File System Security

What does a file system do?

- A **file system** is a method for storing and organizing computer files and the data they contain to make it easy to find and access them.
- File systems exist on hard drives, pen drives, cd's, dvd's and any other form of data storage medium
- Most data storage devices have array of fixed-size blocks, sometimes called sectors, and file system is in charge of organizing these sectors into files and directories. It is also in charge of indexing the media so it knows where and what each file is

Types of File Systems

- Disk file systems – FAT (File Allocation Table), NTFS, HFS (Hierarchical File System), ext2, ext3, ISO9660 and UDF
- FAT(FAT12, FAT16, FAT32), and especially NTFS are primarily used on Windows operating systems. FAT is also the standard file system for floppy drives and is still used today
- HFS is used by Mac OS, and ext2, ext3 are used on various linux operating systems
- ISO9660 and UDF are used on optical media

How does the file system handle security?

- The file system is crucial to data integrity.
- Main method of protection is through access control
- Accessing file system operations (ex. modifying or deleting a file) are controlled through access control lists or capabilities
- Capabilities are more secure so they tend to be used by operating systems on file systems like NTFS or ext3.
- Secondary method of protection is through the use of backup and recovery systems

Attacks on the file system

- Race Condition Attacks
- Using ADS to hide files
- Directory traversal

Race Condition Attacks

- Occurs when a process performs a sequence of operations on a file, under the assumption that they are executed atomically.
- Can be used by the attacker to change the characteristics of that file between two successive operations on it resulting in the victim process to operate on the modified file.

Using ADS to hide Files

- Alternate Data Streams(ADS) allows multiple data streams to be attached to a single file.
- A file can be hidden behind a file as an attached stream that could be hundreds of megabytes in size, however a directory listing will only display the file's normal size.

Directory Traversal

- An exploit caused by lack of insufficient security validation of user supplied input file names
- For example the attacker would pass this as input. ../../../../../../../../../etc/password to retrieve the password file from the server.

How does the file system ensure data integrity?

- There are various methods of protecting the files on a file system.
- Access Controls
- Encryption
- RAID
- Recovery when data is corrupted

Access Control

- Access Control plays a huge part in file system security
- The system should only allow access to files that the user is permitted to access
- Almost all major file systems support ACL's or capabilities in order to prevent malicious activity on the file system
- Depending on the users rights they can be allowed to read, write and/or execute and object. In some file systems schemes only certain users are allowed to alter the ACL on a file or see if a file even exists.
- Ultimately the less the user has access to the less that can go wrong and the integrity of the disk can be more guaranteed.

General File System Encryption

- Encryption is also a method used by file systems to secure data, NTFS for example offers file encryption using DESX
- Two method of disk encryption
  - Full Disk Encryption
  - File System Encryption
- File system encryption has a few advantages over full disk encryption for example
  1. File based key management
  2. Individual management of encrypted files
  3. Access control can be further strengthened through the use of public key cryptography
  4. Keys are only held in memory while the file is being used

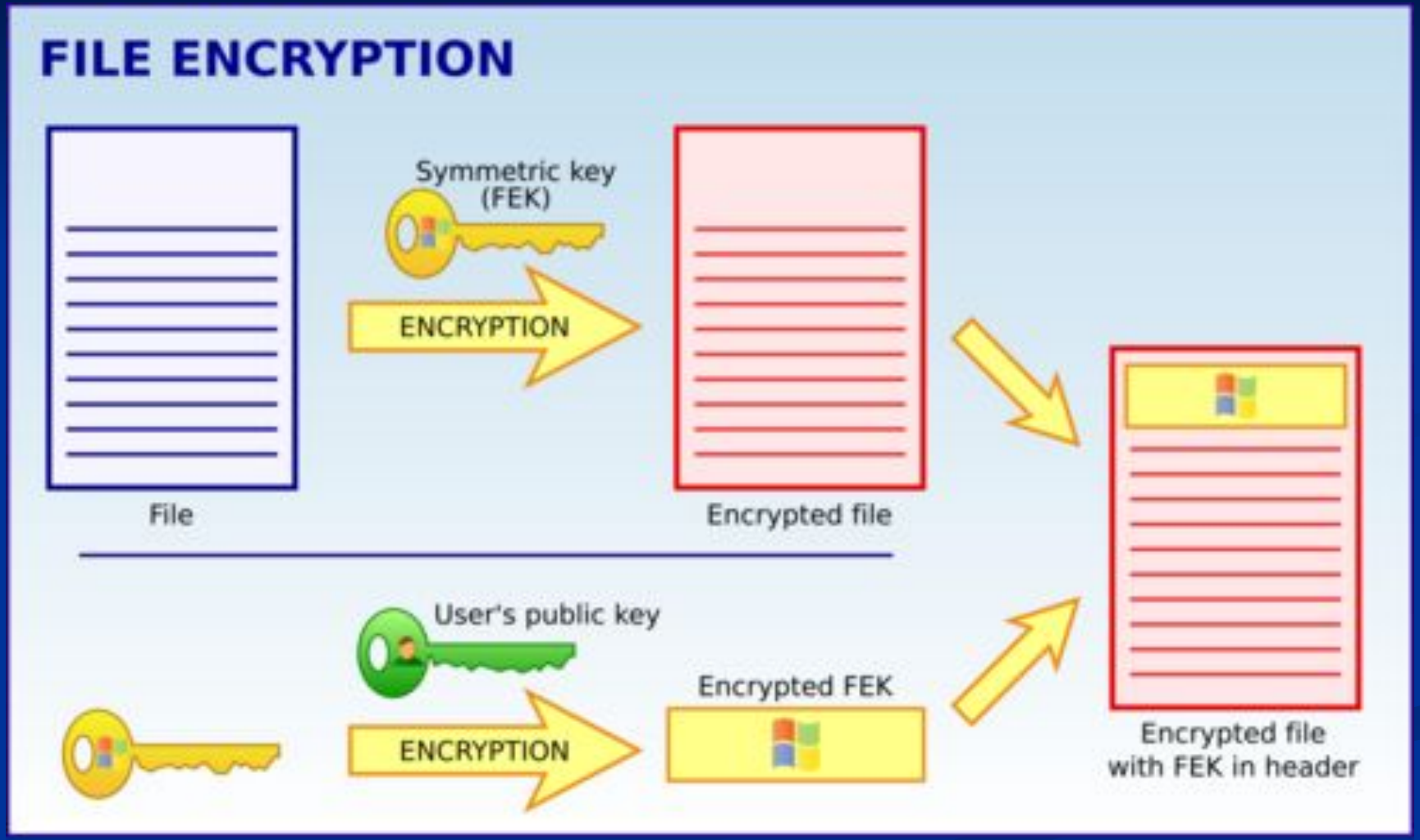
Encrypting File System(EFS)

