Hosting your own media and other homelab shenanigans

Morgan Gangwere, Shea Polansky
SCaLE 18x

Morgan: whoami

- I hack things
- Internet Fox
- I yell at people: @indrora
- Also on mastodon: @indrora@vulpine.club
- By day: I describe solutions to problems people have come up with in words other people can understand
- By night, I do stupid things with computers for fun.

Shea: whoami

- Also hacks things
- Internet Dragon
- Breaks things for money
- Occasionally posts @0x5ca1e5
- Occasionally posts longer things at polansky.co
- Tells people they're wrong
- By night, also does stupid things with computers for fun

The following content is our own. These are our words, not those of our respective employers.

Don’t ask about our work.

Disclaimer

> “Computers were a mistake”

- Author unknown

Basics

What is a homelab?

Homelab
/hōm-lab/

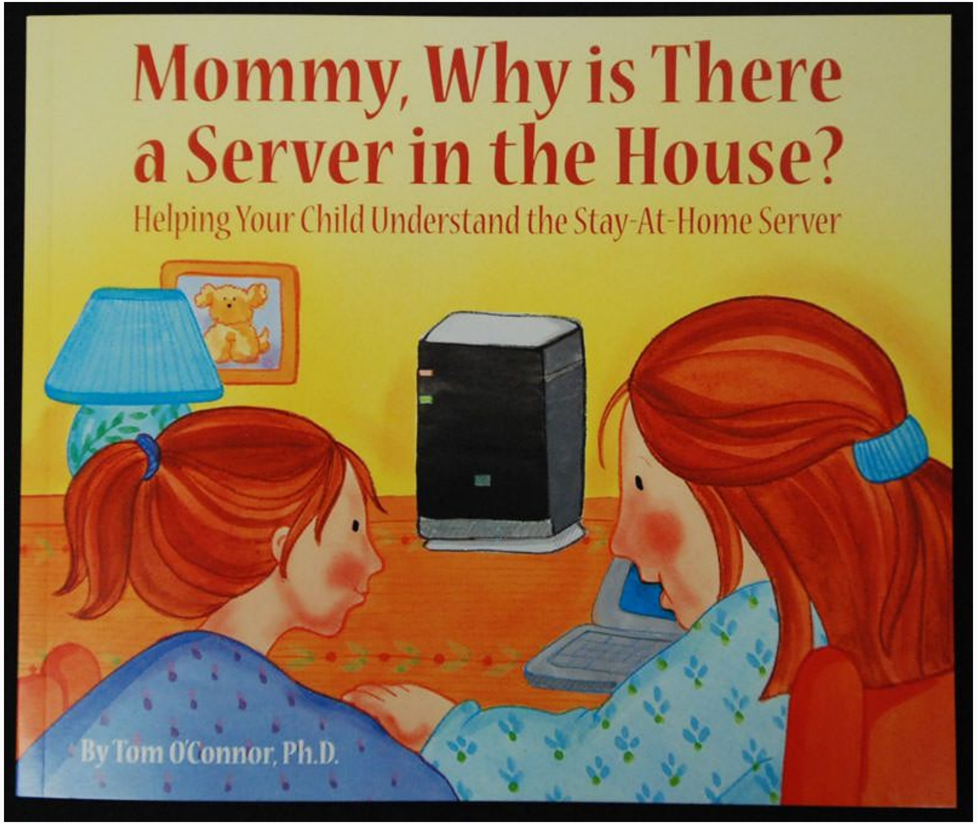
- A justification for a higher power bill and a better internet connection
- A fantastic way to learn how to admin things
- 100% home-grown, organic, cruelty-free technical debt

https://redd.it/bsxz2e

Why build a homelab?

Why build a homelab?

- “Privacy” is a common one
  - Generally considered a good one, even.
- Learning how the Big Kids do things in a sandbox is a good way to do it
  - The only person who’ll cry is you, not you *and* your entire management chain
- Autonomy over any number of things
  - How your data is managed
  - How your code is handled
  - How your downtime is bad


Mommy, Why is There a Server in the House?
Helping Your Child Understand the Stay-At-Home Server
By Tom O'Connor, Ph.D.

It’s also an excuse to get the greatest book of all time and read it as a bedtime story to your and/or your friends’ children.

By the way...

...this is also Small Business IT 101

If you do this for a living, you'll be very familiar with some of what we're going to tell you today.

If you *want* to do this for a living, this is how you get marketable skills.

Things you can do at home

“You can build a colo from the things you find at home”

Scenario 1: hosting your stuff

The typical file and media server

Storage:

- Learn the horrifying things RAID controllers do
- Put a bunch of disks together
  - Software vs Hardware RAID
- There's lots of things to explore:
  - ZFS: The filesystem for every atom
  - XFS: The 90s called and want netflix
  - ReFS: REdmond's new Filesystem

File Sharing:

- The sane use Samba
  - Supported by all clients
  - Sane security/permissions model
- The insane use NFS
- The more insane use Tahoe LAFS/Gluster/Ceph
- There's also Apple File Protocol for the fruit-inclined
  - Actually serving this on Linux/BSD is… fun. Consider Samba instead.

Streaming your Grandparents can use

Now that you've got all that storage, you need a nice interface to stream your Linux Distros

All-in-one Servers:

- Plex: Commercial all-in-one media server
- Emby: "Open source" all-in-one media server
- Jellyfin: Actually open source fork of Emby

You're mostly limited by disk space, unless you're doing a lot of transcoding—that's CPU bound.

Specialized Servers:

- Subsonic: audiophile music streaming server
- Kodi: GUI for streaming media
  - Integrates well with Emby/Jellyfin
  - Lots of customization
- Universal Media Server: Dead simple DLNA server
- Other software can make the server download things automagically

Scenario 2: The personal proxy

A ~~proxy~~ cache, filter, etc.

You can easily

- Cache Steam content for faster downloads in your family
- Block ad/tracking domains with a DNS system
- Cache web content if you're on a slow network link (i.e. stuck in the 90s)

These all have different needs:

- Steam and other content caches need a lot of either RAM or disk, or both
  - Don't let the internet touch it though
  - https://is.gd/jOKTiN
- DNS blockers and caches can be done with barely any resources at all
  - Some beneficial things are blocked however, since privacy folk go a little nuts.
  - Pi-Hole is a good example of this

Personal VPN

Storage:

- Don’t worry
- Most cheap routers have more storage than you need
- Most of the issue is network bandwidth
- If you’ve got a lot of that, CPU will be your next bottleneck
    - You can run this on your server if necessary
    - (but requires some router tinkering)

The actual magic:

- OpenVPN
- Wireguard
- ZeroTier*
- Tor

Scenario 3: Tomfoolery

Home Automation

Make your lights turn off from your phone, *without* the cloud

Automation servers:

- HomeAssistant is the standard choice
  - Python Based, runs on anything
  - Has support for everything including the kitchen sink
  - (…if the sink has a network connection)
- OpenHAB is an alternative
- Both allow remote control and automation
- Minimal server resources required

https://youtu.be/BI3qaJqKtEQ

Stuff they can talk to:

- Anything ZWave or ZigBee
  - Dongle or bridge required
- Philips Hue/Samsung SmartThings
- Alexa/Google Assistant
- HomeKit
  - HA can emulate a Home Hub or talk to a real one
- Arbitrary HTTP/MQTT/etc hosts
- Lots and lots and lots of other stuff
  - home-assistant.io/integrations

Random Home Automation Ideas

Lots of stuff your partner(s)/roommate(s) won't be nearly as enthusiastic as you about

- Easy: Add voice control to something that doesn't already have it
  - Emulated Hue Bridge
  - <voice assistant here>
- Easy: Turn lights on at sunset
  - HomeAssistant Automation Example
- Easy: Turn off the AC when you leave
  - Presence Detection + Climate Controller
- Fun: turn your lights blue when the International Space Station is above
  - ISS Location Integration
- Harder: Use OpenCV to detect faces on a front door camera
  - OpenCV Integration
- Nerdcore: APRS presence detection
  - APRS Integration
- All the notifications
  - Telegram message when a package is delivered?
  - PushBullet when someone rings your doorbell?
    - ...and only if you're not home?
- Web dev mode: Custom web UI theme/cards
  - UI System Info

Enterprise Stuff

Want to get that high end Cisco certification?

Want to be VMWare ESXi certified?

Want more redundancy than the department of redundancy department’s redundant department in the redundancy department’s redundant second office?

Ever wanted to explore Infiniband?

Ever thought to yourself “I have too much free time”?

🎶Do you wanna run a colo?🎶

The possibilities are endless!

