A Look at Copperhead OS
Security-focused Android

Jim Campbell

Penguicon!!!

April 30th, 2017

Introduction to Copperhead OS

What we'll talk about . . .

Introduction to Copperhead OS

What we'll talk about . . .

- Background
- Good for me? Not good for me?
- Key Features
- Copperhead IRL
- Useful F-Droid applications
- Links / Resources

What is Copperhead OS?

- Security-focused Android based on Android Open Source Project

What is Copperhead OS?

- Security-focused Android based on Android Open Source Project
- If phone == car, using Copperhead == putting new engine in car.

What is Copperhead OS?

- Security-focused Android based on Android Open Source Project
- If phone == car, using Copperhead == putting new engine in car.
- Only for Google-branded devices

What is Copperhead OS?

- Security-focused Android based on Android Open Source Project
- If phone == car, using Copperhead == putting new engine in car.
- Only for Google-branded devices
- Supported for as long as Google offers support

What is Copperhead OS?

- Security-focused Android based on Android Open Source Project
- If phone == car, using Copperhead == putting new engine in car.
- Only for Google-branded devices
- Supported for as long as Google offers support
- 5x / 6p - Get version upgrades until Sept of 2017
- 5x / 6p - Security updates until Sept of 2018

What is Copperhead OS?

- Security-focused Android based on Android Open Source Project
- If phone == car, using Copperhead == putting new engine in car.
- Only for Google-branded devices
- Supported for as long as Google offers support
- 5x / 6p - Get version upgrades until Sept of 2017
- 5x / 6p - Security updates until Sept of 2018
- Pixel - Get version upgrades until October of 2018
- Pixel - Security updates until October of 2019

What is Copperhead OS?

- Security-focused Android based on Android Open Source Project
- If phone == car, using Copperhead == putting new engine in car.
- Only for Google-branded devices
- Supported for as long as Google offers support
- 5x / 6p - Get version upgrades until Sept of 2017
- 5x / 6p - Security updates until Sept of 2018
- Pixel - Get version upgrades until October of 2018
- Pixel - Security updates until October of 2019

Who Develops Copperhead

Lead developer of Copperhead OS is former maintainer of GR Security and PaX patches on Arch Linux.

Who Develops Copperhead

Lead developer of Copperhead OS is former maintainer of GR Security and PaX patches on Arch Linux.
Started consultancy to provide security services to organizations, and to build Copperhead OS protect sensitive mobile communications.

Good For You

Copperhead OS is cool if:

Good For You

Copperhead OS is cool if:

- You're a free software enthusiast
- You don't want apps that eat personal data and privacy
- You can live without Spotify and Snapchat
- . . . or are willing to fuss (i.e., side-load apps)
- You like the supported phones (Google Phones)

Maybe For Someone Else

Copperhead may not be the best if:

Maybe For Someone Else

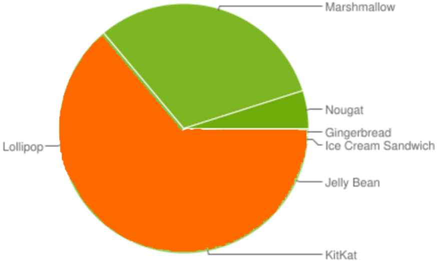
Copperhead may not be the best if:

- You want a Libre phone
- You want to use Spotify without fuss
- You don't want to tinker or device isn't what you want
- There's a proprietary app that you have to use for work

WHY??

Why does this even exist?

Android device support == * Sad Emoji *



63.9%

But my phone has support!

Android Security Compromises

Even among supported devices, security is less than ideal:

- AOSP doesn't always choose most secure defaults

Android Security Compromises

Even among supported devices, security is less than ideal:

- AOSP doesn't always choose most secure defaults
- OEMs are slow to update (at best, 1x/month)

Android Security Compromises

Even among supported devices, security is less than ideal:

- AOSP doesn't always choose most secure defaults
- OEMs are slow to update (at best, 1x/month)
- Encryption not always on by default

Android Security Compromises

Even among supported devices, security is less than ideal:

