

9P IS PERFECT FOR THE IoT

Paris - 2024-12-04

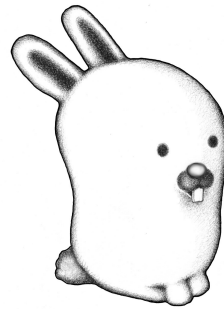
Edouard Klein

Open Source Experience

9P ?

Plan 9

Transistor, Laser,
CCD, Shannon,
Unix, C, etc.



Build a UNIX out of little systems,
not a system out of little UNIXes

Inferno



Hayes 2024: Plan 9 - Theorizing The
Abandonment of The UNIX Design

IoT ?

IN IOT, THE 8
STANDS
FOR SECURITY



REMEMBER MIRAI ?



Up to 1Tb/s

scanner.c::add_auth_entry

IoT ARCHITECTURE

Web app code written by a junior dev, for Ruby on Rails 5,
with comments like `# Don't run this in prod lol`

Privileged web
server running
with no isolation



Non-mainline
Kernel, last
updated: 2018

login: root
pwd: 123456

Custom musl libc,
3182 commits
behind master

9P DESIGN PHILOSOPHY

Local or remote, all fs access through 9P

EVERYTHING is a file

Per process isolation (namespace)

9P

Qemu

WSL

v9fs

Authentication and
encryption baked in

```
size[4] Tversion tag[2] msize[4] version[s]
size[4] Rversion tag[2] msize[4] version[s]

size[4] Tauth tag[2] afid[4] uname[s] aname[s]
size[4] Rauth tag[2] aqid[13]

size[4] Rerror tag[2] ename[s]

size[4] Tflush tag[2] oldtag[2]
size[4] Rflush tag[2]

size[4] Tattach tag[2] fid[4] afid[4] uname[s] aname[s]
size[4] Rattach tag[2] qid[13]

size[4] Twalk tag[2] fid[4] newfid[4] nwname[2] nwname*(wname[s])
size[4] Rwalk tag[2] nwqid[2] nwqid*(wqid[13])

size[4] Topen tag[2] fid[4] mode[1]
size[4] Ropen tag[2] qid[13] iounit[4]

size[4] Tcreate tag[2] fid[4] name[s] perm[4] mode[1]
size[4] Rcreate tag[2] qid[13] iounit[4]

size[4] Tread tag[2] fid[4] offset[8] count[4]
size[4] Rread tag[2] count[4] data[count]

size[4] Twrite tag[2] fid[4] offset[8] count[4] data[count]
size[4] Rwrite tag[2] count[4]

size[4] Tclunk tag[2] fid[4]
size[4] Rclunk tag[2]

size[4] Tremove tag[2] fid[4]
size[4] Rremove tag[2]

size[4] Tstat tag[2] fid[4]
size[4] Rstat tag[2] stat[n]

size[4] Twstat tag[2] fid[4] stat[n]
size[4] Rwstat tag[2]
```


PER PROCESS NAMESPACE

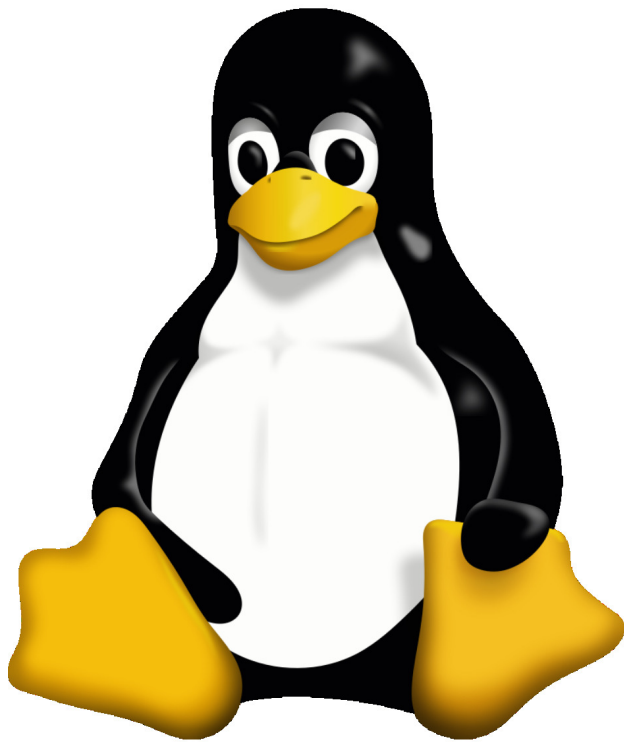


Each process
in its own
namespace

If one falls, the others don't.
The attacker gains no privilege.
This is containerization.*