A note about hosting stuff for other people

Or: how to not get ping'd on your day off by annoyed loved ones

You may be tempted to share your hobby by hosting stuff for other people:

- Maybe you want to let your partner watch your movie collection on your TV
- Maybe you want to let your mom backup her pictures to your unnecessarily massive storage array

This is great! But: **When you host something for others, they will have expectations about uptime and availability**

- Communicate uptime expectations
  - If it's going down for maintenance, tell them
- If you're letting someone else use something, don't tinker with it - make a copy and test on that
- Try to proactively monitor and keep good backups

<u>Basically, treat it like the homelab's equivalent of production</u>

… A less fun note about hosting other people's content

Sometimes, your friends are great. They chip in for the power bill, slip you another 10TB NAS disk. Take you out for `$DRINK_OF_CHOICE`.

Other times your friends end up getting raided by the FBI, DHS, etc and then those friendly loving federal agents come knocking on your door.

Keep that in mind. This happens on occasion. Ever been deposed by the SEC and the FBI at the same time?

Hardware

Some terminology

- A U is 1.75in. This is the unit in which servers are measured.
- Networks are measured as theoretical throughput in Gbit/S
- Rack equipment comes in two other dimensions:
    - Half Rack: roughly 9.5in wide, somewhat common in audio equipment
    - “Full Depth” to “Switch Depth”: 1 metre or 30cm, give or take.
    - Switch Depth cases can often be mounted “on their ears”
    - Full depth equipment **MUST** be supported on rails.

Power & stuff

- Observe safety precautions with electricity
- Just because you can put a 30A plug onto a 15A circuit doesn't mean you *should* or that it won't *catch fire or worse*.
- ***Never circumvent safety equipment because you want the blinkies***
  - Electrical fires are NOT fun. Your insurance will NOT be happy when they find that you've done something stupid
- ***Never chain power strips, they will lead you to fire***
- If you need to do electrical stuff, *get an electrician to do it* or be judicious in your use of tested equipment.

https://www.edn.com/what-caused-this-outlet-strips-catastrophic-failure/

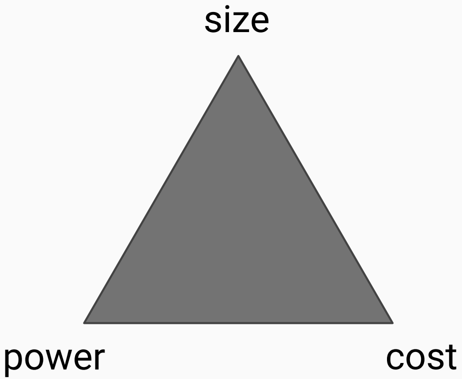
Servers: from paperback book to 4U beasts

There’s a lot of options, but take into consideration the following:

The more power, the higher the bill

The older, the less efficient, but less $

The bigger the more expandable...



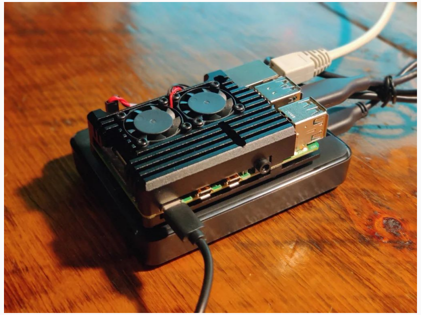
The best servers are on your desk

Desktop PCs are highly optimized for a fairly good balance of bang for buck performance and power consumption.

There is no shame in using smaller “thin client” machines that are common today.

(Note: RasPis are a mixed bag)

https://redd.it/8d2g90



https://redd.it/eknip3

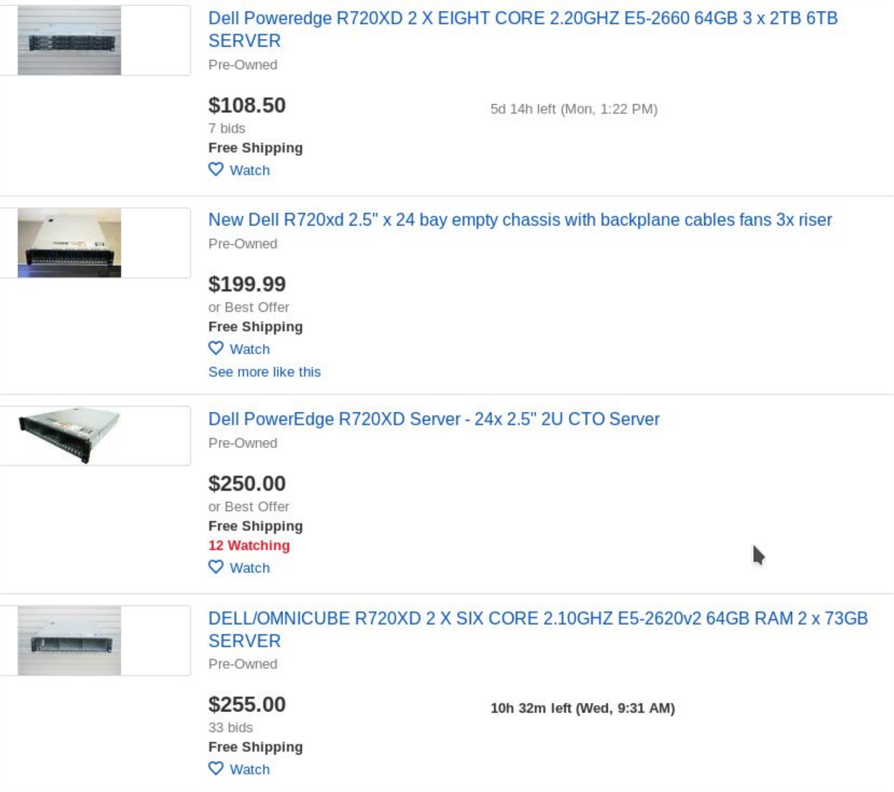
https://redd.it/ejou3v

There is 1&2U rack equipment everywhere

Enterprises throw out equipment all the time, and often there are plenty of cheap dual and single Xeon machines on ebay, even craigslist

Getting several generation old rack gear can be a really cheap way to get into things

If you keep an ear out, you can find the leftovers of datacenter replacements; knowing that a city hosts $bigco servers means there's going to be lots of hardware nearby...



Dell Poweredge R720XD 2 X EIGHT CORE 2.20GHZ E5-2660 64GB 3 x 2TB 6TB SERVER
Pre-Owned
$108.50
7 bids
Free Shipping
♡ Watch
5d 14h left (Mon, 1:22 PM)

New Dell R720xd 2.5" x 24 bay empty chassis with backplane cables fans 3x riser
Pre-Owned
$199.99
or Best Offer
Free Shipping
♡ Watch
See more like this

Dell PowerEdge R720XD Server - 24x 2.5" 2U CTO Server
Pre-Owned
$250.00
or Best Offer
Free Shipping
12 Watching
♡ Watch

DELL/OMNICUBE R720XD 2 X SIX CORE 2.10GHZ E5-2620v2 64GB RAM 2 x 73GB SERVER
Pre-Owned
$255.00
33 bids
Free Shipping
♡ Watch
10h 32m left (Wed, 9:31 AM)

Storage

Disks come in three basic flavors:

- SAS: Serial Attached SCSI
- SATA: Serial AT Attachment
- U.2: aka NVMe, can use SAS connectors in 2.5in form

Don’t mix SATA and SAS on a RAID.

https://redd.it/bk8khf

Networking

Sane:

- Most hardware already has gigabit
- Older Cisco catalyst switches, etc. are great
- Everyone has a favorite vendor and a reviled, hated vendor
- Everyone agrees that Intel still has some of the best 1000baseT NICs

Insane:

- Chelsio produces cheap ($50 used) dual SFP+ 10GbE cards
- SFP+ 10GbE fiber adapters are cheap
- MikroTik and QNAP make 10GbE switches

Sundry:

- Cat6 and fiber are really cheap.
- There’s a lot of non-2.4Ghz wireless networking

