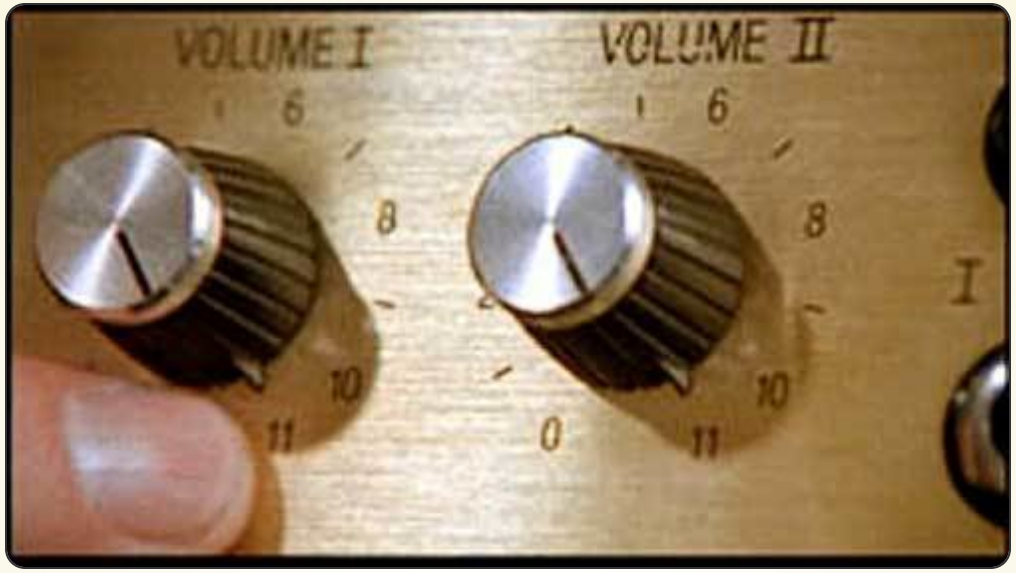
LIFE BEHIND THE TINFOIL CURTAIN

A look at QubesOS and CopperheadOS

Konstantin Ryabitsev

The Linux Foundation

Linux Security Summit, 2018



TOPICS COVERED

- Why did you do this to yourself?
- Qubes OS
- Copperhead OS

INCLUDING

- guiding principles
- device requirements
- installation
- daily use
  - what you will like
  - what will drive you mad
  - convenience vs. security trade-offs
- future outlook

PLEASE INTERRUPT AT ANY TIME

FOR QUESTIONS OR CLARIFICATIONS

ABOUT ME

- Professional Russian Hacker
  - before it was popular
  - (you've probably never heard of me)
- Linux on the desktop user since 1998
  - ask me about Corel Linux (or, actually, don't)
- Member of the Linux Foundation IT team since 2011
- Running Qubes OS since August 2016
- Running Copperhead OS since September 2017
  - until June 2018
  - (but I hope to go back)

CAVEAT AUDITOR

- I am a systems administrator
- I am not a security researcher
- I am not a kernel developer
- I am *a bit* paranoid
  - not nearly enough for some people

My goal is to share my experience using Linux-based tools aimed at significantly improving my security and privacy.

QUBES OS

QUBES OS: GUIDING PRINCIPLES

- compartmentalization via virtualization
  - using type-1 hypervisor (XEN)
  - dom0 runs the graphical interface
  - all applications run inside AppVMs
- hardware isolation
  - I/O devices must be assigned to VMs
  - convenient management tools
- network isolation
  - full control over how appVMs get to the net
  - (or not at all for vault VMs)

