SSH

Develop Intelligence

Secure Shell (SSH)

Develop Intelligence

SSH is a protocol for creating a secure tunnel between two machines.

- Commands
- Remote terminal
- Files
- (or really any network traffic!)

SSH command

Develop Intelligence

Runs commands or opens interactive terminal on remote machine

```
ssh [-i identity_file] ... [user@]hostname [command]
```

Example:

```
$ ssh bob@10.4.0.5
```

SCP command

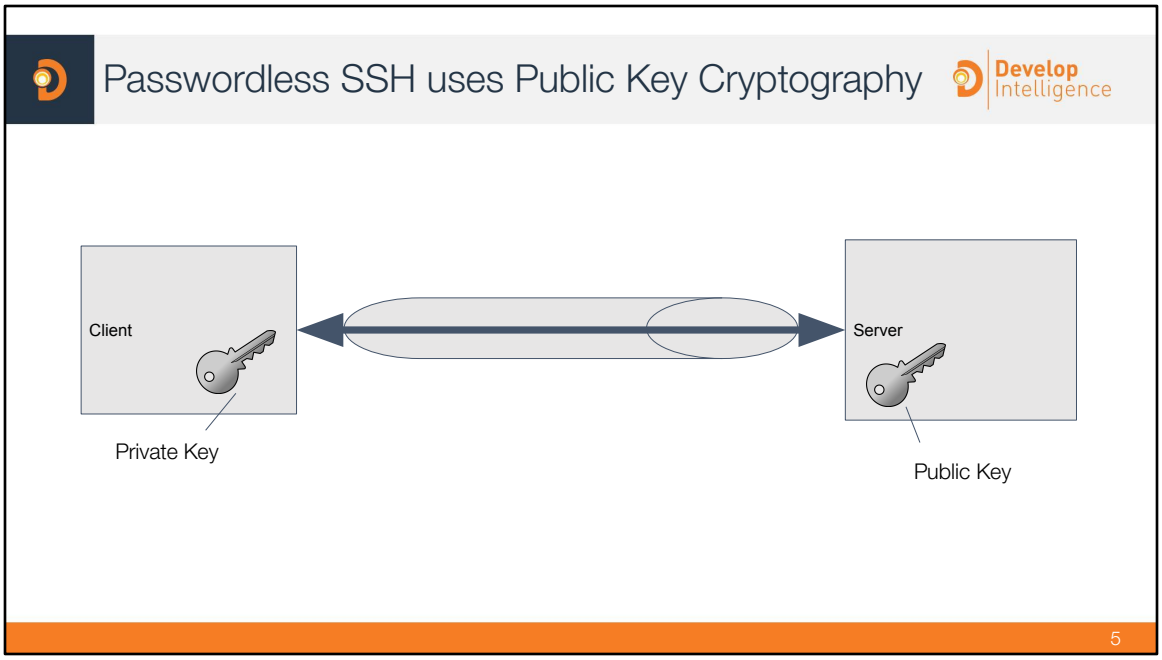
Develop Intelligence

Used for copying files to, from, and between remote systems

```
scp [-i identity_file] ... [[user@]host:]file1 [[user@]host:]file2
```

Example:

```
$ scp local_file.txt bob@10.4.0.5:/etc/
```



Each side gives the other side their public key. Further communication between the two is then encrypted with the other ends public key, only allowing the owner of the corresponding private key to decrypt the message.

https://en.wikipedia.org/wiki/Public-key_cryptography

Private vs Public key

Develop Intelligence

Private

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAp+l01+sUAZLxb0vqRXRVGPn
xlc+9aESIJzV5M/ye7E1C+dFxHyZPdWOJieyNlBFm
...
assVAoGBAMI4qr/0krzcSRu/xTdQIHncCPiqYKO6nR
ufratQ2yMtLvi2wfWU6BBR9M2Nkmi2J4MoF6PglfyA
MHqZ0AbckrWREzyxBhrp+OFH/Xsq5uNgiB7jzTizx9
-----END RSA PRIVATE KEY-----
```

Public

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCn6XTX6
xQBkvFvS+pFdFUY+cOmbWKf8SsPhouiVkKJwxYR
2X/Ehz71oRlgnNXkz/J7sTUL50XEfJk91Y4mJ7I2UE
WYZQoVdw58BeJvNVGuaYLM4pXSf1Me5Ekgbk6w
HJT9upqEPamjpaD7QST72q7qgMGiFyAYR3IcVZB3
UFhJzyeDlBv+mW+u+Akatt15EWDJ+/rmVy1QlEVeoi
Djdc25WA63UU/Wl9vloSHSaNd1MvPiDU27v/TlTwy
38rhgBOSFT3lw2H6urljYqVaGAOLd4QpZCNMfiVR6
LNQvjMtLmtf9a5z3iLIM/2NZtlVVPUNc1mWGcxTEs
mgswY5MyjVl myuser@host.local
```