* But in 1987

LINUX'S 'EVERYTHING' IS A FILE



/dev/sd*
/dev/mem
/proc

/dev/stdout

/dev/input/js0

/dev/dsp

/dev/stdin

LINUX'S 'EVERYTHING' IS A FILE

`/dev/stdout`
`/dev/fb*`
`ioctl()`

`ioctl()`
`/dev/video1`
`/proc`



`/dev/input/js0`

`/dev/video0`
`ioctl()`

`/dev/stdin`
`/dev/input/event0`
`/dev/input/event...`

`ioctl()`

`/dev/input/mouse0`
`/dev/input/mouse...`
`/dev/input/mice`

LINUX'S 'EVERYTHING' IS A FILE

`ioperm()`

`mmap()`

`dev/stdout`
`/dev/fb*`
`/dev/ari*`
`ioctl()`
`/dev/video1`
`/proc`

`io_uring*`
`ioctl()`



`/dev/input/js0`

`/dev/video0`

`/dev/stdin`

`/dev/input/event0`

`/dev/input/event...`

`ioctl()`

`/dev/input/mouse0`

`/dev/input/mouse...`

`/dev/input/mice`

`ioctl()`

`evdev`

`evdev`

INFERNO'S EVERYTHING IS A FILE

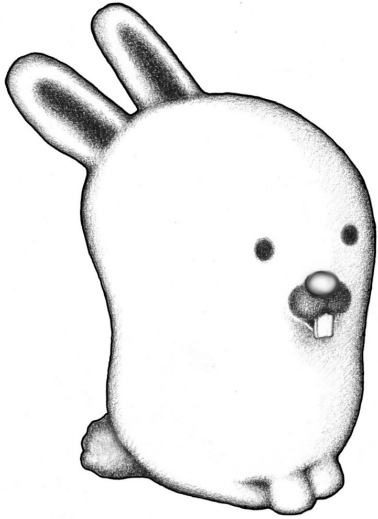
/cmd

/dev/fpga*
/dev/eia*
/dev/usb*
/dev/gpio*

/net /dev/snarf
/env /dev/time

/dev/sd*
/prog

/dev/draw/*



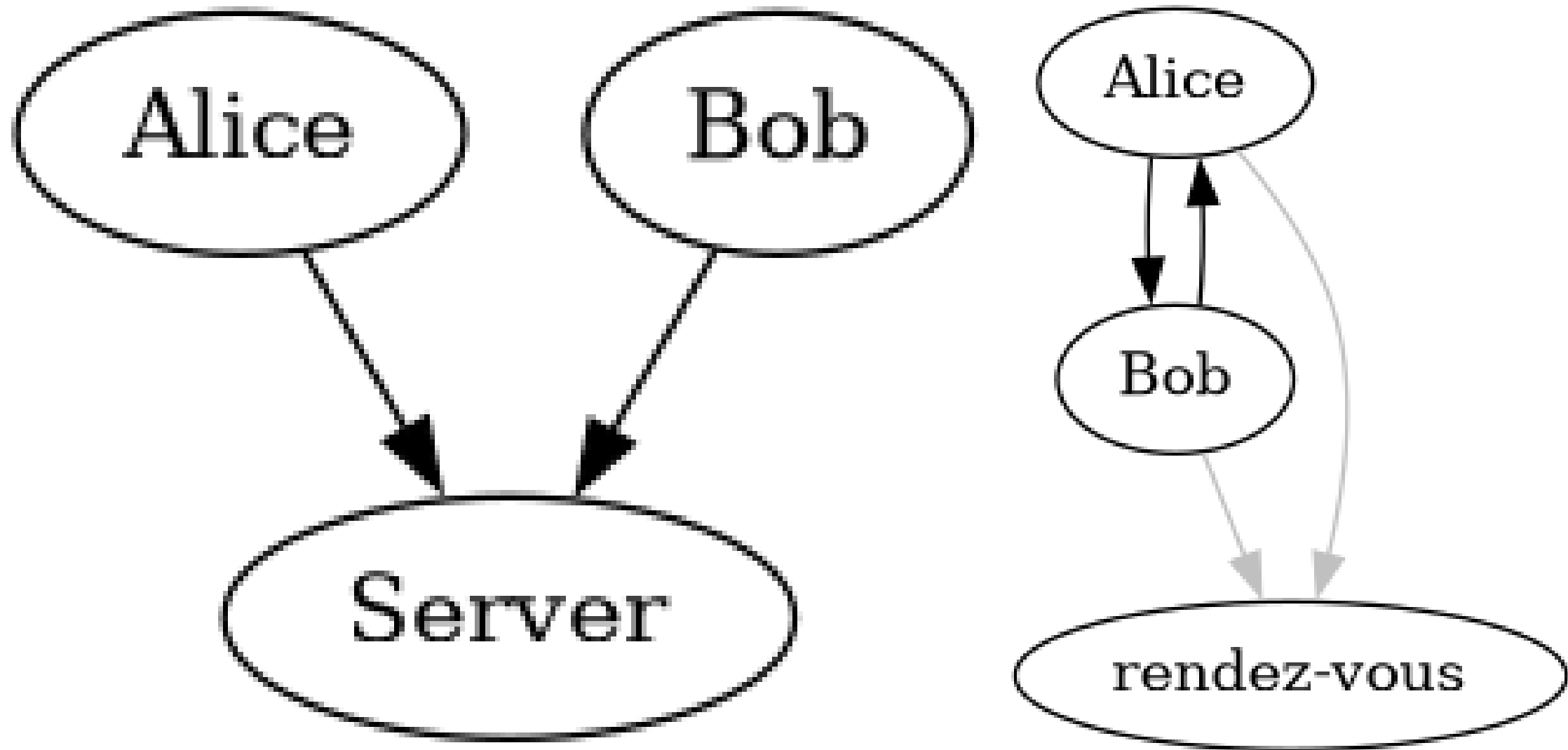
/dev/audio /dev/cons /dev/touch* /dev/pointer
/dev/audioctl /dev/keyboard

