Global Proceedings Repository
American Research Foundation

ISSN 2476-017X

Available online at http://proceedings.sriweb.org

شبكة المؤتمرات العربية
http://arab.kmshare.net/

AASRC-ARF JOINT INTERNATIONAL ACADEMIC CONGRESS ON POLITICS, ENGINEERING, SOCIOLOGY, INFORMATION, HEALTH & MEDICAL, EDUCATION AND COMMUNICATION 25-26 October, 2017 Istanbul Aydın University, Istanbul

المؤتمر الاكاديمي الدولي الثامن عشر - في رحاب جامعة اسطنبول ايدن

25-26 اكتوبر 2017 اسطنبول - تركيا

Unified Extensible Firmware Interface (UEFI) between Speed and Security

Sabah Mohammed Mlkat Almutoki
The Dean Of Alsamawa University of Alfurat Alawsat

Alaa Abd Ali Hade

Technical Institute of Alsamawa / Iraq

Ahmed Fadhil Mohammed

Directorate of Education Muthanna Governorate

Abstract

This paper gives an overview of the (Unified Extensible Firmware Interface) and describes the capabilities and supports operating systems and refers to the interest rate offered in this area. UEFI is a new interface deal between operating systems and the hardware inside your computer. Since more than thirty years and we are dealing with a blue screen. BIOS is an IC 16-bit is available on the memory 1 megabyte. The control of all hardware in the computer and through which the preparation of these settings that appear at the beginning of the run. which It works on the examination of the pieces associated hardware to the computer and make sure it works well, but show contains some the problems of security vulnerabilities and lack of sufficient flexibility in the adjustment and modernization. Recently with the development of technology they became working on more data processors than its predecessors, such as processors 32-bit and 64-bit the Intel creates a new innovation called (Unified Extensible Firmware Interface). which will address many of the problems related to the BIOS and these problems, velocities and with the size of the systems, overload of programs as well as the speed of the startup where the BIOS takes more than thirty seconds to startup and show the system but now does not need to this time as well as the most important problems in terms of security where a problem of breakthrough devices and access them with the beginning of the startup has been processed and also allows us the ease of movement in the choice of settings. UEFI resolves the place and there is no need to have the old BIOS.

Introduction:

In this paper, we will talk about a very important issue, but did not know a lot or maybe heard it was not clear to him the idea and what is the purpose or goal of this topic and the development that we are seeing in the field of rapid and substantial technology and there is no time to stand on every issue, and as far as this topic a broad and important I did not find a lot of explanation and detail and clarification on this matter and found that a lot of users of services and employees do not know them and do not realize this topic and what is useful and how to deal with. Most often we hear there are problems in the BIOS in terms of security as well as speed and ask spite of this development and technology in software and hardware, but why is there no updated sufficient in the matter of the BIOS that like other computer components, so it launched Intel Corp. after 1998 first issuing a specification EFI, which means use Itanium processors with 64-bit rather than 16-bit allocated to work with maids and included other processors such as X86. After all has been the development of release as what is known now as the UEFI and this is an abbreviation for Unified Extensible Firmware Interface, which will address new technology many flaws left over to use the BIOS for much more than expected with the lack of development of pursuing a similar development in hardware and operating systems, all this does not can continue with the old techniques began precipitant Motherboard manufacturers the transition to this new technology.

1- What is firmware?

Firmware is a program that's written to the read only exists within the hardware devices. It is small programs that make control persons in electronic devices such as remote devices, calculators, TVs, phones, and even some computer components such as the hard disk or memory. firmware that is programmed to a fixed program memory differs cannot modifying the contents easily. The firmware contained in these devices provides the lowlevel control program for the device. As of 2013, most firmware can be updated.[1]

Often on the (flash ROMs) or (binary image file) can be downloaded to the hardware by the user and programmers. Firmware play an important role in many electronic devices these days.

"Firmware" generally refers to programs that help the machine and do what they are supposed to do. It's programming background who runs the device. This is in contrast to the "software" that we use to do things on the device, such as games and software on a computer, and music files on MP3 player and discs. Most of the hardware devices that we use today, such as computer and audio or video. In this way, and sometimes the manufacturer makes improvements to the programs that run on the device (firmware). These improvements launches as firmware updates. We can expect to see firmware updates in everything.

