WHATSAPP END-TO-END ENCRYPTION

The term 'end-to-end encryption' (E2EE) has entered the common lexical use and is no more restricted to the geeks, thanks to WhatsApp which popularised it and brought it to over a billion users globally. It has become the part of our daily digital life as it is the definitive security mechanism that protects our personal data (messages etc.) such that it can only be read on by the sender, and by the recipient on the other end. No one else, including the hackers or the government, can snoop and read the encrypted data.

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 senders 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.

BASIC INPUT / OUTPUT SYSTEM (BIOS)

A BIOS (Basic Input/Output System) Short for ROM is boot firmware program that a computer uses to successfully start operating. The BIOS is located on a chip inside of the computer and is designed in a way that protects it from disk failure.

When you turn on a PC, the BIOS first conduct a basic hardware check, called a Power-On Self Test (POST), to determine whether all of the attachments are present and working. Then it loads the operating system into your computer's random access memory, or RAM. The BIOS also manages data flow between the computer's operating system and attached devices such as the hard disk, video card, keyboard, mouse, and printer. The BIOS stores the date, the time, and your system configuration information in a battery-powered, non-volatile memory chip, called a CMOS (Complementary Metal Oxide Semiconductor) after its manufacturing process.

Functions of BIOS

(i) BIOS Power on Self Test (POST): It is a built-in diagnostic program. This self test ensures that the computer has all of the necessary parts and functionality needed to successfully start itself, such as use of memory, a keyboard and other parts. Then additional tests are done during booting. If errors are detected during the test, the BIOS instruct the computer to give a code that reveals the problem. Error codes are typically a series of beeps heard shortly after startup.

The BIOS also works to give the computer basic information about how to interact with some critical components, such as drives and memory that it will need to load the operating system. Once the basic instructions have been loaded and the self-test has been passed, the computer can proceed with loading the operating system from one of the attached drives. Computer users can often make certain adjustments to the BIOS through a configuration screen on the computer. The setup screen is typically accessed with a special key sequence during the first moments of startup. This setup screen often allows users to change the order in which drives are accessed during startup and control the functionality of a number of critical devices. Features vary among individual BIOS versions.

We can also use flash-memory cards to hold BIOS information. This allows users to update the BIOS version on computers after a vendor releases an update. This system was designed to solve problems with the original BIOS or to add new functionality. Users can periodically check for updated BIOS versions, as some vendors release a dozen or more updates over the course of a product's lifetime. Mother board (System) BIOS, Video adapter firmware (BIOS), Drive controller firmware (BIOS), Modem Card firmware (BIOS), Network adapter board BIOS, SCSI adapter BIOS. The mother board BIOS provides routines to support motherboard features. BIOS ROM chips for major sub systems of computer such as video and drive control must also be included.

Actually BIOS can be placed in between the computer and external devices as its name tells it is used for reading the keystroke, displaying values on screen, Reading and writing to and from floppy and hard disks etc.

The keyboard is assigned the port number 60, which is known to BIOS. BIOS read this port and data from keyboard goes to computer.

(ii) **Bootstrap Loader**: To boot the operating system. The BIOS contains a program known as bootstrap loader whose responsibility is to search and start the operating system boot program. Then the boot program of operating system controls the computer system and boots the operating system.

(iii) BIOS Setup Utility Program: A non volatile memory (NVRAM) is used to store information about the computer system. During installation of a system, the user run BIOS setup program and enter the correct parameters. The settings of memory, disk types and other settings are stored in NVRAM and not in BIOS chip itself. To construct NVRAM, the material required is CMOS (Complementary metal oxide semiconductor). These CMOS chips are very efficient storage devices as they store and maintain data on very low values of current. The system's configurations therefore are also termed as CMOS settings, which we can set using BIOS set up program. The BIOS reads the parameters from CMOS RAM as and when required.

CMOS settings can be maintained by battery backup either by using capacitor or by a battery built into NVRAM chip. This chip also has system clock. If there is no battery, the setting remains for short period of time and we need to reset the system. With it there is loss of BIOS password which protects BIOS set up program.

To clear the CMOS RAM contents, two methods used are

(i) By using clear CMOS jumper.

(ii) By holding down enter key during booting of the system.

For Pentium III motherboards, different set ups are there in AMI BIOS. These are:

• **Standard CMOS Setup:**It is used to set time date, hard disk type, type of floppy drive, type of monitor and keyboard.

Advanced CMOS Setup: It is used to set typematic rate and delay, above 1 MB memory test, memory test tick sound, Hil < Del> message display, system boot up sequence etc.

• **Advanced Chipset Setup:**It is used to set features of chipset.

• **Power Management Setup:**It is used to control power conservation options.

• **PCI/Plug and Play Setup:**It is used to set options of PCI bus and that of plug and play devices.

• **Peripherals Setup:**It is used to control options related to I/O controllers.

• **CPU Configuration Setup:**This setup is used to select the types of CPU installed in the motherboard. In AMI BIOS, the settings are auto as it automatically finds out the type of CPU in the computer system.

(iv) **System Service Routines:** The BIOS provides various software routines (subprograms) that can be called by higher-level software such, as DOS, Windows, or their applications, to perform different tasks. Virtually every task that involves accessing the system hardware has traditionally been controlled using one or more of the BIOS programs (although many newer operating systems now bypass the BIOS for improved performance). This includes actions like reading and writing from the hard disk, processing information received from devices, etc.

BIOS services are accessed using software interrupts, which are similar to the hardware interrupts except that they are generated inside the processor by programs instead of being generated outside the processor by hardware devices. One thing that this use of interrupts does is to allow access to the BIOS without knowing where in memory each routine is located.

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.

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.

The order of booting –

In order for a computer to successfully boot, its BIOS, operating system and hardware components must all be working properly; failure of any one of these three elements will likely result in a failed boot sequence.

When the computer's power is first turned on, the CPU initializes itself, which is triggered by a series of clock ticks generated by the system clock. Part of the CPU's initialization is to look to the system's ROM BIOS for its first instruction in the startup program. The ROM BIOS stores the first instruction, which is the instruction to run the power-on self test (POST), in a predetermined memory address. POST begins by checking the BIOS chip and then tests CMOS RAM. If the POST does not detect a battery failure, it then continues to initialize the CPU, checking the inventoried hardware devices (such as the video card), secondary storage devices, such as hard drives and floppy drives, ports and other hardware devices, such as the keyboard and mouse, to ensure they are functioning properly.

Once the POST has determined that all components are functioning properly and the CPU has successfully initialized, the BIOS looks for an OS to load.

The BIOS typically looks to the CMOS chip to tell it where to find the OS, and in most PCs, the OS loads from the C drive on the hard drive even though the BIOS has the capability to load the OS from a floppy disk, CD or ZIP drive. The order of drives that the CMOS looks to in order to locate the OS is called the boot sequence, which can be changed by altering the CMOS setup. Looking to the appropriate boot drive, the BIOS will first encounter the boot record, which tells it where to find the beginning of the OS and the subsequent program file that will initialize the OS.

Once the OS initializes, the BIOS copies its files into memory and the OS basically takes over control of the boot process. Now in control, the OS performs another inventory of the system's memory and memory availability (which the BIOS already checked) and loads the device drivers that it needs to control the peripheral devices, such as a printer, scanner, optical drive, mouse and

keyboard. This is the final stage in the boot process, after which the user can access the system's applications to perform tasks.

RAID AND LVM

S.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 loosing 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. Its 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.