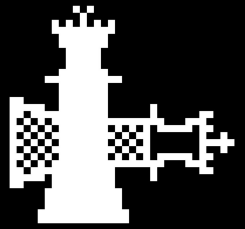
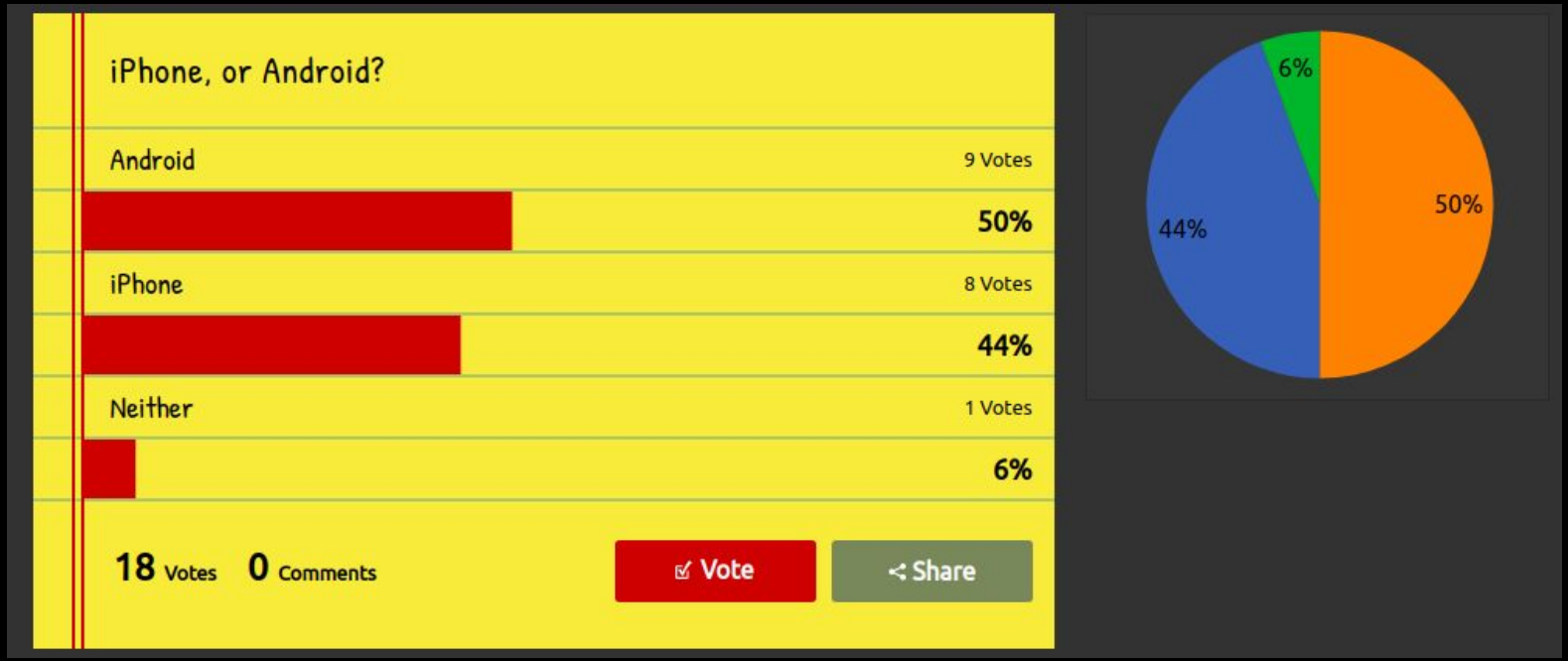
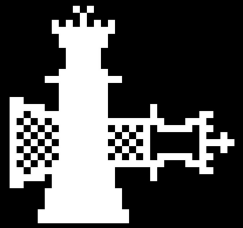


checkm8 in 1:

The Rev-olution that Nobody is Really Talking About

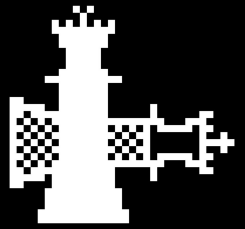
Survey Results





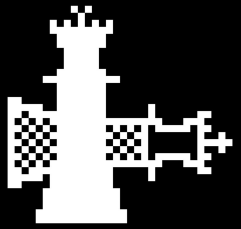
Jailbreaking?

