Efficiency of Trusted Platform Module Against Computer Attacks

Elior Vila, Plamenka Borovska
Technical University of Sofia, Bulgaria

Abstract: *This paper addresses the computer attacks emerged in contemporary computer systems and in particular attacks against trusted computing platforms. In respect of successful responses against such attacks, Trusted Computing Technology promises to effectively enable a trusted system where the data are safely processed and stored while not being compromised from any outside attack. We investigate the efficiency of presumed tamper resistant Trusted Platform Module -TPM that carries out functions such as data protection or authentication. The investigation is based on multiple assumed attack scenarios and practical experiments with password crackers involving a mobile computer equipped with embedded trusted platform module.*

Keywords: *Trusted Platform Module, Computer Attacks, Viruses, Passive Attacks, Physical Attacks, Side Channel Attacks, Password Crackers.*

1. INTRODUCTION

Trusted Computing has managed in the last years to come as a new trusted technology in many IT companies and to extend on variety of application fields [1]. The new trusted hardware modules TPM should provide an efficient protection against attacks, viruses or malicious codes, which could compromise critical information stored or processed on computing machines. The users rely on it for protection of the own information including passwords, certificates, authentication credentials, encryption and decryption keys. However an investigation of its efficiency by means of different attacking scenarios is necessary in order to practically identify the advantages and possible weaknesses of the trusted platform. This would help the users to better estimate and utilize their machines equipped with trusted module in respect of increasing the overall computer trustworthiness.

The main challenges faced by security architects nowadays are protection of valuable data and computing environment from the attacks which are being more and more sophisticated. The targets vary from personal to financial data. In the recent years many attacks are directed against the financial assets especially in online applications [2]. The current protection tools, mainly based on software, have not satisfied the requirements for safe data storage and computing environment since the attacks against are taking place frequently. Trusted Computing responded to such requirements with new concepts by providing a combination of software and hardware in order to increase the level of protection for all critical data stored or processed in computer systems.

In a system equipped with trusted component the data are supposed to be stored in such way that an outside attack would be ineffective. The processing environment is isolated and controlled against any process attempt of unauthorized actions. Therefore the compromising of the processes in execution should fail. In order to estimate the efficiency of trusted platforms it is necessary to look at the well know attacks which usually work against contemporary computer systems.

2. OVERVIEW OF COMPUTER ATTACKS

Computer attacks have become in the last years one of the crucial challenge for the security experts. The attacks are not only getting more specific, but also increasing in sophistication. Since they target the most critical data stored on machines or transmitted over the networks the need for protection has emerged as an urgent task for security designers. Computer attacks diverse from type and the way how they work. Against the existing infrastructure for security they represent purposive actions for overcoming of the protective mechanisms, which it contains.
The purposes, which the attacker has, can be different but most important are:

- having more privileged access
- steal of confidential information
- misuse of computing and network resources

The attacks of above indented purposes are usually directed against the systems or networks depending on the source and the place of targets. They can be generally classified as system and network attacks*.*

2.1 *System Attacks*

The system attacks take place usually inside the computer system. Most often they are connected with obtaining of privileged access to storage devices, computing and network resources. They include theft of passwords, ownership or administrator rights for reading, writing or executing of files and applications. These attacks use most often weaknesses in the design of the security system, in attention from the side of users with higher level of access or program errors. In this category of attacks are usually included:

