Deploying Trusted Computing on TPM Enabled Mobile Computers*

E. Vila, N. Sinjagina, P. Borovska

Key Words: *Data security; secure box; computer attacks; trusted computing; trusted platform module; AES; RSA; daisy chain encryption.*

Abstract. *Several research studies are devoted to improving the security of personal and confidential information which is stored on a wide variety of data resources. The ongoing new threats such as viruses or malicious codes circulating around should be countered not only from the current methods and tools available but also from new techniques capable to overcome numerous existing problems on contemporary computer systems. This paper presents an experimental study of the trusted computing technology implementation as an eminent alternative to actual approaches with respect to data security. Our work focuses on the deployment and properties of systems based on trusted computing technology principles. Apart from facilitating deployment of forthcoming applications, the ability to enable trustworthy computing at low cost can also address many of existing data security concerns. We base our analyses on practical framework and data collected from investigation of experiments with various data file formats in respect of some performance evaluation parameters. Several references for the future work are also made.*

1. Introduction

Data storage and processing systems have become a needful part of every enterprise or private and state organizations which depend on the efficient use of information. The advantages of such systems are evident due to high evaluation factors such as processing time, capacity or quality of services. In respect of security issues the key factors representing security requirements in particular have to be safeguarded continually since the data security is generally accepted to be essential for modern businesses and technology, namely, for defense against malicious intruders as well as for communications. The increasing volumes of computer viruses, malicious codes and successful corresponding attacks suggest that current protection measures are not sufficient [1]. There are numerous examples of data losses or exposal of classified information such as personal details and credit card numbers. According to [2] the biggest part of such information loss belongs to stolen laptops containing valuable data which could be easily compromised if not protected properly. Therefore it is necessary to deploy the most advanced protection methods in order to make sure that at any time and situation the data is safe. Cryptography among others is one of the efficient and widely used techniques to provide information security. Through deployment of cryptographic instruments one should ensure that information is kept confident and read only by authorized users, and the content is not allowed to be altered by unauthorized parties [3]. The majority of approaches to set up and maintain the security based on the requirements for each specific system are built upon software. However the hardware can also be utilized to increase the level of system and data security through introduction of embedded chips with particular security functions [4].

This paper explores how trusted computing technology – TC [5] can be deployed in order to contribute to an effective preservation of the classified information. TC relies on utilization of combination of software and hardware in order to accomplish the security tasks with maximum efficiency while keeping the costs low. It aims to provide a new generation of computing platforms based on improved hardware and software architectures. TC achievements have been results of collaboration between wide range vendors of software developers being commercial or open source, hardware producers and educational institutions. This paper also extends and unifies our previous work done on this topic. It extends by reporting how this technology can be practically implemented and unifies by showing how our earlier contributions can be applied together coherently and effectively.

2. Existing Problems and Approaches to Data Security

Numerous technical security measures such as antivirus programs, firewalls and intrusion detection systems can effectively solve a variety of security related problems if they keep current with the latest patches to remedy vulnerabilities. However, the lag time between discovery of vulnerability and an exploit is rapidly dwindling.

Inherited architectural weaknesses and complexity of contemporary computer systems themselves cause most computing platform to suffer from various security problems. Apart from stolen hardware the majority of data security problems are related to the data exposure and compromise caused by various threats such as viruses and malicious coded injection or unauthorized access when the protection measures are not effective. The most prominent threats to the data are computer attacks often coordinated with viruses and malicious codes. According to [6] the computer attacks are classified in three groups.

Configuration attacks lie mostly with so called human errors. They basically exploit a vulnerability supplied with default configuration, systems administrator or user who configures the software. Misconfiguration in respect of permitted improper access to privileged functionality is a common source of vulnerabilities. If an attacker gains access to privileged resources there is a high possibility that the data in there can be compromised. In such cases the system administrators or the people responsible for the configuration should have well enough knowledge about the deployment of well understood and pre analyzed configurations.

* *This research paper has been supported by DVU/430 project funded by Ministry of Education and Science.*

Technology attacks exploit programming or design errors in software running on the object of the attack. Inadequate specifications can cause unintended side effects which could be exploited by attackers. The majority of attacks nowadays are directed against hosts operating with such programs. One of the most difficult attacks to be countered in this class is zero day attacks which exploit vulnerabilities in software until the corresponding patch is released from the vendor of the software.

