WHATSAPP SECURITY

WhatsApp's end-to-end encryption ensures that only you and the person you're communicating with can read what's sent. Nobody in between, not even WhatsApp, can read the messages. The messages are secured with locks, and only the recipient has the special key to unlock and read the messages. WhatsApp uses Signal Protocol developed by Open Whisper Systems.

The following steps describes the working of E2EE when two people communicate on WhatsApp.

1. When the user first opens the WhatsApp, two different keys (public & private) are generated. The encryption process takes place on the phone itself
2. The private key must remain with the user whereas the public key is transferred to the receiver via the centralized WhatsApp server
3. The public key encrypts the senders message on the phone even before it reaches the centralized server
4. The server is only used to transmit the encrypted message. The message can only be unlocked by the private key of the receiver. No third part, including WhatsApp can intercept and read the message
5. If a hacker tries to hack and read the messages, they would fail because of the encryption

How do I verify that WhatsApp is using end-to-end encryption?

To manually verify the encryption between the sender and the receiver, simply tap on the contacts name on WhatsApp to open the info screen. Now tap on 'Encryption' to view the QR code and 60-digit number. You can scan your contacts' QR code or visually compare the 60-digit number. If you scan the QR code, and if they match, then your chats are encrypted and no one is intercepting your messages or calls.

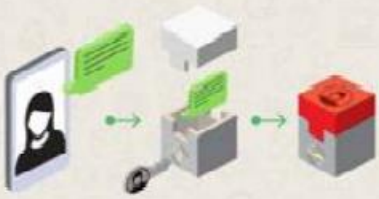
WhatsApp is Secure

How end-to-end encryption works

1. Two keys, public and private are generated when a user opens WhatsApp for the first time. The encryption process takes place on your phone.

2. The private key remains with the user on the phone. The public key is transmitted through the server to the receiver.

3. The public key encrypts the sender's message on the phone even before it reaches the server.



4. The server is only used to transmit the encrypted message. Only the receiver's private key can unlock the message. No third party including WhatsApp can read the message.

A hacker's nightmare

If someone tries to hack WhatsApp, they will not be able to reach any messages because they are end-to-end encrypted.

Verify end-to-end encryption yourself

Simply tap on the contact name, open the contact info screen. Tap Encryption to view the QR code and 60-digit number.

BIOS

BIOS is short for Basic Input Output System. BIOS is a firmware, in short. It is stored on a chip on the part of the computer motherboard and is basically, a set of instructions that run to help load the operating system. You OS would fail to load, if not for the BIOS!

When you turn on the computer, BIOS instructions are initiated. These instructions make it check the RAM and the Processor (for faults) on your computer.

1. It enumerates the RAM by checking each compartment to see if all of them are working.

2. After checking out RAM and Processor, it checks for other devices attached to the computer

3. It detects all the peripherals, including the keyboard and mouse and then checks for the boot options

4. Boot options are checked in the sequence configured in your BIOS: Boot from CD-ROM, Boot From Hard Drive, Boot from LAN, etc.

5. It checks for bootstraps on the devices in the order you or the machine vendor configured the BIOS.

6. It passes reigns of the computer to the operating system by loading the essential parts of the OS into the random access memory (RAM) reserved for the OS, after bootstrap is located.

This is not a comprehensive list of functions of the BIOS. It also checks up CMOS, and other chips to set up the date and time on the computer, and to load the device drivers into the memory. It checks and uploads input and output interrupts (signals) to the RAM so that the operating system knows what is happening. For example, if a user presses a key, an interrupt request is created and passed on to the BIOS which sends it to the operating system. The operating system then decides what action to take, according to the way it is programmed.

BOOTING PROCESS

Booting (also known as booting up) is the initial set of operations that a computer system performs when electrical power is switched on. The process begins when a computer that has been turned off is re-energized, and ends when the computer is ready to perform its normal operations. On modern general purpose computers, this can take tens of seconds and typically involves performing power-on self-test, locating and initializing peripheral devices, and then finding, loading and starting an operating system. Many computer systems also allow these operations to be initiated by a software command without cycling power, in what is known as a soft reboot, though some of the initial operations might be skipped on a soft reboot. A boot loader is a computer program that loads the main operating system or runtime environment for the computer after completion of self-tests.

The computer term boot is short for bootstrap or bootstrap load and derives from the phrase to pull oneself up by one's bootstraps. The usage calls attention to the paradox that a computer cannot run without first loading software but some software must run before any software can be loaded. Early computers used a variety of ad-hoc methods to get a fragment of software into memory to solve this problem. The invention of integrated circuit Read-only memory (ROM) of various types solved the paradox by allowing computers to be shipped with a start up program that could not be erased, but growth in the size of ROM has allowed ever more elaborate start up procedures to be implemented.

