Peculiar SSH(1)

#BalCCon2k17!

@MacLemon

Raise your hand!

Peculiar SSH(1)

Somewhat advanced SSH things…

From Zero to Hero*ine
Today 16:00 - 18:00
Room: PUPIN

SSH beginners' workshop
with Hetti and MacLemon

SSH(1)

Two-Factor Authentication

Pictures of RSA Tokens on Webcams

(Google Image Search)

My Webcam (avara...

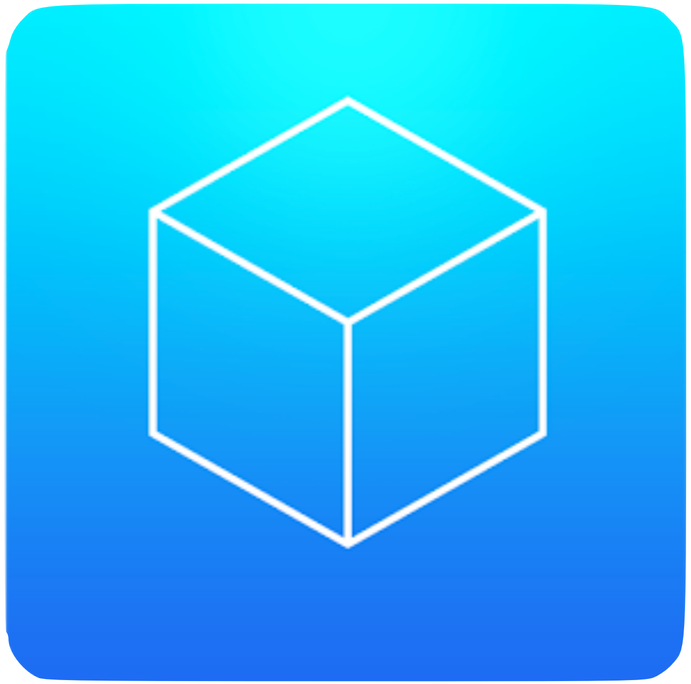
File Webcam Help

Broadcast Pause

Broadcasting - 0 Viewer(s)


Immanuel Kant
Kritik der
reinen Vernunft
RSA SecurID®
CALLER ID MODULE
review

Time base One-Time Pads



Time-Based One-Time Password Algorithm RFC 6238


yubico
yubico

HOTP: An HMAC-Based One-Time Password Algorithm RFC 4226

```
AuthenticationMethods publickey, publickey,
  keyboard-interactive:pam

ChallengeResponseAuthentication yes
```

Crypto Config

`kex, mac, key, key-plain, key-cert, cipher, cipher-auth`

Crypto Config

`kex, mac, key, key-plain, key-cert, cipher, cipher-auth`

Server HostKey

/etc/sshd_config

```
# HostKey /etc/ssh/ssh_host_rsa_key
# HostKey /etc/ssh/ssh_host_ecdsa_key
# HostKey /etc/ssh/ssh_host_dsa_key
# HostKey /etc/ssh/ssh_host_ed25519_key
```

/etc/sshd_config

```
# HostKey /etc/ssh/ssh_host_rsa_key
# HostKey /etc/ssh/ssh_host_ecdsa_key
# HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
```

KexAlgorithms

ssh -Q kex

```
Host *

   KexAlgorithms \
      curve25519-sha256@libssh.org
```

PubkeyAcceptedKeyTypes

`ssh -Q key`

```
Host *

    PubkeyAcceptedKeyTypes
      ssh-ed25519-cert-v01@openssh.com, \
      ssh-ed25519
```

MACs

ssh -Q mac

```
Host *
    MACs \
      hmac-sha2-512-etm@openssh.com, \
      hmac-sha2-256-etm@openssh.com
```

Ciphers

ssh -Q cipher-auth

```
Host *
  Ciphers \
    chacha20-poly1305@openssh.com, \
    aes256-gcm@openssh.com
```

Bastion Hosts

```
Host balccon
  ProxyJump jumpjump

Host jumpjump
  […]
```

```
Host balccon
  ProxyJump krisskross,jumpjump
```

```
$ ssh -J krisskross,jumpjump balccon
```

Legacy Systems

The real world

```
Host vintagebox
  KexAlgorithms diffie-hellman-group14-sha256
  Ciphers aes256-ctr
  PubkeyAcceptedKeyTypes  ssh-rsa
  MACs  umac-128@openssh.com
```

Debugging

Y U NO CONNECT?