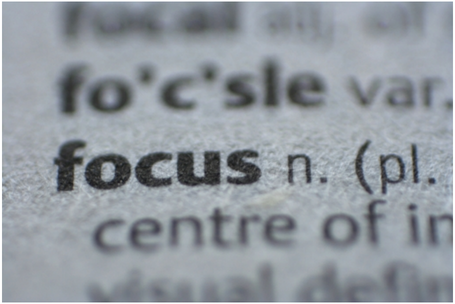
- AOSP doesn't always choose most secure defaults
- OEMs are slow to update (at best, 1x/month)
- Encryption not always on by default
- Default applications don't provide E2E encryption

Android Security Compromises

Even among supported devices, security is less than ideal:

- AOSP doesn't always choose most secure defaults
- OEMs are slow to update (at best, 1x/month)
- Encryption not always on by default
- Default applications don't provide E2E encryption

Filling This Gap - Hardened OS for well-supported devices



Hardening? What do you mean?

What does hardening entail?

Hardening? What do you mean?

What does hardening entail? Let's look at their blog:

Hardening? What do you mean?

What does hardening entail? Let's look at their blog:

- Memory disclosure mitigations in CopperheadOS

Hardening? What do you mean?

What does hardening entail? Let's look at their blog:

- Memory disclosure mitigations in CopperheadOS
- Hardening Android's Bionic libc

Hardening? What do you mean?

What does hardening entail? Let's look at their blog:

- Memory disclosure mitigations in CopperheadOS
- Hardening Android's Bionic libc
- Separating Android's encryption and lockscreen passwords

Hardening? What do you mean?

What does hardening entail? Let's look at their blog:

- Memory disclosure mitigations in CopperheadOS
- Hardening Android's Bionic libc
- Separating Android's encryption and lockscreen passwords
- Integrating PaX into Android

Hardening? What do you mean?

What does hardening entail? Let's look at their blog:

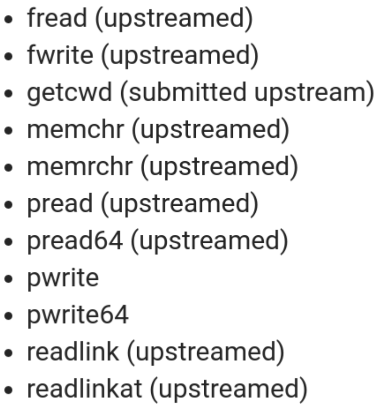
- Memory disclosure mitigations in CopperheadOS
- Hardening Android's Bionic libc
- Separating Android's encryption and lockscreen passwords
- Integrating PaX into Android
- The State of ASLR on Android Lollipop

Hardening? What do you mean?

What does hardening entail? Let's look at their blog:

- Memory disclosure mitigations in CopperheadOS
- Hardening Android's Bionic libc
- Separating Android's encryption and lockscreen passwords
- Integrating PaX into Android
- The State of ASLR on Android Lollipop

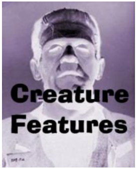
Probably Not Shitty - A Lot is Upstreamed



- fread (upstreamed)
- fwrite (upstreamed)
- getcwd (submitted upstream)
- memchr (upstreamed)
- memrchr (upstreamed)
- pread (upstreamed)
- pread64 (upstreamed)
- pwrite
- pwrite64
- readlink (upstreamed)
- readlinkat (upstreamed)

Source: AOSP repository

What are some of its features?



A Custom ROM like an OEM OS

As a custom ROM, they offer features you'd expect from an OEM OS:

- Signed OS and signed updates

A Custom ROM like an OEM OS

As a custom ROM, they offer features you'd expect from an OEM OS:

- Signed OS and signed updates
- Verified boot

A Custom ROM like an OEM OS

As a custom ROM, they offer features you'd expect from an OEM OS:

- Signed OS and signed updates
- Verified boot
- Device can be OEM locked after install

A Custom ROM like an OEM OS

As a custom ROM, they offer features you'd expect from an OEM OS:

- Signed OS and signed updates
- Verified boot
- Device can be OEM locked after install
- Does not require root

A Custom ROM like an OEM OS

As a custom ROM, they offer features you'd expect from an OEM OS:

- Signed OS and signed updates
- Verified boot
- Device can be OEM locked after install
- Does not require root
- Can leave "untrusted sources" disabled

