Network Working Group L.P. Mitchell
Internet Draft University of Liverpool
Intended status: Informational January 26, 2010
Expires: June 26, 2010

Applying Forensic Science to Trusted Enterprise Network
draft-mitchell-nwg-00.txt

Abstract

The Trusted Platform Module, for the past decade, has shown potential to improve computer security. However, there is growing concerns that the Trusted Platform Module, and its related technologies might be challenging for Forensic Investigators to acquire and analyze certain digital evidence. For example, if the key evidence is encrypted, and cryptographically bound to a set of platform characteristics, then those characteristics must exist on the platform (that is being used to decrypt the evidence) before the evidence can be decrypted.
As a result, it is believed that if a suspect cryptographically bound the evidence to the platform characteristics, and those characteristics in some way got changed, then it might not be possible to decrypt the potential evidence.

For this reason, we explored how Trusted Platform Module and its related technologies might support digital forensic analysis within a trusted enterprise network.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

The Trusted Computing Group (TCG) has been mandated to develop a set of vendor-neutral specifications for the current design of the trusted computing system. The main component of the TCG's specifications is a security chip called the Trusted Platform Module (TPM). The TPM is a tampered-evident security microcontroller that is physically mounted on the mainboard of a trusted platform (such as laptops, PDAs, PCs, servers, and mobile phones).

Although the architectural design of TPM device cannot withstand physical attacks, it is nonetheless tampered-evident, and therefore it is possible to detect most physical tampering, such as de-soldering. In addition, the TPM is complex in design, but small enough for verification. According to [TCG2007], the TPM provides the root of trust, which is used to extend trust to other hardware and/or software components.

The TPM provides two main mechanisms which must be properly configured and managed to assist digital forensic investigations, otherwise digital forensic on trusted platform might be challenging. These two functions include the provision of a crypto co-processor to protect sensitive data or messages, and an integrity, storage and reporting measurement mechanism, which is used to provide evidence of the platform's state or current configuration.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119.

3. The TPM's crypto co-processor data protection system

3.1. Binding Operation

A typical TPM-based binding operation is similar to the conventional asymmetric encryption [Sadeghi2008]. In that, it uses the public key of the intended recipient to encrypt the message, and the private key of the intended recipient to decrypt the message. The encryption keys can be either designated (at creation) as migratable or non-migratable. Interestingly, if a potential digital evidence where bound using a non-migratable key of a particular TPM, then it would only be possible to decrypted that data using the device that has the specific instance of the TPM which holds the corresponding private key [Mason2005];[Sadeghi2008]. Nevertheless, as explained by [TCG2007], "it is possible to create migratable private keys that are transferable between multiple TPM devices".

3.2 Sealed-binding or Sealing Operation

The sealing operation further increased the complexity of evidence acquisition, whereby it allows possible digital evidence to be cryptographically bound to a predetermined configuration (hardware and/or software), which must exist on the target system before the evidence can be decrypted or unsealed [TCG2007].
For instance, the BitLocker Drive Encryption feature available in the ultimate and enterprise versions of Windows Vista, and Windows 7 Operating Systems, encrypts the drives volumes using a key called full volume encryption key (FVMK). The integrity of FVEK is protected by a special encryption master key called the Volume Master Key (VMK), [Syng2007].

Thus, to decrypt the volume contents, the TPM MUST first decrypt the SRK, which decrypts the VMK, which decrypts the FMVK, which is used to decrypt the volume contents (See Figure 1).

```
+---->---+---->---+--->---+----//-----//-----+
|  SRK   |  VRK   | FVEK  |  Volume Contents |
+---->---+---->---+--->---+----//-----//-----+
```

Figure 1: BitLocker Encrypt/Decrypt Operation

As mentioned above, the TPM seals the VMK to certain predetermined configuration, which by default, includes the Core Root of Trust Measurement (CRTM), ROM code, Master Boot Block (MBR) code, the NTFS boot sector, and the NTFS boot block [Micro2008].
The digests for these configurations are taken and stored into Platform Configuration Registers (PCRS), (in particular, at the time when the VMK was created).