- Provides security beyond user authentication and access control lists. For example when the attacker has physical access to the computer.
- EFS uses public key cryptography however it is susceptible to brute-force attacks against the user account passwords.

EFS Encryption

- EFS works by encrypting a file with a bulk symmetric key, aka File Encryption Key or FEK.
- The FEK is encrypted with a public key that is associated with the user that encrypted the file.

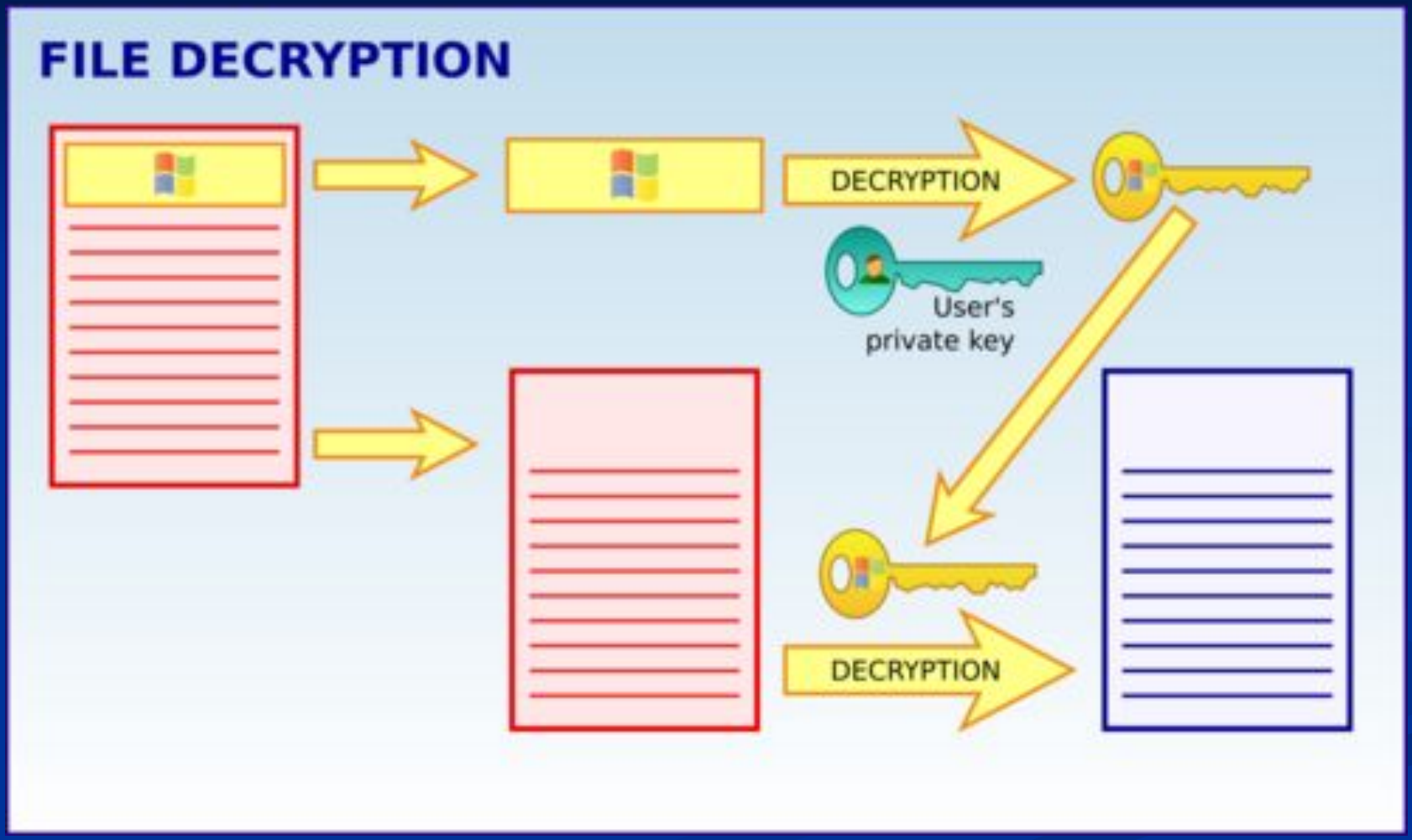
EFS Encryption



EFS Decryption

- The EFS uses the private key that matches the EFS digital certificate (that was used to encrypt the file) to decrypt the symmetric key.
- The resulting symmetric key is then used to decrypt the file.

