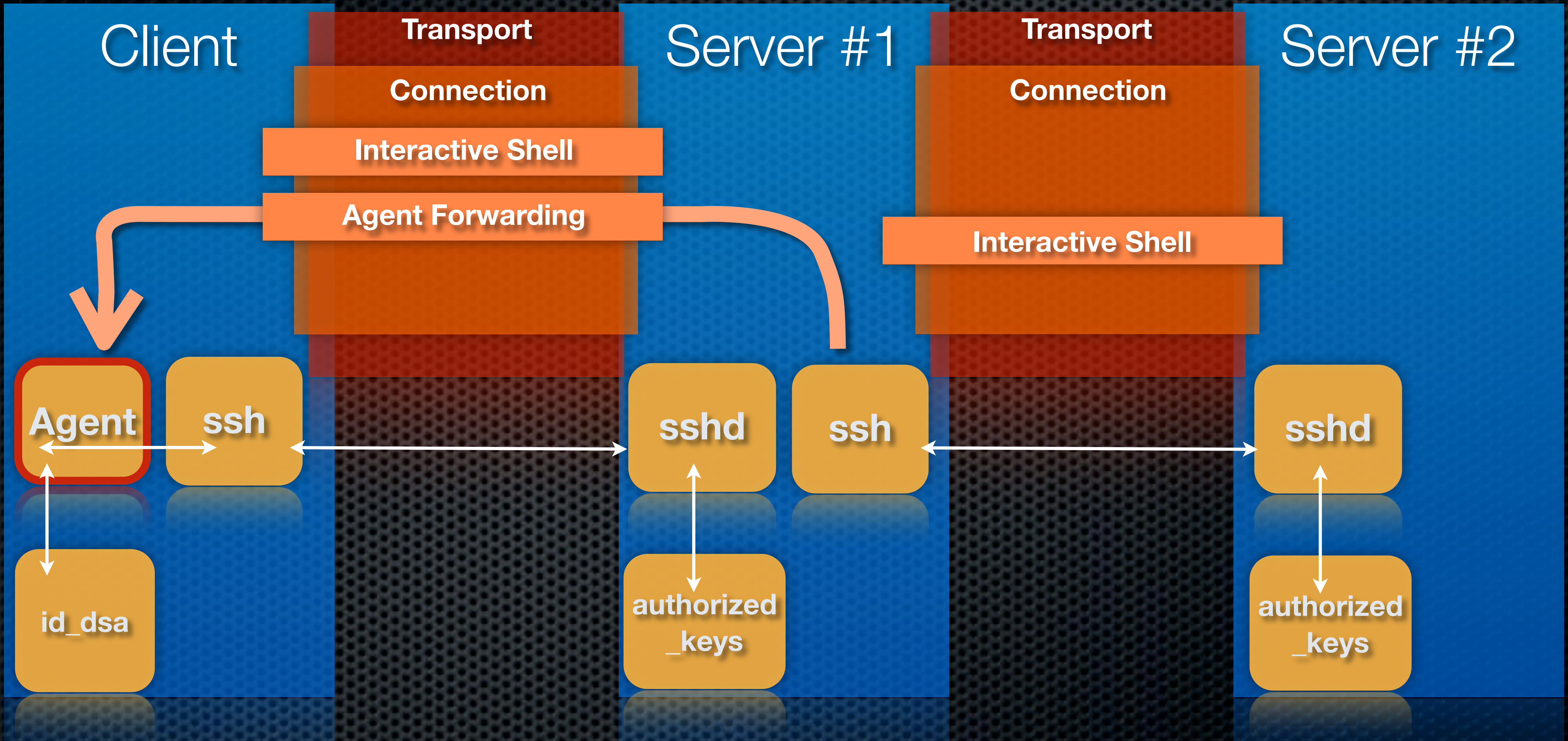

Client
Encrypted Channel Setup
Server
username, use publickey
OK
Signature
Auth Ok / NOk
Agent
ssh
sshd
id_dsa
authorized
_keys

What if I SSH into other servers ??