Therefore, if for any reason the digests for these configurations changed unexpectedly, the TPM will not unseal the VMK, and thus, the volume contents will not be decrypted. However, Windows Vista, and Windows 7 (ultimate and enterprise versions), provide a data recovery solution, which is particularly useful for Enterprises (and possible digital investigators). Thus, if for any reason, a particular condition exists,(such as BIOS upgrades, system board and/or hard drive change) that caused the digests for the predetermined configuration to alter, the VMK will not be decrypted, and the platform would enter into recovery mode. Here the platform would require the system administrator (or possibly the investigator) to enter the recovery key, provided that the key was created, and backed up during the BitLocker setup phase.

3.3. Signing Operation

According to [TCG2007] the TPM "tags some managed keys as signing only keys". Hence, these keys are not used for encrypting data. Instead, they are used to compute the hash of the signed application data and/or messages, and then the private signing key is used to encrypt the hash value. The signing keys may be designated as migratable or non-migratable keys. In general, all keys that are tagged as migratable can be transferred between TPM devices, whereas, the non-migratable are bound to a particular TPM device. An example of a non-migratable signing key is the attestation identity key (AIK), which is "exclusively used to sign data originated by the TPM, (such as TPM capabilities and PCR register values)" [TCG2007]. In essence, when application data or messages are digitally signed, it allows a third party, such as a digital investigator to ascertain the integrity, and possibly the data origin [TCG2007]. For example, since the PCR values are signed by the AIK that resides in the tamper-evident TPM, the investigator can prove the integrity of the PCR values, and by extension, the integrity of the corresponding entries in the stored measurement log (SML).

3.4 Sealed-signing Operation

As part of the signing operation, a particular set of PCRs are collected and included in the message, as well as in the "computation of the signed message digest" [TCG2007]. This allows the investigator to inspect the platform's configuration at the time when the signature was created, as well as to provide stronger association of the possible evidence, the TPM device, and the signatory.

4. The TPM's Integrity Measurement, Integrity Logging, and Integrity Reporting Mechanisms

4.1. Integrity Measurement

The integrity measurement is the process of obtaining measurements of events that might affect the trustworthiness of the platform. The root of trust for measurement (RTM) - which is a reliable engine for computing measurements, uses the SHA-1 algorithm to compute the digests of the program codes or embedded data (otherwise known as the measured values) before transferring execution control to that code (or event). The measurement digests are then stored into the shielded locations of the TPM (i.e. Platform configuration registers or PCRs) for later use, whereas the measured value itself (i.e. program code or embedded data) may be stored into a log file, called the stored measurement log (SML), or recalculated when desired [TCG2007].

4.2 Integrity Logging

Integrity logging implies that the integrity measurements for the platform are often stored for future use. As suggested above, the measured value (or events) may be recalculated, however TCG (2007) recommend that they be stored into the stored measurement log. According to Balfe et al (2005) the SML is synonymous to the Event Log.

4.3. Integrity Reporting

Integrity reporting performs two main functions: (1) it uses the TPM's protected capabilities to access and report the digests of the measured values stored in the PCRs. (2) It uses the attestation identity key (AIK) to sign the PCRs, so that it can later vouch for the integrity of the platform's measurements held inside the PCRs [TCG2007].

Notably, using the TCG's attestation protocol, investigators can now retrieve one or more PCRs values (usually digitally signed by the private portion of the TPM's attestation identity key), and use them as one of the comparators, to prove the trustworthiness of the digital evidence, such as whether the event logs or program files was tampered with. Therefore, the classic Trojan Horse argument that the evidence was planted by a virus or rootkits might not work, especially since a correctly configured trusted computing platform can provide provable statements that its static data or program code (such as, the operating system program files or DLLs) was not altered, as explained in [TCG2007] and [Mason2005].

5. Unique/Class Characteristics of Trusted Platform Module (TPM)

Using the Locard's exchange principle, [Casey2004] grouped evidence into two main categories, i.e. (1) Class characteristics and (2) Individual characteristics. In general terms, class characteristics can be used to identify evidence based on common traits that exist in similar digital objects, whereas, individual characteristics can be used to identify evidence that are based on the unique characteristics which distinctively identify a digital object.

Trusted Platform Modules and its related technologies can provide both class and individual characteristics, which digital investigators can used to provide a stronger association between the evidence, the crime scene, and the TPM instrument used to commit the crime. For instance, the machines' fingerprints (collected by the integrity measurement collector or during attestation), provide class characteristics of a set of devices with common traits on the enterprise network.
Typically, networks that implements TCG's trusted network connect (TNC), or similar protocols, may remediate devices that do not have these common traits. This allows the investigator to identify the machine(s) that might have been involved within the crime.