Hardware resources

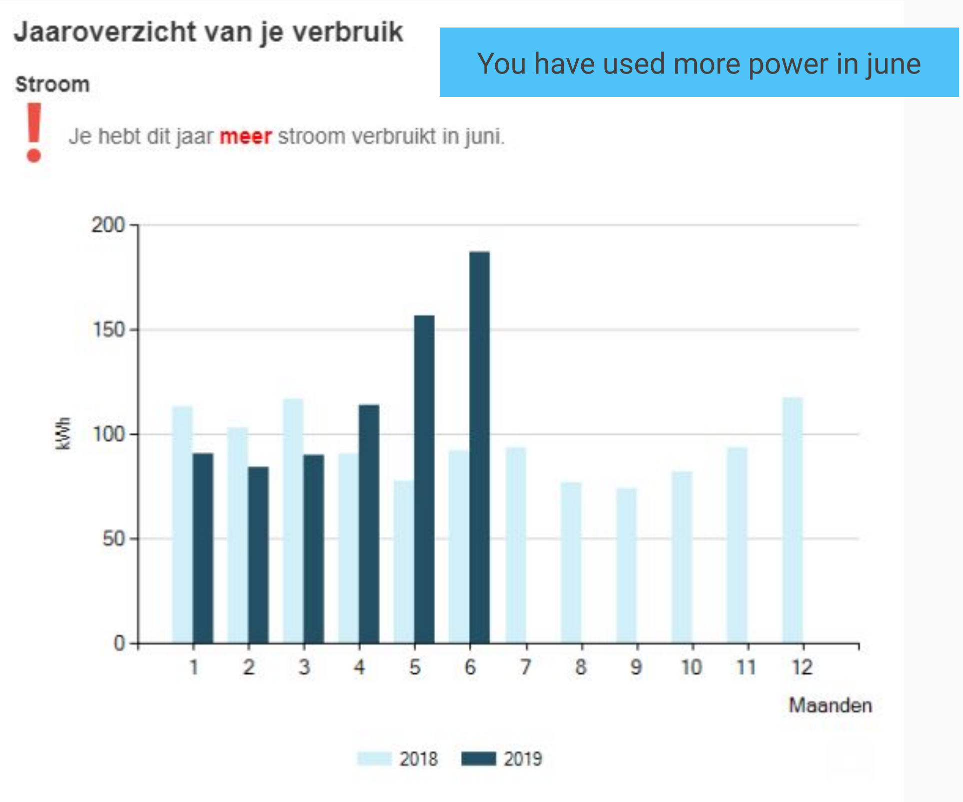
- Intel’s ARK is an archive of the processor information
  - Use it as a reference to compare systems, power usage, etc.
- Dell/HP/etc. all keep records of their previous generations
  - Find the power hogs, or hone down in on specific features you need
- Backblaze has been keeping track of the health of their disks for 10 years
  - All disks must die. They know which ones die early.

Cheap & Free can have a downside

Enterprise equipment, while sometimes dirt cheap to free, can be a costly gamble.

The commodity 2U server is going to, idling, run you between $50-100 a month, depending on where you live.

Consider the cost of running a 3-400W space heater all the time as the cost of running enterprise equipment at idle.



Jaaroverzicht van je verbruik

Stroom

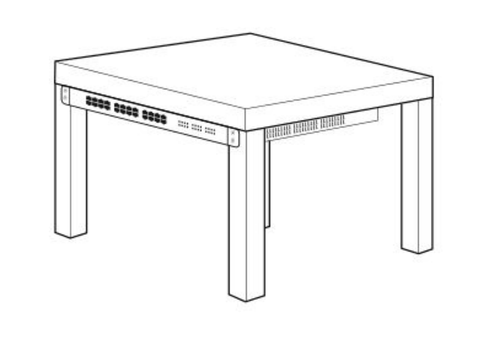
Je hebt dit jaar **meer** stroom verbruikt in juni.

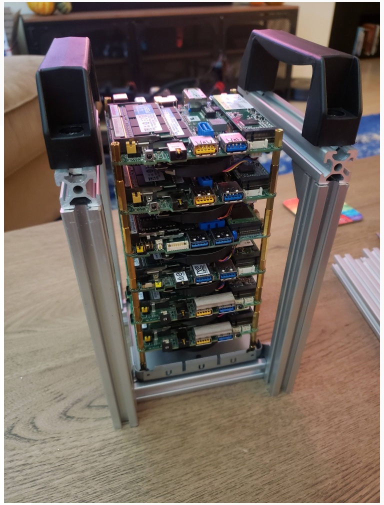
You have used more power in june

https://redd.it/cdeifp

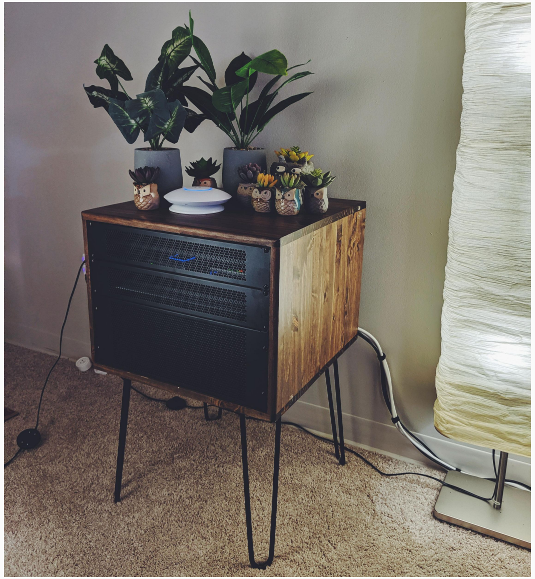
Racks 🦌

The standard 19in rack is so ubiquitous that you will find them littering ebay, craigslist, etc. until your eyes cross. However, if you look around, there's lots of options floating around





https://redd.it/dr2ipp



https://redd.it/cjfrdd

What do we homelab?

Exercise

What could you do with your homelab?

You said email.

I know you said email.

Everyone says email

“Don’t host your own email”

- John “Warthog9” Hawley

Self-hosting your email is Mastermind hard

Sure, actually putting in the infrastructure to send email is simple, but getting it into someone's incoming mail spool and not being considered a spam bot is nigh on impossible

- Basically every ASN used by home users is blocklisted by spamhaus
- Basically every good cloud ASN is too

Google has intense and WILDLY varying requirements for acceptable email:

- DKIM, SPF, DMARC configuration
- A, MX records
- AAAA sooner or later will be necessary
- PTR and rDNS configuration
- Rumors of DNSSec
- TLS on everything? Maybe?
- Hope NOBODY ever accidentally marks you as spam

Moving is hell, moving your email doubly so

In times of insanity, you just want your goddamn email to work.

Don’t host your own 🤬 email

Disasters

Things fail.

- RAID controllers are battery-backed
- Lurking bugs in disks, controllers, memory, processors
- PulseSecure: I don’t need to say more
- SPECTRE, Meltdown, etc.
- Etc. Etc.
- ZFS can be nasty
    - https://blog.tjll.net/when-disks-die-zfs/
    - There’s plenty of other tales

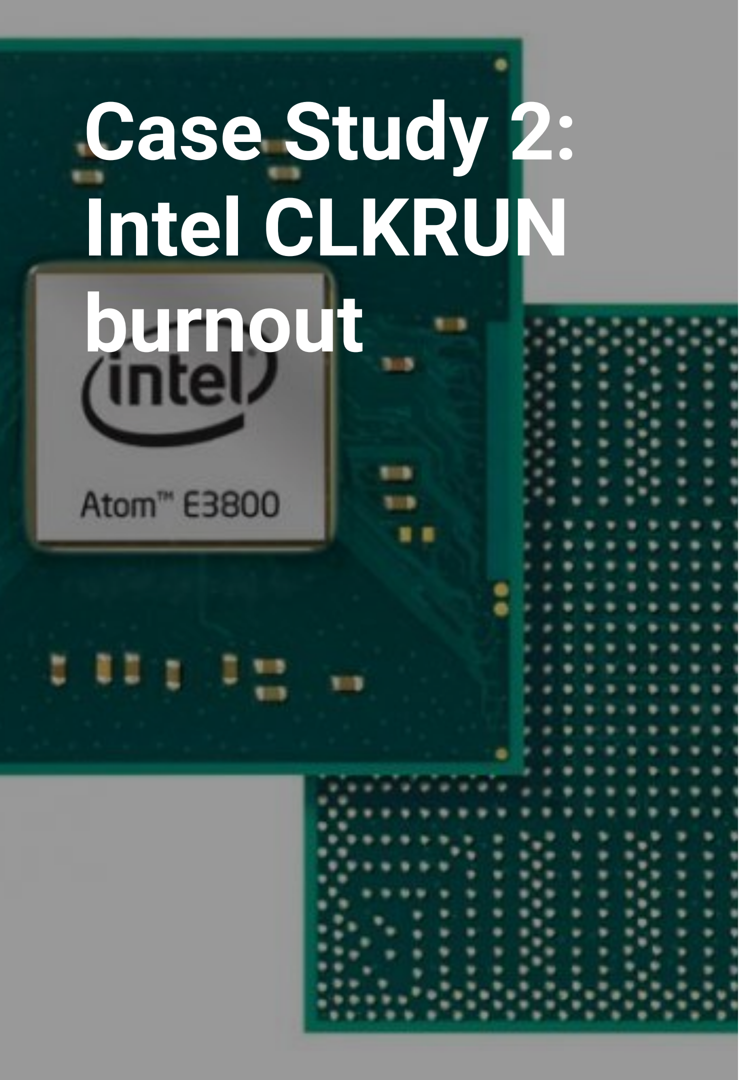
- Remember how I told you to not chain power strips?
    - Two words: Electrical. Fire.
    - Two more: Insurance Claim.
    - Oh god no: Premium Increases
- Burgalry, etc.
- Power outages, etc.
- The internet is not permanently up.