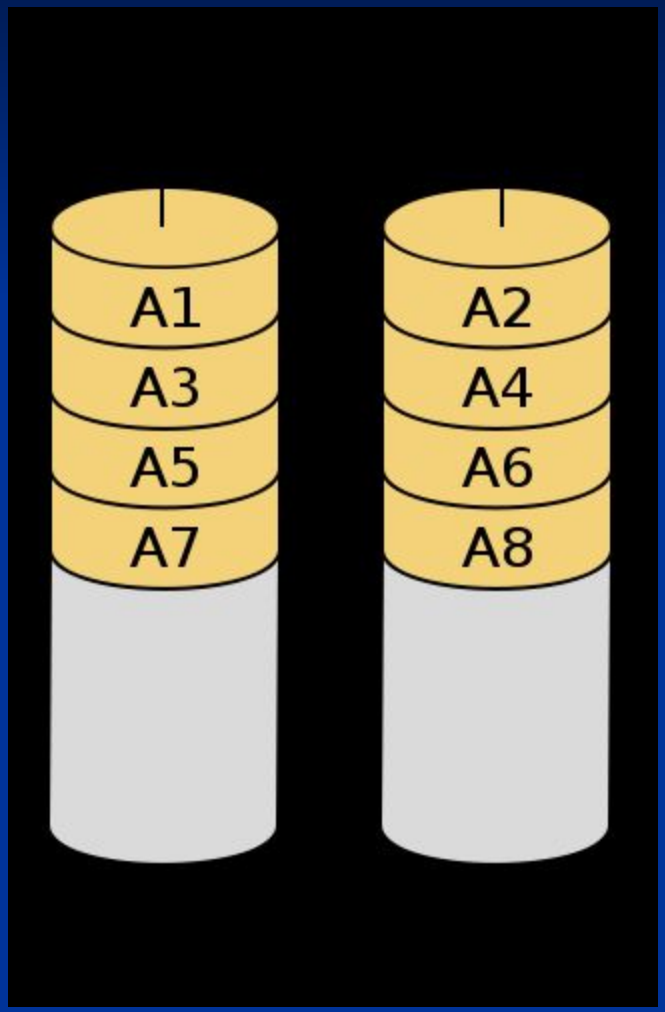
EFS Decryption

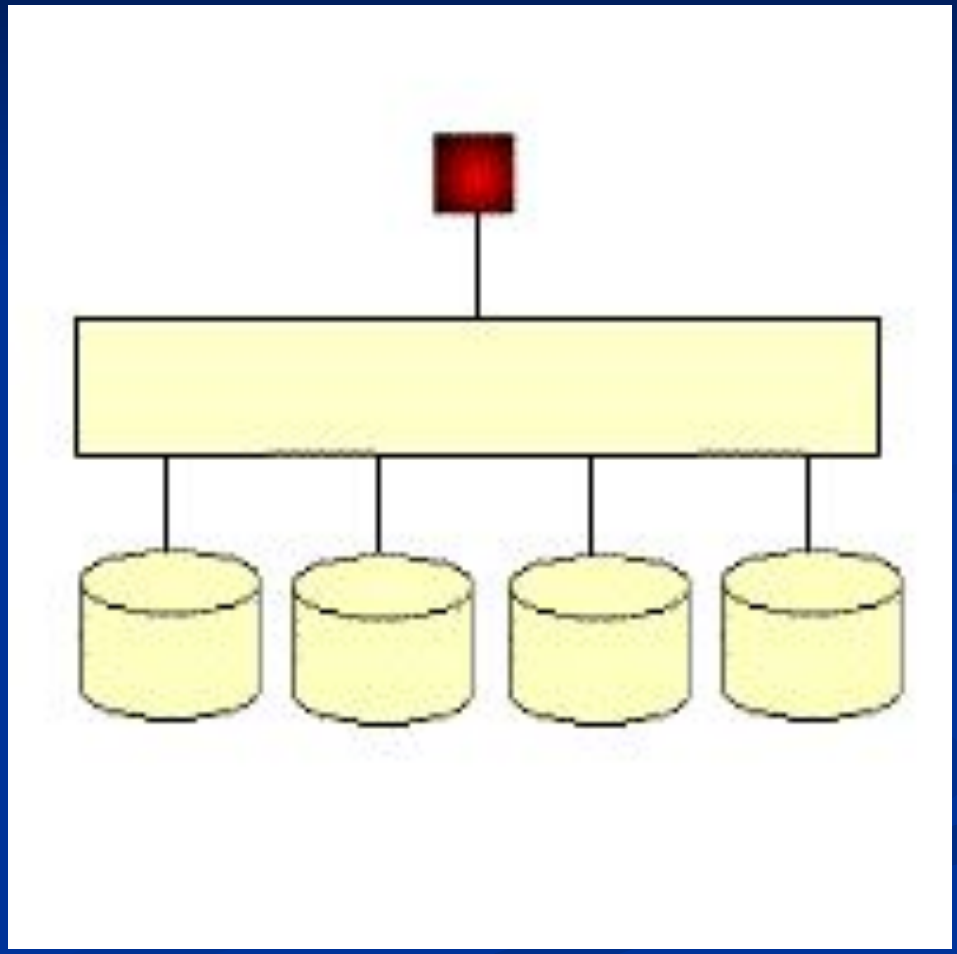


RAID

- RAID stands for Redundant Array of Independent Disks
- Offers drawbacks and advantages over a single disk, each with different applications
- Types of RAID
  - RAID 0 “Striping set without parity”
  - RAID 1 “Mirrored set without parity”
  - RAID 3 “Striped set with byte level parity”
  - RAID 4 “Striped set with block level parity”
  - RAID 5 “Striped set with distributed parity”
  - RAID 6 “Striped set with dual distributed parity”