Conversely, if the digital evidence was sealed, signed-sealed or bind(ed) using a non-migratable key, then the evidence is cryptographically bound to a particular platform.

Since the public portion of the non-migratable key is mathematically related [Anderson2008], using key verification techniques, it is possible to use the public key as the unique characteristic to prove whether the suspect's platform was involved within the crime. Especially, since only the device with the private portion of the non-migratable key can decrypt any information or potential evidence that was originally encrypted with the corresponding public key. Therefore, if investigators can successfully identify the device that can decrypt the message, they would be able to provide provable statements that the device was involved within the crime. Furthermore, it is possible to make strong association between the suspect, the crime scene, and the platform, especially in cases where the enterprise uses a combination of user and machine authentication scheme (i.e. TPM-based authentication), that irrevocably binds the user's credential or claimed identity to a physical tamper-evident TPM device.

6. The Admissibility of Trusted Computing Digital Evidence

According to [Casey2004], "the US Federal Rules of Evidence ACT (FRE), the UK Police and Criminal Evidence Act (PACE) and Civil Evidence Act, and similar rules of evidence in other countries were established to help evaluate evidence". As a result, the US Federal Rule of Evidence was used to appraise the admissibility of TPM-supported evidence. The US Federal Rule of Evidence was chosen because the interpretations of its many rules are readily available in various literatures. The Federal Rules of Evidence Act (FRE) deals primarily with the admissibility of evidence. It mandates that before evidence is admitted, the court must determine if the evidence is hearsay, if the copy of the evidence is acceptable or the original is required, if evidence is reliable, as well as if the evidence is authentic [Casey2004].

6.1. Hearsay

The Federal Rule Evidence 801(c) defines hearsay as "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted". As such, it is common for federal courts to evaluate computer records on the basis of it being potential hearsay [USDOJ2002];[Nolan2005]. Interestingly, computer records can be classified into two types:

(i) Computer-stored records - which are records that "contain writings of some person or persons and happen to be in electronic form", (e.g. TPM-protected word-processing document, or TPM-protected email messages).

(ii) Computer-generated records - which are records that contains output of computer programs, "untouched by human hands" (e.g. the TPM's integrity measurement logs, or attestation logs). It is noteworthy that while computer-stored records can contain hearsay, computer-generated records cannot [USDOJ2002] and [Nolan2005].

However, the business records exception or more precisely Rule 803(6) is commonly used to except computer-stored records from the Hearsay rule. Under Rule 803(6) computer records that falls in the category of being "regularly conducted business activities", such as daily network monitoring logs are usually admissible in court [USDOJ2002]. Furthermore, [USDOJ2002] and [Nolan2005], stated that all computer records must be proven to be authentic and reliable. When computer-stored records contain human statements, the human statements must be proven not to be inadmissible hearsay.

Interestingly, the trusted platform module can store and\or generate various records, which may fall into one or more of the record categories (i.e. computer-stored or computer-generated records). Therefore, in order to have the TPM related evidence admitted in court, the hearsay rules and/or the authenticity of the computer program may be applicable.

6.2 Authentication

The Federal Rule Evidence 901(a) defines authentication "as a condition precedent to admissibility, and is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims" (cited in [Nolan2005]).

For example, a witness who uses the TCG's attestation program to record the integrity measurement of a remote computer and saved the result to a storage device will need to authenticate that the evidence was recorded by him using the attestation program, and that the evidence was saved on the particular storage device [Nolan2005]. According to [USDOJ2002], the witness need not have special qualifications, nor does he need to have programmed the computer himself, or even have understanding of the maintenance and technical operation of computer to authenticate the evidence.

In addition, it is imperative for the proponent to maintain a well documented evidence chain of custody, showing an unquestionable continuity of possession, particularly of who, where, what, why, when and how the evidence was acquired, transferred, removed, analyzed, stored and in some instances destroyed.

Failing to establish this unbroken trail of accountability could result in the integrity of evidence (i.e. free from tampering) being loss and therefore questionable by its opponents. However, as stated by [USDOJ2002], "the mere possibility of tampering does not affect the authenticity of a computer record, but instead its assigned weight".

Therefore, although it is possible to attest the integrity of TPM related evidence, investigators should adhere to internationally accepted procedures, such as those outlined in SWGDE, and IOCE, including the maintenance of a proper chain of custody record.

