**Mobile Phone Weaknesses**

**Baseband Radio Processor**

A chip that manages all the radio functions, uses its own RAM or firmware and the software is usually proprietary

Exploits in this chip can be used to access and modify data on the device remotely

* Even the hardware isn’t trustworthy
* ‘All your basebands are belong to us’

Updates can be forced with backdoors, keyloggers, trojans etc.

Apple could easily send an update to a specific phone

**Wi-Fi and Bluetooth**

When they are on, the access points that are in range can track you

A MAC address is sent out that is observable in the Wi-Fi signal

* Don’t even need to be close to the device, just need a large enough antenna
* Access points have been used to correlate locations whilst a device travels
* As you travel from point to point, the MAC addr gives away where you’re going, at what speed and when

Switch off Wi-Fi and Bluetooth to mitigate this

* Actively change MAC addr whilst moving

Location info can leak from apps

* GPS allows a phone to know where it is
* Cell towers and Wi-Fi network information can also help triangulate this through 3rd party apps
* App provider knows where you are at all time

transmitting this data also means that it could be intercepted at any point

Best mitigation is to disable GPS, Wi-Fi, Bluetooth and to not install the apps

Even Burner phones can be used to correlate your friends, behaviours, co-travellers and other info based on the phone patters

* Can associate burner with other phones you have used

Phones that are switched on occasionally for a short amount of time are marked as burner phones and cross-correlated with other phones in the area to profile

* CyanogenMod
* Ubuntu
* Replicant
* CopperheadOS
* CalyxOS
* LineageOS