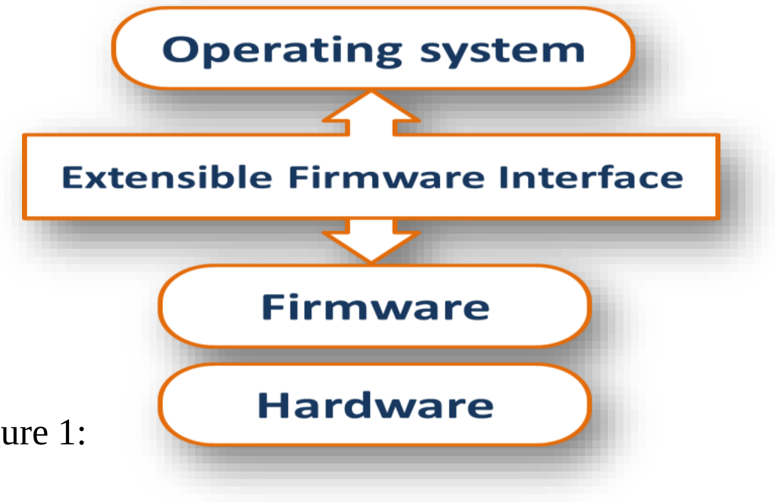


Figure 1:

2- What is UEFI?

Unified Extensible Firmware Interface or UEFI Acronym, is the interface between the operating system and the firmware that controls the computer's internal components such as the motherboard, memory, hard drives and ports. UEFI was introduced as an alternative to the initial system of entrances and exits Basic Input Output System (BIOS) used in all computers compatible with IBM PC about thirty years ago.

The most important problems that UEFI seeks to solve is the problem of malware that attack the primer sector Boot Sector and are installing a preliminary Boot Loader can any harmful antiviral exceeded before the start of the work of the operating system.

UEFI considerable development in the interface your computer starts, While the BIOS is install a small program in the ROM. The UEFI is adjustable program can be part of stored on an intermediate load, such as a hard drive or on the network, in addition to the possibility of storing the fixed memory on the motherboard.

Therefore, UEFI provides so that looks like a miniature operating system, it provides a number of boot services, which operate only at startup, and some operational services, runtime services that the operating system can be used while working. Due to the UEFI is a program adjustable program enhances it and put it as a front «unified» so that it works on all types of processors either Intel, AMD, ARM processors, including 32-bit and 64-bit.[2]

UEFI provides greater flexibility in dealing with hard drives, bypassing traditional boundaries in the MBR (Master Boot Record) system with 4 partitions do not exceed the area of one of them 2terabytes, where UEFI uses a new system called the GPT (GUID Partition Table).[3]

UEFI is available in a number of device drivers and a number of applications, in addition to extensibility by adding extensions.