A Custom ROM like an OEM OS

As a custom ROM, they offer features you'd expect from an OEM OS:

- Signed OS and signed updates
- Verified boot
- Device can be OEM locked after install
- Does not require root
- Can leave "untrusted sources" disabled

Solid Default Settings

Configured with privacy-respecting features from the get-go:

Solid Default Settings

Configured with privacy-respecting features from the get-go:

- Encrypted by default

Solid Default Settings

Configured with privacy-respecting features from the get-go:

- Encrypted by default
- Notifications hidden

Solid Default Settings

Configured with privacy-respecting features from the get-go:

- Encrypted by default
- Notifications hidden
- Longer max pasword length (16 char max upgraded to 64)

Solid Default Settings

Configured with privacy-respecting features from the get-go:

- Encrypted by default
- Notifications hidden
- Longer max pasword length (16 char max upgraded to 64)
- Others: Navigation error correction, contextual search, network prediction, metrics and hyperlink auditing are disabled by default.

Additional Features

And they include security-related features that others don't:

Additional Features

And they include security-related features that others don't:

- MAC address randomization (where supported)

Additional Features

And they include security-related features that others don't:

- MAC address randomization (where supported)
- Can set different login and decrypt passwords

Additional Features

And they include security-related features that others don't:

- MAC address randomization (where supported)
- Can set different login and decrypt passwords
- GR Security and PaX patches, but not all of them. 3.10 kernel is old. Old drivers are an issue

Additional Features

And they include security-related features that others don't:

- MAC address randomization (where supported)
- Can set different login and decrypt passwords
- GR Security and PaX patches, but not all of them. 3.10 kernel is old. Old drivers are an issue
- Weekly updates, even if phone is encrypted

Additional Features

And they include security-related features that others don't:

- MAC address randomization (where supported)
- Can set different login and decrypt passwords
- GR Security and PaX patches, but not all of them. 3.10 kernel is old. Old drivers are an issue
- Weekly updates, even if phone is encrypted
- Can build from source

Additional Features

And they include security-related features that others don't:

- MAC address randomization (where supported)
- Can set different login and decrypt passwords
- GR Security and PaX patches, but not all of them. 3.10 kernel is old. Old drivers are an issue
- Weekly updates, even if phone is encrypted
- Can build from source
- Can build patch updates from source

Additional Features

And they include security-related features that others don't:

- MAC address randomization (where supported)
- Can set different login and decrypt passwords
- GR Security and PaX patches, but not all of them. 3.10 kernel is old. Old drivers are an issue
- Weekly updates, even if phone is encrypted
- Can build from source
- Can build patch updates from source

OS-related Questions?

ASK US!!!!!
Pokemon Sun and Moon Starters!
Please Ask Questions
We will awnser almost anything
Please no Swearing or NSFW Questions

What's it like to use it?

- You can install it or you can buy it

What's it like to use it?

- You can install it or you can buy it
- Installing? Docs are great! Even building from source!

What's it like to use it?

- You can install it or you can buy it
- Installing? Docs are great! Even building from source!
- Make sure USB-C cable has data pins

What’s it like to use it?

- You can install it or you can buy it
- Installing? Docs are great! Even building from source!
- Make sure USB-C cable has data pins
- USB debugging ”USB Configuration” to PTP (Picture Transfer Protocol)

What’s it like to use it?

- You can install it or you can buy it
- Installing? Docs are great! Even building from source!
- Make sure USB-C cable has data pins
- USB debugging ”USB Configuration” to PTP (Picture Transfer Protocol)
- Project Fi and Sprint support are an issue (no data)

What’s it like to use it?

- You can install it or you can buy it
- Installing? Docs are great! Even building from source!
- Make sure USB-C cable has data pins
- USB debugging "USB Configuration" to PTP (Picture Transfer Protocol)
- Project Fi and Sprint support are an issue (no data) Sprint - binary issue (not good) T-mobile - APN issue (config update - Sweet LTE!)

What's it like to use it?