Case study 1: HPE SSDs

“The issue affects SSDs with an HPE firmware version prior to HPD8 that results in SSD failure at 32,768 hours of operation (i.e., 3 years, 270 days 8 hours). After the SSD failure occurs, neither the SSD nor the data can be recovered. In addition, SSDs which were put into service at the same time will likely fail nearly simultaneously.”

https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-a00092491en_us

Case Study 2: Intel CLKRUN burnout



*“**VLI89 System May Experience Inability to Boot or May Cease Operation***

***Problem**: Under certain conditions where activity is high for several years the LPC, USB (low speed and full speed) and SD Card circuitry may stop functioning in the outer years of use.*

***Implication**: LPC circuitry that stops functioning may cause* operation *to cease or inability to boot.”*

Case Study 3: Bdale Garbee and the fire

“Disaster Recovery Lessons I Hoped I'd Never Have to Learn”

The best-worst example of literal act of $DEITY, Bdale, a longtime sysadmin, was forced to evacuate his home and hope that it would survive.

It did not survive.

https://youtu.be/lJcnllq3VYY

Recovering from Disasters

Redundancy

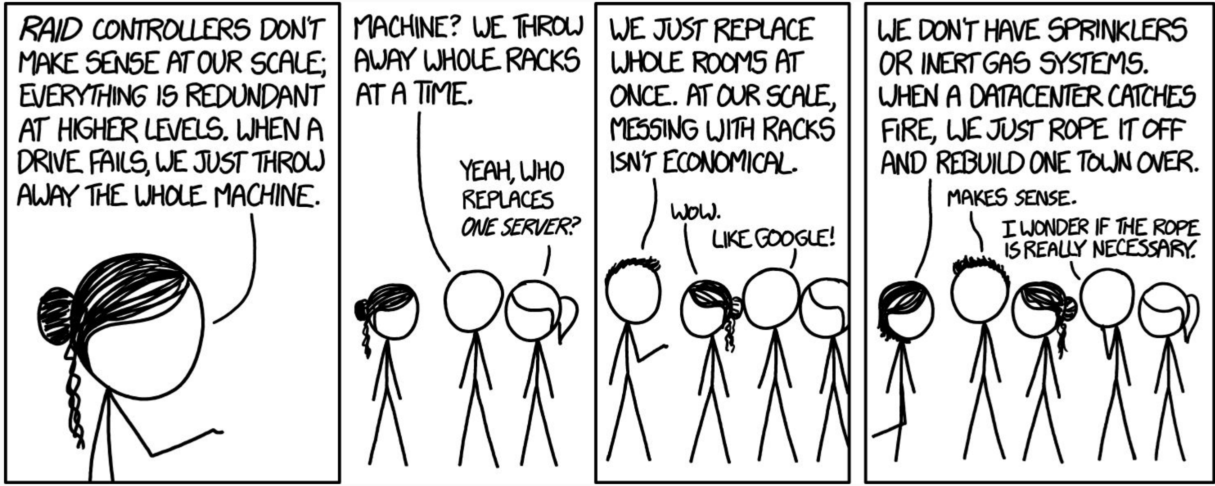
Disk Redundancy (AKA RAID)

RAID Disaster Recovery Considerations

- Look up how to do an array rebuild before your disk fails
  - Try it out before you put any data on the array
  - Add a file, remove a disk, wipe the header, put it back in, rebuild the array
- Setup alerting for when a disk fails
- That doesn't mean "wait until you notice your IOPS have dropped and wonder wtf happened"
- If you're using hardware RAID, figure out where you can get a replacement controller
  - (Ebay, probably)
  - You likely need the exact same model.
  - If it's really old, consider buying a spare preemptively
- `mdraid` can read *some* hardware RAID arrays
  - Test that *before* you need it if you can

Higher Level Redundancy

- High Availability (HA) file/data storage systems abound
    - FreeBSD HA Storage
    - Ceph HA Object Storage
    - Etc.
- HA networking/load balancing
    - HAProxy
    - LACP
- Fun to play with, a bit overkill for home lab
    - But overkill can be half the fun!


RAID CONTROLLERS DON'T MAKE SENSE AT OUR SCALE; EVERYTHING IS REDUNDANT AT HIGHER LEVELS. WHEN A DRIVE FAILS, WE JUST THROW AWAY THE WHOLE MACHINE.
MACHINE? WE THROW AWAY WHOLE RACKS AT A TIME.
YEAH, WHO REPLACES ONE SERVER?
WE JUST REPLACE WHOLE ROOMS AT ONCE. AT OUR SCALE, MESSING WITH RACKS ISN'T ECONOMICAL.
WOW.
LIKE GOOGLE!
WE DON'T HAVE SPRINKLERS OR INERT GAS SYSTEMS. WHEN A DATACENTER CATCHES FIRE, WE JUST ROPE IT OFF AND REBUILD ONE TOWN OVER.
MAKES SENSE.
I WONDER IF THE ROPE IS REALLY NECESSARY.

https://xkcd.com/1737/

Backups

Backups: You need them (too)

Say it with me: *RAID is not backup*.

- RAID is all about making sure your actions are reliably recorded to disk
- If you accidentally delete `irreplacable_photo.jpg`, your RAID controller will ensure it is reliably deleted across all of your disks
- This is where you need to restore from a backup

3-2-1 Rule

Three

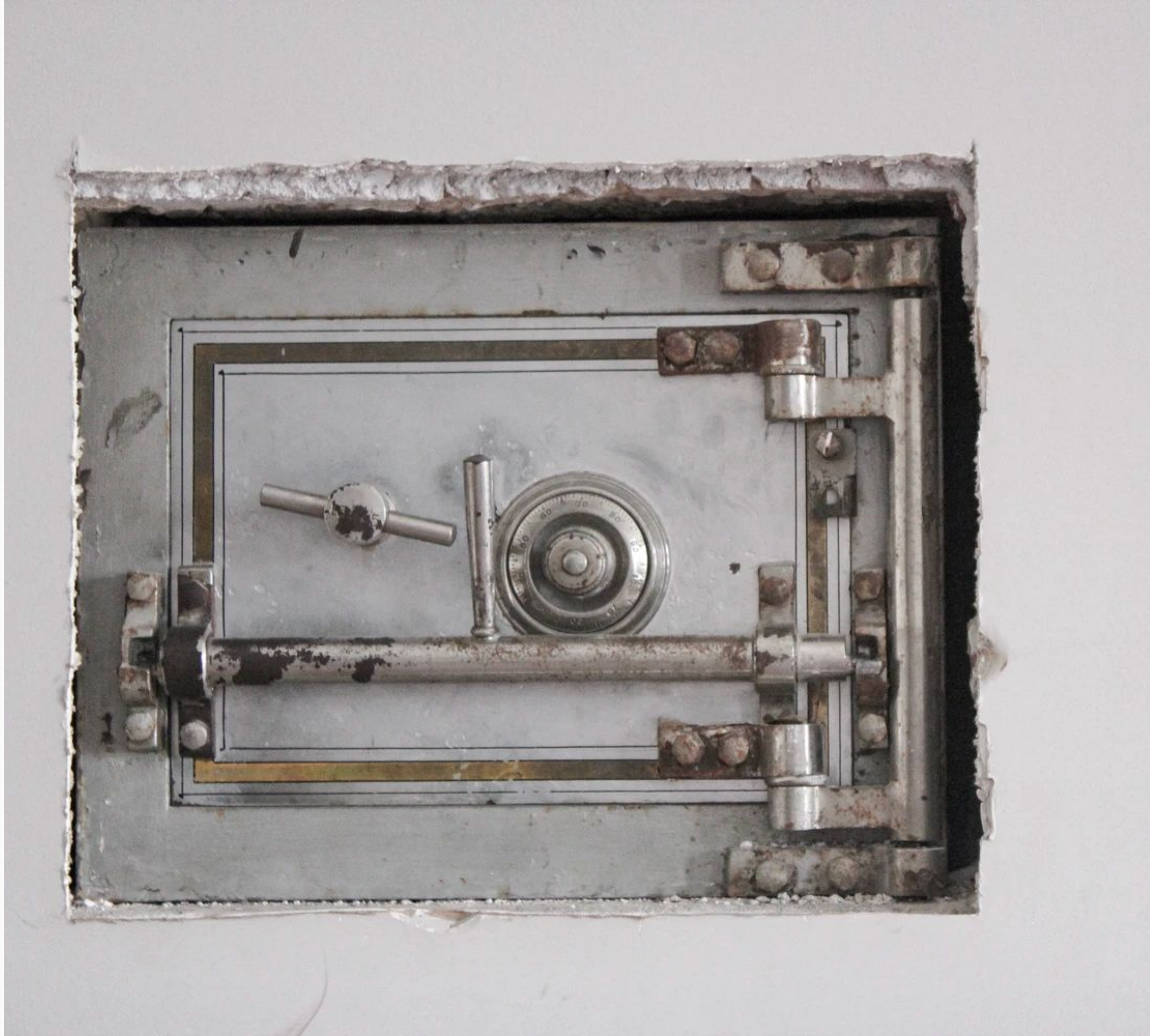
Copies of your data

Two

Formats

One

“Offline”



Types of Backup

Incremental

- Cheap (ish)
- First is big, second is delta
- Needs some fiddling

Complete (Snapshots)

- Good, but expensive (disk space)
- Can be full-system if need be

Complete (live mirror)

- `rm grandmas_last_words.divx` harder to recover from
- Immediate failure recovery easier
- Not a full system option.
- Must have a break-glass of some kind.