QUBES OS: DEVICE REQUIREMENTS

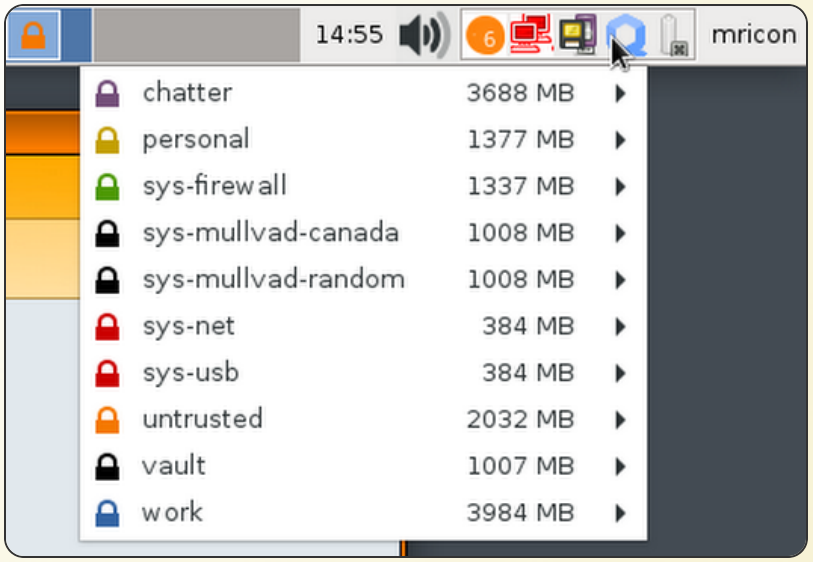
- lots of RAM (16GB+)
- fast, large SSD disks (NVMe)
- multiple processors with many cores
  - but works comfortably with 2x2
- CPU MUST have:
  - Intel VT-x with EPT (or AMD-V with RVI)
  - Intel VT-d (or AMD-Vi aka IOMMU)
- Intel graphics

QUBES OS: INSTALLATION

- modified Fedora installer
- post-installation requires knowledge of what you're doing before you do it
  - sys-usb for your USB devices?
    - which USB controller to assign to it?
  - create regular AppVMs? (probably yes)
    - work
    - personal
    - vault
    - untrusted

QUBES OS: APPVMS

- think of them as isolated logical workspaces
- decide how they all get online
  - does "work" need an employer VPN?
  - does "personal" need a generic VPN?
  - does "untrusted" need to go out via TOR?
- learn to love and use disposable VMs
  - send them through TOR (maybe)
- learn how templates work
  - everything not in /rw is lost
  - you get Fedora, Debian, Whonix
  - community templates available



QUBES OS: DAILY USE

- for the most part, everything works as you expect
- except:
  - copying files
    - you get used to it very quickly
  - copy-pasting
    - Ctrl-Shift-C/V to copy between AppVms
    - (this will drive you crazy)
  - installing software via dnf/apt
    - must be done in TemplateVMs to persist
  - changing global config values
    - symlink things to /rw/config

QUBES OS: WHAT YOU WILL LOVE

- feeling that your data is well protected
- opening mail attachments in disposable VMs
  - at least in Thunderbird
- Sanitizing PDFs
  - opens a DispVM and renders as images
- Fedora (or other template) upgrades
  - don't like it, set it back to the previous template
- VaultVMs
- different endpoint egress per AppVM

QUBES OS: WHAT WILL DRIVE YOU MAD

- copy-pasting
- not being able to screenshare
  - you have to run a standalone windowed VM
- suspend/resume bugs
- launch lag when an AppVM is not running
  - especially if it has to launch NetVMs first
- rare, but random weirdness
  - occasionally, AppVMs won't start
  - or your microphone stops working
  - or the resolver in one of the VMs
- complicated backups

QUBES OS: FUTURE OUTLOOK

- Sponsored by Invisible Things Lab
  - https://invisiblethingslab.com
- Under active development
- Partially user-supported via donations
  - https://opencollective.com/qubes-os
- Uses XEN
  - is written to be able to use other virtualization platforms, if needed
- Has an active and diverse user base

QUBES OS: WHO IS IT FOR?

- Systems administrators
  - or similar gatekeepers with access to privileged data
- Journalists
  - if they have a knowledgeable support department
- Anyone expecting direct precision attacks by well-funded and savvy adversaries
- Anyone working in environments where they are likely to be in trouble if caught by dragnet surveillance

QUBES OS: WHO IS IT NOT FOR?