Trust attacks occur when one machine trusts the source of any request which can be another machine already compromised by an attacker. In those cases the authentication issues between communication parties are of key importance and if deployed properly they could efficiently prevent that kind of attacks.

In order to counter all these attacks at the initial stage it is necessary to identify sensitive data, define methods and policies for securing it, and finally to implement and enforce those policies. The definition of methods and policies should be in fully accordance with the data owner requirements concerning not only the protection aspect but also other aspects such as usability and convenience although the complex protection methods usually counter the usage simplicity. The security researchers have focused on access control, cryptography and hardware based implementations to handle the emerged data security problems. The access control is associated with access permission or denial to the specific data based on the access policy set by the owner or the administrator. The unauthorized users usually try to bypass the access policies in order to gain access to the critical data. Often the authorized users themselves exploit their privileges which lead to the most prevalent attack styles nowadays. Apart from pure software implementations there exist also protection techniques based on hardware item. The hardware serves as an isolated entity capable to store valuable data and authentication credentials. Hardware- based solutions are mostly utilized in smart card or co-processors or recently in trusted platform modules – TPM sharing some common properties with the previous ones. In respect of some key features, TPM is the most advanced hardware-based selection promising to enhance considerable data security. It is attached to the platform thus being always present. Authentication issues are also important items of TPM capabilities.

3. Deployment of Trusted Computing on Mobile Computers

Since 2003 most of the mobile computers mainly from HP, Dell, Fujitsu, Lenovo and others are being sold equipped with TPM which is basically a microchip permanently affixed on the motherboard. Trusted Platform Module is now part of more than 300 million PC and laptops around the world [7] . TPM serves as a peripheral intended to provide various functions in respect of security such as safely storing passwords, keys, certificates and other important credentials. In addition TPM can carry out control functions in providing authorization, integrity and confidentiality services to the host platform. TPM has been subject of various certifications such as EAL 4 of Common Criteria for IT Security Evaluation [8]. TPM functionality is based on specifications provided by TC which is responsible for the maintenance and development of new releases. In our previous works we have showed how the trusted computing can be deployed on machines which are not equipped with trusted platform module. In fact with help of an emulator for TPM, some of the most important functions of trusted computing have been utilized despite of few limitations that exist with respect to special functions which can be utilized only on real modules. In our case we are using a mobile computer of Lenovo model R61 equipped with a TPM chip of ATMEL manufacturer which operates on an open source software environment namely Slackware Linux operating system. The instructions below can serve also as a basis for setting up similar experimental framework on various models of mobile computers, however in more specific case the tasks are carried out on Lenovo R61. The deployment of trusted computing is carried out in the form of successive stages whereas the activation of the chip is first left as a choice for the user. We have labeled those stages as following: activation of the module, kernel configuration and verification of the support for the specific TPM. After successful completion of the stages the computer should be ready to use trusted computing technology.

Activation is the very first step of using TPM. Since almost all the mobile computers are shipped with a disabled TPM it is necessary in the first instance to enable it. The process is accomplished in BIOS where the TPM is listed as part of the hardware. During booting up the system just press F1 and after entering in BIOS follow these steps:

↳Select Security ↳Security Chip ↳Set Active ↳Press F10 for Save and Exit"

It is also advisable to reset the module in order to make it compatible with the next steps for example with the Take Ownership procedure. Usually during the first BIOS interaction the submenu of the TPM contains only three options namely Active, Inactive and Disabled which mean that under these conditions it is impossible to reset the module. However BIOS supports an additional submenu which is invisible for the user at the first time but can be turned visible in order to reveal the BIOS option for clearing the TPM by following another simple procedure:

↳ After activation of the module shut the machine down

↳ Before powering it on hold down the F1 taste and push the power button

↳ When the boot screen message Entering BIOS appears release the F1 key

In the same way as explained above go under Security, Security Chip, and select the „Clear" option which is turned visible now.

Kernel configuration is done after the installation of Linux Slackware. The kernel usually detects automatically the model of the chip since the device driver is included in almost all contemporary Linux kernel modules. The producers of the TPM chips have written their own drivers indented to support them in the kernel of the operating systems but with the frequent changes of the trusted computing specifications the synchronization driver – chip is not always kept. However since 2006 the developers of the chip drivers have agreed to release a specific unified driver, namely a general driver called TPM interface specification – TIS, which can be used for all available contemporary chips.

