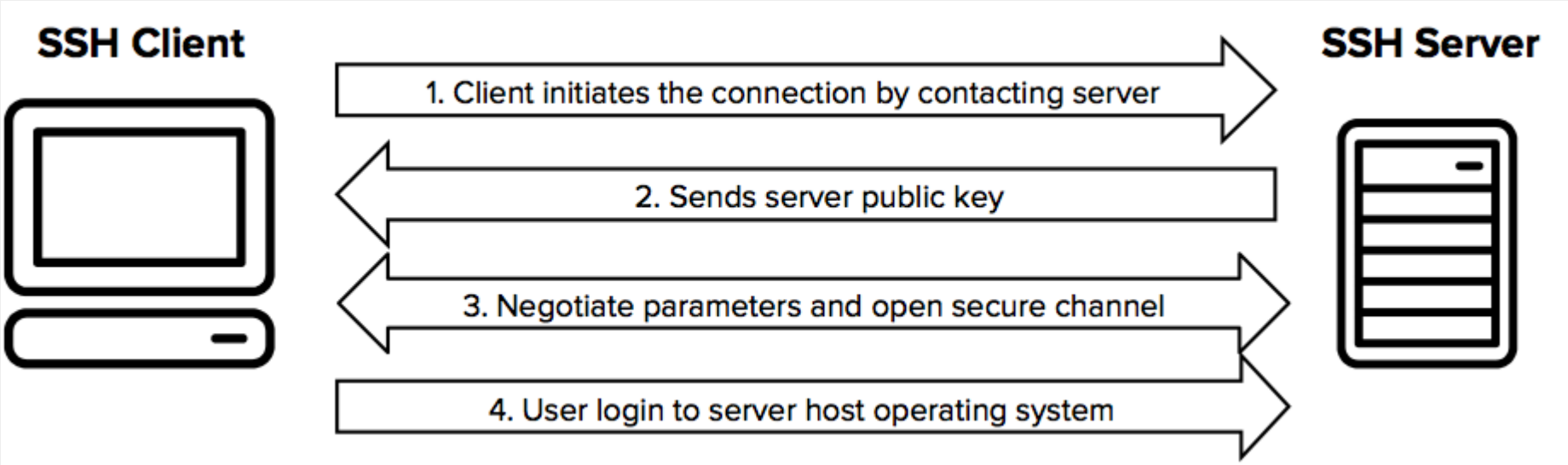
ssh Basics / Tips & Tricks

Patrick Ladd
Senior Technical Account Manager
pladd@redhat.com

ssh Authentication

Red Hat

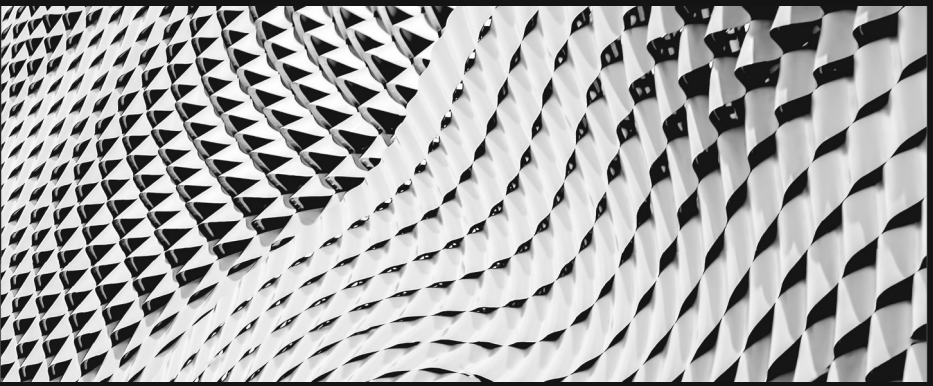
Protocol Flow



https://www.redhat.com/sysadmin/ssh-secure-communication

Red Hat

ssh Authentication



Red Hat

Authentication Types

- **Password**
- **Public key**
- GSSAPI-based (kerberos etc.)
- Host-based
  - Machine listed in `/etc/hosts.equiv` or `/etc/ssh/shosts.equiv`
  - Non-root
  - Usernames match or `~/.rhosts` or `~/.shosts` mapping exists
  - Client host key verified by server
- Challenge-response
  - BSD or PAM based

