Chapter 45: Data Integrity and Protection

1. The Challenge of Data Integrity

- The goal of data integrity is to ensure that the data we read from a storage device is the same as the data we wrote to it.
- Modern disks have complex failure modes that go beyond simple, complete failure.

2. Disk Failure Modes

- **Latent Sector Errors (LSEs):** A disk sector becomes damaged and unreadable. The disk can detect this error and report it.
- **Block Corruption:** A “silent” error where a block of data is altered without the disk detecting the change. This can happen due to misdirected writes or other hardware issues.

3. Handling Latent Sector Errors

- Since LSEs are detected by the drive, they can be handled by storage systems using redundancy (e.g., RAID).
- If a sector is unreadable, the data can be reconstructed from a parity block or a mirrored copy.

4. Detecting Corruption with Checksums

- To detect silent data corruption, we use **checksums**.
- A checksum is a small, fixed-size value computed from a larger block of data.
- **How it works:**
  1. When a data block is written, a checksum is computed and stored with it.
  2. When the data block is read, the checksum is recomputed and compared to the stored checksum.
  3. If the checksums do not match, the data is considered corrupt.

Checksum Code Example

```c
// Simplified checksum logic
int is_corrupt(char *block, int size, uint32_t stored_checksum) {
    uint32_t new_checksum = fletcher32(block, size);
    return (new_checksum != stored_checksum);
}
```

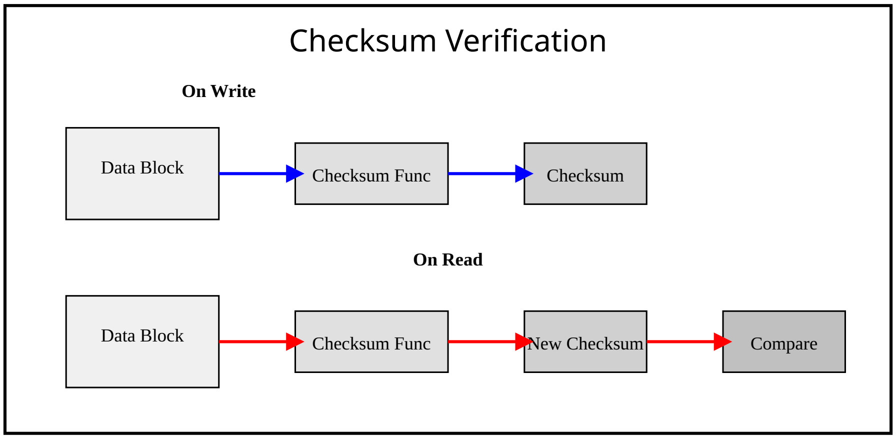

Figure 1: Checksum Verification

5. Checksum Functions

- There are various checksum functions, with a trade-off between speed and protection strength:
  - **XOR-based:** Simple and fast, but not very robust.
  - **Fletcher checksum:** Stronger than simple XOR.
  - **Cyclic Redundancy Check (CRC):** A widely used and robust method.

6. Advanced Data Integrity Problems

- **Misdirected Writes:** A block is written to the wrong location. This can be detected by including the block's physical address in the checksum calculation.
- **Lost Writes:** The disk reports that a write is complete, but the data was never actually written. This is a very difficult problem to solve.

7. Proactive Data Protection: Disk Scrubbing

- **Disk scrubbing** is a proactive approach to finding and fixing latent errors.
- A background process periodically reads all data on the disk, verifies the checksums, and corrects any errors it finds using redundant copies.
- This helps to prevent data loss by finding and fixing errors before they are needed for a reconstruction.

8. Summary

- Data integrity is a critical aspect of modern storage systems.

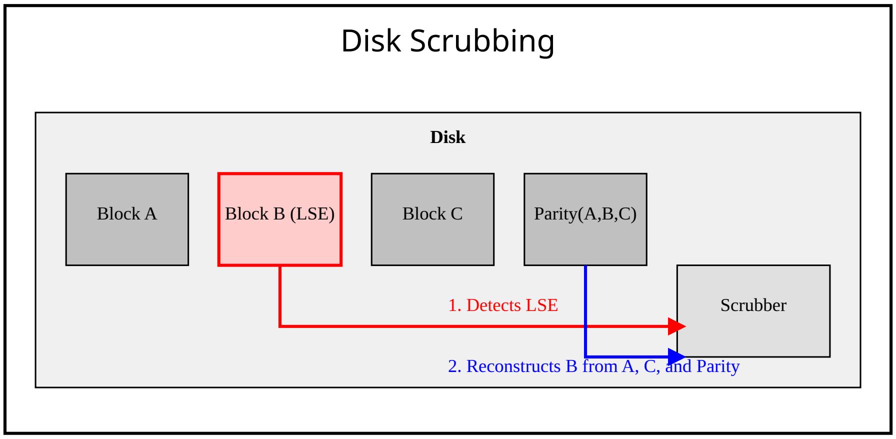

Figure 2: Disk Scrubbing

- Checksums are a powerful tool for detecting silent data corruption.
- Proactive techniques like disk scrubbing can help to find and fix errors before they lead to data loss.