SSH Agent Forwarding

- No need to copy private key to other servers
- Key is kept on the original source host
- Agent is forwarded, using a tunnel
- **Passwordless!**

SSH Agent Forwarding



Control Master

- Connection multiplexing allows for multiple sessions on one connection
- It’s fast
- **No need for extra authentication**

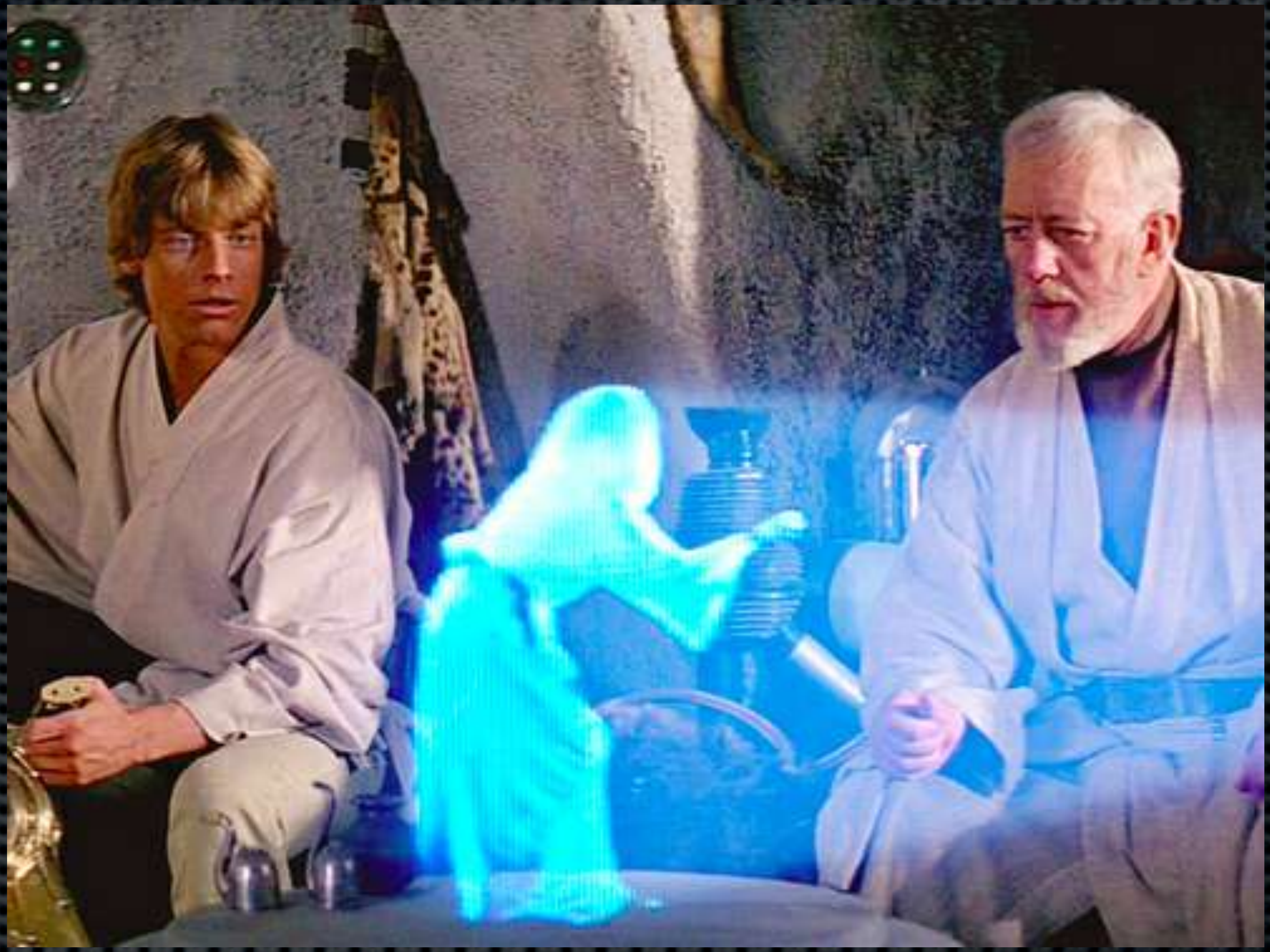
DEMO

Caveat Emptor(s)