6.3. Reliability

As mentioned before, witnesses need not be the person who programmed the computer to authenticate the evidence. However, the authenticity of computer-generated records may be reliant on the reliability of the computer program that generates the record. For instance, the TCG define trust as the "expectation that a device will behave in a particular manner for a specific purpose" [TCG2007]. It is also expected that trusted computing device should be implemented in accordance to the TCG's specifications [TCG2007].

As such, if the TCG's specifications (intentionally or unintentionally) contain some security flaws (such as, earlier TPM versions that are susceptible to PCR reset vulnerability), then those components would intrinsically be inaccurate. Also, given the complexity of the design, it would be difficult, if not impossible, to exhaustively verify every line of code. As a result, it is possible for some computer programs to contain serious programming errors.

In general, the reliability of computer program, and particularly computer-generated records or evidence, can be proven by showing that "users of the program actually do rely on it on a regular basis, such as in the ordinary course of business". For example, data collected by a third party through remote attestation that shows evidence of illicit activities, (e.g. copyright violation), might be admissible in court, if it could be proven that the third party relies on the remote attestation program in his/her normal course of business.

6.4. The Best Evidence Rule

According to [USDOJ2002] "the best evidence rule states that to prove the content of writing, recording, photograph, the 'original' writing, recording, or photograph is ordinarily required".

This rule could be problematic for digital evidence, in that, during the acquisition analysis phase it is possible for the evidence to be damage or altered. For this reason, it is usually recommended to use a bit-by-bit copy instead of the original. Therefore, even if the copy gets damage, the original evidence would still be accessible. Furthermore, under the Federal Rule of Evidence 1001(3) a bit-by-bit copy of the evidence is regarded as being equivalent to the original, and as such, the copy is usually admissible in court (cited in [USDOJ2002];[Nolan2005]).

However, it is not always possible to acquire a bit-by-bit copy of the original, especially when strong encryption mechanisms are used to protect the data. In such cases, how will the court proceed? On one hand, data protection laws and regulations (such as, SOX, HIPAA) are fueling the need for strong data protection mechanisms, such as Full Drive Encryption (FDE), and Microsoft Bitlocker encryption. However, on the other hand, strong encryption is long known to be challenging for law enforcers, lawyers, and digital investigators alike [Mason2005].

As pointed out in the introduction, the proliferation of TPM chips will make available to the general public (including potential criminals) strong hardware-based encryption. It may become necessary to resort to live forensics, which has its own challenges.

7. TPM support for Live Forensic Analysis

Live forensic analysis involves probing a 'live' target system whilst it is kept running. As such, the forensic technique relies on the skillful analysis of the original source disks. It also relies on the software found on the target system to perform the analysis [Carrier2006]. There are two major implications for live forensic, which are (i) the possible alternation of the original evidence. In this regards, the Scientific Working Group on Digital Evidence (SWGDE) recommended that "any action that has the potential to alter, damage, or destroy any aspect of the original evidence must be performed by qualified persons in a forensically sound manner" (SWGDE, 1998).

(ii) As noted by [Carrier2006], "the only difference between live and dead analysis is the reliability of the results." Since live forensics relies on the platform applications, it is usually argued that those applications could be subverted by means of hidden rootkits. According to [Carrier2006] rootkits are "the most common source of false data during live analysis".

In general, rootkits allows an attacker to gain access to the infected system. It allows the attacker to hide his or her activity, by modifying software programs, or by "inserting a filter in the data flow of a computer". Essentially, rootkits allow a platform to lie about its state, and thus, computer-generated records from such system could be viewed by the opponents, as being suspicious or untrustworthy.

Interestingly, trusted computing platform may help to create a trusted computing environment, one in which the platform will not be permitted to lie about its state [TCG2007]. In an experiment conducted by [Sailer2004], it was shown that it is possible to use TPM integrity measurement report to detect suspicious changes made to the platform characteristics. However, subsequent experiments (conducted by the author), revealed that while it is possible to detect platform configurations changes, attritubing those changes to the actual perpetrator, such as a malicious person or rootkits was not possible without examining other supporting evidence.

For instance, figure 2 shows the machine's PCR values (PCR#0 to PCR#3) before its BIOS configurations were changed, and figure 3 shows the platform configuration after the BIOS configuration was changed. While we could easily identify that the hash value for PCR#1 had changed, we could not easily determine what caused the change to the platform. Essentially, the change could have resulted from a software and/or hardware upgrade, and not necessary from rootkits, as claimed by [Sailer2004].

