Android-specific changes to the linux kernel

Need to have finer control over which devices are suspended (eg music still playing while screen turned off
Android added wakelocks to kernel

- kernel is set to suspend as soon and as often as possible
- drivers need to actively prevent system from suspending device (and therefore, kernel)
- Have several wakelocks, which keep combination of CPU, screen and keyboard awake

Using wakelocks properly is crucial to achieve long battery life

Binder

- Android uses RPCs very frequently
- Add new RPC mechanism called binder to kernel
- copies directly from user space of writer to user space of reader
- integrates capability mechanism into RPC
- use separate thread pool for incoming RPC for system services

Shared memory

Android kernel provides new shared memory mechanism (ashmem)

- provides reference counting so that kernel can reclaim unused resources
- standard use: process opens shared memory region and share obtained file descriptor through binder

Alarm timers

Standard linux kernel timers not sufficient for advanced power management
Android introduces alarm timers:

- Alarm timers wake up particular process even if system is suspended
- Application will grab wakelock once woken up

Low memory killer

- When system runs out of memory, linux kills greedy processes
- Behaviour unpredictable, could kill important components (eg telephony stack, graphic subsystem)
- Remedy: introduce separate process killer which takes time since application was last used and priority into account
- memory killer takes increasingly severe action

Security enhancements

- Assign a separate user id to each app
- Force all data exchange between apps to go via binder, with fine-grained access control mechanisms
- For system services running as root use selinux-kernel extensions, which specify which file can be accessed by which process.
- $\Rightarrow$ Vulnerabilities in system services do not immediately lead to full access

Network security

- Linux kernel allows any process to open socket and initiate network communication
- Android introduces network permission, filtered by group id
- permission needed to access IP, Bluetooth or raw sockets