caphash /dev/user
capuse

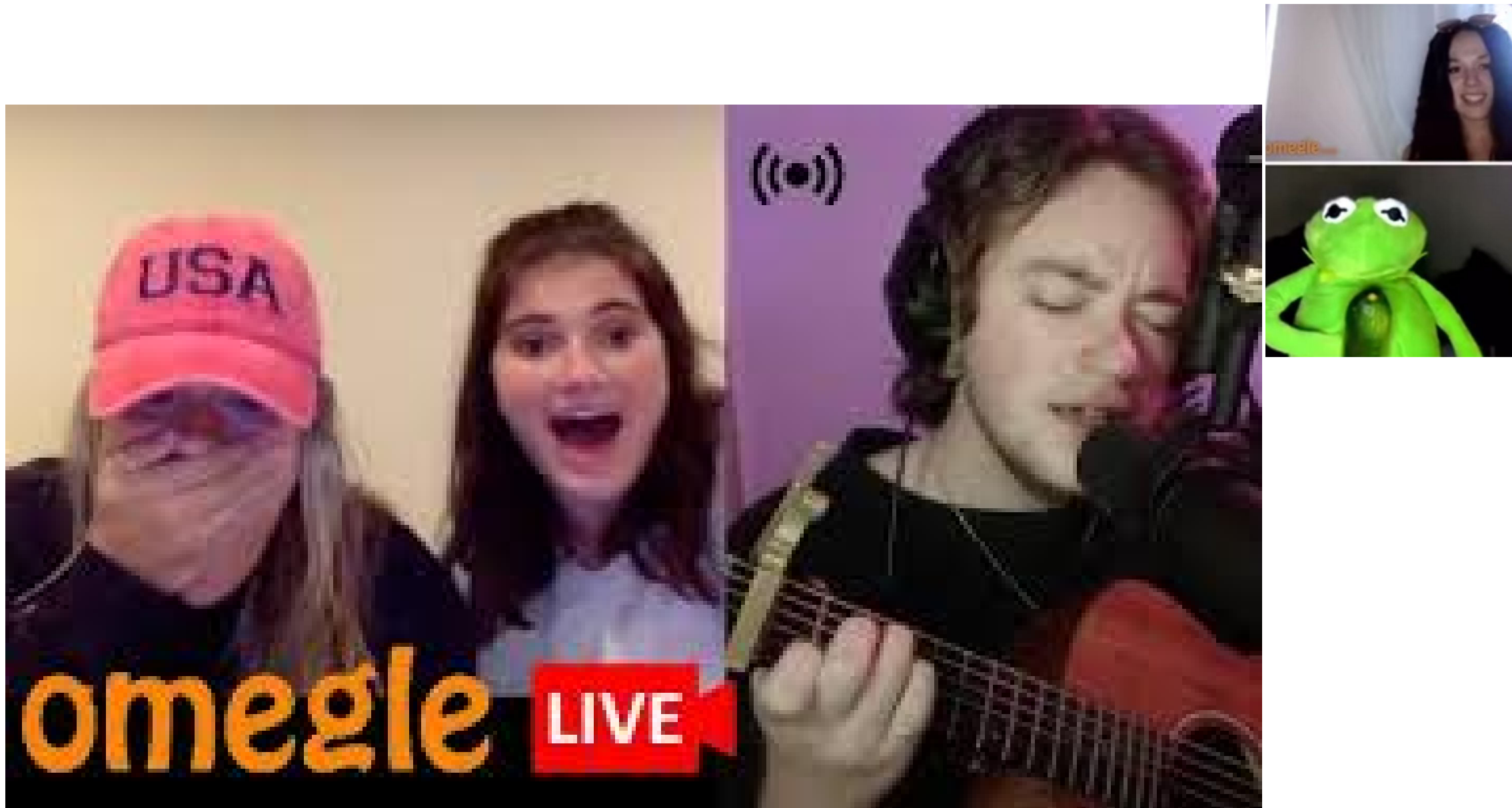
DEMO: VPN

Wireguard: 100k LoC

DEMO: OMEGLE



OMEGLE EXPERIENCE



9P vs. HTTP

	HTTP	9P
Encryption	Transport problem	Transport problem
Auth	Bolted on the layer above	Auth
Access control	Bolted on the layer above	Walk/Open/Attach/Clunk/Stat/Wstat
Content Access	GET	Read
	PUT, POST, PATCH	Write/Create
	GET	Walk
	DELETE	Write/Remove
	GET/HEAD	Stat/Wstat
	OPTIONS	Open, kinda

