WhatsApp End-to-End Encryption

Exchange of Messages

WhatsApp uses XMPP Protocol to transfer the messages between the two clients.

Need to Encryption

- Messages were sent as plain text between two clients.
- All the messages were stored in the server until the messages are read by the recipient..
- WhatsApp's adoption of end-to-end encryption follows Apple's debate with the FBI over the unlocking of a terrorist's iPhone. During the dispute Jan Koum, WhatsApp's co-founder, said that he supported Apple's position and admired its "efforts to protect user data".
- In March it was revealed that WhatsApp had been targeted by court orders asking to access information it holds.

Encryption

- The Signal Protocol, designed by Open Whisper Systems, is the basis for WhatsApp's end-to-end encryption. This end-to-end encryption protocol is designed to prevent third parties and WhatsApp from having plaintext access to messages or calls.
- **Keys used in this encryption are:**

  Public Key Types

  • Identity Key Pair – A long-term Curve25519 key pair, generated at install time.

  • Signed Pre Key – A medium-term Curve25519 key pair, generated at install time, signed by the Identity Key, and rotated on a periodic timed basis.

  • One-Time Pre Keys – A queue of Curve25519 key pairs for one time use, generated at install time, and replenished as needed.

Session Key Types

• Root Key – A 32-byte value that is used to create Chain Keys.

• Chain Key – A 32-byte value that is used to create Message Keys.

• Message Key – An 80-byte value that is used to encrypt message contents. 32 bytes are used for an AES-256 key, 32 bytes for a HMAC-SHA256 key, and 16 bytes for an IV.

Exchanging Messages

- Once a session has been established, clients exchange messages that are protected with a Message Key using AES256 in CBC mode for encryption and HMAC-SHA256 for authentication.
- The Message Key changes for each message transmitted, and is ephemeral, such that the Message Key used to encrypt a message cannot be reconstructed from the session state after a message has been transmitted or received.
- The Message Key is derived from a sender's Chain Key that "ratchets" forward with every message sent. Additionally, a new ECDH agreement is performed with each message roundtrip to create a new Chain Key.

Verifying the keys

The 60-digit number is computed by concatenating the two 30-digit numeric fingerprints for each user's Identity Key. To calculate a 30-digit numeric fingerprint:

1. Iteratively SHA-512 hash the public Identity Key and user identifier 5200 times.
2. Take the first 30 bytes of the final hash output.
3. Split the 30-byte result into six 5-byte chunks.
4. Convert each 5-byte chunk into 5 digits by interpreting each 5-byte chunk as a big-endian unsigned integer and reducing it modulo 100000.
5. Concatenate the six groups of five digits into thirty digits.

Conclusion

Messages between WhatsApp users are protected with an end-to- end encryption protocol so that third parties and WhatsApp cannot read them and so that the messages can only be decrypted by the recipient. All types of WhatsApp messages (including chats, group chats, images, videos, voice messages and files) and WhatsApp calls are protected by end-to-end encryption.

WhatsApp servers do not have access to the private keys of WhatsApp users, and WhatsApp users have the option to verify keys in order to ensure the integrity of their communication.

BIOS (basic input/output system)

BIOS is the program, a personal computer's microprocessor uses to get the computer system started after you turn it on. It also manages data flow between the computer's operating system and attached devices such as the hard disk, video adapter, keyboard, mouse and printer.

BIOS is an integral part of your computer and comes with it when you bring it home. (In contrast, the operating system can either be pre-installed by the manufacturer or vendor or installed by the user.) BIOS is a program that is made accessible to the microprocessor on an erasable programmable read-only memory (EPROM) chip. When you turn on your computer, the microprocessor passes control to the BIOS program, which is always located at the same place on EPROM.

When BIOS boots up (starts up) your computer, it first determines whether all of the attachments are in place and operational and then it loads the operating system (or key parts of it) into your computer's random access memory (RAM) from your hard disk or diskette drive.

With BIOS, your operating system and its applications are freed from having to understand exact details (such as hardware addresses) about the attached input/output devices. When device details change, only the BIOS program needs to be changed. Sometimes this change can be made during your system setup. In any case, neither your operating system or any applications you use need to be changed.

Although BIOS is theoretically always the intermediary between the microprocessor and I/O device control information and data flow, in some cases, BIOS can arrange for data to flow directly to memory from devices (such as video cards) that require faster data flow to be effective.

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.

Booting Process

Booting is a process or set of operations that loads and hence starts the operating system, starting from the point when user switches on the power button.

UEFI(The Unified Extensible Firmware Interface)

The Unified Extensible Firmware Interface aims to resolve what BIOS could not. UEFI itself is the second version (2.*), the former being EFI (1.*). If you bought a computer after 2010, you will probably have a UEFI instead of a BIOS. You read correctly, BIOS and UEFI do the same thing, but they are pretty different in how and what they do. A UEFI can (in addition to what a BIOS can):

- Boot from disks larger than 2TB using GPT (assuming the operating system supports both).
- Provide the user with a graphical user interface which is easier to use than old terminal user interfaces of BIOS.
- Provide support for mouse devices (BIOS can rarely do this).
- Boot securely using a chain-of-trust. (More later on secure boot).
- Network boot (although most BIOS can do that, that's not a given).
- Provide a modular interface which is independent from the CPU architecture.
- Provide a modular interface for applications and devices based on EFI drivers(commonly called EBCs, EFI Byte-Code).

Difference Between LVM & RAID

RAID	LVM
RAID is used for redundancy.	LVM is a way in which you partition the hard disk logically and it contains its own advantages.
A RAID device is a physical grouping of disk devices in order to create a logical presentation of one device to	LVM is a logical layer that that can be manipulated in order to create and, or expand a logical presentation of a disk device to an Operating System.

an Operating System for redundancy or performance or a combination of the two.	
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
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.
RAID is NOT any kind of Data backup solution. Its a solution to prevent one of the SPOFs 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.