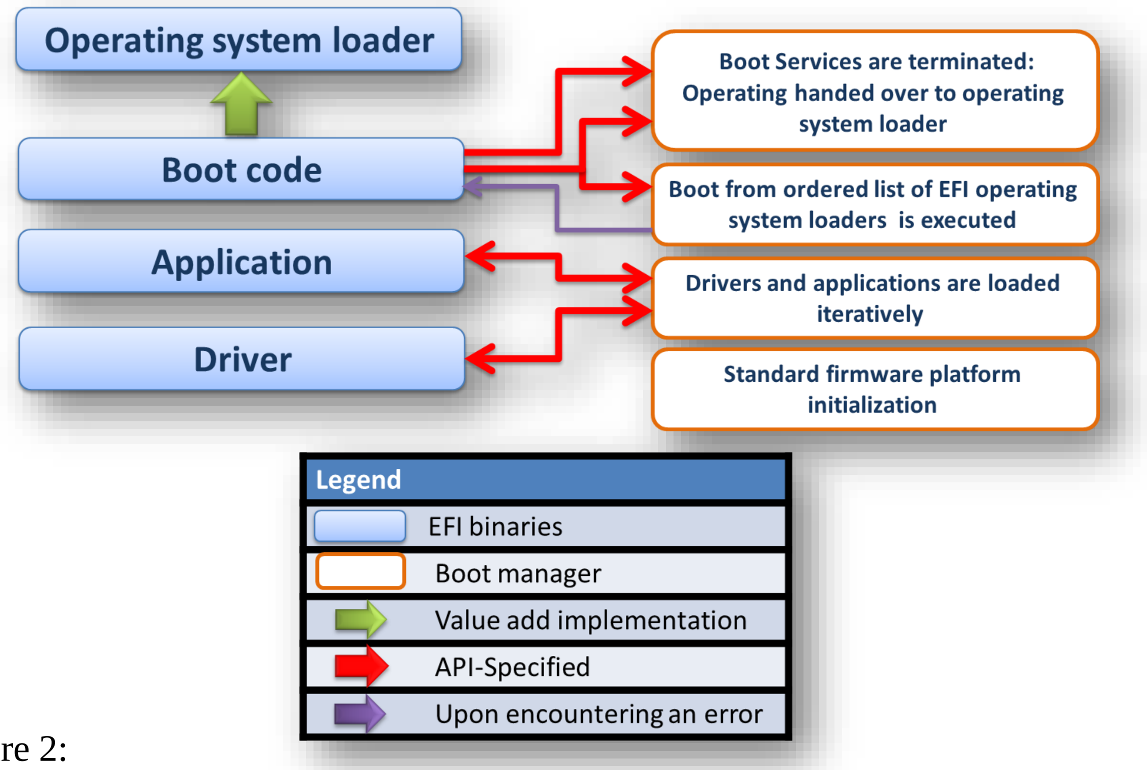

Operating system loader
Boot code
Application
Driver
Boot Services are terminated: Operating handed over to operating system loader
Boot from ordered list of EFI operating system loaders is executed
Drivers and applications are loaded iteratively
Standard firmware platform initialization
Legend
EFI binaries
Boot manager
Value add implementation
API-Specified
Upon encountering an error

Figure 2:

2.1 Features UEFI system:

a. Support the use of the mouse making it easier to navigate and choose the desired options process.

b. The possibility of supporting the modernization of the system BIOS directly (on line)

c. possibility boot loader through with large areas 2TB hard drives and more.

d. The speed of the boot with less time in the Boot-Up Operation

e. Increase in the high security where (Cereal windows in the BIOS), which acts as it does not allow any operating system boots only authorized to the operating system.

f. architectural independent and not dependent on the processor

g. UEFI uses a new system called the GUID Partition Table, or GPT partitioning a hard drive to an infinite number.

2.2 How is the UEFI system design?

The design of a set of Classes we will talk in detail

1- It is the basic class, which will be responsible for downloading EFI program 'where it is loaded by an existing slide on the motherboard, and also can be loaded from the hard disk or a CD or from any other device on the network as well.

2- In this class is loaded identification codes for equipment Drivers program, which will be compatible with EFI system, and at the same time provide a way to deal with devices that do not support the EFI system in a manner consistent with the devices, which has been dealing with the old system BIOS.

3- In this class is loaded operating system on the computer, and allows access to the interface EFI system to adjust the settings that are compatible with the requirements of the user as it happens in the system BIOS.

4- When the operating system starts working and Advanced Configuration and Power Interface remains in working condition to allow EFI system is connected with the operating system to identify the various devices and equipment and adjust the settings and power settings.

3- What is UEFI GPT?

GPT stands for (GUID Partition Table) is a new standard for installation of the walls of the sections and management in the hard drive, which is part of the UEFI BIOS which has been used instead of the old standard MBR with the old BIOS. Information storage partition on the drive. This information includes where partitions start and begin, so your operating system knows which partition belong to each partition and any operable partition. It is a must to use the GPT. With the GPT, you can create a large but undetermined number of primary partitions on your hard disk, although it is generally limited to 128 primary partition. While the traditional partition table, which is in the MBR can be up to three primary partitions and an extended partition if the need for a fourth partitions or four primary partitions. Each partition of the GPT can hold up to 2 ^ 64 blocks in length it uses 64-bit, which is equivalent to 9.44ZB for a 512-byte block (1 ZB is 1 billion terabytes). This size in Microsoft Windows system is limited to 256 terabytes. In hard drive there is two GPT first one be essential at the top of the hard disk and GPT second part is secondary at the bottom of the disk. This is what makes GPT more useful than the MBR. [4]