LESS IS MORE

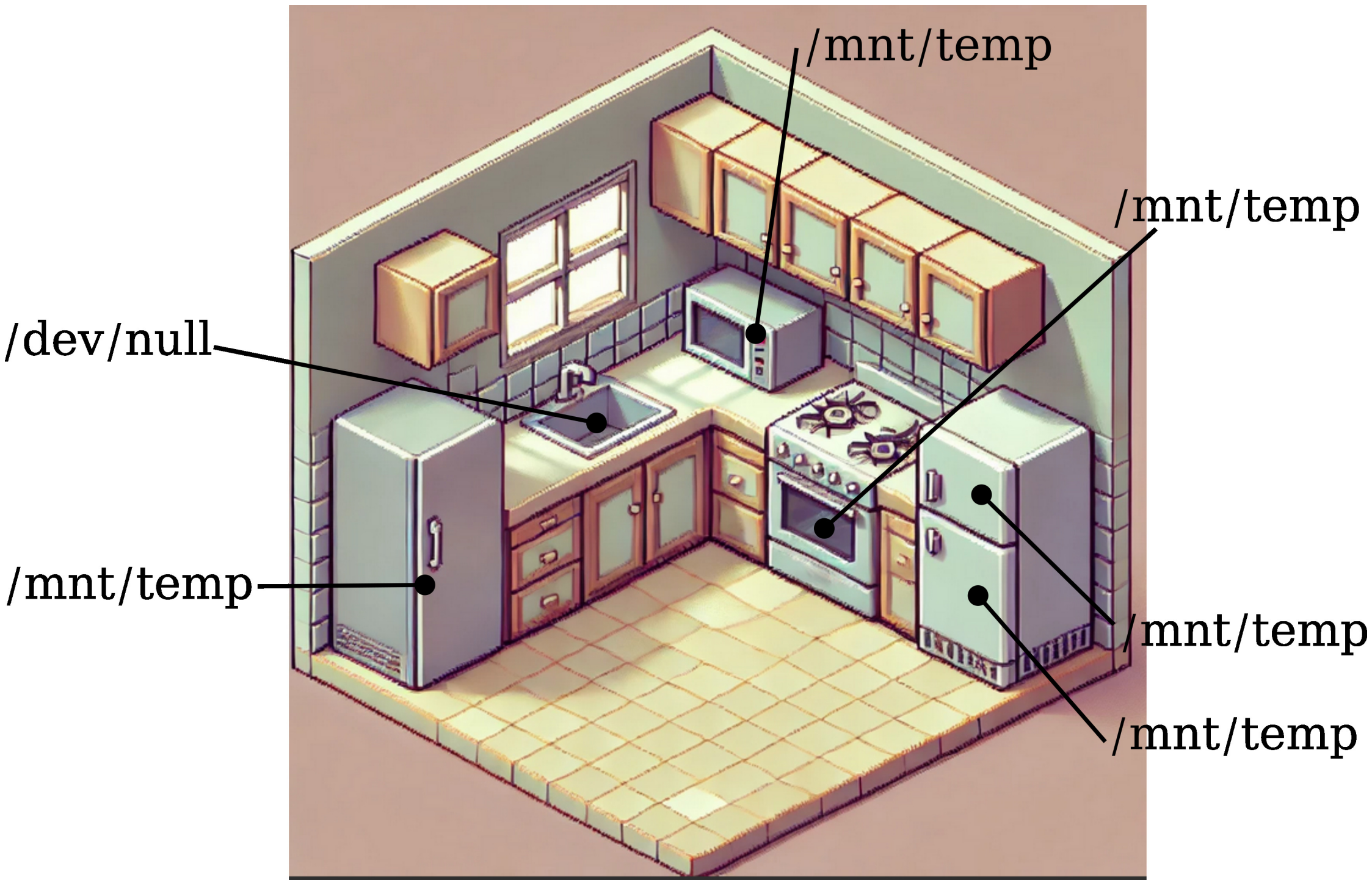
ZigBee

BLE

Runs on a brick

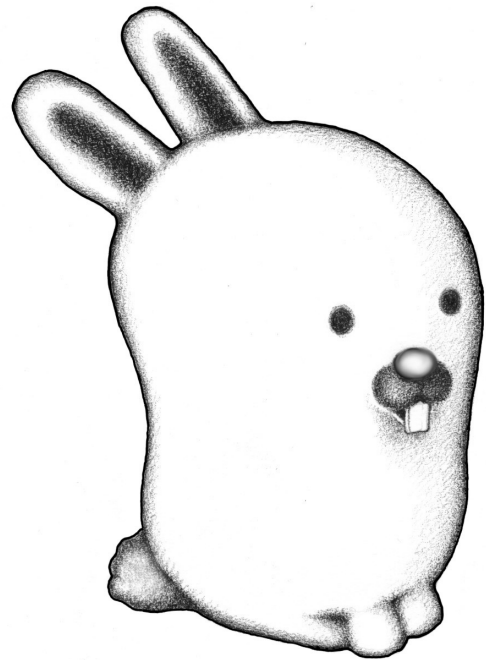
Good ol' serial

EXAMPLE



PARTING WORDS

iwp9.org 22-24 may
2025 PLEASE COME



Thank you

edk@beaver-labs.com

the-dam.org