

Synergy

John Schember



Outline

- What?
- Why?
- How?
- Security?
 - VPN
 - SSH
 - STunnel



What?

- KVM without Video
- Seamless integration
 - Screen edge leads to other screens
- Network based
 - TCP 24800
- Multi-platform
 - Windows
 - *nix
 - OS X



Why?

- One mouse and keyboard for multiple machines
- Clipboard sharing
- Screensaver synchronization
- Free (GPL)
- No need for extra hardware



How?

- Install synergy on each machine
- Create synergy configuration file
- Start synergys
 - synergys -c synergy.conf
- Connect with synergyc
 - synergyc 192.168.0.101



Sample config

```
section: screens
```

```
  Ubox:
```

```
  Cbox:
```

```
end
```

```
section: links
```

```
  Ubox:
```

```
    right = Cbox
```

```
  Cbox:
```

```
    left = Ubox
```

```
end
```



Security?

- There is none
- All traffic sent in plain text
- Not meant for use on insecure network
- Trust no one
- There is hope



VPN

- Set up VPN between computers
- Route server and clients over VPN
 - -a option to listen on specific address
 - synergys -a 10.36.0.1 -c synergy.conf
 - Synergyc 10.36.0.1



SSH


- SSH port forwarding
- Server
 - `synergys -a 127.0.0.1 -c synergy.conf`
- Client
 - `ssh -f -N -L 24800:127.0.0.1:24800 user@server`
 - -f = Background after authentication
 - -N = Do not execute remote command
 - -L = Local port to forward to remote port
 - `synergyc 127.0.0.1`

STunnel

- SSL Encryption
- Server
 - stunnel -p stunnel.pem -d 24801 -r 127.0.0.1:24800
 - synergys -a 127.0.0.1 -c synergy.conf
- Client
 - stunnel3 -c -d 127.0.0.1:24800 -r 192.168.0.101:24801
 - synergyc 127.0.0.1



stunnel.pem

- openssl genrsa -out serverkey.pem
 - openssl req -new -x509 -key serverkey.pem -out servercert.pem -days 365
 - cat serverkey.pem servercert.pem > stunnel.pem
 - openssl gendh 512 >> stunnel.pem
- 

STunnel with Authentication

- Requires
 - CA
 - CA signed public keys
 - Server must have public key of all clients
- Stunnel -f -v3 -a trusted_keys/ -p stunnel.pem -d 24801 -r 127.0.0.1:24800
- stunnel3 -f -v3 -A ./cacert.pem -p clientkeycert.pem -c -d 127.0.0.1:24800 -r 192.168.0.103:24801