PCR values before changes in the platform configuration			
PCR#	Date	Time	Hash Vaues
0	10/28/2009	16:08:10	b09392eff32c687597fa51654d66b37d427124a
1	10/28/2009	16:08:10	537517f3bfb6b45e8498d32c820869e282b4836f
2	10/28/2009	16:08:10	b09392eff32c687597fa51654d66b37d427124a

Figure 2: PCR values before change

PCR values after changes in the platform configuration			
PCR#	Date	Time	Hash Vaues
0	10/28/2009	16:08:10	b09392eff32c687597fa51654d66b37d427124a
1	10/28/2009	16:08:10	ef8b9b159064ba82420b50a98ddd1cb4ee21817a
2	10/28/2009	16:08:10	b09392eff32c687597fa51654d66b37d427124a

Figure 3: PCR values after change

8. Security Considerations

The platform owner MUST have the requisite skills, resources, and motivation to properly configure the trusted platform and/or the trusted computing environment. More specifically, it is assumed that the Enterprise or platform owner has an efficient encryption key management system in place, or similar systems (such as Windows key restoration) to backup, restore, and/or manage its encryption keys.

The Enterprise SHOULD have adequate security mechanisms to protect the integrity of the encryption key management system. This assumption is particularly important since a breach in the key management system could nullify the effects of TPM data protection.

Finally, the Enterprise SHOULD enforced the necessary network policies to protect against unauthorized changes to the TPM device configuration, such as clearing, taking ownership, or turning off the TPM protection.

9. IANA Considerations

This document does not require any IANA actions.

10. Informative References

[Anderson2008] Anderson, R., (2008), Security Engineering: a guide to building dependable distributed systems. 2nd Edition, Wiley Publishing,Inc. Indianapolis, Indiana. ISBN: 978-0-470-06852-6.

[Casey2004] Casey, E., (2004) Digital Evidence and Computer Crime: Forensic Science, computers and Internet. 2nd Edition, Academic Press. ISBN 13: 978-0-12-163104-4.

[Carrier2006] Carrier, B. D. 2006. Risks of live digital forensic analysis. Communications of the ACM Volume 49, No 2, (Feb. 2006), 56-61. DOI http://doi.acm.org/10.1145/1113034.1113069. Accessed on March 10, 2009.

[Mason2005] Mason, S., (2005) Trusted computing and forensic investigations, Digital Investigation, Volume 2,Issue 3, september 2005, Pages 189-192, ScienceDirect ISSN 1742-2876, DOI: 10.1016/j.diin.2005.08.002. Accessed on March 10, 2009.

[Micro2008] Microsoft, (2008) Keys to protecting data with BitLocker drive encryption. Microsoft, Technet. Accessed on September 24, 2009.

[Nolan2005] Nolan, et al., (2005) First Responders Guide to Computer Forensics:CERT Training and Education. Accessed on March 11, 2009.

[Sadeghi2008] Sadeghi, A.R., (2008) Trusted Computing, Special Aspects and Challenges DOI: 10.1007/978-3-540-77566-9, Volume 4910/2008, Year 2008, Pages 98-117. Accessed on March 10, 2009.

[Sailer2004] Sailer, R., Zhang, X., Jaeger, T., and van Doorn, L., (2004) Design and Implementation of TCG-based Integrity Measurement Architecture [Proceedings of the 13th USENIX Security Symposium] Available at: http://www.usenix.org/events/sec04/tech/full_papers/sailer/sailer.pdf. Accessed on May 13, 2009.

[Syng2007] Syngress, 2007 Chapter 4 - Microsoft Vista: Trusted Platform Module Services, TechRepublic, Accessed on June 26, 2010.

[TCG2007] TCG (2007) TCG Specification Architecture Overview: Specification Revision 1.4 Accessed on March 10,2009 www.trustedcomputinggroup.org.

[USDOJ2002] USDOJ (2002) United States Department of Justice. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Accessed on September 2, 2009.

Author's Addresses

Leighton Mitchell
University of Liverpool

80 King Fisher Drive,
Old Harbour Glades,
Old Harbour P.O.,
St. Catherine, Jamaica.

Phone: 876-822-2019
Email: mtchum@yahoo.com