The kernel configuration consists exactly in enabling that driver as a standard device driver for the TPM.

↳ Open a terminal and move to the directory /usr/src/linux

↳ Type „make menuconfig“ command

↳ Select „Device drivers“ and „Character devices“

↳ Select TPM Hardware Support and check the appropriate device driver. Since the TIS driver is exceptionally used, check the TPM Interface Specification 1.2 Interface

↳ Exit by saving the changes and type make command again

The verification of the support for the specific TPM is necessary in order to be sure that that device driver configured in the kernel supports the specific hardware module contained on that machine. During Linux boot the initial ramdisk takes control and loads any needed device drivers. In order to see the available device drivers the following command can be invoked:

```
~# ls /lib/modules/2.6.27.7-smp/kernel/drivers/char/tpm/
tpm.ko      tpm_bios.ko    tpm_atmel.ko  tpm_tis.ko
```

As it is seen above there are two device drivers available which can be used based on the documentation provided with the machine namely tpm_atmel.ko and tpm_tis.ko. If we try to use the first driver it will fail since it refers to the old specifications 1.1 of TC while the present one is 1.2, viz, the TIS driver. However the specific model of the module is not yet known so one should make sure that its identifier is referenced to that driver. Otherwise the driver will not find the module so that an error message will appear. In such case is very important to identify first the exact model of the module and then to make sure that such model is referenced to the device driver TIS. Recognition of the modules is usually done during the installation of the operating system. The Linux kernel gets from the Advanced Configuration and Power Interface – ACPI tables the information about the supported TPM available on the machine but the device driver will not find the device if the device identifier is not already referenced to the device driver. The majority of contemporary TPM's are compatible with the TIS although not all specific models are referenced to. The idea of kernel support verification is first to obtain which specific modules support TIS and then to verify what specific model is contained on the machine. One must be sure that the models supported by TIS are contained on the machine which will mean full support for the TPM from the kernel side. The first is easily done as follows by looking at the source code of TIS.

```
~# cd /usr/src/linux-2.6.27.7/drivers/char/tpm
/usr/src/linux-2.6.27.7/drivers/char/tpm# cat tpm_tis.c
  [......]
        {„PNP0C31“, 0},         /* TPM */
        {„ATM1200“, 0},         /* Atmel */
  [......]
```

The next step is to reveal the exact type of the module contained in the machine. Because the information stored in ACPI tables is in binary form it should be disassembled in readable text. For this purpose we used a tool called iASL provided by ACPI Component Architecture Project [9]. After the compilation of iASL and obtaining the copy of ACPI tables the last step is to disassemble them in clear text with root permissions. As a result the specific model of TPM should be revealed.

```
[......]
Device (TPM)
        {
          Name (_HID, Eisald („ATM1200“))
[......]
```

By looking at both models they match exactly which means that the device driver TIS supports the TPM contained on this machine.

4. Putting TPM on Use

In this paper we focus in particular on data security where the users may benefit most. TPM capabilities in respect of data protection include: utilization of the most moderns and secure cryptographic algorithms such as Advanced Encryptions Standard and RSA with strongest key length available, storage of encryption keys inside secured area, fully controlled cryptographic operations, simplicity of usage and low cost profile. Based on these advantages many organizations being commercial or governmental have decided to put trusted platform module as a part of their systems security [10].

TPM provides two fundamental assurances: *tamper proofing* of software and *read proofing* of secrets. Tamper proofing ensures that the software controlling the functions of TPM can not be modified by unauthorized entities. This is very wishful against configuration attacks mentioned earlier. Read proofing on the other side is necessary to make sure that the secrets protected by TPM, which are used for authentication of TPM, can not be exposed. TPM makes use of one of the most advanced hash algorithm namely SHA-1 intended to protect the authentication credentials during usage or even on their storage. Moreover the TPM authentication capabilities based on certificates and some special functions such as Direct Anonymous Attestation – DAA, can make the host very trusted source in order to protect it against trust attacks.

