WhatsApp-end to end encryption

End-to-end encryption (E2EE) is a system of communication where only the communicating users can read the messages. In principle, it prevents potential eavesdroppers – including telecom providers, Internet providers, and even the provider of the communication service – from being able to access the cryptographic keys needed to decrypt the conversation.

In many messaging systems, including email and many chat networks, messages pass through intermediaries and are stored by a third party, from which they are retrieved by the recipient. Even if the messages are encrypted, they are typically only encrypted 'in transit', and are stored in decrypted form by the third party. This allows the third party to provide search and other features, or to scan for illegal and unacceptable content, but also means they can be read and misused by anyone who has access to the stored messages on the third party system, whether this is by design or via a backdoor. This can be seen as a concern in many cases where privacy is very important, such as persons living under repressive governments, whistleblowing, mass surveillance, businesses whose reputation depends on its ability to protect third party data, negotiations and communications that are important enough to have a risk of targeted 'hacking',

How does end-to-end encryption work?

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 centralised WhatsApp server.

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

BIOS

What is BIOS?

Stands for "Basic Input/Output System." Most people don't need to ever mess with the BIOS on a computer, but it can be helpful to know what it is. The BIOS is a program pre-installed on Windows-based computers (not on Macs) that the computer uses to start up. The CPU accesses the BIOS even before the operating system is loaded. The BIOS then checks all your hardware connections and locates all your devices. If everything is OK, the BIOS loads the operating system into the computer's memory and finishes the boot-up process.

Since the BIOS manages the hard drives, it can't reside on one, and since it is available before the computer boots up, it can't live in the RAM. So where can this amazing, yet elusive BIOS be found? It is actually located in the ROM (Read-Only Memory) of the computer. More specifically, it resides in an erasable programmable read-only memory (EPROM) chip. So, as soon as you turn your computer on, the CPU accesses the EPROM and gives control to the BIOS.

The BIOS also is used after the computer has booted up. It acts as an intermediary between the CPU and the I/O (input/output) devices. Because of the BIOS, your programs and your operating system don't have to know exact details (like hardware addresses) about the I/O devices attached to your PC. When device details change, only the BIOS needs to be updated. You can make these changes by entering the BIOS when your system starts up. To access the BIOS, hold down the DELETE or F2 key as soon as your computer begins to start up.

Purpose of BIOS

BIOS enables computers to perform certain operations as soon as they are turned on. The principal job of a computer's BIOS is to govern the early stages of the startup process, ensuring that the operating system is correctly loaded into memory. BIOS is vital to the operation of most modern computers, and knowing some facts about it could help you troubleshoot issues with your machine.

POST

The first job of the BIOS after you switch your computer on is to perform the Power On Self-Test. During the POST, the BIOS checks the computer's hardware in order to ensure that it is able to complete the startup process. If the POST is completed successfully, the system usually emits a beep. If the test fails, however, the system generally emits a series of beeps. You can use the number, duration and pattern of these beeps to identify the cause of the test failure.

Startup

With the POST completed, the BIOS then attempts to load the operating system through a program known as a bootstrap loader, which is designed to locate any available operating systems; if a legitimate OS is found, it is loaded into memory. BIOS drivers are also loaded at this point. These are programs designed to give the computer basic control over hardware devices such as mice, keyboards, network hardware and storage devices.

Security

The BIOS can also play a role in computer security. Most BIOS software versions have the option to password-protect the boot process, which means that you must enter a password before any BIOS activity can take place. With the BIOS performing virtually all of its functions during startup, this effectively password-protects the operation of the whole computer. However, resetting a lost BIOS password can be time-consuming and involve working on some of the computer's most sensitive components.

Hardware

The BIOS software itself generally resides on a Read-Only Memory, or ROM, or a flash memory chip attached to your computer's motherboard. The location of the BIOS software on the chip is important, as it is the first software to take control of your computer when you turn it on. If the BIOS was not always located in the same place on the same chip, your computer's microprocessor would not know where to locate it, and the boot process could not take place.

Boot loader

A boot loader is a type of program that loads and starts the boot time tasks and processes of an operating system or the computer system. It enables loading the operating system within the computer memory when a computer is started or booted up.

A boot loader is also known as a boot manager or bootstrap loader. 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.

A boot loader primarily manages and executes the boot sequence of a computer system. A boot loader program is typically started after the computer or the BIOS have finished performing the initial power and hardware device checks and tests. It fetches the OS kernel from the hard disk or any specified boot device within the boot sequence, into the main memory. A boot loader is associated with only a single operating system. An operating system can also have multiple boot loader programs classified as primary and secondary boot loaders, where a secondary boot loader might be larger and more capable than the primary boot loader.

UEFI

Unified Extensible Firmware Interface (UEFI) is a specification for a software program that connects a computer's firmware to its operating system (OS). UEFI is expected to eventually replace BIOS. Like BIOS, UEFI is installed at the time of manufacturing and is the first program that runs when a computer is turned on. It checks to see what hardware components the computing device has, wakes the components up and hands them over to the operating system. The new specification addresses several limitations of BIOS, including restrictions on hard disk partition size and the amount of time BIOS takes to perform its tasks.

Because UEFI is programmable, original equipment manufacturer (OEM) developers can add applications and drivers, allowing UEFI to function as a lightweight operating system.

The Unified Extensible Firmware Interface is managed by a group of chipset, hardware, system, firmware, and operating system vendors called the UEFI Forum. The specification is most often pronounced by naming the letters U-E-F-I.

RAID Vs LVM

Sl.No.	RAID	LVM
1.	RAID is used for redundancy.	LVM is a way in which you partition the hard disk logically and it contains its own advantages.
2.	A RAID device is a physical grouping of disk devices in order to create a logical presentation of one device to an Operating System for redundancy or performance or a combination of the two.	LVM is a logical layer that that can be anipulated in order to create and, or expand a logical presentation of a disk device to an Operating System.
3.	RAID is a way to create a redundant or striped block device with redundancy using other physical block devices.	LVM usually sits on top of RAID blocks or even standard block devices to accomplish the same result as a partitioning, however it is much more flexible than partitions. You can create multiple volumes crossing multiple physical devices, remove physical devices without losing data, resize the volumes, create snapshots, etc.

4.	RAID is either a software or a hardware technique to create data storage redundancy across multiple block devices based on required RAID levels.	LVM is a software tool to manage large pool of storage devices making them appear as a single manageable pool of storage resource. LVM can be used to manage a large pool of what we call Just-a-bunch-of-Disk (JBOD) presenting them as a single logical volume and thereby create various partitions for software RAID.
5.	RAID is NOT any kind of Data backup solution. It's a solution to prevent one of the SPOFs (Single Point of Failure) i.e. DISK failure. By configuring RAID you are just providing an emergency substitute for the Primary disk. It NEVER means that you have configured DATA backup.	LVM is a disk management approach that allows us to create, extend, reduce, delete or resize the volume groups or logical volumes.