A Trusted Bootstrapping Scheme Using USB Key Based on UEFI

Abhishek Singh Kushwaha

***Abstract*—Unified Extensible Firmware Interface (UEFI) is a new specification that defines a software interface between the platform firmware and the operating system. UEFI in the near future will replace the conventional Basic Input-Output System (BIOS). Along with this, Trusted Computing has emerged as a new and challenging research field in the domain of computer security. This asserts the need of Trusted Bootstrapping. Here a new idea of Trusted Bootstrapping using the USB key is presented which involves the scheme of Portable Trusted Platform Module, supported with UEFI technology. It aims to reduce motherboard modification and makes the system less vulnerable to human disruption.**

***Index Terms*—Trusted bootstrapping, TPM, UEFI, ESP**

I. Introduction

The need of secure computing is increasing day by day. The issue of how to ensure data security, in the era of highly sophisticated computing, has become a big challenge for security personnel. Although the traditional security services like Firewalls, Anti-Virus, etc. are present, but they need to be updated after every short interval of time. This updating process sometimes acts as overhead. Also, they are not effective in handling the physical intruder. Most of such softwares are resource hungry, which affects the performance of system.

In order to get rid of the shortcomings of such softwares, in 2003 a Trusted Computing Platform Alliance was formed, which is a non-profit organization, headed by companies like IBM, Intel, Microsoft, etc. TCPA proposed a new approach to secure computing named "Trusted Computing". In trusted computing, a trust chain was build and the trust chain was passed from initial boot stage to the final OS running stage. Later the name of alliance was changed to Trusted Computing Group (TCG) [1].

Trusted computing proposes to solve some of today's security problems through hardware changes to the personal computer. Trusted computing ensures data security from hardware layer. This has made it a very fast growing field in research and industry. Ensuring trusted boot means security is maintained from the initial boot sequence. Here, in this paper a new approach to booting, through a USB key, is presented which is itself trusted from the beginning by the Portable Trusted Platform Module.

Manuscript received March 4, 2013; revised May 10, 2013.

Abhishek Kushwaha is with the Cyber Laws and Information Security department of Indian Institute of Information Technology, Allahabad, India (email: kushwahaiiita@gmail.com)

II. EFI Boot Process

BIOS was the de-facto boot device until Intel came up with its Itanium architecture, in 1999, and decided to break the barriers of BIOS. BIOS is programmed in assembly code and stored in ROM or Flash chips on the mainboard. When the personal computer is powered-on, the first instruction from BIOS causes the system to initialize and inspect the hardware and pass control to the operating system. The characteristics of traditional BIOS, 16-bit codes and 1MB memory, severely affected the development of computer technology.

So, Intel advocated substituting the new EFI framework to BIOS. The need of the features like high level coding, modular design, 64-bit architecture, GUI interface was supposed to be fulfilled by EFI. EFI was introduced with a view to standardize the booting process. Initially started as Intel Boot Initiative, over the years it transformed to Unified Extensible Firmware Interface (UEFI) [2].

The EFI programming software module EDK [3] (EFI Development Kit), divides the EFI framework into seven phases such as, SEC, PEI, DXE, TSL, RT and AL, shown in Fig. 1.

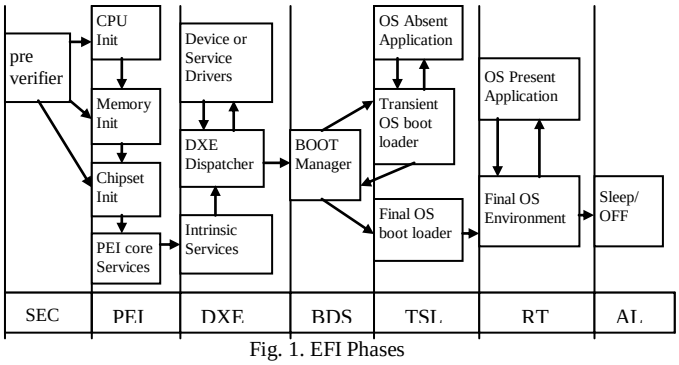

Fig. 1. EFI Phases

III. Trusted Platform Module

Computer security is a major concern, and as new loop-holes are discovered and exploited, the need for new security solution grows. Changes to the design of PC hardware are among the useful tools for improving the security [4]. Trusted computing proposes to solve some of today's security issues through hardware change to the PC. Trusted computing places high degree of trust on the computer. It provides the means for recognizing when the computer environment has changed considerably and prevents the exploitation of vulnerabilities.

