Baseband Attacks on Mobile Devices

Garret Naegle

Baseband

- Baseband: manages radio functionality in mobile devices
- Baseband processors typically do not have same countermeasures as application processor

Attack

- Rogue base station set up
- Base station broadcasts stronger signal to make mobile device connect to it instead of authentic base station
- Rogue base station can snoop on user's calls, text messages, etc and issue commands to baseband processor of mobile device

Reverse Engineering

- Baseband firmware manufacturers do not provide any firmware to public
- Baseband firmware binaries can be found in firmware releases done by mobile device manufacturers
- Attempted reversing baseband firmware of several Android and iOS devices

Reverse Engineering

- Baseband firmware is basically RTOS that runs on ARM baseband processor
- Reversing and trying to understand what the firmware is doing proved to be extremely difficult
- Not a lot of resources or guidance available
- Found a couple places where a buffer overflow was potentially possible, but was unable to test

Hayes (AT) Commands

- Developed in 1981 to communicate with modem; still supported by smartphones
- Can be used in attack by rogue base station redirecting execution to certain command handler
- Auto-answer, make calls/texts, read/write phonebook entries, forward calls, etc
- Supported commands depend on device

Current Countermeasures?

- Baseband manufacturers not revealing any advancements in baseband attack countermeasures
- Detection of rogue base stations is possible by checking if ciphering is present between base station and device
- Cell phones being sold that monitor baseband processor activity and attempt to detect when a baseband attack is being made

Questions?