GPT store the backup and the division head of the table at the end of the disc so that it can be recovered in the event of damage to the primary tables. Also carry CRC32 checksums to detect errors and corruption from the top of the division. While MBR As previously mentioned only identifies four partitions on the hard drive in each partition area of up to 2TB in size only. And you can set the last partition of the extended partition, and will be able to create more sub-partitions (or) inside the logical drives. MBR also uses a 32-bit recording division, and can each partition. This will not work well with large hard disk storage space, the MBR is the only place that holds the partition information. If it was ever damaged it can get damaged very easily, and the result will be the entire hard disk unreadable after which we lose information.[5]

4- Security UEFI:

Basic functionality in the boot security devices to protect against unauthorized operating systems and by rootkit malicious attacks, and to ensure that all the requirements for validation can begin on the system.

When the enable secure boot, UEFI uses public keys and certificates to verify the real programs. It is well known these days when everyone is hearing about Rootkits is a virus that is running the same system or accompanying Operating system is the process of replacing Boot Loader another special Rootkit who shall process auto start Startup or directly from the Bios and works exclusively with the system's Kernel.

Facing many of these malware which differ in their types and ways of being infected with the system and Rootkits became something very well known to all the protection companies and antivirus that work constantly to respond to new types of Malwares Spywares, Trojans, Rootkits and other malicious software. This is one of the most important problems in the system BIOS UEFI, which seeks to solve the problem of malware that attack the primer sector Boot Sector and are installing a preliminary Loader Boot Loader can any harmful antiviral exceeded before the start of the work of the operating system. Where it starts loading the operating system and ensures that all components are signed with a manufacturer's digital certificate. This should go a long way toward disabling rootkits boot, which depends on the ability to download for Windows and programs before the anti-virus software packages. And to prevent advanced malware such as (bootkits & rootkits) from causing damage, and it will stop other boot loader attacks (such as malware that holds operating systems unauthorized.

And that the main work at the front of the firmware of computers that work as a translator between the operating system and firmware computer. And use all of these interfaces in to start the computer to create hardware components and start the operating system which is stored on the hard disk. Differently from the old BIOS. It stores all the information about the configuration and startup file (efi) instead of the firmware. Inside a special partition called the EFI system partition. This file is stored on the hard drive (ESP). ESP also will contain boot partition for the operating system installed on your computer loaded programs.[6-8]

5- How the UEFI is Speed

As previously the old system BIOS, which starts work at the beginning of the computer to be responsive to the requirements and needs of basic and old operating system design that a DOS system. Since the system BIOS performs screening startup Power On Self-Test (POST) through which to ensure that the components and basic parts of the computer work well.

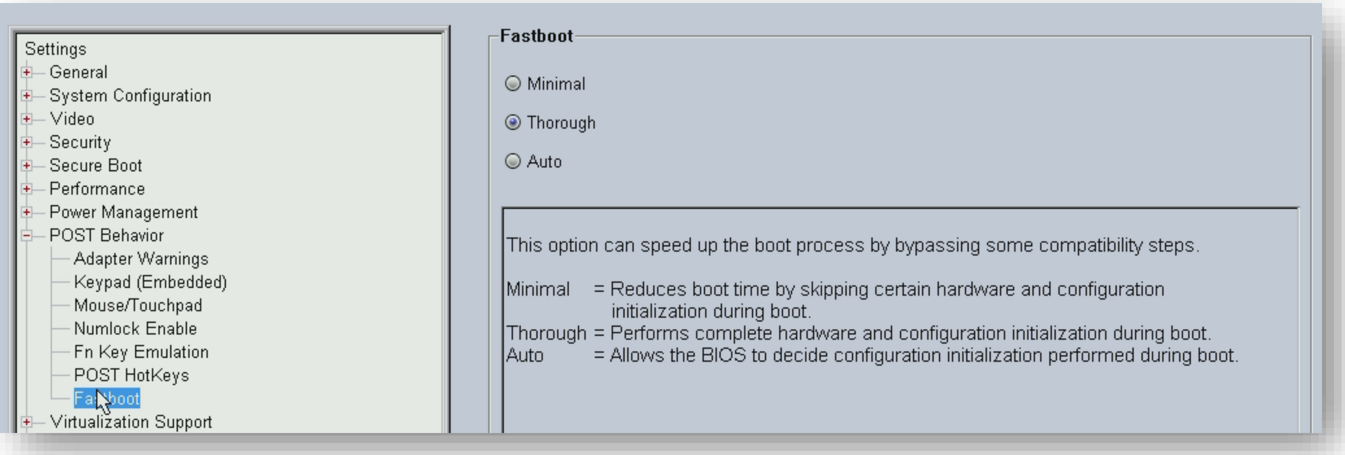
When platform is targeted to boot only in UEFI mode, the firmware can skip initialization of the devices that do take direct part in the boot process. Instead these devices get initialized inside the OS. What previously required up to 10 seconds to do inside the firmware and now be done in as little as two seconds. Operating Systems, like Win8, take advantage of reduced operations when loading the OS through UEFI and are also able to provide must faster boot speeds.[9]