- You can install it or you can buy it
- Installing? Docs are great! Even building from source!
- Make sure USB-C cable has data pins
- USB debugging "USB Configuration" to PTP (Picture Transfer Protocol)
- Project Fi and Sprint support are an issue (no data) Sprint - binary issue (not good) T-mobile - APN issue (config update - Sweet LTE!)
- Fingerprint scanner works

What's it like to use it?

- You can install it or you can buy it
- Installing? Docs are great! Even building from source!
- Make sure USB-C cable has data pins
- USB debugging "USB Configuration" to PTP (Picture Transfer Protocol)
- Project Fi and Sprint support are an issue (no data) Sprint - binary issue (not good) T-mobile - APN issue (config update - Sweet LTE!)
- Fingerprint scanner works
- No swype, must type. Good autocorrect and prediction

What’s it like to use it?

- You can install it or you can buy it
- Installing? Docs are great! Even building from source!
- Make sure USB-C cable has data pins
- USB debugging ”USB Configuration” to PTP (Picture Transfer Protocol)
- Project Fi and Sprint support are an issue (no data) Sprint - binary issue (not good) T-mobile - APN issue (config update - Sweet LTE!)
- Fingerprint scanner works
- No swype, must type. Good autocorrect and prediction
- No Lyft == Jim cold and wet in January rain, but I lived

What’s it like to use it?

- You can install it or you can buy it
- Installing? Docs are great! Even building from source!
- Make sure USB-C cable has data pins
- USB debugging ”USB Configuration” to PTP (Picture Transfer Protocol)
- Project Fi and Sprint support are an issue (no data) Sprint - binary issue (not good) T-mobile - APN issue (config update - Sweet LTE!)
- Fingerprint scanner works
- No swype, must type. Good autocorrect and prediction
- No Lyft == Jim cold and wet in January rain, but I lived

Some cool uses

What makes this legitimately *good to use* as a daily driver?

- Sandboxed social media applications

Some cool uses

What makes this legitimately *good to use* as a daily driver?

- Sandboxed social media applications
- Download youtube videos while on wifi, playback later!

Some cool uses

What makes this legitimately *good to use* as a daily driver?

- Sandboxed social media applications
- Download youtube videos while on wifi, playback later!
- Defaults to DuckDuckGo for web search

Some cool uses

What makes this legitimately *good to use* as a daily driver?

- Sandboxed social media applications
- Download youtube videos while on wifi, playback later!
- Defaults to DuckDuckGo for web search
- Can sync calendar with NextCloud or Sandstorm.io Radicale

Some cool uses

What makes this legitimately *good to use* as a daily driver?

- Sandboxed social media applications
- Download youtube videos while on wifi, playback later!
- Defaults to DuckDuckGo for web search
- Can sync calendar with NextCloud or Sandstorm.io Radicale
- Loyalty cards without location tracking. Nice!

Some cool uses

What makes this legitimately *good to use* as a daily driver?

- Sandboxed social media applications
- Download youtube videos while on wifi, playback later!
- Defaults to DuckDuckGo for web search
- Can sync calendar with NextCloud or Sandstorm.io Radicale
- Loyalty cards without location tracking. Nice!
- Roughly weekly, super-simple updates

What's the application situation?

FDroid is at least as good as the Microsoft Store

What's the application situation?

FDroid is at least as good as the Microsoft Store

- FDroid is getting a major update very soon!

What’s the application situation?

FDroid is at least as good as the Microsoft Store

- FDroid is getting a major update very soon!
- Easy to find applications that use Material Design

What's the application situation?

FDroid is at least as good as the Microsoft Store

- FDroid is getting a major update very soon!
- Easy to find applications that use Material Design
- Look for ones updated recently

What's the application situation?

FDroid is at least as good as the Microsoft Store

- FDroid is getting a major update very soon!
- Easy to find applications that use Material Design
- Look for ones updated recently
- Browse web - 64-bit Chromium

What’s the application situation?

FDroid is at least as good as the Microsoft Store

- FDroid is getting a major update very soon!
- Easy to find applications that use Material Design
- Look for ones updated recently
- Browse web - 64-bit Chromium
- Secure SMS - Silence or Noise (. . . a Signal fork)

What's the application situation?