- Anyone not very familiar with Linux
  - especially if they are doing it on their own without a tech support department
- Anyone who can't afford modern, powerful hardware
  - CPUs capable of VT-x and VT-d, lots of RAM, large SSD come with a high price tag
- Anyone in danger of physical duress threats
  - you probably just want Tails for deniability

QUBES OS: WHAT CAN YOU USE INSTEAD?

- You can reach *some* degree of feature parity with:
  - Firejail for browser sandboxing
  - Flatpak for other app isolation
  - Whonix for persistent anonymous surfing
  - TailsOS for disposable web sessions
- QubesOS offers all of the above plus convenience
  - at the cost of a very steep learning curve

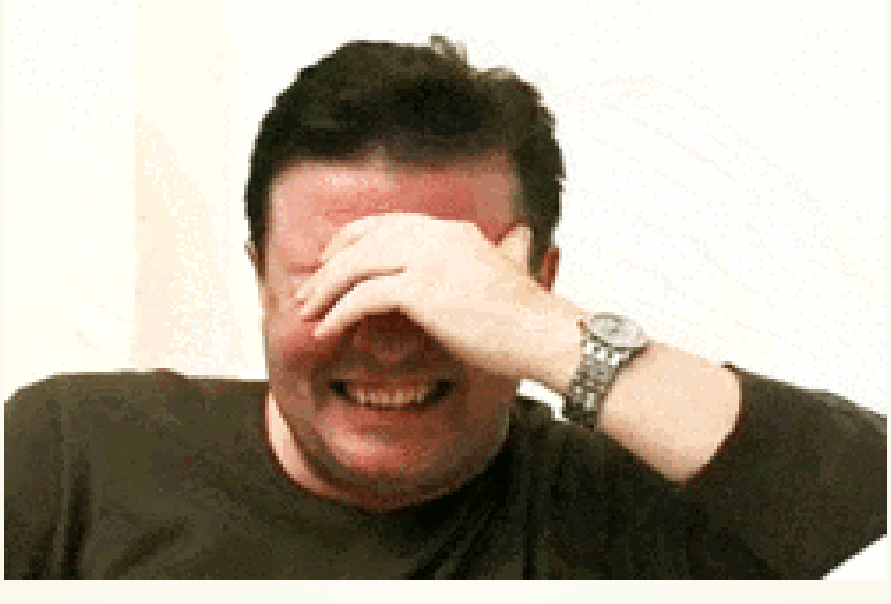
COPPERHEAD OS

SO MUCH HAS HAPPENED SINCE MAY

Copperhead OS in its previous incarnation is dead.
Existing installs won't receive any updates.
Must migrate to newer images.

COPPERHEAD: GUIDING PRINCIPLES

- Also in other "pure AOSP androids":
  - Google-free android experience
  - Fast security patching turnaround
- Unique to Copperhead:
  - Hardened kernel (plus KSPP patches)
  - Hardened compiler toolchain
  - Stricter SELinux policies
  - MAC address randomization
  - Stricter defaults
  - and more



COPPERHEAD: DEVICE REQUIREMENTS

- Only available on a very small set of devices
  - Google Nexus
  - Google Pixel (+XL)
  - Google Pixel 2 (+XL)
  - HiKey dev boards

COPPERHEAD: INSTALLATION

- Downloadable and installable
  - no OTA updates if you do this!
  - a pretty involved process
- Buy a Pixel from CopperheadOS
  - with ~80% markup
- Send in your own Pixel
  - pay quite a lot of money