ssh-keygen

Develop Intelligence

- Creates a public and private key pair
- You can further lock down a private key with a ***passphrase***
- Defaults to storing keys in ~/.ssh/

```
$ ssh-keygen [-N passphrase] [-C comment] ...
```

ssh-copy-id

Develop Intelligence

- Copies public key into **~/.ssh/authorized_keys** on remote server

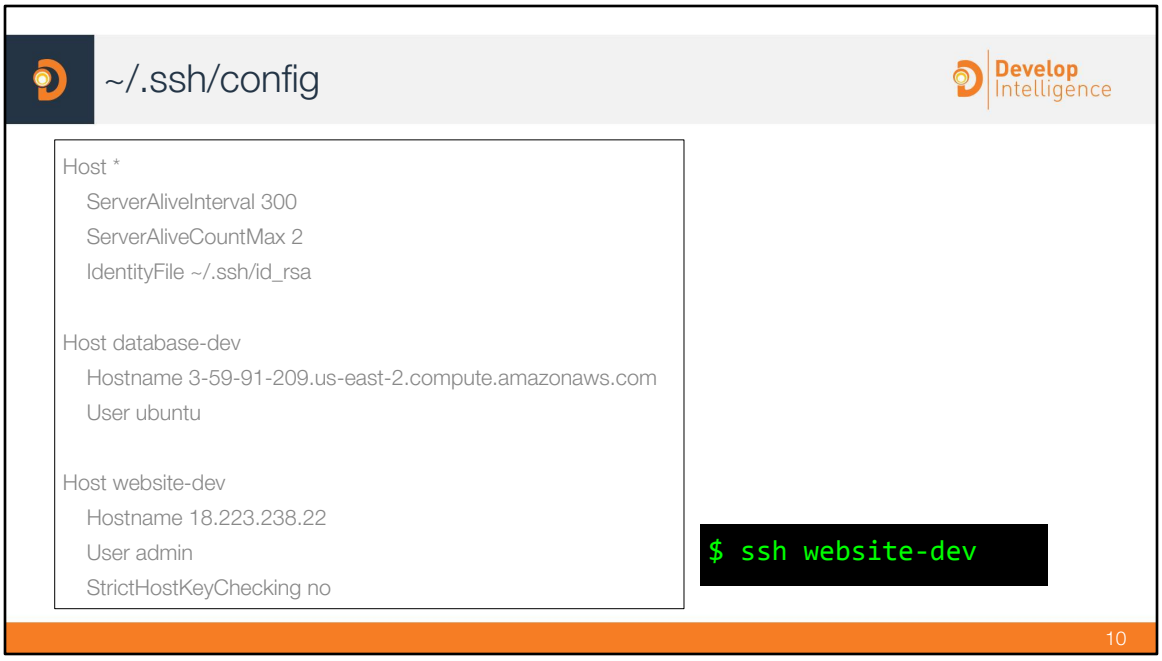
```
ssh-copy-id [-i [identity_file]] [user@]hostname
```

known hosts

Develop Intelligence

- the ~/.ssh/known_hosts files can help detect compromised keys

```
$ ssh bob@10.4.0.5
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    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 ECDSA key sent by the remote host is
SHA256:7RAb2jPhorN2i3qiikAnqjPFKLv/UWDnbnEWKjKKpzc.
Add correct host key in /Users/ameade/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /Users/ameade/.ssh/known_hosts:19
ECDSA host key for 35.188.214.222 has changed and you have requested strict
checking.
Host key verification failed.
```


~/.ssh/config
Develop Intelligence
Host *
ServerAliveInterval 300
ServerAliveCountMax 2
IdentityFile ~/.ssh/id_rsa
Host database-dev
Hostname 3-59-91-209.us-east-2.compute.amazonaws.com
User ubuntu
Host website-dev
Hostname 18.223.238.22
User admin
StrictHostKeyChecking no
$ ssh website-dev
10

Additional Resources

Develop Intelligence

- SSH config file manpage
  https://linux.die.net/man/5/ssh_config