There are numerous examples of single and multi-stage boot sequences that begin with the execution of boot program(s) stored in boot ROMs. During the booting process, the binary code of an operating system or runtime environment may be loaded from nonvolatile secondary storage (such as a hard disk drive) into volatile, or random-access memory (RAM) and then executed. Some simpler embedded systems do not require a noticeable boot sequence to begin functioning and may simply run operational programs stored in read-only memory (ROM) when turned on.

UEFI

Short for Unified Extensible Firmware Interface, UEFI is a specification that defines a more modernized model for the interface between computer operating systems and platform firmware during the boot, or start-up, process.

UEFI originated as the Intel Boot Initiative in the late 1990s before being turned over to the Unified EFI Forum, and today the forum and specification remain the result of a collaborative effort between computer processor manufacturers like AMD and Intel and software operating system companieslikeMicrosoftandApple.

In many ways, UEFI serves as a software-driven, bare-bones operating system that can sit on top of the legacy BIOS boot process, and like BIOS, UEFI is responsible for initializing the hardware of a device or computer before passing control of the hardware to the operating system. Most newer computer platforms support both UEFI and legacy BIOS booting in order to ease the transition to UEFI and accommodate older operating systems that don't have built-in UEFI support.

The UEFI specification offers advanced features over BIOS such as secure boot, low-level cryptography, network authentication and universal graphics drivers. The Secure Boot functionality in UEFI provides the basis for the Microsoft Secure Boot feature in Windows 8 that enables the OS to detect rootkits and similar malware attacks.

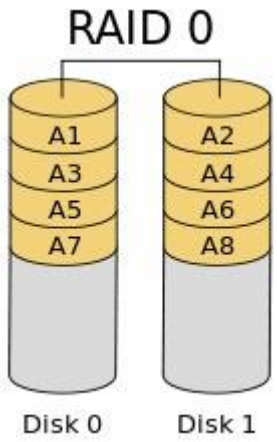
Differentiate RAID and LIM

RAID

RAID (Redundant Array of Independent Disks, originally Redundant Array of Inexpensive Disks) is a data storage virtualization technology that combines multiple physical disk drive components into one or more logical units for the purposes of data redundancy, performance improvement, or both.

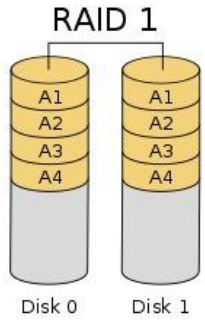
RAID 0

RAID 0 consists of striping, without mirroring or parity. The capacity of a RAID 0 volume is the sum of the capacities of the disks in the set, the same as with a spanned volume. There is no added redundancy for handling disk failures, just as with a spanned volume. Thus, failure of one disk causes the loss of the entire RAID 0 volume, with reduced possibilities of data recovery when compared with a broken spanned volume.



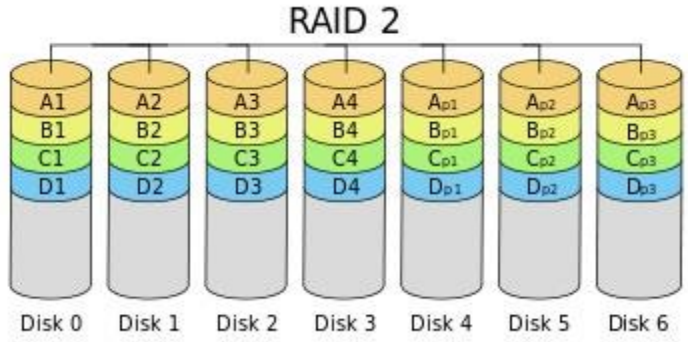
RAID 1

RAID 1 consists of data mirroring, without parity or striping. Data is written identically to two drives, thereby producing a "mirrored set" of drives. Thus, any read request can be serviced by any drive in the set. If a request is broadcast to every drive in the set, it can be serviced by the drive that accesses the data first (depending on its seek time and rotational latency), improving performance.



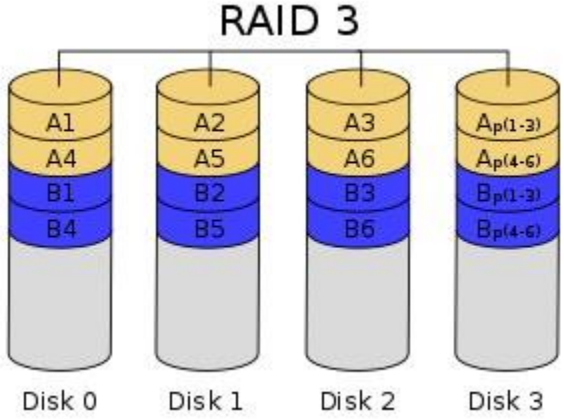
RAID 2

RAID 2 consists of bit-level striping with dedicated Hamming-code parity. All disk spindle rotation is synchronized and data is striped such that each sequential bit is on a different drive. Hamming-code parity is calculated across corresponding bits and stored on at least one parity drive.