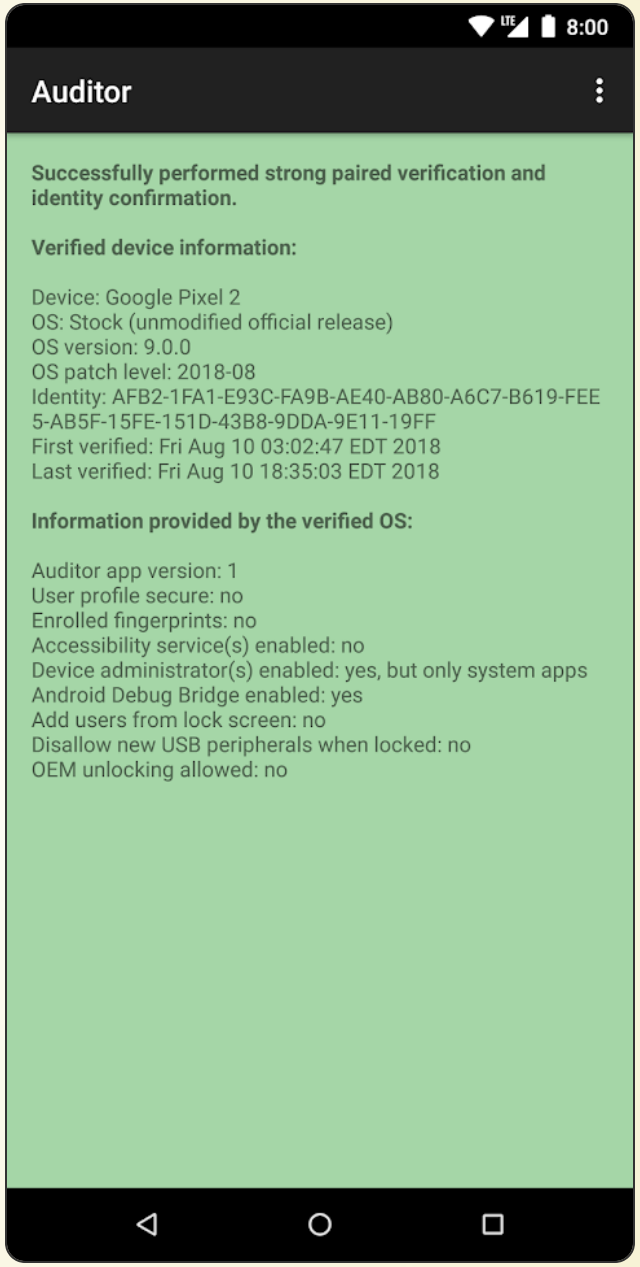
COPPERHEAD: DAILY USE

- For the most part, just like any other "pure AOSP" device
  - Some apps are available from F-Droid
    - K-9 mail
    - Some messengers (Telegram, Riot, Silence)
  - Some others can be side-loaded:
    - YALP
    - APK Mirror
    - Amazon Appstore
    - Many apps may not work right, or at all
      - (no, MicroG didn't work)
  - Excellent for secure communication and browsing
  - Excellent remote attestation feature

COPPERHEAD: AUDITOR

The Auditor app uses hardware security features on supported devices to validate the integrity of the operating system from another Android device. It will verify that the device is running the stock operating system with the bootloader locked and that no tampering with the operating system has occurred. It will also detect downgrades to a previous version.