- You **must** trust the server(s)
- What if the **server** was **compromised** ?
- Can SSH **Agent** be **abused** ?
- Can Control **Master** be **abused** ?

DEMO

Help us Obi Wan



You’re our only hope!

Freak on a Leash

When adding keys to ssh-agent use **ssh-add** with:

- **-t <secs>** to set a maximum lifetime on the identities being added to the agent
- **-c** to indicate that identities being added should be subject to confirmation before being used for auth

Freak on a Leash

- **ssh-agent** queries /usr/libexec/**ssh-askpass** for confirmation
- “ssh-add -c -t 3600 **< /dev/null**” makes ssh-add use env var **SSH_ASKPASS** to query for passphrase

DEMO

But we still need passwords!

If you su / sudo, you still **type** your **password**...

What if we could use the SSH Agent for sudo ?

Yes we can! :)

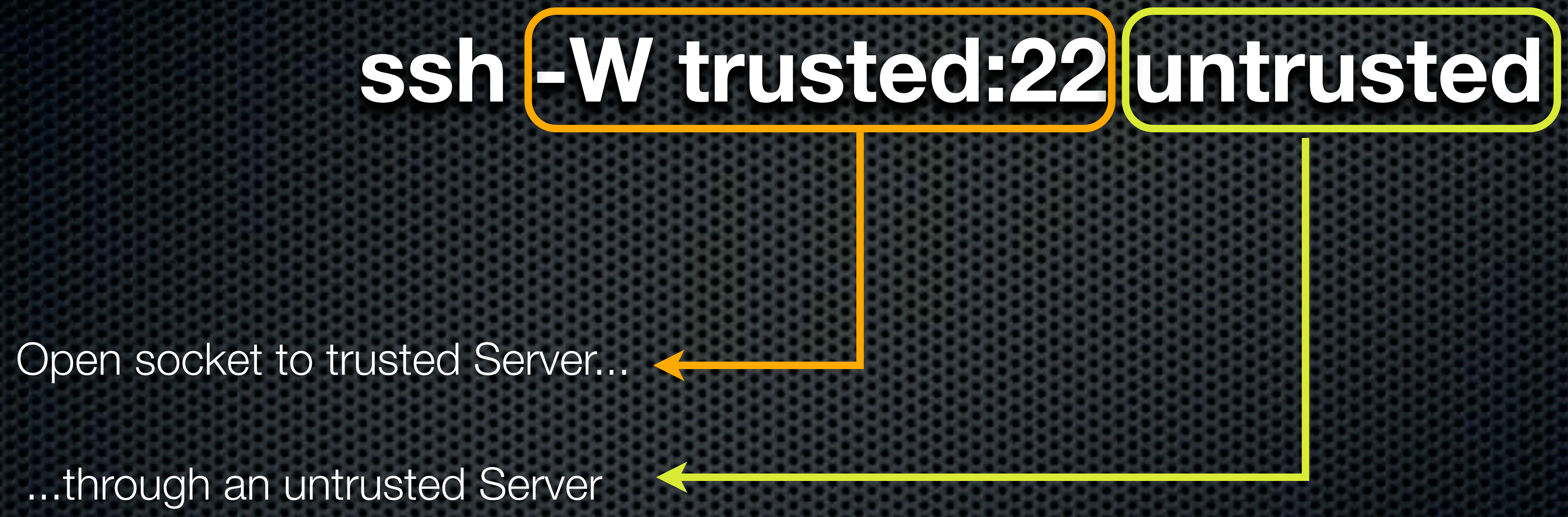
DEMO

Paranoia is reality on a finer scale

LUKE...
USE THE FORCE
Bohemian Grove
FRABZ.COM MEMES & FUNNY PICS

Using SSH w/o using SSH

(but still using SSH)