FDroid is at least as good as the Microsoft Store

- FDroid is getting a major update very soon!
- Easy to find applications that use Material Design
- Look for ones updated recently
- Browse web - 64-bit Chromium
- Secure SMS - Silence or Noise (. . . a Signal fork)
- Twitter - Twidere or SlimSocial

What's the application situation?

FDroid is at least as good as the Microsoft Store

- FDroid is getting a major update very soon!
- Easy to find applications that use Material Design
- Look for ones updated recently
- Browse web - 64-bit Chromium
- Secure SMS - Silence or Noise (. . . a Signal fork)
- Twitter - Twidere or SlimSocial
- Youtube - NewPipe (stream or download videos locally)

What’s the application situation?

FDroid is at least as good as the Microsoft Store

- FDroid is getting a major update very soon!
- Easy to find applications that use Material Design
- Look for ones updated recently
- Browse web - 64-bit Chromium
- Secure SMS - Silence or Noise (. . . a Signal fork)
- Twitter - Twidere or SlimSocial
- Youtube - NewPipe (stream or download videos locally)
- Email - K-9 Material

What’s the application situation?

FDroid is at least as good as the Microsoft Store

- FDroid is getting a major update very soon!
- Easy to find applications that use Material Design
- Look for ones updated recently
- Browse web - 64-bit Chromium
- Secure SMS - Silence or Noise (. . . a Signal fork)
- Twitter - Twidere or SlimSocial
- Youtube - NewPipe (stream or download videos locally)
- Email - K-9 Material
- Calendar / Contacts - Davdroid + Etar / Default Contacts app

A few other applications

What else is useful?

- Maps with turn-by-turn directions - OSM Droid

A few other applications

What else is useful?

- Maps with turn-by-turn directions - OSM Droid
- RSS / News - Newsblur

A few other applications

What else is useful?

- Maps with turn-by-turn directions - OSM Droid
- RSS / News - Newsblur
- Podcasts - AntennaPod

A few other applications

What else is useful?

- Maps with turn-by-turn directions - OSM Droid
- RSS / News - Newsblur
- Podcasts - AntennaPod
- Video - VLC

A few other applications

What else is useful?

- Maps with turn-by-turn directions - OSM Droid
- RSS / News - Newsblur
- Podcasts - AntennaPod
- Video - VLC
- Image Gallery - Gallery

A few other applications

What else is useful?

- Maps with turn-by-turn directions - OSM Droid
- RSS / News - Newsblur
- Podcasts - AntennaPod
- Video - VLC
- Image Gallery - Gallery
- Creatively-named applications like Authenticator and Tasks

A few other applications

What else is useful?

- Maps with turn-by-turn directions - OSM Droid
- RSS / News - Newsblur
- Podcasts - AntennaPod
- Video - VLC
- Image Gallery - Gallery
- Creatively-named applications like Authenticator and Tasks
- Use loyalty cards w/o location tracking! - Loyalty Locker

A few other applications

What else is useful?

- Maps with turn-by-turn directions - OSM Droid
- RSS / News - Newsblur
- Podcasts - AntennaPod
- Video - VLC
- Image Gallery - Gallery
- Creatively-named applications like Authenticator and Tasks
- Use loyalty cards w/o location tracking! - Loyalty Locker
- Can set Chromium web apps on home screen

A few other applications

What else is useful?

- Maps with turn-by-turn directions - OSM Droid
- RSS / News - Newsblur
- Podcasts - AntennaPod
- Video - VLC
- Image Gallery - Gallery
- Creatively-named applications like Authenticator and Tasks
- Use loyalty cards w/o location tracking! - Loyalty Locker
- Can set Chromium web apps on home screen

Even MORE applications

These are useful, too!!

- Connect to Matrix network - Riot (So good!)

Even MORE applications

These are useful, too!!

- Connect to Matrix network - Riot (So good!)
- Games - 1010! Konni (self-paced Tetris!)

Even MORE applications

These are useful, too!!

- Connect to Matrix network - Riot (So good!)
- Games - 1010! Konni (self-paced Tetris!)
- Passwords - Twik

Even MORE applications

These are useful, too!!

- Connect to Matrix network - Riot (So good!)
- Games - 1010! Konni (self-paced Tetris!)
- Passwords - Twik
- Github - Forkhub

Even MORE applications

These are useful, too!!