This leads to the speed of the boot, and then the computer starts to work in addition to the it works the BIOS interface intermediate between the physical components of the device and the operating system and various programs, and programming system BIOS by the language of Assembly and is one of the difficult languages as this complex language programming to a large extent and time consuming, but the system programmable EFI implementation is done in high-level C programming language is easy and common language use and be quick to respond, as well as in the discovery of bugs and treatment process compared to the language of Assembly in addition to the spread of C language in a lot of settings and applications that facilitate dealing with the system (EFI).[10]

UEFI initially designed to work with the Itanium processor that contains a 64-bit and allocated in order to work with servers and also included other processors, including the X86 processors after the BIOS system deals with

16-bit. which is characterized as containing firmware rapid link is to the system to create and define the system as well as the important feature is in operating condition is contacted with display card and will be downloaded defined within this system program and not from your computer system this is through a special protocols are independent of the quality of the processor or motherboard or control segment and due to increased handling capacity from 16-bit to 64-bit as well as the presence of induction programs in this system, leading to increased speed in the boot and speed of response between UEFI and computer components and operating system.

Figure 3: BIOS Fast Boot Setting



Fastboot

○ Minimal
● Thorough
○ Auto

This option can speed up the boot process by bypassing some compatibility steps.

Minimal = Reduces boot time by skipping certain hardware and configuration initialization during boot.
Thorough = Performs complete hardware and configuration initialization during boot.
Auto = Allows the BIOS to decide configuration initialization performed during boot.

Conclusion:

The main characteristic of the development of systems BIOS because the evolution of technology, as well as the evolution of malicious programs and viruses that affect the operating systems work and be hidden inside the system, which starts dealing with the system BIOS so that can not be detected by anti-virus programs after boot startup system. And that the security of the system was exposed to penetrate through these programs, such as rootkit and boot kit. It was created UEFI secure boot to make the operating system less vulnerable to these forms of the risk of attacks. And the discovery of UEFI system is to reduce the security risks that may occur with the system at the beginning of operation. And the use of security and UEFI secure boot process using firmware prevents developers of malicious software to attack systems before the start of the anti-virus programs and malware programs.

References:

1- Mark S., David P.; Scott M., *"Authorized Cert Guide: CompTIA A+*. Pearson Education" September 2012.

2- Michael Krau; Dong Wei ” Clarifying the Ten Most Common Misconceptions About UEFI” April 2014.

3- http://www.uefi.org

4- "FAQ: Drive Partition Limits". UEFI Forum. 2013-11-04.

5- Roderick W. Smith. "Make the most of large drives with GPT and Linux". IBM. July 2012

6- Edge, Jake. "UEFI and "secure boot"". LWN.net. Retrieved 9 September 2012.

7- Matthew Garrett. "Secure Boot distribution support". Retrieved 2014-03-20.

8- R. Wilkins, B. Richardson, Intel Corporation “UEFI Security Boot in Modern Computer Security Solutions” September 2013.

9- Anand Joshi, Kurt Gillespie "UEFI on Dell BizClient Platforms" January 2013.

10- Ben Hardwidge . "LBA explained — Solving the 3TB Problem?". June 2010
http://www.bit-tech.net/hardware/storage/2010/06/01/are-we-ready-for-3tb-hard-disks/2