What to backup

“Must have”

- Content that you cannot recreate
- Content which is essential (e.g. tax stuff, password vaults, etc.)
- Infrastructure which is *bedrock*

These are good for snapshotted backups

“Could Recreate”

- Certain in-progress content
- “Well that sets me back a week”
- Infrastructure that is *fungible*

These are good for incremental & mirror backups

Backup Encryption

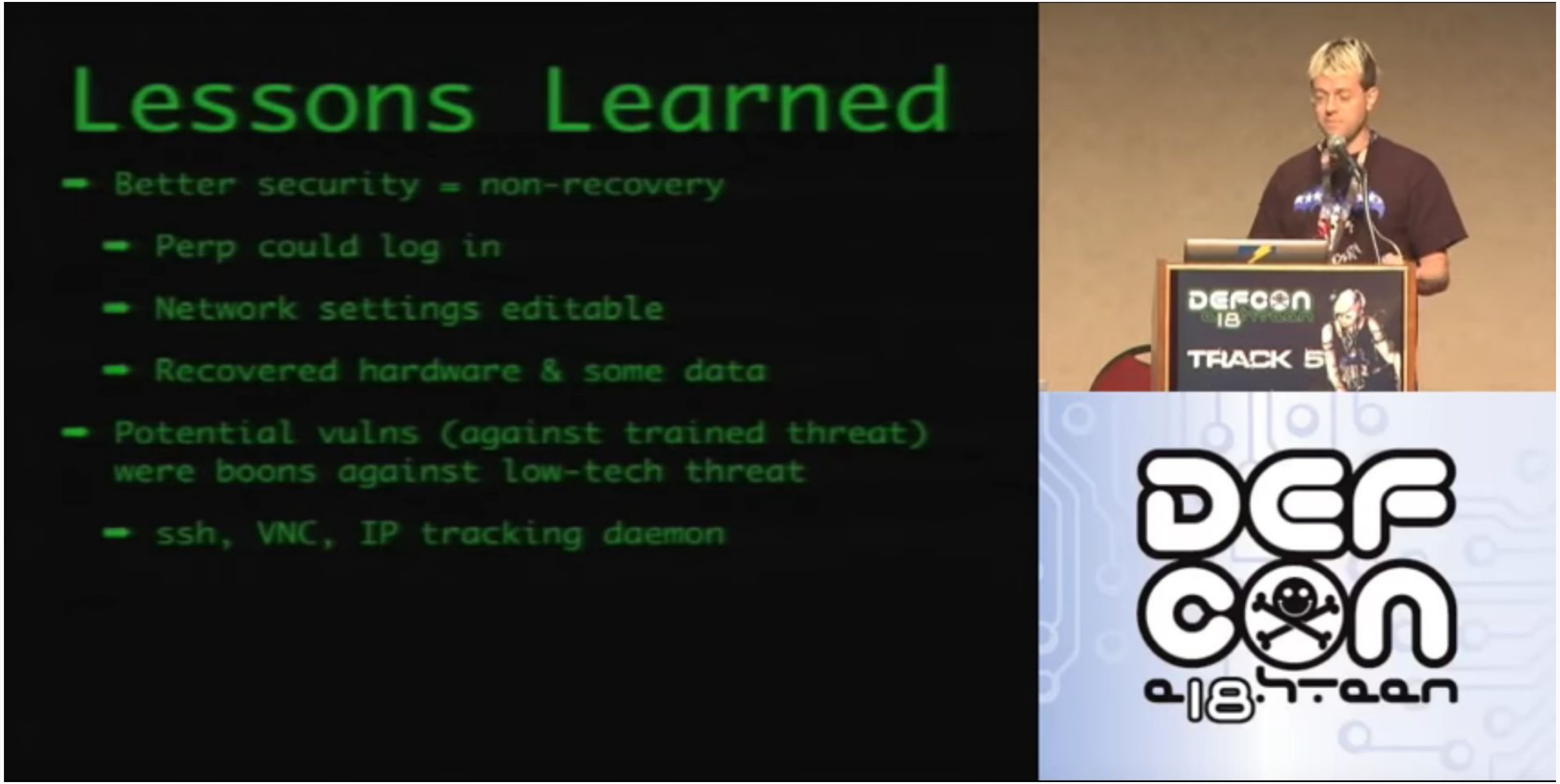
Do you

- Think your off-site backups are unsafe?
- Think your on-site backups are unsafe?
- Take your backup mechanism with you?
- Store backups in *other people's datacenters*?
- Have a break-glass mechanism

Then you should

- Evaluate the kind of encryption you need
- Consider how your backup solution will be affected (speed, size, etc.)
- Consider how you are handling data
- Consider partitioning your backups
- Explore physical security

This is not you. Consider your threat model.



Lessons Learned

- Better security = non-recovery
  - Perp could log in
  - Network settings editable
  - Recovered hardware & some data
- Potential vulns (against trained threat) were boons against low-tech threat
  - ssh, VNC, IP tracking daemon

https://www.youtube.com/watch?v=Jwpg-AwJ0Jc

Monitor your backups *and* test your restore process.

Monitor your backups *and* test your restore process.

- Much data has been lost that was “backed up”
- Your backup software will have some kind of status output. Monitor it.
  - HealthChecks.io is an easy way to get emails if something stops working
- *Also test restores*
  - If you have data backed up but don’t know the encryption key, you don’t have data backed up
- In general, ask yourself “what do I need to restore from a backup”
  - Work from “a computer, electricity, and a network cable” and go up from there
  - Look for circular dependencies, then fix them
    - Example: your LDAP server is on your hypervisor, and your hypervisor uses LDAP for login
    - Example: your hypervisor hosts your DHCP server, and your hypervisor has a dynamic IP

Break-Glass

A break-glass mechanism is a failsafe in order to maintain access in case everything has gone wrong or the usual mechanisms of authentication/access have failed

- What
  - Text file with root credentials and SSH keys
  - PGP keyring with no passphrase
- How
  - Flash drive stored in a safe place
  - Physically separate Yubikey with a PGP key
  - QR code with the raw key data
  - Something you can reconstruct later
- Why
  - *Because one day, you will go “oh fuck I just lost everything”*

Tools

Single Computer Backup

- Restic
  - Modular backends
  - Basically anything that speaks disk access
  - Fully encrypted locally, “zero knowledge” on hosting side
  - Deduplication but no compression
- Rclone
  - Similar to Restic
  - More backends
  - Deduplication/encryption optional

