Exploiting Cell Re-Mapping: The "Ghost Spare" & Spec-Padding Fraud

Enterprise-grade DRAM features internal, vendor-configured spare rows or columns designed to replace faulty silicon natively at the hardware level. Bad actors exploit this tracking and repair logic in two distinct ways:

a) **Falsifying Repaired Modules as "Factory Fresh":** Malicious refurbishers acquire rejected, heavily degraded, or end-of-life server memory. They use specialized hardware fixtures to rewrite the EEPROM (specifically the Serial Presence Detect or SPD chip) or force internal registers to utilize all available factory-re-mapped rows. They mask high defect rates, selling a heavily deteriorated silicon die as pristine, zero-error enterprise stock.

b) **The "Ghost Capacity" Over-Provisioning Fraud:** Sophisticated supply chain threat actors alter the memory controller configuration and SPD information. They program the module to present a clean, fault-free topology to the system. However, they internally route duplicate physical memory addresses to the same re-mapped "healthy" blocks. This creates phantom memory capacity (e.g., selling a modified module as 64GB when it physically only contains 32GB of viable silicon), a technique related to memory aliasing exploits.

Exploiting Cell Fencing: The "BadRAM" Overclocking & Relabeling Scam

Cell fencing is traditionally an operating system or firmware mechanism (like BadRAM parameters in Linux or the Windows {badmemorylist}) used to permanently block out damaged memory pages so a machine doesn't crash. Fraudsters flip this defensive tool into a method for masking systematic hardware defects:

a) **Pre-Fencing Defective Dies:** Fraudulent suppliers source cheap consumer-grade or factory-rejected memory chips with high defect counts. Instead of physically repairing them, they inject pre-configured configurations into the module’s built-in non-volatile memory or custom firmware. This forces the host server's memory controller to automatically "fence" or retire thousands of bad pages upon boot.

b) **The Premium-Grade Spoof:** To the unsuspecting IT procurement department, the module registers as an expensive, high-density server stick. In reality, a significant portion of its capacity is permanently locked out (fenced) from the moment it is plugged in, robbing the enterprise of the actual memory bandwidth and density they paid for