TPM is supported by commercial tools and open source software vendors. Since most of commercial software is property of certain companies we utilize the second in order to have more free space for possible changes. The implementation of all necessary tools for using TPM in respect of data protection is explained in details in our previous work [11]. After taking the ownership of the module it is ready for use. Ownership associates the user called owner with two passwords: owner password which controls the access to privileged commands and an optional Storage Root Key - SRK password needed to perform and control encryption – decryption operations. As mentioned above TPM utilizes the most advanced cryptographic algorithms in use nowadays. Data is encrypted with both symmetric and asymmetric algorithms based on daisy chain principle. According to that principle the data is encrypted first with symmetric key of AES then the key is encrypted with an asymmetric key object which in turn is encrypted with the public part of another asymmetric key. Usually the encryption tools perform operations with only one symmetric and asymmetric key. TPM uses one more asymmetric key in order to bind the encrypted data with the platform which means that the data can only be decrypted

Table 1. Duration of some TPM commands

Format	Size (in KB)	TPM - Duration (in sec)		Emulator - Duration (in sec)	
		tpm_sealdata	tpm_unseal	tpm_sealdata	tpm_unseal
txt	50	1.867	2.148	1.079	0.145
xls	200	1.823	2.251	1.142	0.185
doc	350	1.859	2.315	0.976	0.282
pdf	500	1.842	2.592	1.176	0.430
jpeg	650	1.860	2.736	0.836	0.610

on the platform where they have been already encrypted. On one side, it increases the security level, on the other side the time for the required operations is also increased. We have carried out several experiments on selected file formats presented in *table 1*, which are mostly used for all kind of documentations, in order to evaluate the performance of TPM. Those files are encrypted both with the TPM emulator and the hardware chip installed on this machine.

The measurements are taken through the utilization of the Linux command *time + tpm_sealdata/tpm_unseal*. The execution results embrace the elapsed real time between invocation and termination of the given command. Because the tpm_sealdata command requires the SRK password we have removed it in order to avoid the delay during password typing. The real time is obtained by successively pressing two times the enter key. For purpose of increasing the accuracy we carried out 10 measurements for each file and calculated the average time.

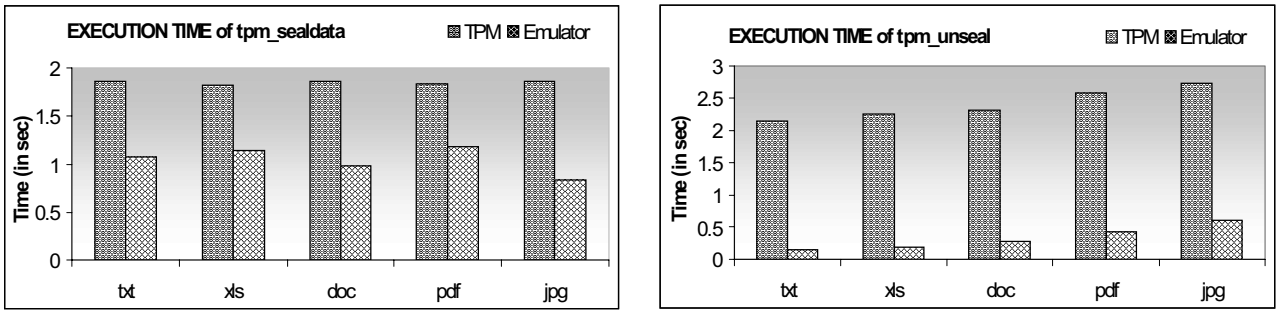

Figure 1. Execution Time of tpm_sealdata and tpm_unseal

As it is shown on the charts based on empirical data obtained, we have observed that the emulator performs significantly faster than the hardware. Especially during decryption it performs about 20 times faster. We have also observed that the encryption time is not affected by the file size in both cases while the decryption time grows when the file size increases. In case of hardware the decryption time grows slightly but in the emulator it grows rapidly when the file size increases. The slowdown of the chip is mostly dedicated to the low operation speed around 33 MHZ and the interface with the other parts of the motherboard is done through Low Pin Count bus with typical transfer rate of 2.56 Mbyte/s. Moreover during cryptographic functions the majority of operations take place inside the chip. Those facts suggest that TPM is not a cryptographic accelerator and it is not much suitable for serving to many requests successively in short time sequences. However we think that in order to evaluate the overall performance of the TPM it is necessary to evaluate first the protection capabilities which promise to be significantly better than the existing solutions. That is needed to justify the disadvantages in respect of slow operation which is not of great concern in case of individual use on mobile computers.