Multi-Computer Backup

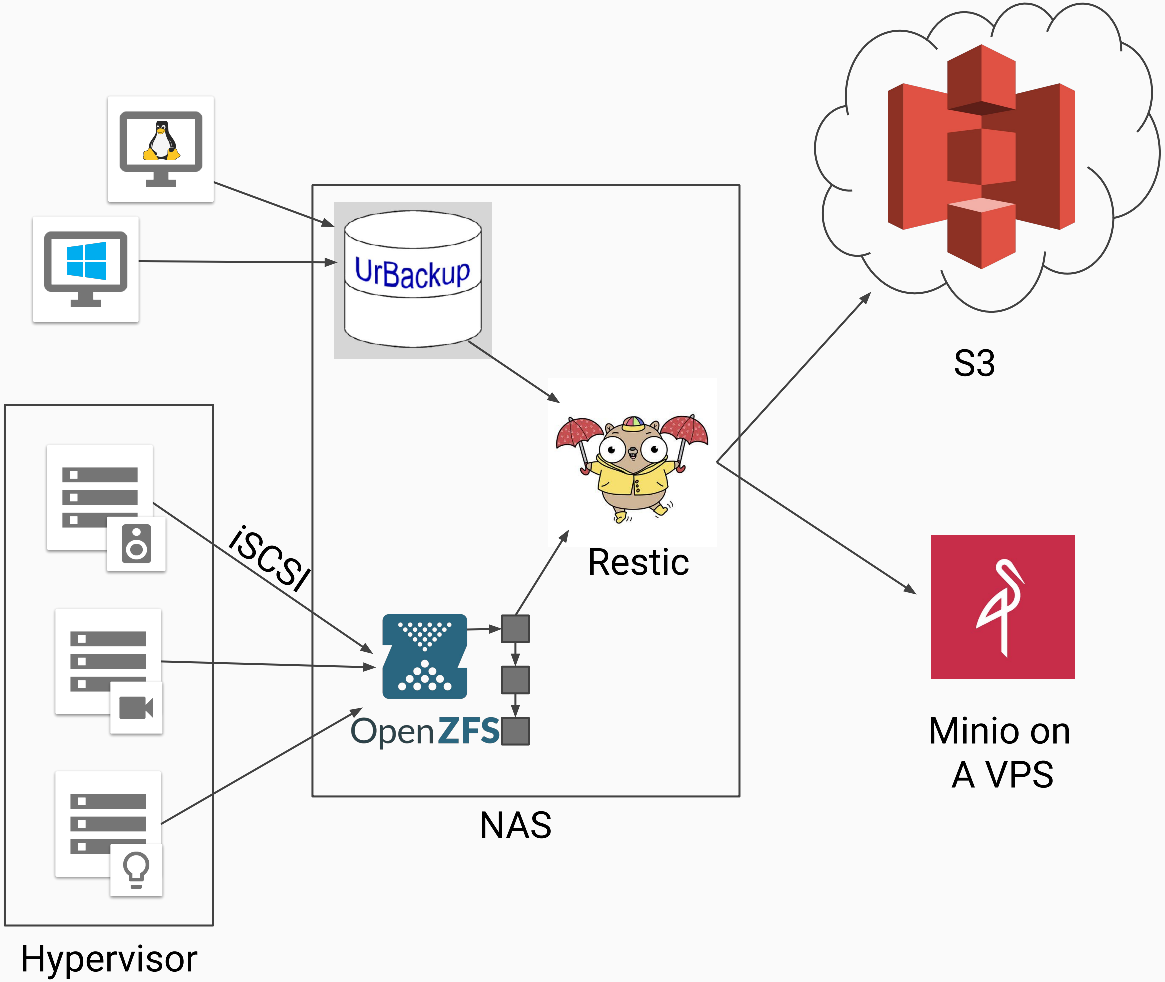
- Bacula
  - “Enterprise” backup software
  - Client/Server/Storage are separate daemons
  - Supports encryption but not mandatory
- UrBackup
  - Client/server backup software
  - Simpler, less features than Bacula

Example Backup Strategy

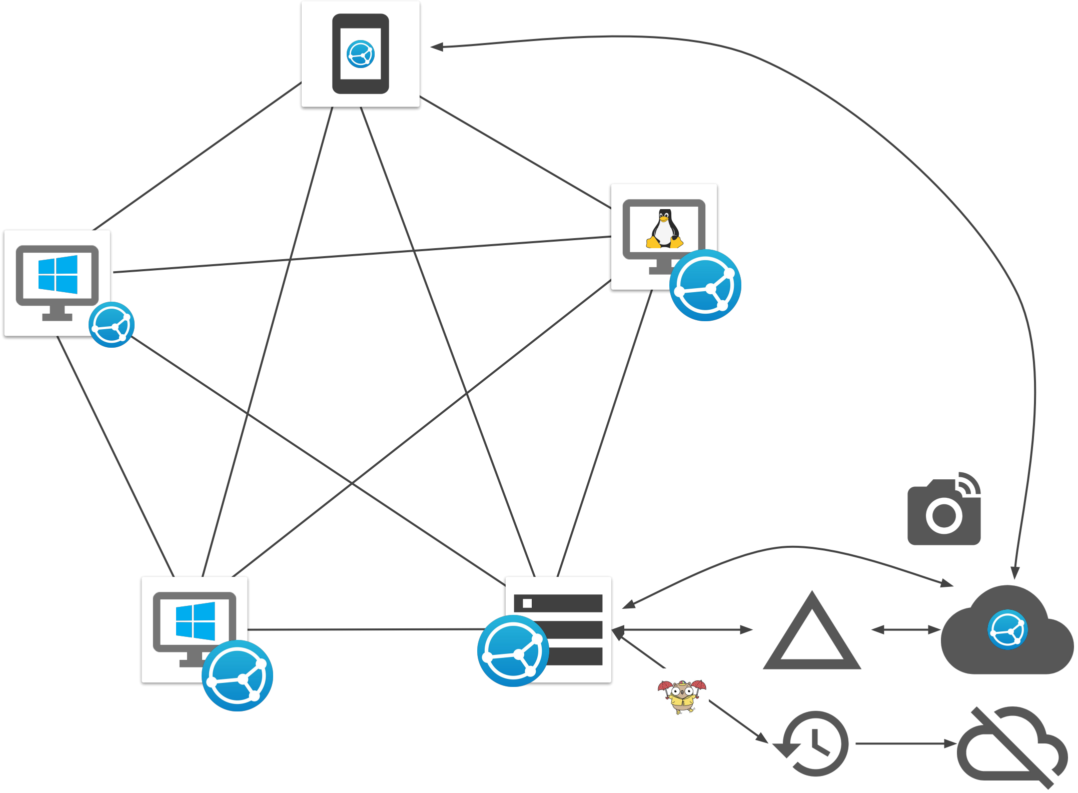
- PCs backup to NAS via UrBackup
- NAS does daily ZFS snapshots of VMs
- Nightly backups of both sent to S3/B2/Wasabi/etc. for offsite

That’s 3 copies (Host, NAS, S3), 2 places (here and S3), 1 “offline”* (S3).

*Offline: Not on a file system that you can easily accidentally `rm -rf`



My Backup Strategy



Reasons behind my insane design

- Only data matters. The OS does not
    - I don’t care about the tools themselves: much of my backup strategy includes support files
- I have limited storage space: Full disk backup isn’t something I care for
- I have more time: I can afford reinstalling an OS, re-syncing information
- Data that I care about is always backed up elsewhere
- No central point of failure: Loss of my servers doesn’t mean loss of data synchronization

Disadvantages to my design

- Complex: I have to make sure that no less than 5 devices have SyncThing running and configured to mumble with one another
- Merge Conflicts: They happen and I get to sort them out by hand.
- Off-Site storage is expensive, local storage is fragile

Exercise

List the things that you store. How are you going to back them up? Where

Documentation

(you won’t “get around to it later”)

Document, Document, Document

You aren't going to touch every system every day, so...

- Document stuff as you do it
- What's running, where it is, how you access it, what it depends on, how you get it to boot/run
- Document any "temporary hacks" (because temporary they aren't)

- Passwords/keys probably go in your password manager
- Everything else goes in your note system:
  - OneNote
  - Zim Desktop Wiki
  - Text files
  - MediaWiki if you want to get fancy
  - Org-mode

Make sure you can access your notes if your lab/network/server/whatever is down!