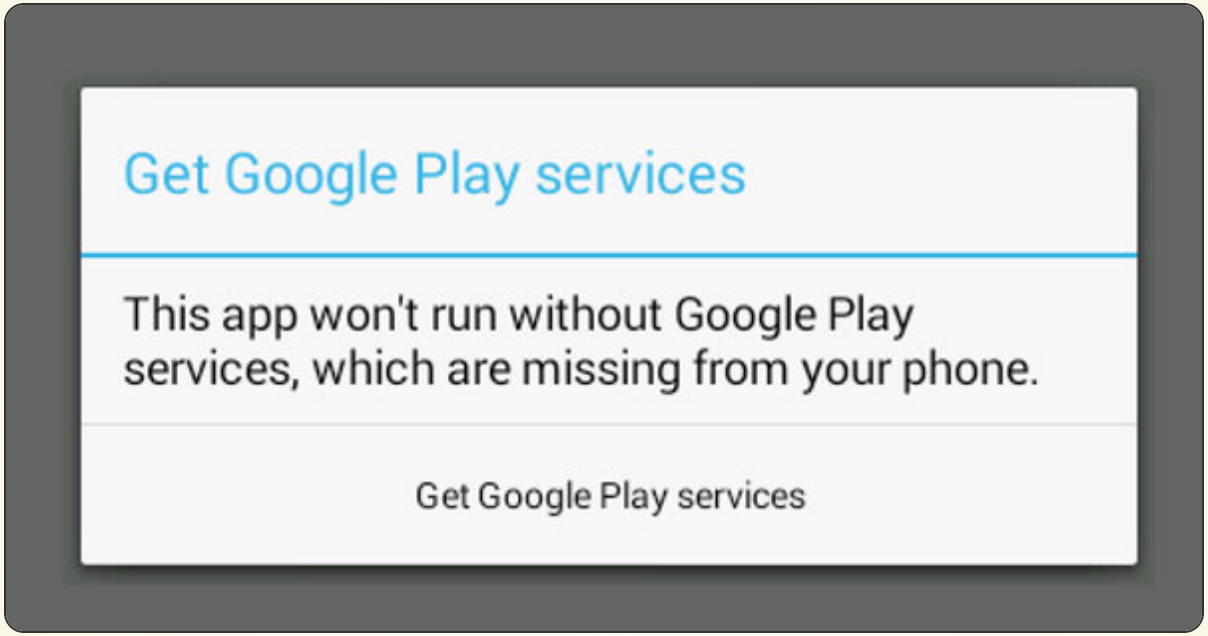
App store



PURE AOSP: WHAT YOU'LL LOVE

- Battery life
- Knowledge that you're not being tracked
  - ... as much
  - depends on which apps you install and use
  - your mobile service provider still tracks you
- Fast security patches
  - depends on which Pure AOSP build you're using
  - LineageOS is pretty good
- Knowledge that you're using free software
  - F-Droid supports reproducible builds
  - (some features may be source-available)

PURE AOSP: WHAT YOU'LL HATE



PURE AOSP: WHAT YOU'LL HATE

- Huge loss of convenient perks we've come to associate with owning a mobile device
  - Side-loaded apps may or may not work
    - they probably won't deliver notifications
    - they may stop working at any time
    - app authors don't care about your weird setup
- True, you can communicate securely
  - but only with people using the same 3 messaging apps
  - your team members are probably on Slack
  - your friends are probably on Facebook Messenger
    - which actually works great
    - but then what's the point?

OWNING A PURE-AOSP DEVICE COMES WITH ALL THE SOCIAL PERKS OF BEING A GLUTEN-INTOLERANT VEGAN WITH A PEANUT ALLERGY

ALSO, YOU CAN'T PLAY POKEMON GO

COPPERHEAD: FUTURE OUTLOOK

COPPERHEAD: WHO IS IT FOR?