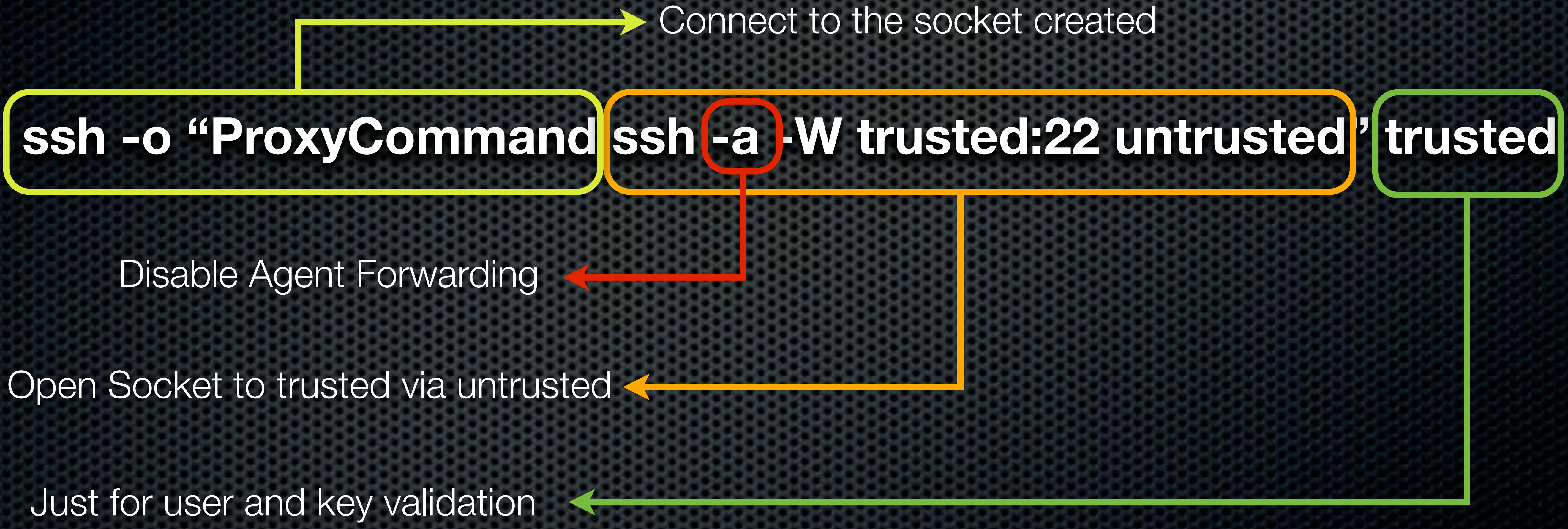
```
ssh -W trusted:22 untrusted
```

Open socket to trusted Server...

...through an untrusted Server

Using SSH w/o using SSH

(but still using SSH)



```
ssh -o “ProxyCommand ssh -a -W trusted:22 untrusted’ trusted
```