- Viruses - are computer programs that copy and reproduce themselves in order to infect a computer without permission or knowledge of the user. The majority of viruses are usually spread through emails incorporated into other programs or data. Thus all the users working with the program can be potentially infected if the countermeasures such as firewalls or antivirus programs are not properly configured and updated respectively.
- Worms - are similar to computer viruses. While the viruses attach themselves to other programs, the worms are independent and do not require to be part of other programs, to spread themselves. Usually the worms spread through the computer network and pass from one computer to other, using errors or weaknesses of the network protocols.
- Trojan Horses - are the mostly used on modern attacks. Trojan horse is essentially a program, which presents itself as useful software. Unlike the viruses and worms, the Trojan horses have not their own mechanism for spreading. That is why they only rely on the poor knowledge and the imprudence of the users. For example, the Trojan horses can be added deliberately in the installation packages of useful software. Another popular way for spreading the Trojan horses is through email - as attached files. Trojan horses are used in many scenarios such as for getting more privileges in the infected system, stealing passwords and key logging or even to initiate attacks to a given server.
- Bombs - are malicious programs of types of Trojan horses, which can be used to infect with viruses or worms or realizing of other types attacks. The bombs are independent programs and often they represent part of the programming securitization and they are usually integrated in the system from the system

programmer. The bombs are activated by appearance of particular conditions for example date or time. But they can be also triggered by certain conditions such as events or particular actions.

- Backdoors - in computer systems are methods in order to detour the normal way for authentication or having remote access to the system, as this must remain unnoticed for the administrator who controls the system. Most often back doors are integrated in the code of the systems from their creators.

2.1.1 Password attacks

Since the authentication methods on the majority contemporary systems are mainly based on user names and passwords, the attacks for cracking passwords are prevailing among the others. After such successful attack the attacker can take the control of any application or have access on the data belonging to the others. In the technical aspect the attacker may operate like a legitimate user since he logs on with the attributes of the victims. The prominent password attacks taking place frequently are brutal force and dictionary attacks.

- Brute force attacks aim to find legitimate authentication credentials. In cryptanalysis they represent a method of defeating a cryptographic scheme by trying a large number of possibilities for instance, exhaustively working through all possible cryptographic keys in order to decrypt a message. Attackers can also use brute force applications, such as password guessing tools and scripts, in order to try all the combinations of well-known usernames and passwords. Such applications may use default password databases or dictionaries that contain commonly used passwords or they may try all combinations of the accepted character set in the password field. The brute force attack could be combined with a dictionary attack.
- Dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or pass phrase by searching a large number of possibilities. In contrast with a brute force attack, where all possibilities are searched through, a dictionary attack only tries possibilities which are most likely to succeed, typically derived from a list of words in a dictionary. Generally, dictionary attacks succeed because many people have a tendency to choose passwords which are short, single words in a dictionary, or are simple variations that are easy to predict, such as appending a single digit to a word. The modern password crackers use very large world lists which contain million of words from different subjects thus increasing the possibility that any work contained in the list might be the password.

2.2 *Network Attacks*

Attacks against networks are classified in different categories according to the object of attack, passive or active, local or remote by the effect type and so on. These kinds of attacks may belong also to systems attacks however they are more prominent against networks. Many attacks are actually performed by automated tools release on the Internet. While passive attacks only monitor the information the active attacks alter it with intent to corrupt & destroy or prevent access to the data [3].

In the category of active attacks the most popular attack is called denial of service (DoS). The attacker usually attempts to prevent the legitimate user from accessing information or services. An extended method of DoS is to use the machine of a victim in order to attack another computer. That is called distributed DoS since the attacker uses

multiple computers to initiate DoS's. Monitoring of the communication between parties and then capturing and controlling of it results in the attack named man in the middle. In such case the attacker is able to change the data or to reroute their exchange.

Passive attacks usually concern the interception of the messages between the sender and receiver while the content of the information remains unchanged. The process of listening the communication is known as eavesdropping. When the messages are exchanged in clear form then the eavesdropper can practically read all the information content. Usually the data are transferred in encrypted forms which need to be decrypted first in order to be read.

The information gained from the physical implementation of a cryptosystem can also serve to initiate attacks called side - channel. For example, timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information which can be exploited to break the system. The theoretical weaknesses in the algorithms are less in question. However such attacks require considerable technical knowledge of the internal operation of the system on which the cryptography is implemented. Moreover the physical contact to the machine is prerequisites.

