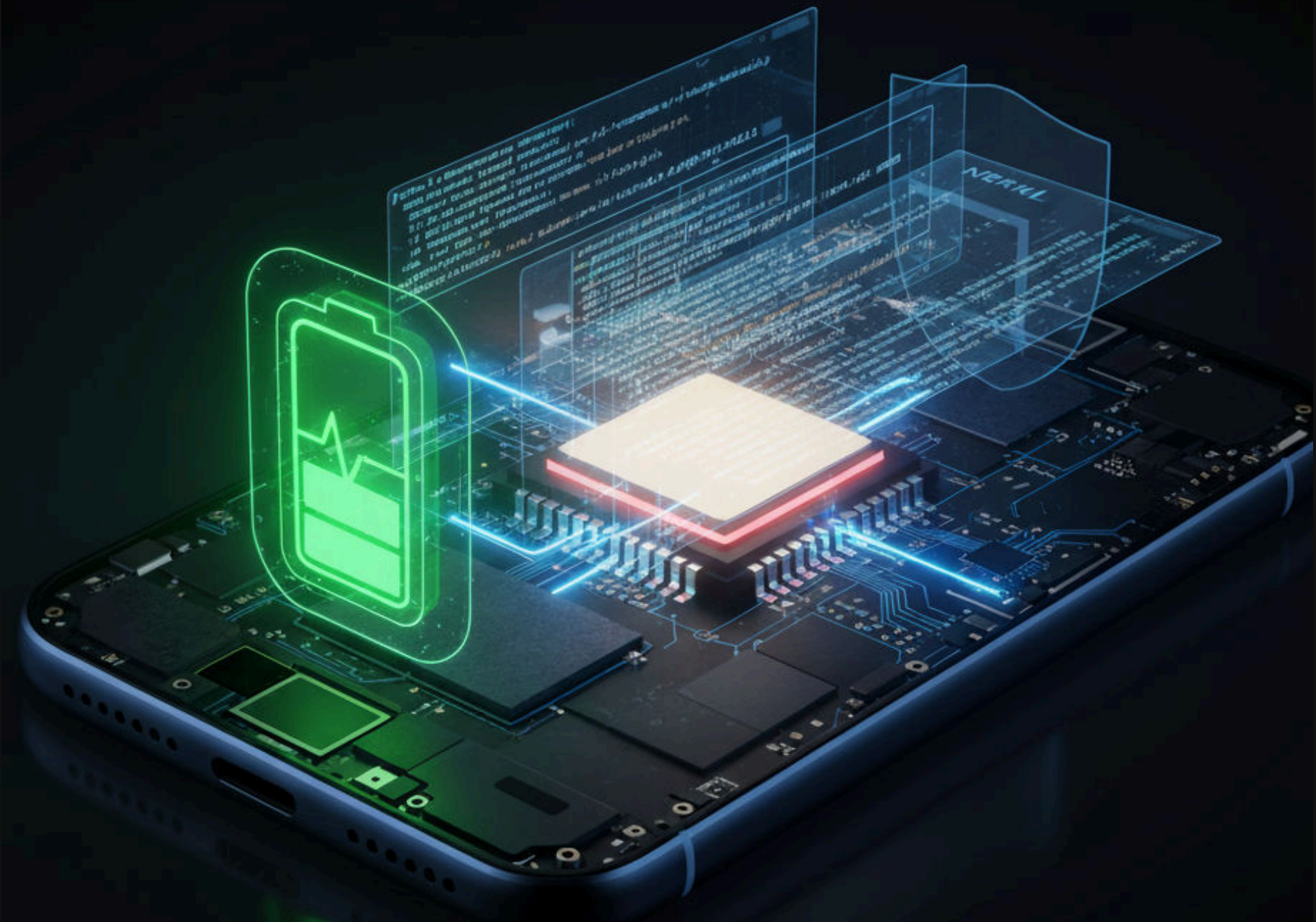


Binder IPC:

The Secret to Secure and Instant Communication in Android

Why Android replaced standard Linux IPC methods (Sockets, Pipes) with its own bespoke Kernel driver.



Esmaeel Moradi
@esmaeel-moradi700



Binder IPC: The Secret to Secure and Instant Communication in Android

**Why Android replaced standard Linux IPC
methods (Sockets, Pipes) with its own bespoke
Kernel driver.
(Swipe to see how it achieves Single-Copy.)**



Esmameeil Moradi
@esmaeeil-moradi700



The Problem with Traditional Linux IPC

The Bottleneck: Double-Copy

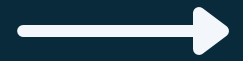
Standard Linux IPC (like Pipes or Sockets) requires the data to be copied at least twice to move between processes (A and B):

1. **Copy 1:** From Process A's User Space to the Kernel Space.
2. **Copy 2:** From the Kernel Space back out to Process B's User Space.

This Double-Copy leads to excessive CPU overhead and Latency, unacceptable for a responsive mobile OS.



Esmaeel Moradi
@esmaeeil-moradi700



The Binder Solution:Single-Copy

Binder's Innovation: Memory Remapping

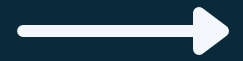
Binder solves the Double-Copy problem using a clever mechanism:

- **The Kernel Buffer:** Each process maps a shared memory buffer into the Kernel Space via `mmap`.
- **The Process:** Data is copied only once (from Sender's User Space to the shared Kernel Buffer).
- **Zero-Copy to Receiver:** The Kernel then uses Memory Remapping to make the data instantly available in the Receiver's User Space.

Result: A single, fast copy operation instead of two.



Esmaeel Moradi
@esmaeeil-moradi700



Security at the Kernel Level

Why Binder is Safe:

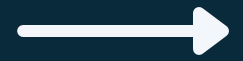
Binder is implemented as a Linux Kernel Driver, giving it powerful capabilities:

- **Context Management:** It tracks which process (PID/UID) is sending and receiving, managing Context Switching efficiently.
- **Security Validation:** The Kernel validates the PID and UID of the caller before granting access to a service. This is the foundation of Android's permission model.

Crucially: Security decisions (who can talk to whom) are made and enforced deep inside the trusted Kernel, not in User Space.



Esmaeel Moradi
@esmaeeil-moradi700



Parcel and Conclusion

The Data Unit: Parcel

- **Parcel:** Binder's light-weight serialization object. It's optimized for efficiency and speed within the IPC process.
- **Conclusion:** Binder is not just an IPC mechanism; it's a security and performance contract between all Android processes, managed entirely by the Kernel.



Esmaeeil Moradi
@esmaeeil-moradi700

✦✦ How does the system
prevent RAM starvation?

We analyze LMKD and the OOM
Score mechanism.

Follow the thread! ✦✦



Esmaeel Moradi
@esmaeeil-moradi700