**GUIs & Security**

Unix/Linux use X Windows
client/server design over TCP/IP

Normal Config
- Single user mode or Networked mode

**Single User Mode**

![Diagram of single user mode](image)

- Network access is blocked

**Networked Mode**

![Diagram of networked mode](image)

- DISPLAY variable tells server which client to send GUI data to/from

---

**Notes:**

- 2nd computer
- Monitor
- Keyboard
- Mouse
XClient

Laptop

Send GUI data to/from

:0.0 is the native monitor

host: num, sub are remote monitors

localhost: 10.0 for example

Using ssh to do X11 forwarding

```bash
ssh -Y username @ host

-Y enables full X11 forwarding
-X does old X11 forwarding (old systems)
```

echo $DISPLAY

```
DISPLAY = :0.0

DISPLAY = localhost :10.0
```

Processes & Linux

PID every process has a numeric identifier
Command command-line used to start process

```
kill needs PID
killall needs command
```

TTY terminal associated with process
all logins are given a unique terminal

```
who | shows all current logins
```

Protecting Info on the Internet

Encryption

Bad encryption -> no encryption
WEP, WPA2, anything based on RC4 can be broken if the initial exchange & sufficient packets are seen.

AES, Serpent, Twofish

Bad keys/key exchange → no encryption
Good key exchange is Diffie-Hellman
Anyone intercepting traffic cannot recover key
New key generated for every session
Used by:
  SSH
  SSL with Perfect Forward Security

Regular SSL uses a key exchange that could be broken if someone retrieves the server’s private key

Cryptanalysis is a whole area focused on analyzing encryption & finding weaknesses