Connect to the socket created

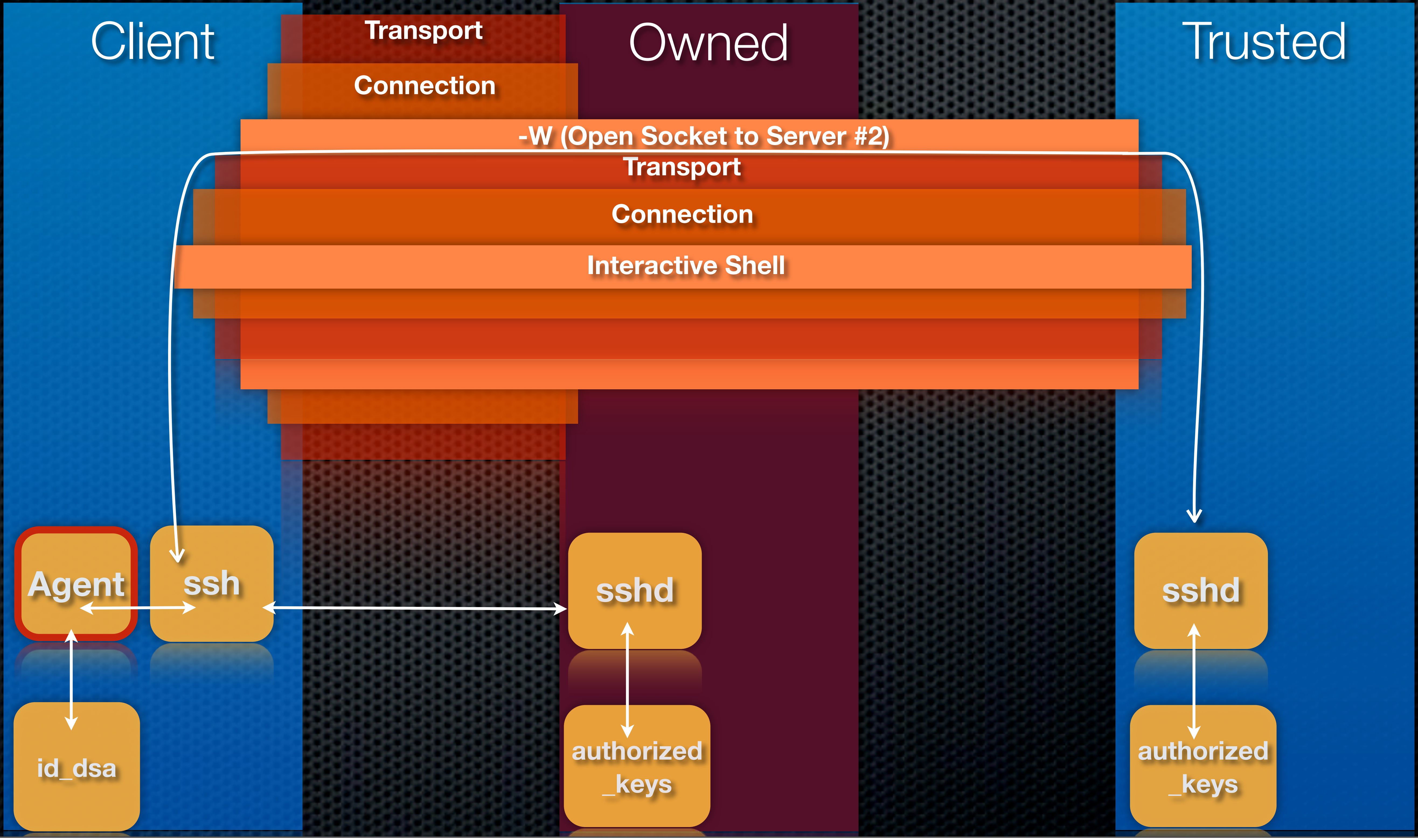
Disable Agent Forwarding

Open Socket to trusted via untrusted

Just for user and key validation

Using SSH w/o using SSH

(but still using SSH)