- Patching the XNU kernel that your 🍎 device boots into
  - Used to be just patching `fstab`, but things change
  - Grants write, execute access on the entire filesystem, removes code signing
  - Opens up a world of possibilities
- Useful, or harmful, depending on context…
  - Security research? Very nice!
  - Granting new life to old hardware? Very resourceful!
  - Can leave your device vulnerable (root password unchanged, downloaded sus app )
- Legal, for now...
  - DMCA (Digital Millennium Copyright Act) Section 1201: illegal to circumvent DRM/protections
  - Exemptions list, broadened thanks to EFF and other right to repair activists!
  - Normal people can’t do it, but “security researchers” can!
  - Do your research, and take this presentation with a grain of salt, because this can change



Types of Jailbreaks

- Tethered
  - Boots jailbroken only once, will soft brick in recovery mode if you don’t use a tool on next boot
  - Bruh
- Untethered
  - Survives resets and remains jailbroken w/o assistance
  - The ideal jailbreak type
- Semi-Tethered
  - Will not survive resets, but reverts to usable stock iOS
- Semi-Untethered
  - Survives resets, but requires running an app or visiting a webpage to restore escalated priv

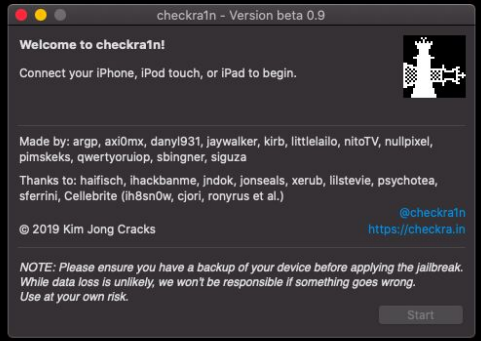


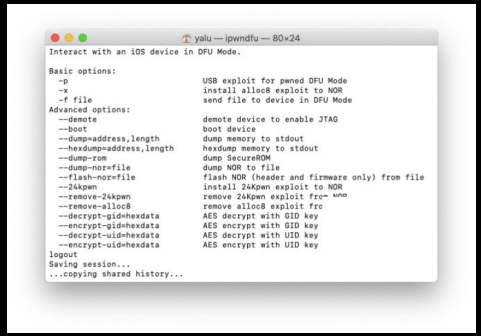
checkm8?

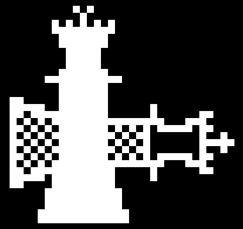
- BootROM exploit discovered by axi0mX in 2019
  - Back to back: alloc8 for the iPhone 3GS (~7 years apart)
  - Apple was hella mad (again)
- Exploits heap overflow in the USB DFU stack
  - Device firmware update
- Affects iOS, iPadOS, tvOS, watchOS, bridgeOS, audioOS, and Haywire
  - Literally everything
- Unpatchable
  - Devices with A5 thru A11 processors will have this vulnerability forever and ever
  - Not unreasonable to expect a similar bootROM exploit later for A12 and onward...

Tools Leveraging checkm8

- checkra1n
  - Personal favorite, although semi-tethered
  - Works on any iOS version if you enable “allow untested iOS/iPadOS/tvOS versions”
  - Works for MacOS and Linux
- bootra1n
  - Void Linux image w/ checkra1n
  - Boot from USB, good workaround for Windows users
- ipwndfu
  - Never used it personally
  - axi0mX made it, so it’s gotta be 💯

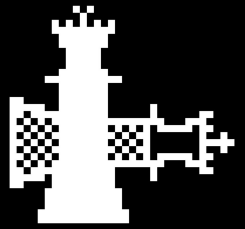






OK, now what?

- Install amazing homebrew
- Intercept and decrypt application traffic
  - Discover mobile-only endpoints
  - See what your fav social app is *really* phoning home about
- See what your apps are leaving on your device
  - Contact lists, cached photos, message logs
  - sqlite3 databases, plists, XML, etc.
- ssh in like a normal device would let you
  - Great for learning about iOS system internals
- PLEASE buy a designated research device
  - Don’t risk pwning yourself...



Resources

- The iPhone Wiki (courtesy of geohot)
  - https://www.theiphonewiki.com/wiki/Main_Page
- iOS App Reverse Engineering (amazing book)
  - https://github.com/iosre/iOSAppReverseEngineering/blob/master/iOSAppReverseEngineering.pdf
- Pangu8's writeup on checkm8
  - https://pangu8.com/jailbreak/checkm8/