Make sure your SO can stand things up when you die

- Death is highly inconvenient.
  - Bad timing
  - Bad execution
  - Rarely ever does something go right
- You won’t be around to make sure that you can orchestrate those containers across six layers of abstraction that only you know and

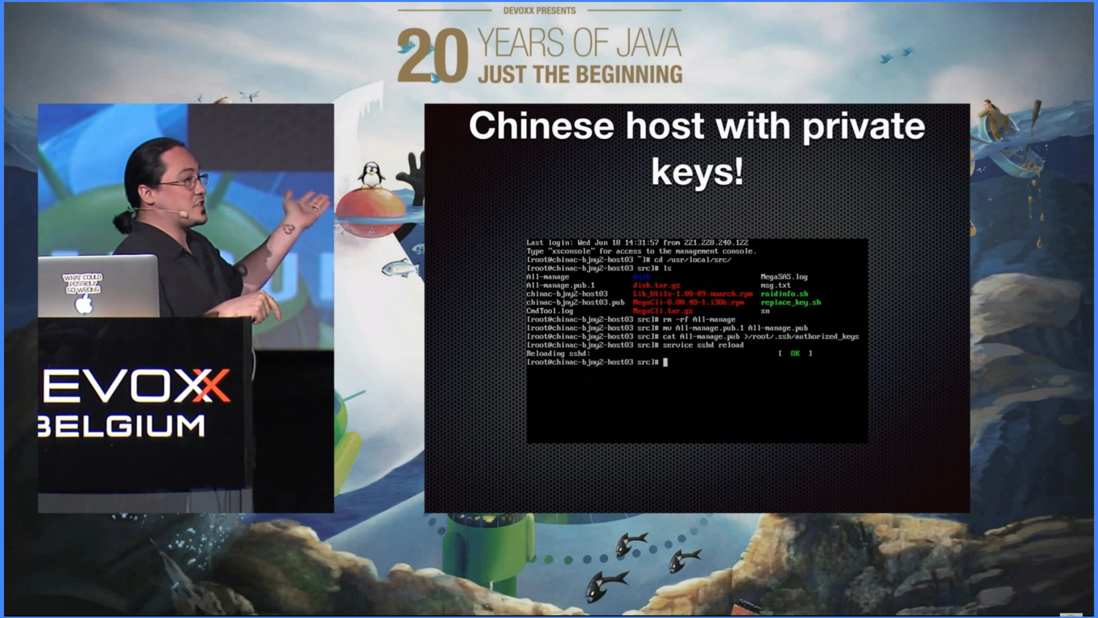
Security

SSH Keys are important

Just because you can FDE your system doesn’t mean you should

Don’t be an idiot

https://youtu.be/hMtu7vV_HmY



Chinese host with private keys!

```
Last login: Wed Jun 18 14:31:57 from 221.228.240.122
Type "xsconsole" for access to the management console.
[root@chinac-bjny2-host03 ~]# cd /usr/local/src/
[root@chinac-bjny2-host03 src]# ls
All-manage              disk                          MegaSAS.log
All-manage.pub.1        disk.tar.gz                   msg.txt
chinac-bjny2-host03     Lib_Utils-1.00-09.noarch.rpm  raidinfo.sh
chinac-bjny2-host03.pub MegaCli-8.00.48-1.i386.rpm    replace_key.sh
CmdTool.log             MegaCli.tar.gz                sn
[root@chinac-bjny2-host03 src]# rm -rf All-manage
[root@chinac-bjny2-host03 src]# mv All-manage.pub.1 All-manage.pub
[root@chinac-bjny2-host03 src]# cat All-manage.pub >/root/.ssh/authorized_keys
[root@chinac-bjny2-host03 src]# service sshd reload
Reloading sshd:                                             [  OK  ]
[root@chinac-bjny2-host03 src]# █
```

Ask yourself

- Does it really need to be on the internet?
- What is your threat model?
    - 13yo Falun Gong skids?
    - Port scanners?
    - `ssh pi@$IP?`
    - A five year old with the hail mary button in Armitage?
    - $5 pipe wrench
    - Mossad?
        - Mossad wins.
- Why do I need remote access?
- Am I right? Am I wrong?
- My God, What have I done?

Some services offer *good* remote access

- Plex
- HomeAssistant (via Nabu Casa)

If you really need remote access:

- Wireguard
- Zerotier*
- Cisco AnyConnect

Q: “Where was IPSec on that last slide?”

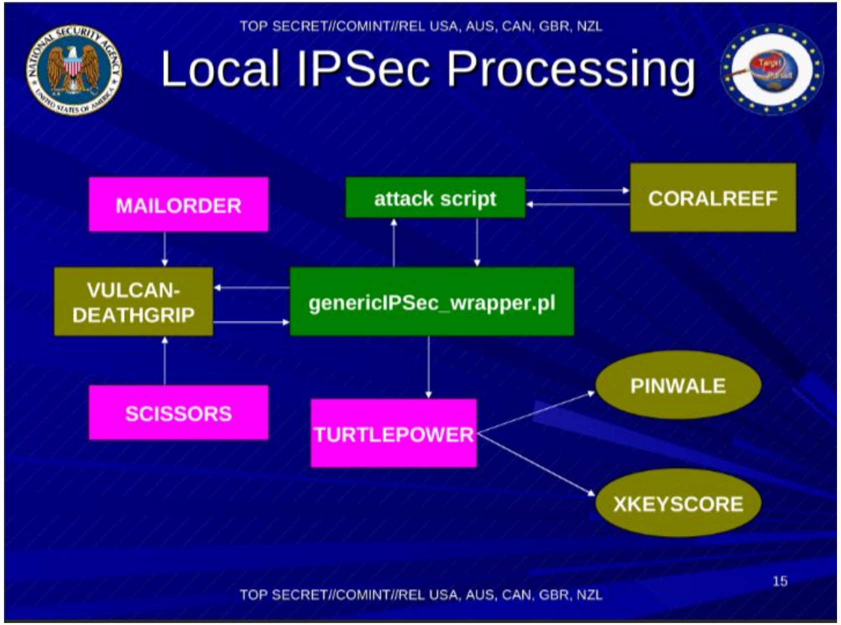
—

A: “Don’t use IPSec.”

IPSec is annoying to configure.

IPSec is built entirely out of footguns.

IPSec’s “cross platform” support is a lie.



TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL

Local IPSec Processing

MAILORDER

attack script

CORALREEF

VULCAN-DEATHGRIP

genericIPSec_wrapper.pl

SCISSORS

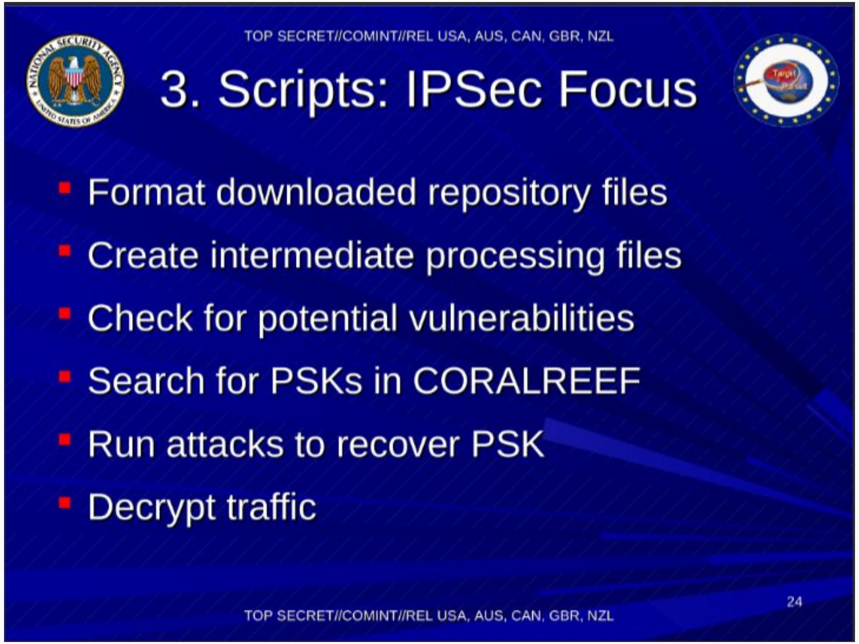
TURTLEPOWER

PINWALE

XKEYSCORE

15

TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL



TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL

3. Scripts: IPSec Focus

- Format downloaded repository files
- Create intermediate processing files
- Check for potential vulnerabilities
- Search for PSKs in CORALREEF
- Run attacks to recover PSK
- Decrypt traffic

24

TOP SECRET//COMINT//REL USA, AUS, CAN, GBR, NZL

The NSA figured out IPSec and just dumps IPSec into XKeyScore anyway.

Sadly, the NSA probably doesn’t care about you.

:(

Wireguard, routers, and other fun things

Wireguard

- Highly integrated kernel-level tunnel
- *It's not IPSec*
- As few footguns as possible
- Has Windows, Linux, MacOS, Android interfaces
- *It's in the kernel now, so you don't need a custom kernel anymore*
  - Unless you run Debian
  - Sadist.