The TPM provides two classes of keys, migratable and non-migratable [5]. Migratable keys are used to protect the data that can be used on more than one platform. Whereas, non-migratable keys make the data useless for any other

DOI: 10.7763/IJCCE.2013.V2.245

platform. If the particular platform fails or the keys are lost the data is also lost. But the migratable keys provide facility for sharing among multiple platforms and users. Also the keys can be restored from defective system.

In a trusted computer, the TPM chip is embedded into the motherboard. It cannot be pulled out or replaced or reprogrammed. TPM has enough cryptographic modules which are able to provide the required security to the user. TPM provides a safe place for storage of encrypted keys and signatures. TPM along with software provide a protected area for secure key operations.

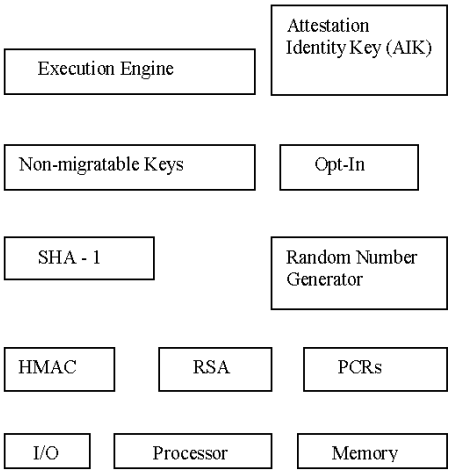

Fig. 2. Components of TPM

The Fig. 2 outlines the different component of TPM [6]. The protected storage in TPM includes the Platform Configuration Registers (PCRs), and limited volatile and non-volatile memory. The random number generator and RSA engine support the creation of RSA and symmetric keys. The SHA-1 digest is also stored in TPM.

A. Key Concepts

Trusted computing encompasses five key technology concepts, of which all are required for a fully trusted system [4].

- Endorsement key

The endorsement key is a 2048-bit RSA public private key pair which is created randomly on the chip at manufacture time and cannot be changed. This key is used to allow the execution of secure transactions.

- Memory curtaining

Memory curtaining refers to a strong, hardware enforced memory isolation technique to prevent programs from being able to read or write into one another's memory. Even the Operating System does not have full access to the curtained memory.

- Sealed storage

Sealed storage is an ingenious invention that generates keys based in part on the identity of the software requesting to use them and in part on the identity of the computer on which that software is running. The result is that the keys themselves need not be stored on the hard drive but can be generated whenever they are needed -- provided that authorized software tries to generate them on an authorized machine.

- Secure input/output

Secure I/O provides a secure hardware path from the keyboard to an application -- and from the application back to the screen. No other software running on the same PC will be able to determine what the user typed, or how the application responded.

- Remote attestation

Remote attestation allows changes to the user's computer to be detected by authorized parties. For examples, software companies can identify unauthorized changes to software, including users' tampering with their software to circumvent technological protection measures. It works by having the hardware generate a certificate stating what software is currently running. The computer can then present this certificate to a remote party to show that unaltered software is currently executing.

B. Trusted Boot Process

The major components of Trusted Computing Platform are Root of Trust and Chain of Trust.

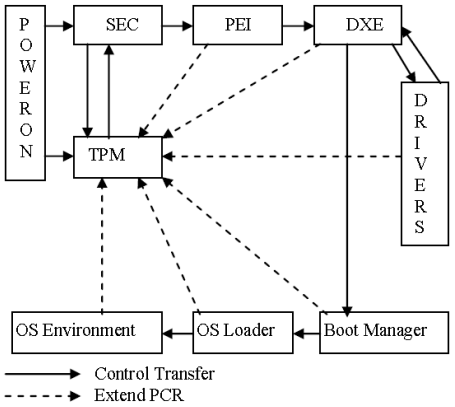

Fig. 3. Chain of Trust model

A Root of Trust is a set of minimum, unconditionally trusted functions. There are three Roots of Trust.