Red Hat

Public Key Authentication

- Public / Private Key Tech
- **`ssh-keygen`**
  - Creates:
    - Public key: `~/.ssh/id_rsa.pub`
      ```
      ssh-rsa xxxxxxxxx username@example.com
      ```
    - Private key: `~/.ssh/id_rsa`
      ```
      -----BEGIN RSA PRIVATE KEY-----
      xxxxxxx
      -----END RSA PRIVATE KEY-----
      ```
- Copy public key to server
- **PROTECT YOUR PRIVATE KEY**
  - Created as u+rw/go-a permissions
- Details & Troubleshooting: https://access.redhat.com/solutions/9194

Red Hat

Move Public Key To Host

- End result: added to ~/.ssh/authorized_keys
- Ways to do it:
  - **`ssh-copy-id example.com`**
  - Ansible play
    - **`authorized_key`** task

```
- name: Set authorized key taken from file
  authorized_key:
    user: charlie
    state: present
    key: "{{ lookup('file', '/home/charlie/.ssh/id_rsa.pub') }}"
```

  - Copy / paste

```
$ mkdir ~/.ssh/
$ chmod 700 ~/.ssh  # this is important
$ touch ~/.ssh/authorized_keys
$ chmod 600 ~/.ssh/authorized_keys  #this is important
$ cat >> ~/.ssh/authorized_keys
```


Red Hat

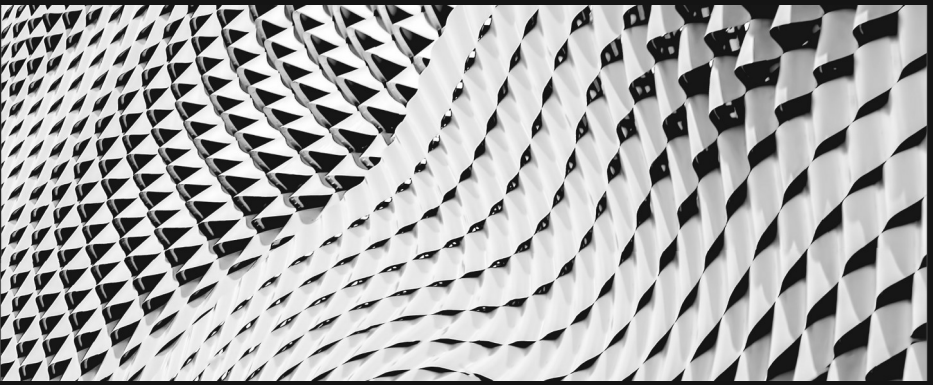
Getting fancier

- sshpass
  https://www.redhat.com/sysadmin/ssh-automation-sshpass
- Multiple key pairs
  https://www.redhat.com/sysadmin/manage-multiple-ssh-key-pairs

- ssh file copy:
  - https://www.redhat.com/sysadmin/ssh-file-copy-magic
  - scp mylocalfile somebody@somehost.net:a_remote_file

Red Hat

Hardening ssh



Red Hat

Hardening Tips

- https://www.redhat.com/sysadmin/eight-ways-secure-ssh

1)Backup the config file

2)Set a banner message

Create `/etc/issue.net`

`/etc/ssh/sshd_config`:

```
Banner /etc/issue.net
```

3)Prevent empty passwords:

```
PermitEmptyPasswords no
```

4)Prevent the root user from crossing the network via SSH

```
PermitRootLogin no
```


Red Hat

Hardening Tips (continued)

- https://www.redhat.com/sysadmin/eight-ways-secure-ssh

1) Whitelist specific user accounts

```
AllowUsers user1
```

6)No more port 22

```
#Run SSH on a non-standard port
Port 2222
 ssh -p 2222 user1@10.1.0.42
```

7)Time's up!

```
ClientAliveInterval 60
ClientAliveCountMax 3
```


Red Hat

Going farther

- Session recording and containerized isolation
  https://www.redhat.com/sysadmin/secure-session-recording
  https://www.redhat.com/sysadmin/session-recording-tlog
- Proxy / jump host
  https://www.redhat.com/sysadmin/ssh-proxy-bastion-proxyjump

Red Hat

Resources

- Enable Sysadmin blog: https://www.redhat.com/sysadmin/
  - https://www.redhat.com/sysadmin/ssh-secure-communication
  - https://www.redhat.com/sysadmin/configure-ssh-keygen
  - https://www.redhat.com/sysadmin/eight-ways-secure-ssh
  - https://www.redhat.com/sysadmin/secure-session-recording
  - https://www.redhat.com/sysadmin/session-recording-tlog
  - https://www.redhat.com/sysadmin/ssh-proxy-bastion-proxyjump

Red Hat

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat

Red Hat