DEMO

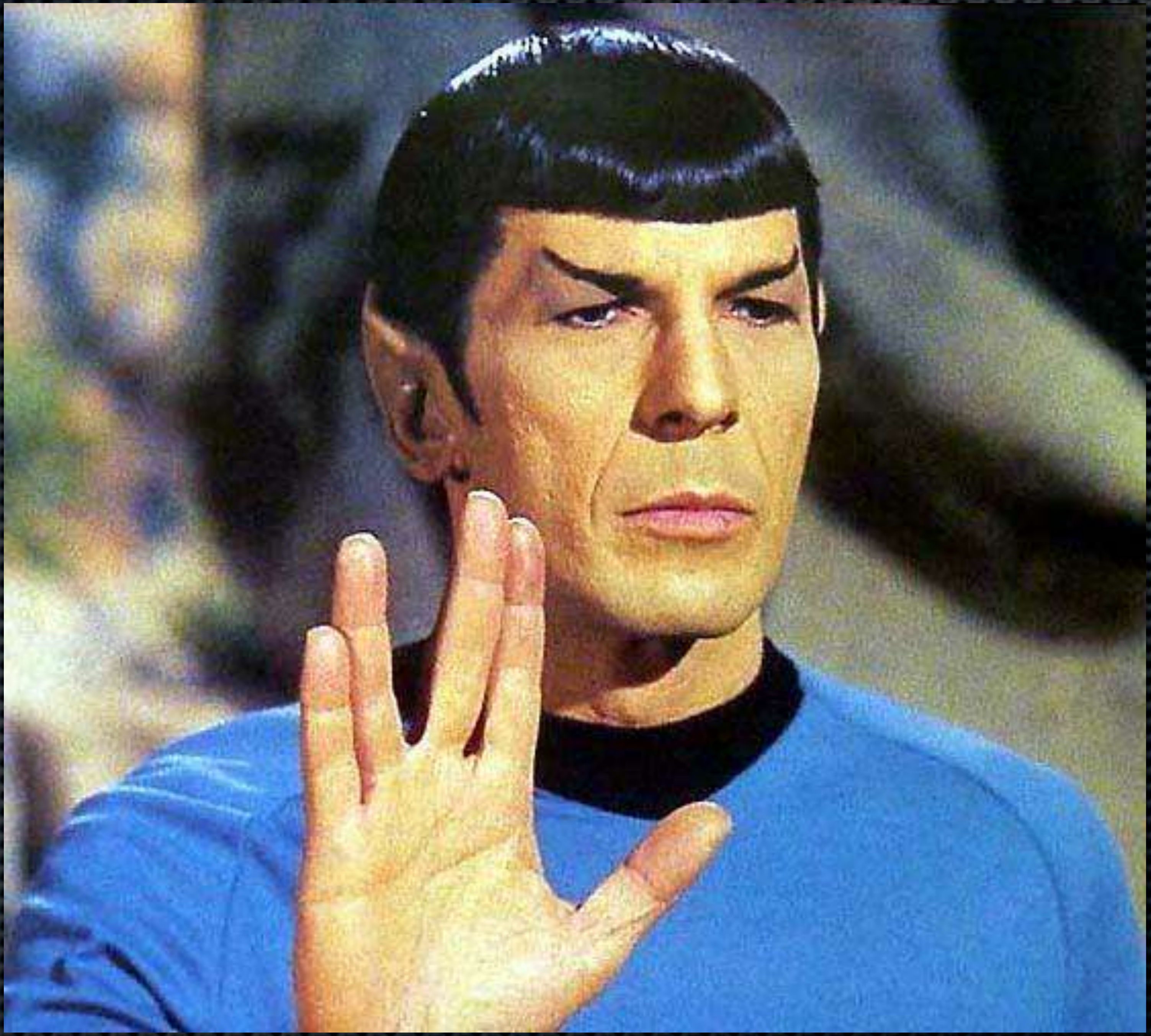
Control your SSH

.ssh/config

```
Host trusted1 trusted2 trusted3
ForwardAgent yes
ProxyCommand ssh -a -W %h:22 untrusted.server.com

Host *
ControlMaster no
ForwardAgent no
PasswordAuthentication no
HashKnownHosts yes
```

Live long and prosper



References

- RTFM :)
- RFCs 4251-4256,4335,4344,4345,4419,4432,4462,4716,5656
- http://www.linuxjournal.com/article/9566
- http://pamsshagentauth.sourceforge.net/
- http://www.jedi.be/blog/2010/08/27/ssh-tricks-the-usual-and-beyond/