`ssh -G <Host>`

Applied config directive

```
ssh vintagebox
Unable to negotiate with 203.0.113.17
 port 2017: no matching cipher found. Their
offer: aes256-ctr, aes128-ctr
```

```
# Setting defaults
Host *
  Ciphers chacha20-poly1305@openssh.com

Host vintagebox
  Ciphers aes256-ctr
```

```
ssh vintagebox -G | grep ciphers
ciphers chacha20-poly1305@openssh.com
```

```
# Setting defaults
Host *
  Ciphers chacha20-poly1305@openssh.com

Host vintagebox
  Ciphers +aes256-ctr
```

```
ssh vintagebox -G | grep ciphers

ciphers chacha20-poly1305@openssh.com,aes128-
ctr,aes192-ctr,aes256-ctr,aes128-
gcm@openssh.com,aes256-gcm@openssh.com,aes128-
cbc,aes192-cbc,aes256-cbc,3des-cbc
```

```
Host vintagebox
  Ciphers aes256-ctr


# Setting directives not already set!
Host *
  Ciphers chacha20-poly1305@openssh.com
```

```
ssh vintagebox -G | grep ciphers

aes256-ctr
```

```
ssh -v <Host>
```

verbosity, up to -vvv

```
$ ssh example.maclemon.at -v

OpenSSH_7.4p1, LibreSSL 2.5.0
debug1: Reading configuration data /Users/MacLemon/.ssh/config
debug1: /Users/MacLemon/.ssh/config line 3: Applying options for *
debug1: /Users/MacLemon/.ssh/config line 500: Applying options for mirror
debug1: /Users/MacLemon/.ssh/config line 1198: Applying options for *
debug1: /Users/MacLemon/.ssh/config line 1228: Deprecated option "useroaming"
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: UpdateHostKeys=ask is incompatible with ControlPersist; disabling
debug1: auto-mux: Trying existing master
debug1: Requesting forwarding of local forward LOCALHOST:16901 ->
127.0.0.1:16901
debug1: mux_client_request_session: master session id: 12
Last login: Sat Sep 16 11:48:08 2017 from 82.117.211.154
```

ssh_scan

https://github.com/mozilla/ssh_scan

ssh_scan installation

```
gem install ssh_scan
```

```
git clone https://github.com/mozilla/ssh_scan.git

cd ssh_scan

gem install bundler
bundle install
```

```
./ssh_scan  -t example.maclemon.at -p 2017
```

```
[
  {
    "ssh_scan_version": "0.0.27",
    "ip": "203.0.113.17",
    "hostname": "example.maclemon.at",
    "port": 2017,
    "server_banner": "SSH-2.0-OpenSSH_5.2",
    "ssh_version": 2.0,
    "os": "unknown",
    "os_cpe": "o:unknown",
    "ssh_lib": "openssh",
    "ssh_lib_cpe": "a:openssh:openssh:5.2",
    "key_algorithms": [
      "diffie-hellman-group-exchange-sha256",
      "diffie-hellman-group-exchange-sha1",
```

```
    "compliance": {
      "policy": "Mozilla Modern",
      "compliant": false,
      "recommendations": [
        "Add these key exchange algorithms:
curve25519-sha256@libssh.org,ecdh-sha2-
nistp521,ecdh-sha2-nistp384,ecdh-sha2-
nistp256",
        "Add these MAC algorithms: hmac-
sha2-512-etm@openssh.com,hmac-sha2-256-
etm@openssh.com,umac-128-etm@openssh.com,hmac-
sha2-512,hmac-sha2-256,umac-128@openssh.com",
        "Add these encryption ciphers:
```

```
"grade": "F"
```

The *Future*…

OpenSSH 7.5+

RC4, Blowfish
RIPE-MD160

RSA < 1.024bits

CBC mode ciphers

You have been warned!

Questions?

More questions…

…over a beverage!

Thanks #BaICCon2k17!

@MacLemon