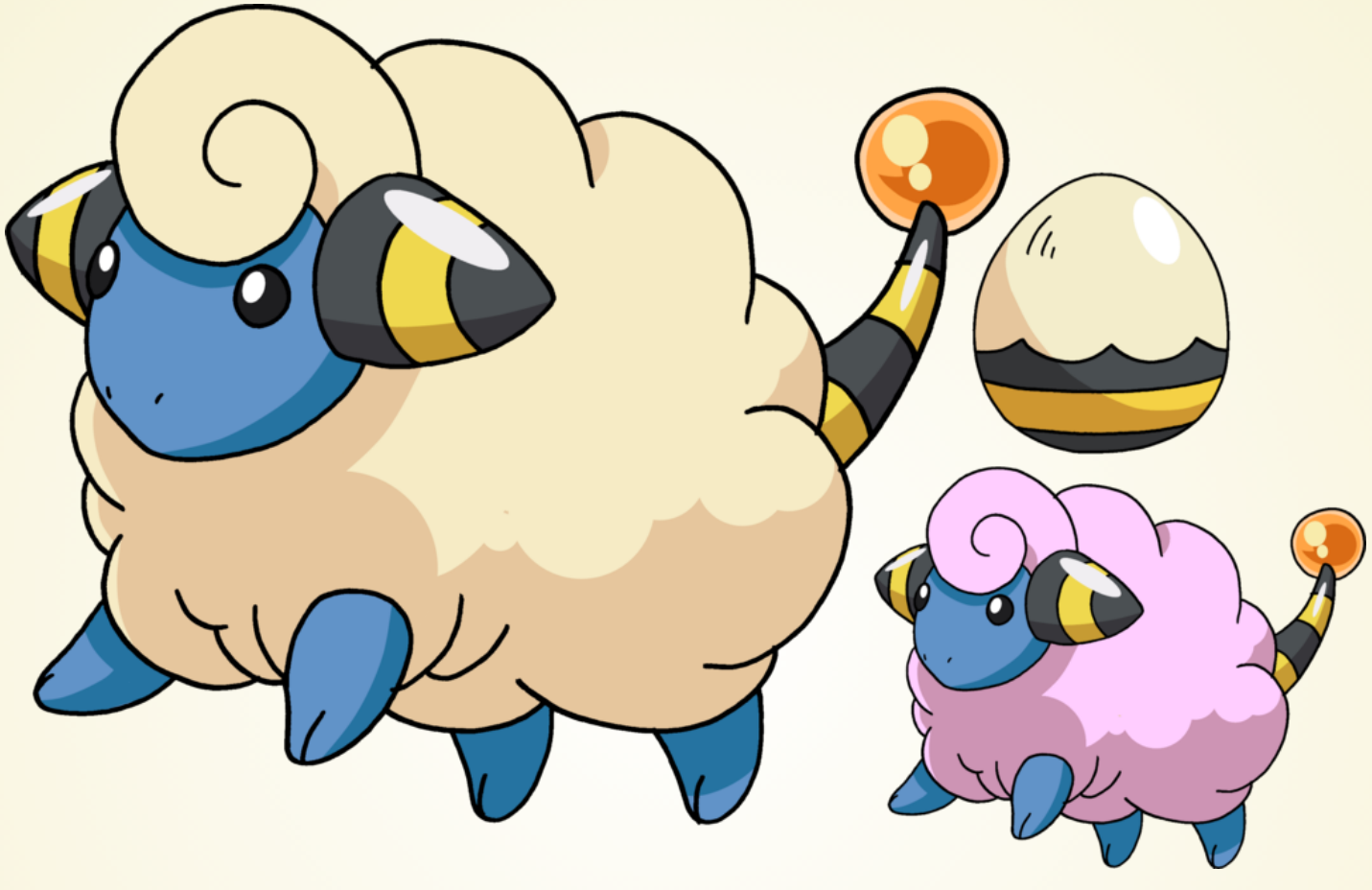
- Anyone really worried about dragnet private data collection by governments or large corporations
  - true for most Pure-AOSP builds
- Anyone expecting direct precision attacks by well-funded and savvy adversaries
  - Government employees
  - Journalists
  - Activists

COPPERHEAD: WHO IS IT NOT FOR?

- Anyone who needs to use their device for more than secure communication
  - or is dependent on apps that do not work well in a pure-aosp environment

COPPERHEAD: WHAT AM I USING NOW?

- I am back to stock Google Pie
  - with some privacy tweaks
- I try to limit which apps I use
  - use the mobile web version, if available
  - the Hermit app makes this easier
- I don't intend to switch to LineageOS
  - Not getting notifications was impacting my work
  - Security improvements in stock Google Pie are impressive and are probably sufficient for my needs
- I will probably go back to CopperheadOS when I need a newer phone, if all goes well with the company



DOES THAT MAKE ME A SHEEP?

Maybe, for now...

But at least I have an option to evolve.

EOF