- Root of Trust for Measurement
- Root of Trust for Storage
- Root of Trust for Reporting

Each root is expected to function correctly. In the framework of EFI, the codes of SEC (Security) and PEI (Pre EFI Initialization) phases can be considered as RTM, as these are first codes that are executed and it is not easy to alter them.

The function of data sealing and binding and information storing, performed by TPM, can be treated as RTS.

The function of reporting to TPM can be regarded as RTR.

Chain of Trust in Trusted Computing is established by performing integration and validation checks before execution of every instruction codes [7]. The start point of Trust Chain is RTM, which initializes the TPM, which in turn perform integration and validation checks on next stage. This process is continued and a chain is established known as Chain of Trust. If the integration or validation check fails at any stage, the error is reported to the user.

IV. The New Scheme

The new scheme of trusted bootstrapping, presented here utilizes a USB key to boot the system. In addition the USB key also serves the purpose of Portable TPM as described by Weiwei Fang *et al.* [8].

In the EFI framework, a new partition known as ESP (EFI System Partition) is created on the hard disk. The ESP

contains the bootloader program for all the operating systems installed on the system, device driver files for other devices and system utility programs that are intended to be run before an operating system is booted.

The new scheme leads to the creation of ESP on the USB key. Now, since the ESP contains the bootloader and other critical codes for booting, the system always needs the USB key to boot the system to a running state. Therefore, the system will never boot from hard drive, because the bootloader will not be present to transfer the controls to the operating system.

V. Key Components in New Scheme

A. EFI System Partition

The ESP is the first partition on the hard disk in an EFI framework. The ESP contains the bootloader program for all the operating installed on the system, device driver files for other devices and system utility programs that are intended to be run before an operating system is booted.

During the installation of the operating system, if any USB is detected already attached to the system, then an option regarding the bootloader is prompted to the user. The option requires the user to select the device on which the bootloader will be installed. If the user selects the USB key, an ESP is created on the USB key and bootloader with all the necessary partition table and other data, is loaded on the USB key. Every time the system is powered-on, user will have to insert the USB key first.

B. Portable TPM

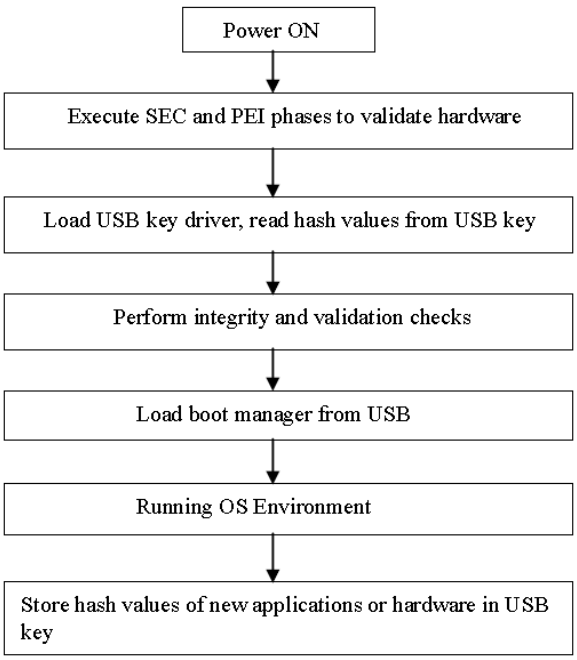

Fig. 4. Working process of Portable TPM.

The traditional form of TPM is an embedded soldered chip, which is soldered to the motherboard. This integrated TPM is fixed and cannot be removed from the system. One key feature of traditional TPM is that it is specific to a Trusted Computing Platform. If a new Trusted Computing Platform is developed a new corresponding TPM will have to be developed. This deprives the user's ability of completely controlling their system. To overcome this situation, a new technology named Portable TPM is proposed by Weiwei Fang et al., which is further enhanced in this paper.

Here the USB key is linked to computer by Universal Serial Bus. The USB key is applied as secure chip for storing and running encryption and decryption algorithm. The Fig. 4 shows the working methodology of the Portable TPM.