How it works:

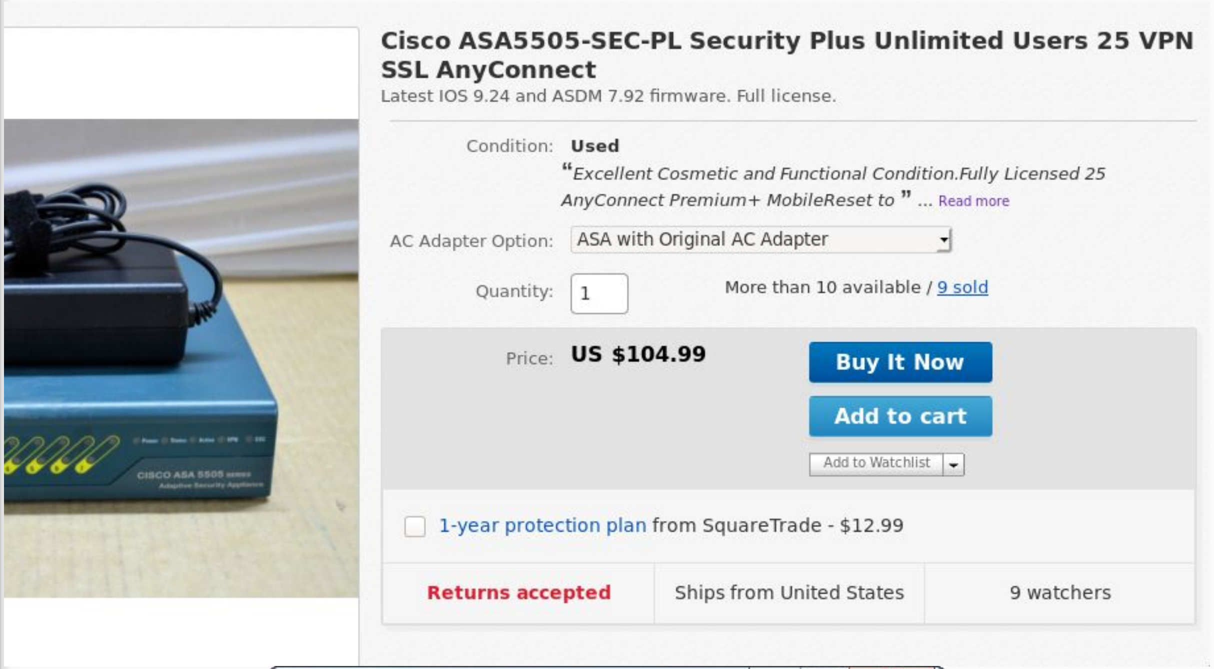
- You route from an interface wg0
- You route to your normal IP network
- Set up static routes or RIP, etc.
- Learn how routing protocols weren't designed for today's problems

https://github.com/subspacecloud/subspace
(A wireguard frontend)

Enterprise Mode: Cisco AnyConnect

Cisco ASAs support a thing called Cisco AnyConnect.

- Bog standard TLS based L2/3 VPN solution
- Typically licensed in volumes of 10,000 active connections
- *Can be licensed to hardware*
- Available as a VPN-only perpetual license in used ASA appliances for ~$100US



Cisco ASA5505-SEC-PL Security Plus Unlimited Users 25 VPN SSL AnyConnect

Latest IOS 9.24 and ASDM 7.92 firmware. Full license.

Condition: **Used**

"*Excellent Cosmetic and Functional Condition.Fully Licensed 25 AnyConnect Premium+ MobileReset to* " ... Read more

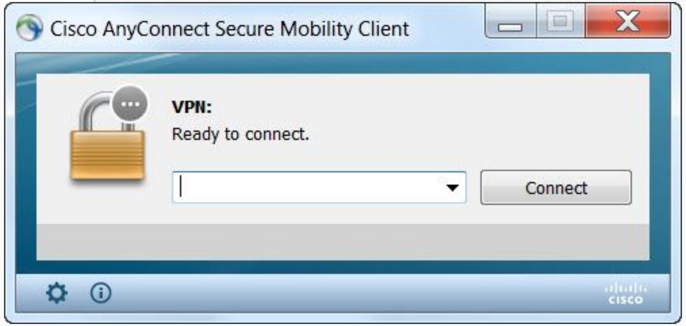
AC Adapter Option: ASA with Original AC Adapter

Quantity: 1 More than 10 available / 9 sold

Price: **US $104.99**

□ 1-year protection plan from SquareTrade - $12.99

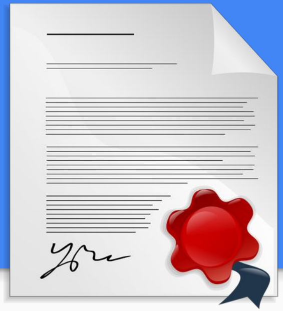
Returns accepted | Ships from United States | 9 watchers



Cisco AnyConnect Secure Mobility Client

VPN:
Ready to connect.

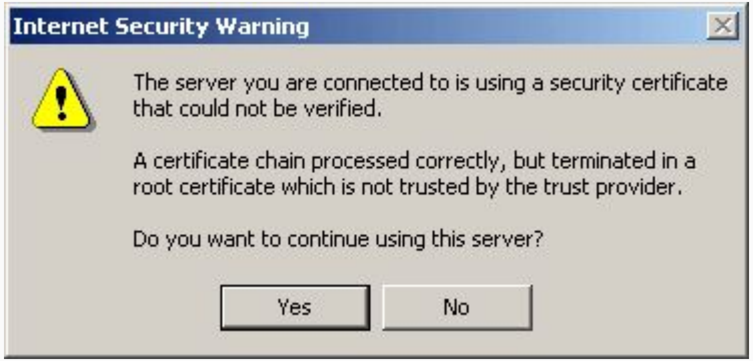
PKI, because you’re a raving lunatic.



~~“Hi, I’m Shea, and I run my own CA”~~

~~Best 12 step program intro 5/7~~

- Want to issue your own HTTPS certs?
- Want strong authentication on your SSL VPN?
- Want to run WPA2-Enterprise wifi for some reason?
- Do you want to be the next Honest Achmed?



The server you are connected to is using a security certificate that could not be verified.

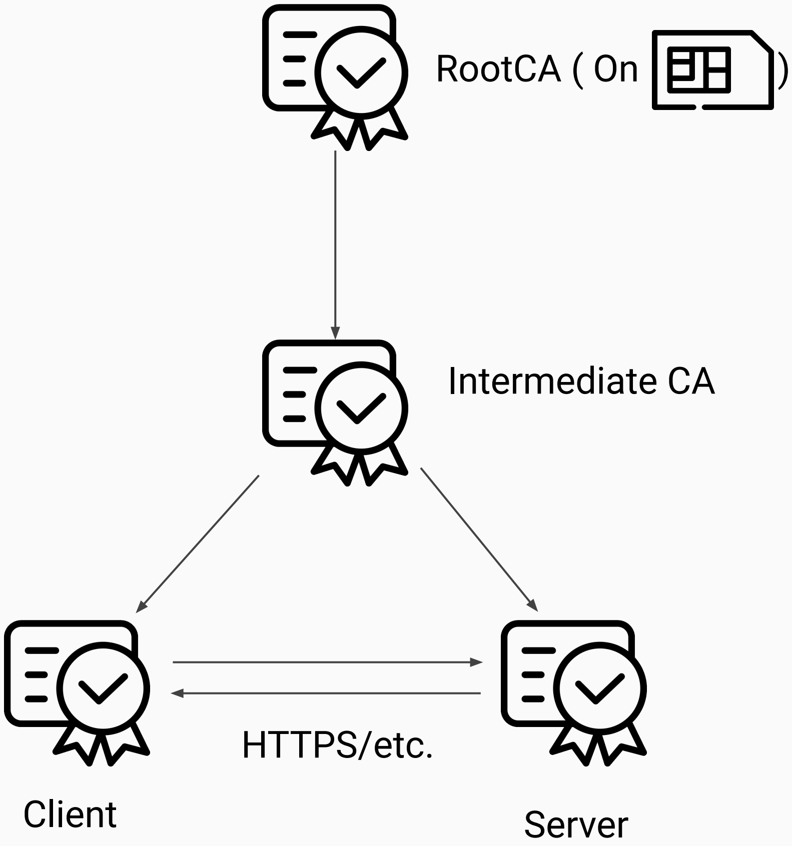
A certificate chain processed correctly, but terminated in a root certificate which is not trusted by the trust provider.

Do you want to continue using this server?

...Then you need your own CA!

PKI for the Homelab

- https://github.com/smallstep/certificates
  - SSH, ACME, etc.
  - All the hot buzzwords
- https://hohnstaedt.de/xca/
  - Graphical CA
- Consider LetsEncrypt for TLS server certificates
  - Lots of HTTPd's already support ACME, the shared protocol



Conclusions

Home labs are fun as h*ck

- Learn enterprise-y things
- Get skills in Small Biz IT
- Learn new and creative swear words
- Don’t chain power strips. They will lead you to fire.

More importantly:

- Good for learning new skills in a controlled environment
- The only person you can blame is you.
  - And maybe Jerry, because… *Jerry*.
- Always have an escape plan
- Your new hobby isn’t cheap but at least it’s not amateur radio!

Resources

Reddit /r/selfhosted /r/homelab

GitHub:
https://github.com/awesome-selfhosted/awesome-selfhosted

ServeTheHome: https://www.servethehome.com/

These slides online at
https://is.gd/ovikav

Thanks!

Bottom text