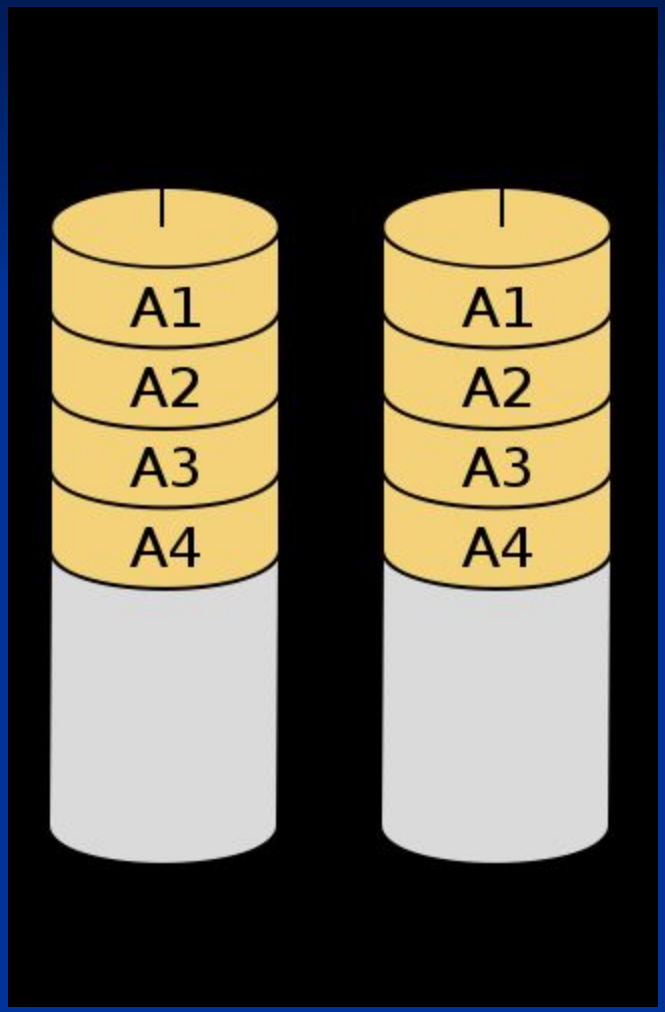
RAID 0

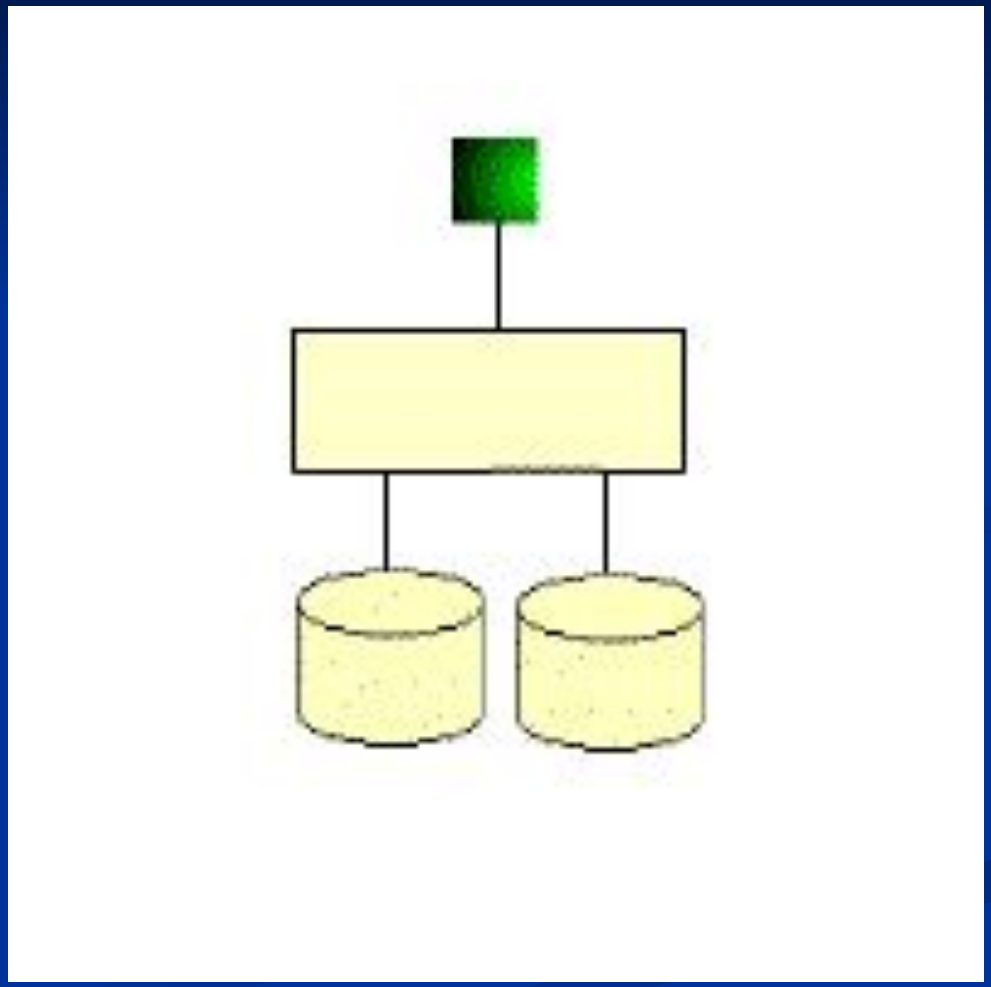




Striping set without parity

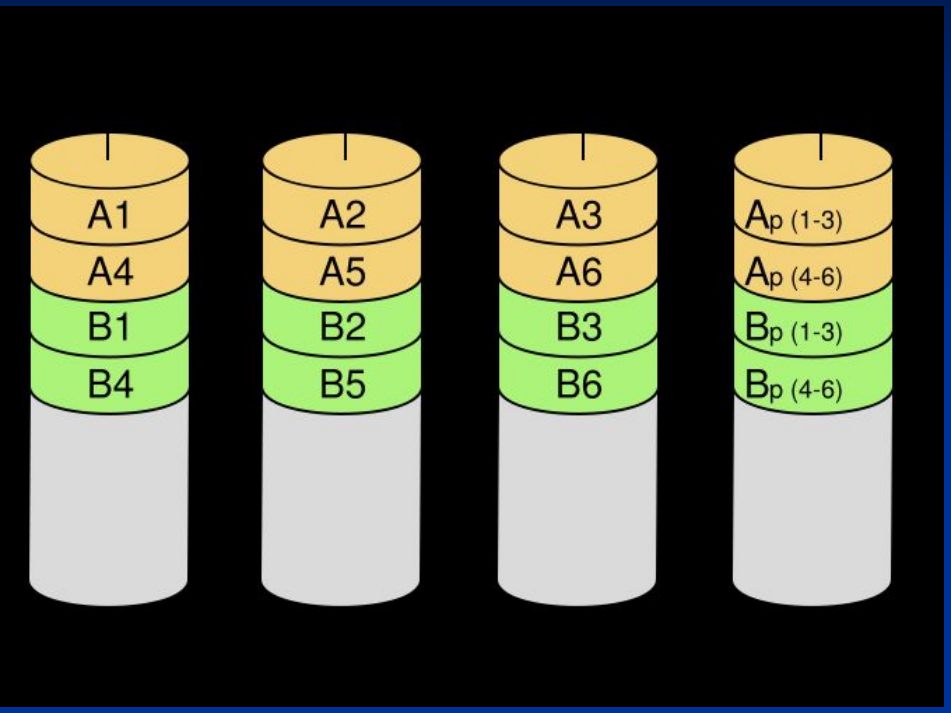
RAID 1

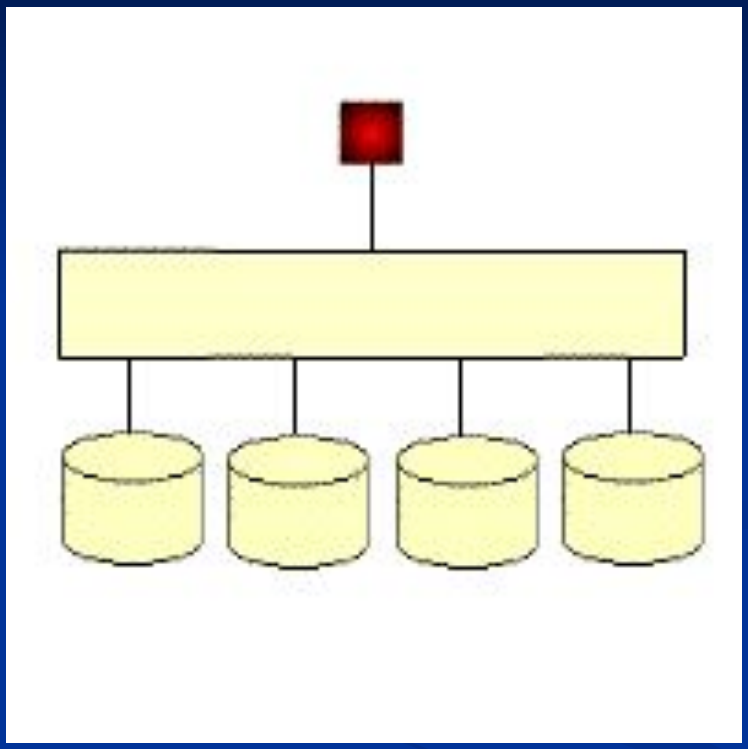




Mirrored set without parity