5. Conclusion and Future Work

In this work we have investigated in detail how the Trusted Computing can be deployed on TPM enabled mobile computers. Trusted Computing nowadays is one out of more alternative solutions to be used successfully against threats on valuable data if deployed properly. Low cost profile, utilization of most advanced cryptographic algorithms and simplicity of use are some of the advantages. High level of data security is achieved through isolation of the encrypted data from the credentials needed to decrypt them. Those credentials always reside on protected locations inside TPM under the complete owner control because TPM is guaranteed to be always present in trusted computing platform. Such beneficent solution is very effective and desirable especially against stolen or lost laptops containing critical data. We carried out several experiments in order to prove and verify the correctness of TPM functions and specific operations. Based on the results of the experiments we made some conclusions in respect of TPM properties such as time performance. TPM is a uniquely good solution as a secure box but not as a cryptographic accelerator since it performs relatively slow compared to software. However, for the individual machines where the frequency of cryptographic operations is not high, TPM does not negatively affect the overall computing performance. With respect to our future work we will focus on some improvements on existing software and access control issues. They can considerably increase the overall security performance

of TPM in respect of data security against malicious codes as well as against rogue users.

6. References

1. <http://www.pandasecurity.com/about/corporate-news/new-60.htm>
2. <http://datalossdb.org/statistics>
3. Menezes. A, P. Van Oorschot, S. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996.
4. <http://media.techtarget.com/searchSecurity/downloads0321434838_Ch16.pdf>
5. <www.trustedcomputinggroup.org>
6. Schneider B. F., P. K. Birman. The Monoculture Risk Put into Context. IEEE Security & Privacy 2009, 14-17.
7. <www.trustedcomputinggroup.org/solutions/authentication>
8. <www.trustedcomputinggroup.org/files/resource_files/B5F98F50-1D09-3519-ADBB86FAF51D5490/pp0030a.pdf>
9. <www.acpica.org>
10. <www.trustedcomputinggroup.org/resources/replacing_vulnerable_software_with_secure_hardware>
11. Vila. E, P. Borovska. Data Protection Utilizing Trusted Platform Module. Proceedings of International Conference on Computer Systems and Technologies „CompSysTech '08", 13, 12 - 13 June 2008, Gabrovo, Bulgaria.

Manuscript received on 06.07.2009

Elior Vila *received in 2002 his diploma (M.Sc) degree In Electronic and Computer Engineering from Faculty of Electrical Engineering of the Polytechnic University of Tirana, Albania. In 2004 he obtained the M.Sc degree in Business Studies from Faculty of German Engineering Education and Industrial Management of Technical University – Sofia. Since 2005, he has been working toward the PhD degree in Computer Science at the Department of Computer Systems of Technical University – Sofia. He works currently as Assistant Professor at the Technical University – Sofia. His main research interests include trusted computing platforms, computer security, cryptographic algorithms and implementation of hardware-based security solutions.*

Contacts:
Department of Computer Systems
Technical University – Sofia
Room: 3311A
Phone: + 359 965 2652
e-mail: eliordr@yahoo.de

Prof. Dr. Nina Sinyagina *is a main researcher in the Institute for Parallel Processing – Bulgarian Academy of Sciences. Her field of research covers varions aspects of computer sciences especially Computer security, Fault-tolerance systems, Computer architecture, ect. Prof. Sinaygina the auther or co-author of numbebus scientific articles (more than 90) and books (17). Currently she is Gost-Proffessor in New Bulgarian University, University in Blagoevgrad and Sofia University.*

Contacts:
Prof. Dr. Nina Sinjagina
Bulgarian Academy of Sciences
Phone: (+ 359 2) 979 66 48
e-mail: nisi@acad.bg

Prof. PhD Plamenka Borovska *graduated from Technical University of Sofia, specialty „Computer Systems and Technologies". Currently, she is head of Computer systems dept., Technical University of Sofia. Research interests: parallel computing, parallel computer architectures, high performance computing, parallel algorithms, parallel programming, trusted computer platforms.*

Contacts:
Department of Computer Systems, Technical University – Sofia
Phone: + 359 965 2524
e-mail: pborovska@tu-sofia.bg