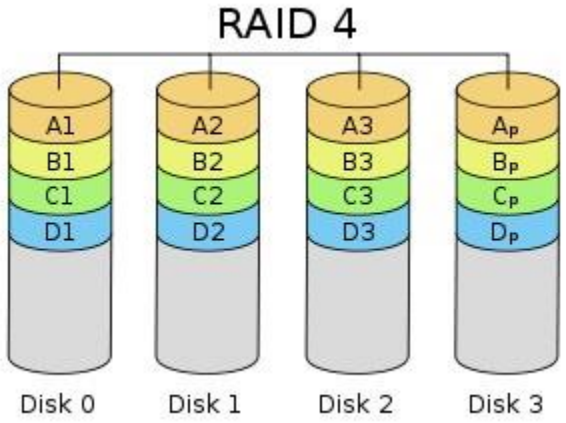
RAID 3

RAID 3 consists of byte-level striping with dedicated parity. All disk spindle rotation is synchronized and data is striped such that each sequential byte is on a different drive. Parity is calculated across corresponding bytes and stored on a dedicated parity drive.



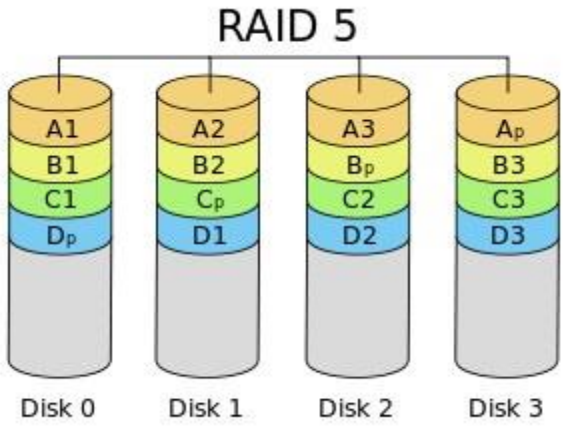
RAID 4

RAID 4 consists of block-level striping with dedicated parity. This level was previously used by NetApp, but has now been largely replaced by a proprietary implementation of RAID 4 with two parity disks, called RAID-DP. in RAID 4 one I/O read operation does not have to spread across all data drives. As a result, more I/O operations can be executed in parallel, improving the performance of small transfers.



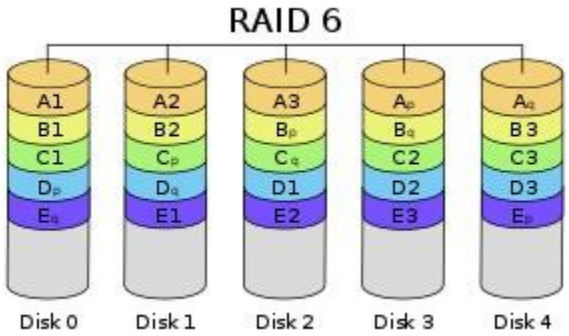
RAID 5

RAID 5 consists of block-level striping with distributed parity. Unlike RAID 4, parity information is distributed among the drives, requiring all drives but one to be present to operate. Upon failure of a single drive, subsequent reads can be calculated from the distributed parity such that no data is lost. RAID 5 requires at least three disks. RAID 5 implementations are susceptible to system failures because of trends regarding array rebuild time and the chance of drive failure during rebuild.



RAID 6

RAID 6 consists of block-level striping with double distributed parity. Double parity provides fault tolerance up to two failed drives. This makes larger RAID groups more practical, especially for high-availability systems, as large-capacity drives take longer to restore. RAID 6 requires a minimum of four disks. As with RAID 5, a single drive failure results in reduced performance of the entire array until the failed drive has been replaced



LVM

Logical volume management (LVM) is a form of storage virtualization that offers system administrators a more flexible approach to managing disk storage space than traditional partitioning. This type of virtualization tool is located within the device-driver stack on the operating system. It works by chunking the physical volumes (PVs) into physical extents (PEs). The PEs are mapped onto logical extents (LEs) which are then pooled into volume groups (VGs). These groups are linked together

into logical volumes (LVs) that act as virtual disk partitions and that can be managed as such by using LVM.

The goal of LVM is to facilitate managing the sometimes conflicting storage needs of multiple end users. Using the volume management approach, the administrator is not required to allocate all disk storage space at initial setup. Some can be held in reserve for later allocation. The sysadmin can use LVM to segment logically sequential data or combine partitions, increasing throughput and making it simpler to resize and move storage volumes as needed. Storage volumes may be defined for various user groups within the enterprise, and new storage can be added to a particular group when desired without requiring user files to be redistributed to make the most efficient use of space. When old drives are retired, the data they contain can be transitioned to new drives -- ideally without disrupting availability of service for end users.