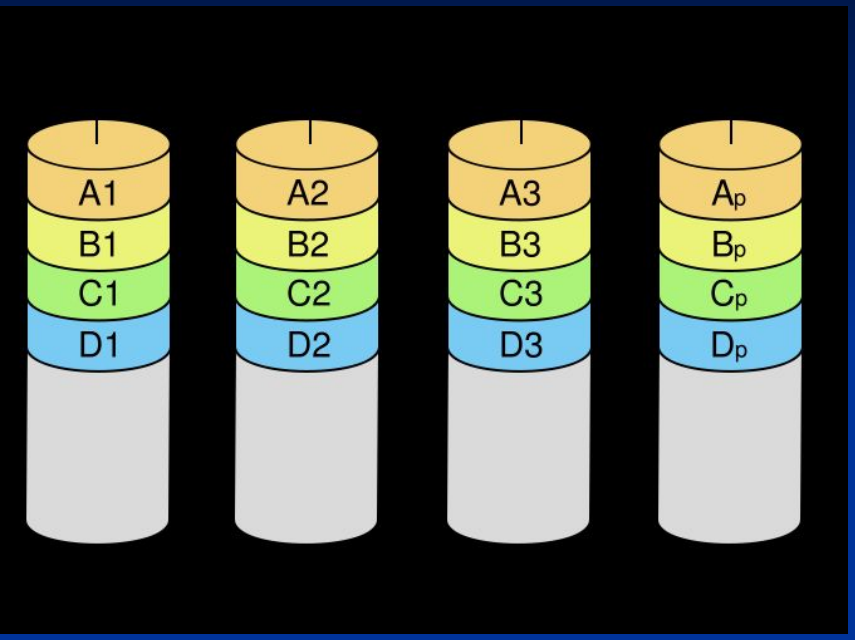
RAID 3

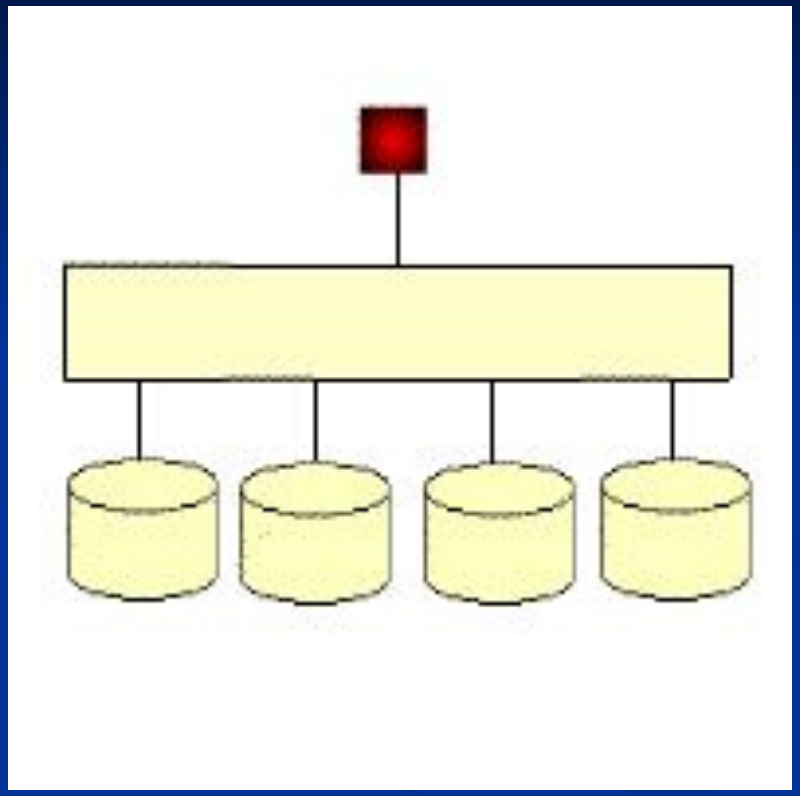




Striped set with byte level parity

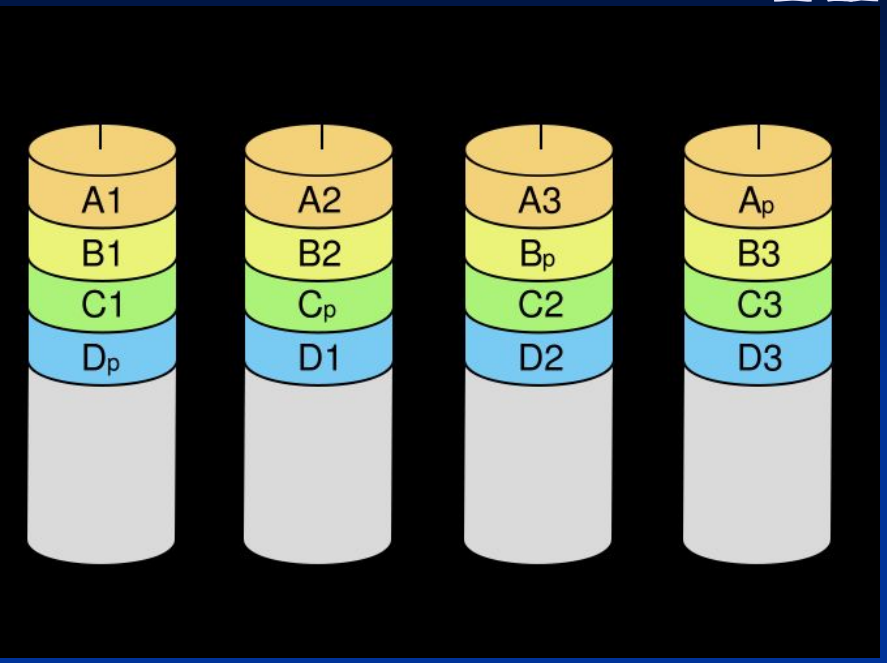
RAID 4

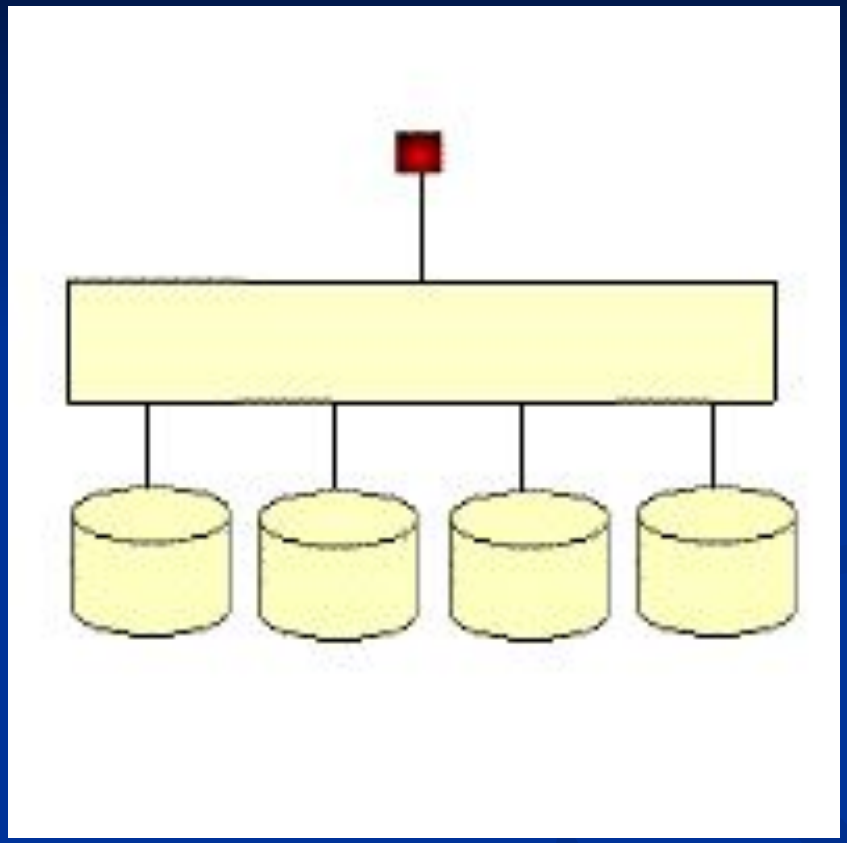




Striped set with block level parity

