A Cloud in Every Home

Host servers at home with zero sysadmin skills
$ whoami

Nolan Leake

• Linux user/developer since 1995
• Hosted my own email/web/etc since 2001.
• Cumulus Linux – Linux for network switches
  – Debian derived
  – Commercially supported, w/ wide deployment
Poll

• Who here has a home server, a colocated server, or a VM?
Poll

Who runs their own mail server?

or

Uses a mail server run by friends/family?

http://www.iconarchive.com/artist/graphicloads.html
Poll

Who used to run their own mail server, but stopped?

¯\_(ツ)_/¯
Poll

• Who would run their own mail server, if it required no OS/software setup and maintenance, and minimal hardware setup and maintenance?
Motivations/Goals

- Store your data in your own home.
  - Stronger 4th amendment protection
  - Really obvious if criminals or government agents do this:
Motivations/Goals

• Store your data on hardware you own.
  – No one has an immediate pressing need to do abusive things to "monetize" you to pay for the storage you're using.
  – Even ignoring privacy, eliminating ads, tracking and other “dark pattern” tricks will result in a better experience!
Motivations/Goals

• Must provide similarly easy experience as 3rd party hosted cloud services like gmail.
  – No software administration
  – Absolute minimum hardware administration.
    • Replace failed storage devices
    • Replace failed server

• Must handle this:
Approach

- Use techniques developed by Internet giants that allow <100 people to manage a >100,000 server cluster.
  - These techniques are designed for large companies with huge clusters attacking massive problems.
  - We can adapt them to be both simpler and more appropriate for human/family scale problems.
Approach

- Use techniques developed for smartphone apps to allow non-technical users to install and use software.
  - Self-contained applications
  - Isolated
  - Automatic updates
  - Simplified config and sane defaults
Approach

• Use cheap hardware.
  – Raspberry Pi 3 is $35. Old laptops are cheap.
  – Even non-tech-nerds have spare USB flash sticks.
    • If you have to buy one, a 64GB stick is ~$10.
Approach
Approach

- Immutable images, with explicit data volumes.
  - Easier updates.
  - Harder to corrupt while running.
  - Filesystems are writable or executable, never both.
- Not just application containers – Host OS too.
Approach

- Encrypted overlay network: 🤝 ZERO TIER
- Connects server, laptops, tablets and phones.
  - Punches holes through NATs.
  - Non-public services aren’t exposed on Internet.
Approach

- Isolate different parts of the system, different applications, and parts of applications in separate containers with separate networks.
  - Ephemeral containers like SMTP and Spamassassin can be started on demand and immediately torn down.
  - An email that exploits a Spamassassin bug:
    1) can’t see the mail spool.
    2) can’t see previous or subsequent emails.
    3) can’t attack other internal services, like IMAP.
Approach

Incoming Mail Port 25

Big Bad Internet

SMTP (Postfix) → LMTP Port 24 → Spamassassin → LMTP Port 24 → IMAP(S) Dovecot

Outgoing Mail Port 25

Outgoing SMTP (Postfix) → LMTP Port 24

Outgoing Mail Port 25

ZeroTier Overlay

Reading Mail Port 993
Approach

• If you're emailing someone else with this setup, your message is only plaintext on their client, their server, your server and your client.
  – Never plaintext on any network.
  – Never plaintext on any disk.

• Not quite Signal-level end-to-end cryptography, but a lot better than normal email.
  – But of course, all is lost if you’re talking to a gmail user.
Problem One

• Residential ISPs usually block outgoing SMTP.
  – even if they don't recievers ignore mail from residential IPs because of SPAM.

• Run a proxy on a clean IP
  – The TLS session is negotiated from server to server
    • So the proxy never sees the email.
    • It does get some insight into who is emailing whom.
Problem Two

• We’ve built an open-relay – A SPAM CANNON!

• Must rate limit.
  – But due to mailserver to mailserver TLS, we can’t see the message!
    • Is a 10MB SMTP session to gmail one big picture going to one person, or a 1KB spam going to 5000 people?
  – Solution: The replies back from the destination server are proportional in size to the number of recipients.
    • >>> RCPT TO: Whoever <whoever@whereever.com>
      <<< 250 2.1.5 <whoever@whereever.com>... Recipient ok
    • So we rate limit based on the number of bytes coming back.
Problem Three

- A few ISPs block *incoming* SMTP, either due to misguided policy or CGNAT.
  - Also, some people will be unable or unwilling to enable port forwarding of port 25 on their home router.

- Need a reverse version of the proxy, that determines which home server IP the incoming mail is for using the "EHLO" name.
  - EHLO sends the MX server’s name before STARTTLS starts encrypting the session.
What’s missing

• What you just saw is between a proof-of-concept and Alpha.

• What remains to be done to make this Beta?
DNS and DynDNS

• Right now I used a 3\textsuperscript{rd} party DynDNS
  – Would be better to bring this in-house to reduce the number of accounts to create.

• Internal services on the overlay must be referred to by IP.
  – It is straightforward to setup automatic DNS.
  – But Let’s Encrypt doesn’t support wildcard certs yet.
    • Supposedly coming March 5\textsuperscript{th}
    • That’s 5 days ago.
Better integration with ZeroTier

- Must specify API key in file on SDCard.
- Must manually install app on phones/laptops.
- Must manually authorize new phones/laptops.
- Automate all this!
App Store

• I baked the email app into the OS.
  – This is obviously not scalable.

• Need to build an app store
  – Simple UI (Web, iOS app, Android app) to choose apps.
  – Server downloads application containers.
Supply-chain Security/Transparency

- Reproducable Builds
  - Thanks to basing on Debian, we’re ½ way there.

- Open Source firmware
  - Almost there for Raspberry Pi3
  - Still a ways to go on most x86 PC platforms.
Package More Apps!

- Email is just the start
- Backend services for various IoT devices
- Seafile, SyncThing, or NextCloud (Dropbox)
- Wordpress
- Mastodon instance (Twitter)
- Gitlab (Github)
- Mattermost (Slack)
- More! There is lots of great Open Source software.
Backup/Restore

• Now, if your house burns down, you’re screwed.
  – I mean, you have no email. This is an emergency!

• Global backup scheme.
  – Encrypt, stripe, and redundantly encode files.
  – Spread the encrypted fragments to thousands of other users.
    • In return, you store fragments for them.
  – Encryption key never leaves your house.
    • Well, actually, you should probably have a few copies, perhaps at a trusted family member’s house or in a safe-deposit box.
Sound Interesting?

- Gitlab: https://git.sigbus.net/projectx/os
- IRC: #prjx on Freenode
- Want to be notified when there are pre-built images that are more fully baked?
  - Email prjx@sigbus.net and I’ll let you know.