2.3 *Attacks on Trusted Computing Platforms*

A key principle of trusted computing platforms and TPM respectively, is the capability to safely keep and use secrets from attempts made by an adversary perhaps with direct physical access to the platform. Most of the attacks against TPMs lie in the category of the system attacks. Until know there are no traces of any successful attack against TPM. However in a presentation named "TPMkit: Breaking the Legend of Trusted Computing and Vista (Bit Locker)" [4] the authors claimed they have developed an attack on how to compromise the TPM but the demonstration didn't take place. Despite of the range broadness of possible attack avenues, by considering the hardware-based nature of TCP the following attacks can be taken mostly into consideration [5].

2.3.1 Physical Attacks

This kind of attacks initiated from outside TCP, aim to actively penetrate or otherwise disrupt the internal device. The target of the TCP is TPM as the core of secrets. By physically attacking the TPM, an adversary hopes to subvert its security correctness properties somehow, usually by extracting some secrets. The natural way to achieve this goal is the direct approach by trying somehow to bypass the TPM protections and read the data stored there. In TCG architecture, the TPM uses machine resources for some computations. This fact can be utilized by an attacker to do useful things by exploiting the unprotected nature of I/O channels. The reverses engineering, which is the process of discovering the technological principles of a device, can also introduced to obtain data for analyses in order to discover any vulnerability in the platform. The first countermeasure against such attacks would be the isolation of the TPM and the I/O channels or the application of techniques which can detect the interference. However such measures are not yet specified in the TPM specifications. The correctness of the functionality of TPM should also be taken into consideration. Not only the synchronization of the requested actions in accordance with the system security policy is key principle but also the functionality according to the specification of the TPM is of vital importance. For Linux systems are released some tools capable to detect weather the TPM behaves in accordance with TCG specifications [6].

2.3.2 Side-channel attacks

The physical action of computation can often result in physical effects an adversary can observe. These observations can sometimes betray sensitive internal data the TCP - TPM architecture was supposed to protect. In respect of trusted computing platforms this style attack is often called side-channel analysis, since the TPM leaks information via channels other than its main intended interfaces. The computation or generation of necessary signals and data inside TPM takes time. The exact combination and sequence of actions and signals depends on the operational data, and the duration depends on this combination. But if the actions depend on secret data, the duration can betray this information.

In addition to the time-of-operation operation approach, physical devices have other observable physical characteristics that depend on hidden secrets. One natural characteristic is power. The power consummation for certain operations can be measured by an adversary in order to deduce clues about the operation mode. This is called power analyses which can be simple or advanced. The observation of the electromagnetic radiation is also a potential method of exploiting the properties of the module operation mode. As it is mentioned in the previous paragraphs such attacks require technical knowledge of the internal operations and also equipments necessary for the measurements.

3. EXAMPLE OF A SIMPLE EXPERIMENTAL FRAMEWORK

In the frame of attacks on TCPs and effectiveness of trusted platforms we have set up an experimental environment by considering some aspects of TPM such as the ownership or permissions for certain command. As discussed in our first paper [7] the process of data decryption requires disabling of SRK password. It means that if an attacker assumes administrator privileges he can easily decrypt the data protected by TPM. So the level of TPM protection would depend on the administrator credentials. In case the SRK is always enabled then this attacks scenario is ineffective.

3.1 *John the Ripper Attack on Linux Administrator Password*

John the Ripper – JTR is a fast password cracking program designed for use on different operating systems. Although it is mainly indented for detecting the weak passwords in terms of positive education purposes it can also be used for cracking the passwords hash types which contain the administrator or users passwords etc. According to the official website [8] John currently is supported on most popular OS such as Windows and UNIX based. The operation of JTR is based on a combination of dictionary and birthday attacks whereas the latest is a sort of brutal force attack. Although the world list provide contains some million words the idea behind a successful attack is that the assumed password must be contained in the word list. JTR is successfully used only if three conditions are met. 1. The cracker should have access to the hashed password file. 2. The hash algorithm used, should be supported by the JTR. 3. The password must be contained in the wordlist list. In order to validate the correctness of the three conditions we put a very complex password on the wordlist which resulted in successful try of JTR. In the block schema below on the figure 1 is explained the attack carried out on machine of type Lenovo R61 with OS Linux Slackware 12.1 after successful installation of JTR.