- Connect to Matrix network - Riot (So good!)
- Games - 1010! Konni (self-paced Tetris!)
- Passwords - Twik
- Github - Forkhub
- Facebook - MaterialFBook

Even MORE applications

These are useful, too!!

- Connect to Matrix network - Riot (So good!)
- Games - 1010! Konni (self-paced Tetris!)
- Passwords - Twik
- Github - Forkhub
- Facebook - MaterialFBook
- Notes - OmniNotes

Even MORE applications

These are useful, too!!

- Connect to Matrix network - Riot (So good!)
- Games - 1010! Konni (self-paced Tetris!)
- Passwords - Twik
- Github - Forkhub
- Facebook - MaterialFBook
- Notes - OmniNotes
- Weight Tracking - openScale

Even MORE applications

These are useful, too!!

- Connect to Matrix network - Riot (So good!)
- Games - 1010! Konni (self-paced Tetris!)
- Passwords - Twik
- Github - Forkhub
- Facebook - MaterialFBook
- Notes - OmniNotes
- Weight Tracking - openScale
- Two-Factor Authentication - OTP Autheticator

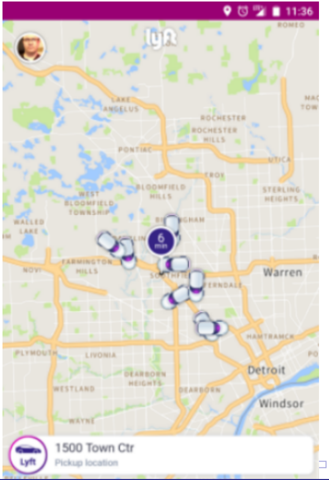
Even MORE applications

These are useful, too!!

- Connect to Matrix network - Riot (So good!)
- Games - 1010! Konni (self-paced Tetris!)
- Passwords - Twik
- Github - Forkhub
- Facebook - MaterialFBook
- Notes - OmniNotes
- Weight Tracking - openScale
- Two-Factor Authentication - OTP Autheticator

OHAI WEB APPZ

5 months in, I discover https://m.lyft.com



What about Google Play Services

- Can use it!

What about Google Play Services

- Can use it! if you want to bork your device!

What about Google Play Services

- Can use it! if you want to bork your device!
- Adding Google Play services wrecks veried boot

What about Google Play Services

- Can use it! if you want to bork your device!
- Adding Google Play services wrecks veried boot
- Can build Copperhead w/Google Play from source and self-sign, but you're on your own

What about Google Play Services

- Can use it! if you want to bork your device!
- Adding Google Play services wrecks veried boot
- Can build Copperhead w/Google Play from source and self-sign, but you're on your own
- Can side-load apps, but that's hackish

What about Google Play Services

- Can use it! if you want to bork your device!
- Adding Google Play services wrecks veried boot
- Can build Copperhead w/Google Play from source and self-sign, but you're on your own
- Can side-load apps, but that's hackish

Discussion

Let's talk:

Discussion

Let's talk:

- How does this stack up with IOS security?

Discussion

Let's talk:

- How does this stack up with IOS security?
- "Bro, do you even compile your kernel?" (Am I just being a privacy bro?)

Discussion

Let's talk:

- How does this stack up with IOS security?
- "Bro, do you even compile your kernel?" (Am I just being a privacy bro?)
- Would you use this?

Discussion

Let's talk:

- How does this stack up with IOS security?
- "Bro, do you even compile your kernel?" (Am I just being a privacy bro?)
- Would you use this? Encourage someone else to use it?

Discussion

Let's talk:

- How does this stack up with IOS security?
- "Bro, do you even compile your kernel?" (Am I just being a privacy bro?)
- Would you use this? Encourage someone else to use it?
- Other considerations?

Discussion

Let’s talk:

- How does this stack up with IOS security?
- ”Bro, do you even compile your kernel?” (Am I just being a privacy bro?)
- Would you use this? Encourage someone else to use it?
- Other considerations?

Additional Resources

- Copperhead OS Website
- Copperhead OS on Github
- Copperhead OS forum on Reddit
- Copperhead OS on Twitter

Thank you!
– jcampbell - ate - gnome - dote - org –