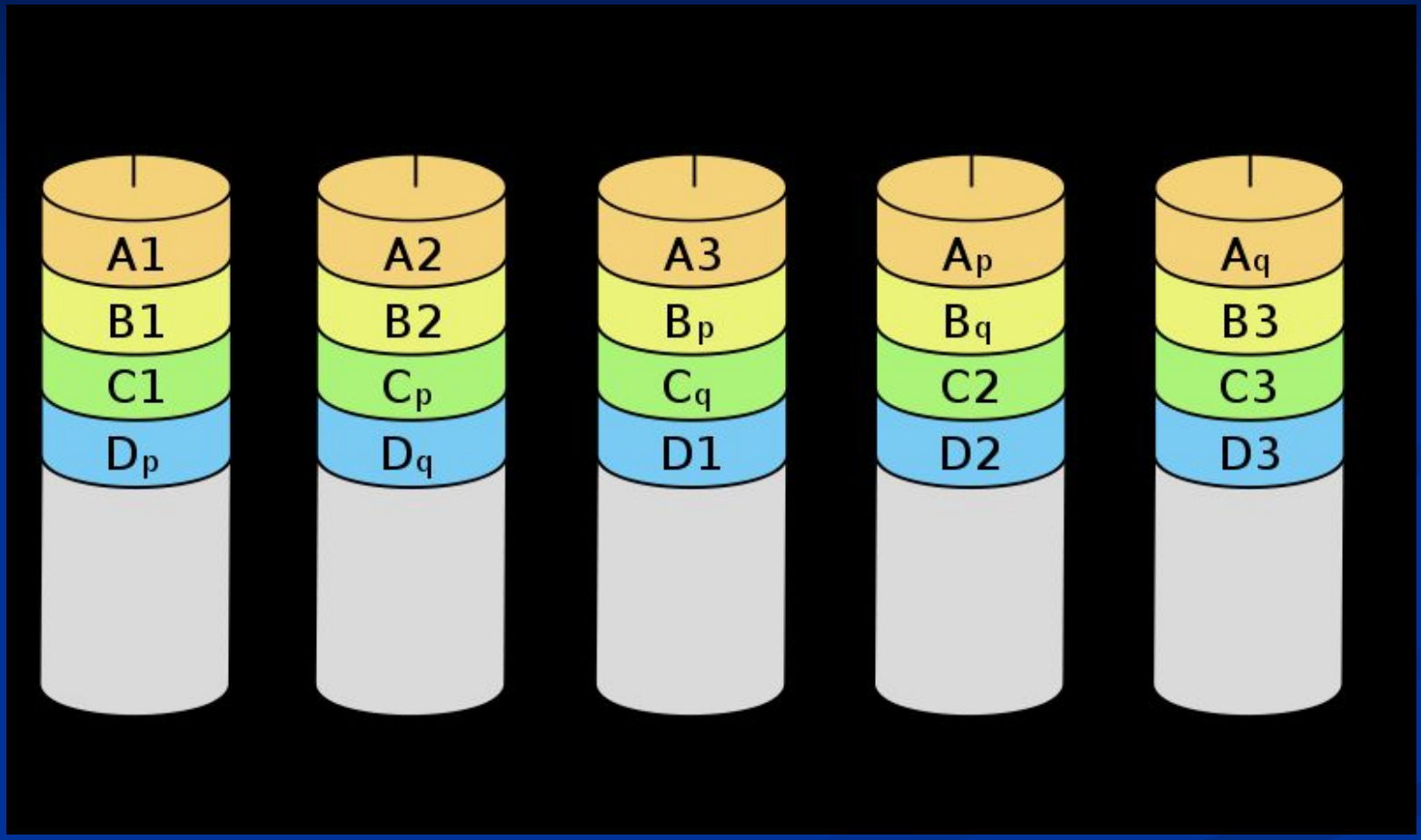
RAID 5





Striped set with distributed parity

RAID 6



Striped set with dual distributed parity

What happens when something is corrupted?

- Checksum codes
- Reed Soloman Codes (cd's to fix errors caused by scratches)
- Given the right type of RAID, the system can recover easily.
  - Parity Schemes
  - Protection against individual drive failure

File System Security's Future

- Example: Sun's ZFS
  - Released in 2006
  - Marked a departure from file systems of previous years by integrating new methods of storage, access and security
- Has two advantages in computer security compared with other file systems
  - Copy-on-write technology
  - Self Healing File system