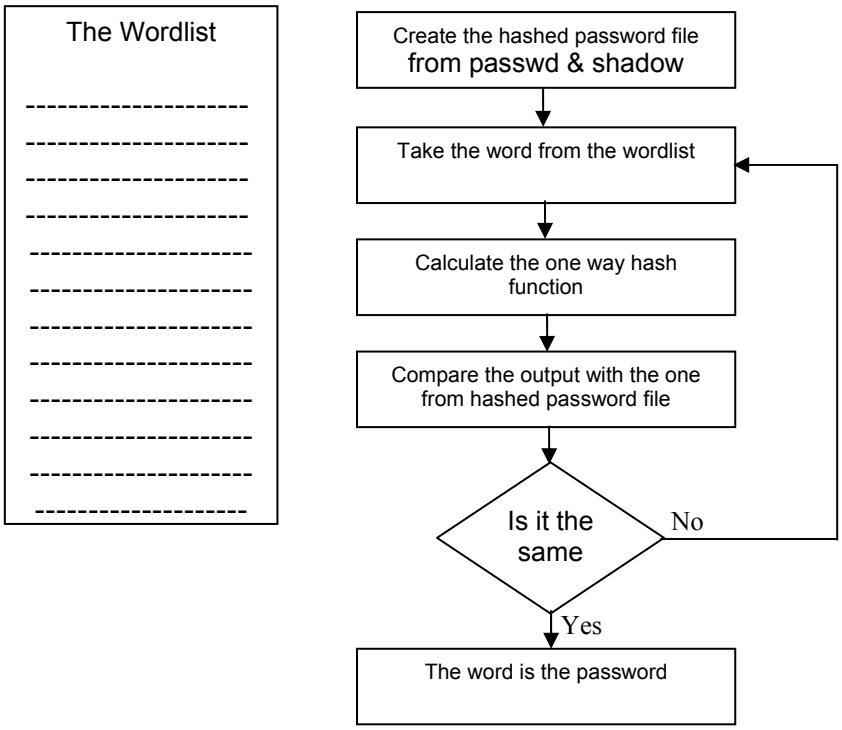

Fig.1: Attack Scenario

4. CONCLUSIONS AND FUTURE WORK

The investigated possible attack scenarios and experiments carried out with TPM show that there are still no results which would prove non efficiency of TPM. The well known attacks are a challenge for trusted platforms although many of them work under assumptions sometimes hard to be implemented in real conditions. However TPM efficiency would be guaranteed in case of real working conditions by considering all possible implementation in protection of critical data. We are working to develop such experimental frameworks in order to carry out more specific active attacks with software and malicious code which can directly harm the TPM during optimal operation. The essence of encryption/decryption key protection needs to be investigated since this is considered to be an advantage of trusted solutions.

5. REFERENCES

[1] TCG. (2008) Enterprise Security: Putting the TPM to Work <www.trustedcomputinggroup.org/home>
[2] Sanders. Tom, (2007), Online Apps Facing Barrage Of Attacks <www.vnunet.com/vnunet/news/2174407/internet-programming-threats>
[3] http://openlearn.open.ac.uk/course/view.php?id=2587
[4] <www.networkworld.com/news/2007/062707-black-hat-abstract.html>
[5] Smith. W Sean, (2005) Trusted Computing Platforms, Design and Applications.
[6] <www.trust.rub.de/home/concluded-projects/trustedgrub/>
[7] Vila. E, Borovska. P, (2008), Implementation of Cryptographic Tools for Data Protection Utilizing Trusted Platform Module, Computer Science'08.
[8] www.openwall.com/john/