C. Integration and Validation Checks

Integration and validation checks are an important step in trusted booting process. These checks are performed every time the system is booted. The hashes relevant to files and hardware are stored in the TPM during the install process and as alteration is not possible in TPM, it is considered safe.

Now, every time the system is booted the hash algorithms are run to calculate the file's hash value and compare it with the previously stored value. If the two values match, this means that the file or hardware has not been altered and it is safe to run it. If the values do not match, the error is reported to the user and waits for the response. The system may also try to solve the issue by itself, by going for a reboot or in recovery mode.

When the system goes for a shutdown, the operating system records all the changes made in the system to the corresponding hashes stored in the USB. Like if a newer version of some movie player is installed then the hashes in the USB, for that movie player, change before the system is shutdown, if not at runtime. If some new document or file is created than also its hashes are stored in the USB for validation when the system is powered up next time. This ensures that the correct USB is present when the system is powered up and when shutting down, else error may occur.

When the USB key needs to be removed, for some purpose, it should be removed "safely". During the process of removing safely the contents of the ESP in USB key are copied in the RAM. The portion of the RAM where the contents are copied is protected by Memory Curtaining technique. This will facilitate the integration and validation checks, when the USB key is not present and the system is running.

D. Securing USB

Since the USB stores all the cryptographic hashes and is crucial to booting the system, it must be secured. The USB keys are available in various sizes (2GB, 4GB,…) in the market. The ESP created on USB will be normally between 100-200 MB in size formatted with FAT file system. It would not be wise to use a 2GB USB key alone for the ESP, the remaining space on the USB should be made available for general use while securing the ESP on the USB.

One way to do this is to partition the USB key and hide the partition belonging to ESP and use the other partition for storing data. However, this is not very useful since the hidden partitions can easily be accessed by various softwares.

In order to achieve better security, along with hiding the partition, the memory curtaining feature is used. Memory Curtaining refers to a strong, hardware enforced memory isolation feature to prevent programs from being able to read or write into one another's memory. This prevents any intruder or malicious code to read or alter sensitive data in the ESP.

To add more security, sealed storage is used to do away with the process of storing the cryptographic keys in the system or in USB key. The keys are generated, every time at boot up, based in part of the identity of system requesting to use them and in part of the USB attached. If the USB is attached to another system or any other USB is attached to the system, the boot process fails since the correct keys are not generated.

VI. Conclusion

In this paper the need of hardware enhancement to improve the computer security has been emphasized. But efforts have been made to keep the hardware modifications minimum by utilizing the Portable TPM technology. The key technologies discussed, memory curtaining and sealed storage, will surely be the most sought after security techniques in the future.

References

[1] TPM Main Design Principles Specification version 1.2. (July 2007). [Online]. Available: http://www.trustedcomputinggroup.org

[2] Unified Extensible Firmware Interface Specification version 2.3. (July 2010). [Online]. Available: http://www.uefi.org

[3] W. Fang, B. Yang Z. Peng, Z. Tang, "Research and realization of trusted computing platform based on EFI," in *Proc. 2nd International Symposium on Electronic Commerce and Security*, 2009, pp. 43-46.

[4] S. Schoen, "Trusted computing: Promise and risk," *Electronic Frontier Foundation*, 2003.

[5] TCG, Design, Implementation and Usage Principles version 2.0. (December 2005). [Online]. Available: http://www.trustedcomputinggroup.org

[6] TCG Specification Architecture Overview version 1.4. (August 2007). [Online]. Available: http://www.trustedcomputinggroup.org

[7] R. Zhang, J. Liu, and S. Peng, "A trusted bootstrap scheme on EFI," in *Proc. International Conference on Multimedia Information Networking and Security*, 2009, pp. 200-204.

[8] W. Fang, C. Zhou, Y. Zhang, and L. Zhang, "Research and application of trusted computing platform based on portable TPM," in *Proc. 2nd International Conference on Computer Science and Information Technology*, 2009, pp. 506-509.

Abhishek Singh Kushwaha is currently a master student in the Department of Cyber Laws and Information Security at Indian Institute of Information Technology, Allahabad. He holds a B.Tech. in Computer Science & Engineering from Gautam Buddh Technical University, Lucknow, India. His research interests include Information Security and Cloud Computing.